科学研究費補助金 特定領域研究

新世代の計算限界
— その解明と打破 —

平成17年度 成果報告書

平成18年 4月

領域代表者　岩間 一雄
京都大学 大学院 情報学研究科　教授

目 次

1. 総括班活動報告 **1**
総括班活動報告 . . . 3
教科書シリーズ . . . 5
電子ジャーナル . . . 5
ニュースレター . . . 6
ミニプロジェクト . . . 7
電子情報通信学会和文論文誌 A 「新世代の計算限界 招待解説論文特集号」 . . . 8
電子情報通信学会英文論文誌 D 「新世代の計算限界 招待論文特集号」 . . . 9
国際ワークショップ iETA の企画 . . . 10
Randomness and Computation . . . 11
NHC 国際会議 . . . 13
第 18 回 回路とシステム軽井沢ワークショップ 特別講演セッション . . . 16
研究集会 (モデル班) . . . 17
ミニ研究集会 (組合せゲーム・パズル) . . . 18
ミニ研究集会 (複雑ネットワーク, ウェブグラフ) . . . 20
ミニ研究集会 (列挙合宿) . . . 21
ミニ研究集会 (Complexity) . . . 22
ミニ研究集会 (暗号理論) . . . 24
ミニ研究集会 (ジオメトリ) . . . 26
電子情報通信学会 COMP-NHC 学生シンポジウム . . . 27
第 19 回 回路とシステム軽井沢ワークショップ 講演企画 . . . 28

2. 研究課題別活動報告 **29**
A01: オンライン予測の手法を用いた意思決定モデルに関する研究 . . . 31
A02: 計算理論的設計による知識抽出モデルに関する研究 . . . 45
A03: 論理関数表現のモデルとシンボリックアルゴリズム . . . 54
A04: 組み合わせ最適化における指数サイズ・多項式時間近傍の設計 . . . 62
A05: ハードウェアアルゴリズムの性能評価に関する研究 . . . 70
A06: 幾何的配置問題の計算量限界と近似可能性の研究 . . . 78
A07: 現実的な状況下での量子計算の能力に関する研究 . . . 89
A08: 動的な構造をもつネットワーク上の資源割当て問題の研究 . . . 103
A09: 非明示的表現に対するアルゴリズムの開発 . . . 114
A10: 変移する要素間の関係を条件とする組合せ最適化モデル . . . 124
B01: 代数的および確率的手法による離散構造の限界の究明 . . . 132
B02: 暗号解析手法の計算量理論による改良とそれに基づく暗号方式 . . . 143
B03: 量子論理回路の最適化に関する研究 . . . 157
B04: 回路計算量の下限の研究とその応用 . . . 168

B05: ブール理論に基づく離散システムの構造解析と計算限界の研究 172
B06: 暗号システムに対する実装攻撃の適用と限界に関する計算的研究 180
C01: グラフ描画アルゴリズムとその Web 情報検索への応用 190
C02: 連続と離散の統合によるロバストアルゴリズム構築 201
C03: ネットワーク上での社会的効用と個人的効用の対立問題に対するアルゴリズム的研究 . 222
C04: 実践的な列挙アルゴリズムの理論構築 233
C05: 幾つかの画像関連問題の計算複雑度の解析と効率的な解決法の提案 240
C06: グラフ構造を有する問題に対する近似アルゴリズムの設計 254
C07: Web コンテンツ活用に関連した離散最適化問題の研究 273
C08: 高性能近似アルゴリズムの設計法に関する研究 287
C09: ネットワーク問題のモデル化とアルゴリズムの研究 301
C10: 情報基盤アルゴリズムとしてのメタヒューリスティクスの研究 322
C11: 大量データ処理のための領域効率の良いアルゴリズム 335

3. 各種資料 **341**
ニュースレター 第 3 号 343
ニュースレター 第 4 号 350
平成 17 年度 第 1 回 全体会議 講演資料 358
平成 17 年度 第 2 回 全体会議 講演資料 381
NHC Spring School and Workshop on Discrete Algorithms 講演資料 413

1.　総括班活動報告

1　総括班活動報告

担当：岩間一雄，伊藤大雄，堀山貴史 (京都大学)

1.1　活動の概略

今年度は，春学校と国際会議（連続開催）１件，特定領域研究「確率的情報処理」との合同ワークショップ１件，電子情報通信学会総合大会の学生シンポジウム１件，電子情報通信学会回路とシステム軽井沢ワークショップの招待講演セッション１件，モデル研究班研究集会１件，ミニ研究集会6件，全体会議２件，幹事会２件を行った．さらに計画中の企画として，国際会議ICALP'06のワークショップiETA，電子情報通信学会回路とシステム軽井沢ワークショップの第２回目の招待講演セッション，進行中の企画として教科書シリーズの発行と電子情報通信学会誌和文論文誌Aおよび英文論文誌Dの特集号が順調に進捗している．そして現在５件のミニプロジェクトが進行中である．それから海外から20名の研究者を招聘（上記の国際会議等の招待講演者を含む）し，ポスドクを２名雇用した．また，会員間の情報交換のためのニュースレターを２回発行した．その他に，電子ジャーナルの発行の可能性を探っている．まずそれぞれの概要を以下で説明し，詳細は次節以降で述べる．なお，全体会議と幹事会の詳細は，ニュースレターを参照のこと．

春学校と国際会議

本特定領域研究の主催で，以下の春学校と国際会議を連続開催した．

会議名 NHC Spring School and Workshop on Discrete Algorithms

日程 2006年2月27日〜3月3日（2月27日〜3月1日: 春学校，3月2日〜3月3日: 国際会議）

場所 電気通信大学（春学校），調布クレストンホテル（国際会議）

内容 招待者による講義5件（春学校），招待講演10件（国際会議）

参加登録者数 104名（うち学生58名）

合同ワークショップ

特定領域研究「確率的情報処理」との合同ワークショップを以下のように開催した．

会議名 Randomness and Computation (RC2005)

日時 2005年7月18日〜21日

場所 仙台国際センター

内容 チュートリアル講演４件，一般公演25件．

学生シンポジウム

電子情報通信学会2006年総合大会においてコンピューテーション研究会と合同で学生シンポジウムを行った．

企画名 COMP-NHC学生シンポジウム

日時 2006年3月26日 9時〜17時

場所 国士舘大学

内容 学生講演16件，投票により優秀発表賞を1件選出．他に特別講演1件．

ワークショップ招待講演セッション

本特定領域研究の広報の意味も込め，電子情報通信学会の第18回 回路とシステム軽井沢ワークショップにおいて，招待講演セッションを行った．

企画名 走り出した特定領域研究「新世代の計算限界」

日時 2005年4月26日 9時30分〜12時

場所 軽井沢プリンスホテル西館

内容 講演3件．

モデル研究班研究集会

モデル研究班の情報交換や共同研究促進のため，研究集会を行った．

日時 2005年5月26日〜27日

場所 東北大学

内容 講演9件，ディスカッション．

ミニ研究集会

研究を活性化するために，テーマ毎のミニ研究集会を奨励した．以下の6件が実施された．

組合せゲーム・パズル

2005年9月12日, 京都大学

複雑ネットワーク，ウェブグラフ

2005 年 9 月 13 日, 関西学院大学 理工学部

列挙アルゴリズム

2005 年 9 月 27 日〜29 日, 群馬大学

Complexity

2005 年 10 月 11 日, 東京工業大学

暗号

2006 年 2 月 16 日, はこだて未来大学

ジオメトリ

2006 年 3 月 15 日〜17 日, コミュニティ嵯峨野（京都市）

全体会議（2005 年度第 1 回目）

日時 2005 年 6 月 16 日〜17 日

場所 国立情報学研究所

内容 班別に各研究課題の研究紹介の講演とポスターセッション．講演 4 件．全体討論

全体会議（2005 年度第 2 回目）

日時 2005 年 11 月 21 日〜22 日

場所 名古屋大学

内容 未解決問題セッション（6 件），その後未解決問題に対するグループ討論．講演 5 件．全体討論

幹事会

本特定領域研究は，総括班に数名加えた幹事団によって運営される．本年度は 2 回の幹事会を行った．

メンバー (17 名) 浅野孝夫（中央大），浅野哲夫（北陸先端大），伊藤大雄（京大），岩間一雄（京大），宇野毅明（国立情報学研究所），加藤直樹（京大），櫻井幸一（九大），杉原厚吉（東大），瀧本英二（東北大），田中圭介（東工大），徳山豪（東北大），西関隆夫（東北大），平田富夫（名大），堀山貴史（京大），牧野和久（東大），山下雅史（九大），渡辺治（東工大）．

第１回 2005 年 6 月 16 日 12 時〜14 時, 国立情報学研究所

第２回 2005 年 11 月 21 日 12 時〜13 時 30 分, 名古屋大学

招聘研究者

以下の研究者を招聘した．なお，*印は春学校の講師または国際会議の招待講演者でもある．

1. Sergey Bereg (University of Texas at Dallas), 2005.5.9–2005.5.19
2. Otfried Cheong (Korean Advanced Institute of Science and Technology), 2005.7.17–2005.7.23
3. Illena Streinu (Smith College), 2005.7.2–2005.7.31
4. Ruediger Reischuk (University Luebeck), 2005.9.10–2005.9.30
5. Dorothea Wagner (University Karlsrube), 2005.9.23–2005.10.1
6. Ludek Kucera (Charles University), 2005.10.27–2005.11.15
7. Rudolf Hans Fleischer (Fudan University), 2006.1.12–2006.2.12
8. Zhang Guochuan (Zhe Jiang University), 2006.1.22–2006.2.16
9. Marek Karpinski (University of Bonn), 2006.2.15–2006.3.5 *
10. Eva Trados (Cornell University), 2006.2.22–2006.3.3 *
11. Jens Vygen (University of Bonn), 2006.2.23–2006.3.4 *
12. Magnus Halldorsson (University of Iceland), 2006.2.23–2006.3.10 *
13. Bernard Chazelle (Princeton University), 2006.2.24–2006.3.1 *
14. Alexander Wolff (Karlsruhe University), 2006.2.24–2006.3.4 *
15. Timothy Chan (University of Waterloo), 2006.2.26–2006.3.4 *
16. Vijay Vazirani (Georgia Institute of Technology), 2006.2.24–2006.3.2 *
17. Der Tsai Lee (Academia Sinica), 2006.2.26–2006.3.4 *

18. Leonidas Guibas (Stanford University), 2006.2.27–2006.2.28 *
19. Bernhard Korte (University of Bonn), 2006.2.28–2006.3.5 *
20. James Lee (Institute for Advanced Study), 2006.2.28–2006.3.6 *

ポスドク

若手の支援と育成のためにポスドクを雇用する．本年度は以下の２名の採用を行った．

1. **氏名** Jesper Jansson
   期間 2005.4.20–2005.8.31
   機関 九州大学
2. **氏名** 西村 治道
   期間 2005.10.1–2006.3.31
   機関 京都大学

2　教科書シリーズ

担当：杉原厚吉 (東京大学)，山下雅史 (九州大学)

2.1　シリーズ趣旨

本特定領域研究では, 領域の学問的深化とともに, 領域を支える人材の教育・養成を重要な課題と考えている．このためには, 本領域を高校生あるいは大学初年度生に紹介し, 若年層のこの分野に対する興味を喚起するとともに, 本領域を学問体系として整理し，本領域を志す学習者および研究者のための適切な学習指針を整備する必要がある．そこで, その目的を達成する一助として, 共立出版社の御協力を得て教科書シリーズ「アルゴリズム・サイエンス シリーズ」を企画した．

著者への依頼文書の一部として配られたシリーズ趣旨には本特定領域がカバーするアルゴリズム・サイエンス領域に対する時代の要請を以下の４点にまとめている．

> まず，並列計算機や分散計算環境が容易に手に入る時代となり，このような新しい計算環境のもとで上手に問題を解決するための新しい解法の開発が必要とされていることである．
>
> 次に，バイオインフォマティクスやナノ技術など多くの応用分野が巨大な問題を上手に扱うための新しい計算パラダイムを必要としていることである．
>
> 第三に，情報セキュリティという重要な応用分野の出現が，従来は応用に乏しい理論研究と考えられてきた整数論や計算困難性理論の実学としての再構築を迫っていることである．
>
> そして最後に，これらの要請に応える健全なアルゴリズム・サイエンスの発展を担う人材の教育・養成である．

2.2　現状

本シリーズは本特定領域研究が採択された直後からその検討に入った．幾度かの会議を経て, 平成１７年４月に著者の方に依頼書を送付した．平成１６年度末までの状況は昨年度の報告書に記載した．平成１７年度末までの刊行の進行状況を以下にまとめる．

本シリーズの特徴の一つは２つの入門編をおいたことである．すなわち, 1. 入口からの超入門 (浅野哲夫著) と 2. 出口からの超入門 (岩間一雄著) である．ともに, 既に編集委員の査読が終了し, 刊行の準備が整いつつある．また, 計算幾何 (浅野哲夫著) と複雑性の階層 (荻原光徳著) についても, 同様の状況にあり, 本シリーズの刊行が順調に進むものと考えている．依頼からわずか１年に満たない期間で原稿を頂いた浅野, 岩間, 荻原の各先生にこの場を借りて感謝したい．

本シリーズでは, まだ１０巻を越える巻の発行が予定されている．これら残りの巻についても, おおよそ目次案を確定できている．著者の方々には原稿の完成に向けてご努力頂いているので, 次回にはよりよい報告ができるのではないかと期待している．

3　電子ジャーナル

担当：徳山 豪 (東北大学)，定兼 邦彦 (九州大学)

前年度からの検討事項として，電子ジャーナル，具体的にはプレプリントのアーカイブシステ

ムを構築し，特定研究メンバーの成果を含めて世界に情報発信をするとともに，理論計算機科学の活性化に貢献する企画が提案されており，その実現性について検討を行うことが 6 月 16 日の全体会議で幹事団から要請され，定兼を中心に技術的な実現性の検討に入った．

具体的には，論文サーバ構築用フリーソフトである EPrints (http://www.eprints.org/) を入手し，評価用のサーバを立ち上げた．URL は http://eprints.csce.kyushu-u.ac.jp/ である．現在は以下のことが可能である．

- 論文の閲覧 (非登録ユーザでも可)
- Web 上での新ユーザの登録
- 登録済みユーザからの論文の投稿
- エディタによる投稿論文の掲載の可否の決定

ユーザアカウントは機械的に作成されるが，エディタ用のアカウントは管理者のみが作成できる．

新しい論文が掲載された場合に，その情報を RSS として発信している．URL は http://eprints.csce.kyushu-u.ac.jp/perl/latest_tool?output=rss である．

今後は，論文へコメントをつけられるようにする予定である．

また，技術的な検討の後に，過大なワークロードを伴わずに設立・運営する方策について検討し，可能であると判断した場合には，原稿投稿の仕組みや著作権などの検討に入ることが出来る見通しである．

4 ニュースレター

編集委員長： 宇野 毅明 (国立情報学研究所)
副編集委員長： 牧野 和久 (大阪大学)

ニュースレターは，特定領域・新世代の計算限界のメンバーの情報交換と交流を目的とした情報発信誌となるべく企画された．近年，個別の研究成果に関しては多くの情報が簡単に手に入るようになったが，その裏に隠れている，研究者の思想や，研究推進のノウハウ，基礎的なアイディアといった点については，目に付かずに隠れている場合が多い．具体的は，研究のゴールどこに設定しているか，この理論のアイディアはどのあたりからどのように設定していたのか，この研究において主観的に評価の高いところはどこであるか，今後どのようなテーマがありうるか，応用，他分野などからの反応，問われている必要性はどのようなものであるか，といった点である．このような事柄を広く研究者間で共有することは，日本のアルゴリズム研究の全身のためになくてはならないことである．しかし，現時点でこのような情報を効率良く収集することは，それほど容易なことではなく，各研究者の個人的なつながりを中心として細々と行われているにとどまっている．

ニュースレターは，このような研究者間の情報交換を促進させることを目的として企画された．年 2-3 回の発行を行い，毎回，いくつかの研究関連の記事と，特定領域のスケジュール・活動報告と，各研究者の活動予定などを掲載する．本年度は，第 3 号を 7 月中旬に，第 4 号を 1 月下旬に発行した．

各号は電子メールで配布を行う．短い記事や連絡事項は全て掲載するが，長い記事，イベントの詳細などは web ページに掲載し，簡便に閲覧できる電子メール媒体と，詳細を効率よく閲覧できる web ページにてお互いを補完する．web 版は，
http://keisan-genkai.lab2.kuis.kyoto-u.ac.jp/newsletter/news.html
に掲載されている．

情報交換のため，各号に 1 つ，2000-4000 字程度研究に関わる記事を掲載する．これは，1 つの研究課題が担当する．通常，このようなニュースレターでは，研究成果を報告するのが一般的であるが，この特定領域では「研究者の交流」に焦点を当てたいため,「研究の成果以外」の記事を，面白く解説する．例えば，最近参加した国際会議の情報を，どのようなものが流行っていたか，何が面白かったか，などの主観的な解説を交えて報告したり，最近考えている問題，あるいはオープン問題を，この辺までは解けるがここがうまくいかない，といった解説を交えて紹介する，という形である．

また，研究者間の交流を促進するため，各研究者の，国内外の会議への出席予定を集約して掲載する．研究者の交流には，顔をあわせる回数を増やすことが肝要であり，他の研究者の参加予定が

わかれば，会議への出席のモチベーションを高め，ディスカッションや研究成果を生むきっかけにもなる．

以下に，今年度発行した第 3 号・第 4 号について，それらの目次を示す．3 号では徳山教授に，第 4 号では高木教授の記事を掲載した．研究の仕方における自分なりのポリシーの話，所属する研究科の位置づけに関する自分なりの意見と，研究において重要だが公的な機会で語られることの少ない，貴重な記事になったと感じている．また全体会議の報告においても，形式的な報告だけでなく，会議における意味的な成果までが具体的に報告されており，この点においても良い報告ができた．

第 3 号目次:
1.「群れ派」の研究の仕方
— 徳山 豪 (東北大学)
2．第 2 回全体会議を振り返って
— 浅野 哲夫 (JAIST)
3．2005 年度第 1 回幹事会議事録
— 事務局
4．イベントカレンダー ＋ 事務連絡
5．このニュースレターについて

第 4 号目次:
1．中心？隙間？それとも辺境？
— 高木 直史 (名古屋大学)
2．第 3 回全体会議の報告
— 平田富夫（名古屋大学）
3．2005 年度第 2 回幹事会議事録
— 事務局
4．イベントカレンダー ＋ 事務連絡
5．このニュースレターについて

5　ミニプロジェクト

5.1　計算幾何学

担当： 加藤 直樹 (京都大学)

計算幾何学は多次元の情報検索，地理情報処理などの技術基盤として幅広い応用価値がある．にも関わらず，計算幾何学を系統的に教えている大学，大学院は数少ない．そこで，大学院生や若手研究者を対象に計算幾何学の基礎を系統的に講義することを目的とするミニスクールを開催することとなった．3 月 15 日午後から 3 月 17 日昼まで京都市右京区「コミュニテイ嵯峨野」において計算幾何学に関するミニスクールを実施した．大学院生や若手研究者を主たる対象として参加者は，講師（浅野哲夫，徳山豪，David Avis，岡本吉央，加藤直樹）も含め 33 名で，東北大学，東京大学，名古屋大学，北陸先端大，京都大学の学生と 5 名の教員が参加した．計算幾何学の基礎概念として，凸包，三角形分割，ボロノイ図，領域探索，パラメトリック探索法，組合せ幾何を中心に講義がおこなわれた．またいくつかの未解決問題についての紹介もおこなわれた．

5.2　列挙アルゴリズム

担当： 中野 眞一 (群馬大学)

最適化，人工知能，データベース，知識発見など様々な分野で列挙を用いたモデル化が行なわれ，関連研究が急速に進んでいる．列挙アルゴリズムに関する研究集会を 2005 年 9 月 27 日から 29 日まで群馬大学伊香保研修所において開催した．参加者は 21 名で，所属は 12 大学/組織に及んだ．列挙をキーワードに，多様なテーマで 13 件の研究発表があり，活発に討論が行なわれた．今後も，半年ごとに開催予定の研究集会を基盤として，列挙アルゴリズムに関する多様な共同研究をさらに推進していく予定である．

5.3　ゲーム

担当： 伊藤 大雄 (京都大学)

ゲームの理論には様々な方向性があり，その応用も広範囲に及ぶ．近代理論としての起源は 1940 年代のノイマンの著書までさかのぼると言われているが，近年，ネットオークションや無秩序損 (cost of anarchy) の理論などでまた注目を浴びつつある．本ミニプロジェクトはこれらの近年注目を浴びている部分に留まらず，ゲームに関する知的好奇心を重視して，自由な研究の促進を目的としている．

その一環として本年度は，組合せゲームとパズルに関するミニ研究集会を 2005 年 9 月 12 日に京

都大学で行った．数学者であり，ゲーム・パズルの分野にも造詣の深い東海大学教育開発研究所の中村義作教授にチュートリアル講演をお願いした他，９件の一般講演を行った．発表の内容は広範囲に及び，活発な意見交換が行われ，成功裏に終わった．完成した発表でなくとも発表できるこういう機会は貴重であるなど，今後の継続を期待する意見が多く寄せられた．

次年度も継続していくが，この形の集会に留まらず，一つの話題に限定してのワークショップや学校形式の集会なども考えている．

5.4 計算量・ブール関数

担当： 垂井 淳 (電気通信大学)

未解決問題と現在取り組んでいる問題の発表を積極的に取り上げるミニ研究集会を 2005 年 10 月に開いた．ここで発表された複数の課題についてその後共同研究が進んでおりこの集会は特に若手の研究者が関係する共同研究促進に効果的だったと思われる．この集会以外にも渡辺（東工大）や垂井（電通大）が世話人をつとめる東京地区における complexity に関する定期的セミナーなどは本分野の研究展開に効果的なものとなっている．来年度以降はさらに新たな研究促進の企画を打ち出して行きたい．未解決問題について議論するネット上の掲示板，計算量理論にとって重要でありかつ本特定領域内全般において興味を持つ研究者が多いトピック（expander graph など）を集中的にとりあげる研究集会，大学院博士後期課程学生の発表を重視する研究集会などを検討している．

5.5 アルゴリズムサイエンスと地球環境問題

担当： 杉原 厚吉 (東京大学)

本特定領域研究が実は地球環境問題に貢献できる側面を強くもっているということを，我々自身でも再確認し，一般の人へも発信したいという目的で，このミニプロジェクトを企画中である．たとえば，各種の最短路探索は，燃料節約を目指すものであり，地球資源の有効利用と，二酸化炭素排出量の削減という効果をもたらす．その他，多くの最適化手法が地球環境を守るために役立つ．そこで，本研究で扱っている問題や解法を，地球環境を守るという観点から解釈し直し，整理する作業をすすめるために，来年度はミニシンポジウムを開く予定である．そして，その成果を冊子にまとめ，本特定領域が社会に貢献できる姿を発信する．

6 電子情報通信学会和文論文誌 A「新世代の計算限界 －その解明と打破－ 招待解説論文特集号」

特集号委員長： 増山 繁 (豊橋技術科学大学)
副委員長： 上野 修一 (東京工業大学)
幹事： 石井 利昌 (小樽商科大学)
委員： 永持 仁 (京都大学)，櫻井 幸一 (九州大学)，巳波 弘佳 (関西学院大学)

6.1 趣旨

２１世紀を迎え計算機を用いた問題解決は、社会のあらゆる場面で用いられてきている．それと共に様々な新たな計算困難問題が出現してきた．本特集ではこれらの問題の計算限界を解明し，それを打破すべく果敢に挑戦している，世界で最先端かつトップレベルの研究活動を電子情報通信学会会員を主な対象として，分かりやすく紹介する．そのことにより，本分野の研究への理解を広めるとともに，より一層発展させることを目的として本特集を企画した．

6.2 内容

本特集では，総括班から 1 編，A, B, C の各班からそれぞれ 2，3 編ずつ，計 9 編の招待解説論文により，本特定領域の研究活動の一端を紹介する．著者とタイトルは以下のとおりである．

1. 岩間 一雄（京都大学），計算限界の最前線
2. 瀧本 英二（東北大学），オンライン予測の理論に基づく意思決定
3. 徳山 豪（東北大学），関数近似における幾何学アルゴリズムの最近の進展：データ解析への応用に向けて

4. 藤田 聡（広島大学），分散ネットワーク上の故障診断問題について
5. 田中圭介，林良太郎（東京工業大学），匿名性をもつ公開鍵暗号
6. 西野 哲朗（電気通信大学），量子計算量の下界の評価手法
7. 伊藤 大雄（京都大学），ハラリイの一般化三並べ
8. 定兼 邦彦（九州大学），圧縮データ構造
9. 浅野 泰仁（東北大学），サイトを活用したWeb上の情報発見手法

まさに今世紀に入って新たに出現してきた現実に解決を迫られている問題に果敢に挑戦すべく，理論的にも応用的にも多様な方向に展開し深化してきている現状がみてとれるのではないかと思う．

6.3 むすび

本特集は当初の計画通り本年６月に発行予定である．末筆ですが，この機会を賜わった今井浩編集委員長，御多用にもかかわらずすばらしい原稿をお寄せいただいた岩間一雄領域代表を始めとする執筆者の方々，丁寧に閲読いただいた編集委員の方々，お世話になりました学会事務局の高木さんに心より厚くお礼申し上げます．

7 電子情報通信学会英文論文誌 D「新世代の計算限界 －その解明と打破－ 招待論文特集号」

特集号委員長： 和田 幸一 (名古屋工業大学)

7.1 趣旨

特定領域研究「新世代の計算限界－その解明と打破－」は，アルゴリズムの目指すものがスピードから解の品質へと大きな変革を迎えつつあるこの時期において，計算困難問題に対して実用性の高い品質と性能保証をいかに行うかを真正面から取り組んでおり，数学的な興味のみならず，実用性とわかりやすさを兼ね備えた成果をだすことを目標としている．本招待論文特集号は、本特定研究をさらに発展させ，本特定研究への理解を深めることを目的として，世界でのトップレベルの研究活動及び成果を主として電子情報通信学会員に紹介するために企画されたものである．

7.2 内容

本特集号は全て招待論文で構成されており，研究代表者である岩間先生（京都大学）から10編を推薦していただいた．今回は，通常の論文と同程度の査読を行ない，論文賞として3編が査読者より推薦されるなど論文のレベルは高いものであった．タイトルと著者は以下のとおりである．

(1) The bump hunting method using the genetic algorithm with the extreme-value statistics (Takahiro Yukizane, Shin-ya Ohi, Eiji Miyano, Hideo Hirose)

(2) Online Allocation with Risk Information (Shigeaki Harada, Eiji Takimoto, Akira Maruoka)

(3) Inserting Points Uniformly at Every Instance (Sachio Teramoto, Tetsuo Asano, Benjamin Doerr, Naoki Katoh)

(4) A Polynomial Time Algorithm for Obtaining the Minimum Vertex Ranking Spanning Tree on Outerplanar Graphs (Shin-ichi Nakayama, Shigeru Masuyama)

(5) Triangular Mesh Generation with Constant Number of Different Edge Lengths (Shin-ichi Tanigawa, Naoki Katoh)

(6) Efficient Algorithm for Evacuation Problems in Dynamic network Flows with Uniform Edge Capacity, (Naoyuki Kamiyama, Naoki Katoh Atsushi Takizawa)

(7) Approximation Algorithm for the Stable Marriage Problem (Kazuo Iwama, Shuichi Miyazaki, Kazuya Okamoto)

(8) Computing automorphism groups of chordal graphs whose simplicial components are of small size (Seinosuke Toda)

(9) The even outdegree conjecture for acyclic *PLCP*-cubes in dimension five (Sonoko Moriyama, Yoshio Okamoto)

(10) Approximated Vertex Cover for Graphs with Perfect Matchings (Tomokazu Imamura, Kazuo Iwama, Tatsuie Tsukiji)

7.3 おわりに

本特集号は 2006 年 8 月に発行予定である．最後になりましたが，ご推薦いただいた岩間一雄先生，ご執筆を快諾していただいた著者の皆様，丁寧に閲読いただいた査読者の皆様，お世話になりました学会事務局の百田さんに心より感謝申し上げます．

8 国際ワークショップ iETA の企画

担当： 渡辺 治 (東京工業大学)

本研究領域の研究者を中心として，以下のようなワークショップを開く予定である．

会議名： Improving Exponential-Time Algorithms (iETA)
場　所： イタリア，ヴェニス（下記説明参照）
開催日： 2006 年 7 月 16 日
代　表： 渡辺 治，R. Niedermeier（代表）
委　員： 伊藤大雄，岩間一雄，F. Fomin, D. Kratcsh, J. Rothe

このワークショップは，国際会議　ICALP'06 に連続開催されるワークショップ群の一つとして，開催を計画している．ICALP'06 (Internatinal Colloquium on Automata, Language and Programming) は，ヨーロッパ理論計算機科学学会 (EATCS, European Association of Theoretical Computer Science) が毎年主催する理論計算機科学の重要な国際会議であるが，ヴェニスで開かれる今回の第 33 回会議では，様々な分野の研究者に，専門的なワークショップの連続開催の呼びかけがあった．

それに対し，本特定研究領域の研究者らが中心となり，海外の研究者とも呼応して，指数関数的な難しさを持つ問題に対する挑戦とその限界について議論するワークショップの提案をしたところ，ICALP'06 ならびに EATCS により採択され，上記のように開催する計画となった．

このワークショップでは，上記の実行委員会らによるチュートリアル，参加者による発表，などの他，研究者間の議論の場を設け，困難といわれている問題に対して，我々がどの程度のアルゴリズムまで達成できるか，を見極めるための手法について議論する予定である．

会議の案内については以下の Web Page に掲載中である．

`http://www.is.titech.ac.jp/~watanabe/iETA/`

Randomness and Computation

担当： 田中 和之 (東北大学), 渡辺 治 (東京工業大学)

1 会議の概要

平成 17 年 7 月 18 日から 21 日の 4 日間にかけて，仙台国際センターにおいて，Randomness and Computation と題するワークショップを開催した．

このワークショップは，本特定領域研究ともう１つの特定領域研究「確率的情報処理への統計力学的アプローチ」の共同企画として両特定領域研究が主催し，以下の学会に協賛して頂いて行われた：電子情報通信学会，日本神経回路学会，計測自動制御学会，日本物理学会，人工知能学会，情報処理学会，システム制御情報学会．会議は，田中和之（東北大学,「確率的情報処理」領域代表）と渡辺治（東京工業大学）を委員長とし，徳山豪（東北大学），樺島祥介（東京工業大学），田中利幸（首都大東京），西森秀稔（東京工業大学）の各委員からなる実行委員会により運営された．

上記２つの特定領域研究にかかわる研究者集団は，どちらも情報処理を理論的に研究している者たちの集まりであるが，本領域はコンピュータ・サイエンス系,「確率的情報処理」は統計力学系の研究者が多く，研究スタイルや物の見方が大きく異なっている．その２つのグループに，ほぼ共通する話題「ランダムネスと計算」を選び，このテーマに関する研究発表を通して，お互いの考え方や手法，結果を披露し，意見を交換する場として，このワークショップを企画した．

2 会議の内容

会議のテーマは「ランダムネスと計算」である．ランダムネス（ランダム性やランダムリソースなどの総称）は，多くの現象に現われるが，情報や計算（アルゴリズム）にも，様々な形でかかわってきている．計算が扱う対象の中に含まれるランダムネスはもちろんのこと，ランダムネスを計算の効率化に積極的に応用しよう，という考えかたも，最近のアルゴリズム設計の基本方針の一つになりつつある．このように，情報やその処理に密接に関係するランダムネスを，今回の会議のテーマとしたのである．

チュートリアル講演では，なランダムネスと計算に関係の深い次の 4 つの講演が行われた．

1. 田中和之（東北大学 院情報科学研究科）
   Probabilistic image processing
   and Bayesian network
2. 福島孝治（東京大学 院総合文化研究科）
   Monte Carlo method
   – sampling from an extended ensemble –
3. O. Cheong (Comp. Sci., KAIST, Korea)
   On finding a guard that sees most
   and a shop that sells most
4. 松井知己（東京大学 院情報理工学系研究科）
   CFTP を用いたパーフェクトサンプリング

一般講演では，全部で 25 件の講演があった．内訳は，ランダムの定義に関係する基礎理論，ランダムな現象の解析，ランダムネスを計算に応用し効率を上げたアルゴリズムの提案，確率解析を計算に応用したアルゴリズムの提案，量子的な振る舞いの解析と量子計算アルゴリズムの提案などである．講演者は以下のとおりである．

1. 河内亮周 （東京工業大学 院情報理工学研究科）
2. 天野一幸 （東北大学 院情報科学研究科）
3. 築地立家 （東京電機大学 院理工学研究科）
4. 高橋勇人 （東京工業大学 院情報理工学研究科）
5. 只木孝太郎 （中央大学 21 世紀 COE プログラム）
6. 三好直人 （東京工業大学 院情報理工学研究科）

7. 渡辺治（東京工業大学 院情報理工学研究科）
8. 伊東利哉 （東京工業大学 学術国際情報センター）
9. 白石友一 （総合研究大学院大学 複合科学研究科）
10. 来嶋秀治 （東京大学 院情報理工学系研究科）
11. 鈴木晶子 （東北大学 院情報科学研究科）
12. 徳山豪 （東北大学大学院情報科学研究科）
13. 西森秀稔 （東京工業大学 院理工学研究科）
14. 樺島祥介 （東京工業大学 院総合理工学研究科）
15. 池田思朗 （統計数理研究所）
16. 村田昇 （早稲田大学 理工学部）
17. 鈴木正 （東京大学 院新領域創成科学研究科）
18. 井上純一 （北海道大学 院情報科学研究科）
19. 大久保潤 （東北大学 院情報科学研究科）
20. 森直樹 （大阪府立大学 工学部）
21. 本村陽一 （独立行政法人産業技術総合研究所デジタルヒューマン研究センター）
22. 村山立人 （NTT コミュニケーション科学基礎研究所）
23. 田中利幸 （首都大学東京 システムデザイン学部）
24. 中村一尊 （慶應義塾大学 理工学部）
25. 庄野逸 （山口大学 工学部）

3 総括と参考資料

全部で 4 日間と少々長い日程でしたが，学生を含め 110 人程度の参加者のうち，かなりの方がほぼ全日程に参加した．

コンピュータサイエンスと理論物理学では手法や考え方にかなりの違いがあり，研究者同士の交流も活発ではなかったが，ランダムネスと計算というテーマでは，ほとんど同じ問題を考えていることに多くの参加者が気づかされたように思う．また，発表の前後や休憩時間を含めて議論も盛り上り，両分野のアプローチの違いや特徴が明らかになるという一面もあった．このワークショップが契機となって，今後の共同研究が生まれることを期待したい．

ワークショップの実際の運営は，もう一人の実行委員長の田中和之氏が中心に行って頂いた．本ワークショップが成功したのも，氏の綿密な計画と実行力に負うところが多い．最後にこの点を記し，田中氏に感謝したい．

会議の詳しいプログラムやチュートリアル講演の資料は以下の Web Page に掲載中である．

http://www.smapip.is.tohoku.ac.jp/~smapip/2005/NHC+SMAPIP/

NHC国際会議

担当： 岩間 一雄，伊藤 大雄，堀山 貴史 (京都大学),
西野 哲朗，垂井 淳，武永 康彦 (電気通信大学),
浅野 孝夫 (中央大学)

1　会議のあらまし

本特定領域研究の第２回国際会議として、平成 18 年２月 27 日から３月３日の５日間、NHC Spring School and Workshop on Discrete Algorithms（離散アルゴリズムに関する春学校とワークショップ）を開催した。前半の春学校は２月 27 日から３月１日の３日間電気通信大学で開催し、後半のワークショップは３月２日と３日の２日間調布クレストンホテルで開催した。組織委員会のメンバーは、岩間一雄（NHC 代表、京都大学)、西野哲朗（組織委員長, 電気通信大学)、浅野孝夫（プログラム委員長、中央大学)、伊藤大雄（京都大学)、武永康彦（電気通信大学)、垂井淳（電気通信大学)、堀山貴史（京都大学）である。

春学校では、Bernard Chazelle (Princeton University), Leonidas J. Guibas (Stanford University), Eva Tardos (Cornell University), Vijay V. Vazirani (Georgia Institute of Technology), Marek Karpinski (University of Bonn) の５人の招待講師が、それぞれ３時間の講義 (およびそれに続く質疑応答と討論) を行った。

ワークショップでは Eva Tardos (Cornell University), Marek Karpinski (University of Bonn), Bernhard Korte (University of Bonn), Jens Vygen (University of Bonn), Magnus M. Halldorsson (University of Iceland), D. T. Lee (Academia Sinica), Timothy M. Chan (University of Waterloo), Alexander Wolff (University of Karlsruhe), James R. Lee (UC Berkeley), Takeshi Tokuyama (Tohoku University) の 10 人の招待講演者が、それぞれ 60 分の講演 (およびそれに続く質疑応答と討論) を行った。

参加登録者は 104 名で、うち 58 名が学生であった。

2　会議の目的

「理論的な計算限界による様々な困難を解明し打破する」という本特定領域研究の目標を達成するため、最先端のアプローチの調査と世界的な共同研究体制の構築という昨年度の国際会議の目的を引き継いで本国際会議が行われた。ただし、今年度は ACM の STOC、IEEE の FOCS、ACM/SIAM の SODA などの最先端の研究発表に出席する機会の少ない若手の研究者や学生が、その分野で活躍する世界第一線の研究者の研究トピックスに関心を持ち、将来的にはそのような国際会議で発表できるようになることを、心から願って計画した。とはいっても、本特定領域で扱う理論分野は多岐にわたるので、今回はテーマを離散アルゴリズム、その中でも、計算幾何学と組合せ最適化、に限定して行った。

招待講演者の人選においては、上記の ACM の STOC、IEEE の FOCS、ACM/SIAM の SODA などで中心的な役割を果たしている研究者あるいは当該分野で指導的な役割を果たしたベテランの研究者の他に、最近の研究成果のめざましい若手の研究者にも講演依頼をした。この分野の最先端の研究における若手の研究者の活躍が、日本の若手の研究者や学生にも強いインパクトを与えてくれるであろうという期待もあったからである。

3　会議の内容

前述の目的を達成するため、前半を春学校とし、後半をワークショップとして、以下のプログラムで行った。

春学校プログラム
開催場所：電気通信大学総合研究棟 301 号室（および 306 号室）

２月 27 日（月）
9:00–12:30 Data-Driven Computing (Bernard Chazelle, Princeton University)
12:30–14:00 昼食
14:00–17:30 Sensor Networks: A Digital Bridge to the Physical World (Leonidas J. Guibas, Stanford University)
２月 28 日（火）
9:00–12:30 Games in Networks: Routing, Network Design and Potential Games (Eva Tardos, Cornell University)
12:30–14:00 昼食
14:00–17:30 Polynomial Time Algorithms for Market Equilibria (Vijay V. Vazirani, Georgia Institute of Technology)
３月１日（水）
9:00–12:30 Random Sampling Techniques and Approximation of MAX-CSP (Marek Karpinski, University of Bonn)
12:30–14:00 昼食
14:00–17:00 自由討論
ワークショッププログラム
開催場所： 調布クレセントホテル
３月２日（木）
9:30–10:30 Games in Networks, Equilibria, and Inefficiency (Eva Tardos, Cornell University)
10:30–11:00 休憩（討論）
11:00–12:00 Approximation Schemes for Metric Clustering and Partitioning (Marek Karpinski, University of Bonn)
12:00–13:30 昼食
13:30–14:30 Discrete Optimization and VLSI-Design (Bernhard Korte, University of Bonn)
14:30–15:00 休憩（討論）
15:00–16:00 Approximation Algorithms for Facility Location (Jens Vygen, University of Bonn)
16:00–16:30 休憩（討論）
16:30–17:30 Algorithms for a Networked World (Magnus M. Halldorsson, University of Iceland)
18:00– バンケット
３月３日（金）
9:30–10:30 Algorithms for String Manipulation and Related Problems (D. T. Lee, Academia Sinica)
10:30–11:00 休憩（討論）
11:00–12:00 Dynamic Data Structures in Computational Geometry (Timothy M. Chan, University of Waterloo)
12:00–13:30 昼食
13:30–14:30 Geometric Networks: Integer Linear Programming and Combinatorial Algorithms (Alexander Wolff, University of Karlsruhe)
14:30–15:00 休憩（討論）15:00–16:00 Geometric Embeddings and Graph Expansion (James R. Lee, UC Berkeley)
16:30–17:30 Distance Trisector and Voronoi Diagram with Neurtal Zone (Takeshi Tokuyama, Tohoku University)

春学校では、各講師とも講義を 60 分３回とし間に２回の休憩（討論）を含めた。最初はトピックスへの導入と研究背景、次に研究の詳細、そして最後に最近の研究動向を解説してもらった。講義で使用する資料は前もって送ってもらい印刷して配布し、聴講者の理解の手助けになるようにした。第１日目の講義は、計算幾何学およびそれから派生したトピックスが主体であった。第２日目の講義は、アルゴリズム的ゲーム理論の分野で社会的効用と個人的効用の対立問題に関するトピックスであった。第３日目の講義は、近似アルゴリズムの近似困難性に関するトピックスであった。どの講義でも、講義中にも質問を受け、聴講者の理解がスムーズになるように工夫されていた。さらに、３月１日午後の自由討論では、実際に確保していた５つの部屋をフルに稼動して熱心に議論がなされていたのも印象的であった。

ワークショップでは、現在関心を持っている研究テーマについて、10 人の招待講演者に各自の最新の研究成果を紹介してもらった。こちらも、講演で使用する資料はできるだけ前もって配布し、聴講者の理解の手助けになるようにした。内容的には、主として、計算幾何学、組合せ最適化、近似アルゴリズムの分野の成果で、最近の STOC、FOCS、SODA などに掲載されたあるいはこれから掲載されるものが多かった。いずれの講演も印象的であったが、そのなかでも若手の James R. Lee の講演は特に印象的であった。その内容は、最素カット (sparsest cut) の近似アルゴリズムの性能改善に結びつく、グラフの辺の長さをそれほど

拡大しないで空間に埋め込むアルゴリズムの研究で、近似アルゴリズムの分野で最近最も注目されている研究分野の１つである。講演の資料や講演の仕方についても極めて学ぶべきものが多かった。

4　総括と課題

「理論的な計算限界の解明と打破」という本特定領域研究の目標達成に対して、今回の会議は離散アルゴリズムに限定しての国際会議であったため、聴講者の前提知識にばらつきがあり、講演内容の理解が全体的になかなかスムーズに行かなった点があったかもしれない。これを補うため、講演で用いる資料を事前に聴講者にカラー印刷して配布しておいたのはよかったと思われる。なお、どの講演者も、配布した資料をこの報告書に含めたり、あるいは NHC のホームページにおくことについては、快諾している。

多忙な招待講演者の日程により、聴講者と講演者との討論の時間が十分にとれなかった点も反省材料である。これは、アメリカの大学の新学期が１月中に始まり、２月末に海外に出張するには講義をかなり休講にしなければならない、という点に由来するものである。開催の日本側としては時期的に有利かもしれないが、第一線で活躍する研究者を招待する上では、考慮すべき点かもしれない。なお、ヨーロッパ（特にドイツ）の大学は学期がほぼ日本と同じで、この時期の海外出張は比較的好都合なようである。

また、会議が５日間に渡るのは主催者側にも参加者側にもかなり大変なものがあるようであった。さらには、春学校の招待講師がワークショップでも講演したが、内容的には同じトピックスで重複が目立ち効果が薄かったのではないかという、聴講者の意見もあった。

一方で、バンケットでは、専門的な情報交換とともに、招待講演者との文化交流を行うことができた。またバンケット以外でも、国内の他大学の学生間で情報交換をすることもできた。

最後に、学生をこの会議に積極的に参加するように推薦してくれた本特定領域のメンバーに心から感謝する。

第18回 回路とシステム軽井沢ワークショップ
特別講演セッション

世話役： 巳波 弘佳 (関西学院大学)

第18回 回路とシステム軽井沢ワークショップ

【日程】 2005年4月25日(月), 26日(火)

【場所】 軽井沢プリンスホテル・西館・国際会議場

【URL】 http://www.ieice.or.jp/ess/kws/

本特定領域研究の活動の広報と他分野の研究者との交流を目的に，電子情報通信学会 回路とシステム軽井沢ワークショップに招待講演セッションを企画・実施した．

本ワークショップは，回路とシステムに関連した分野の研究者や技術者が集い，招待論文や投稿論文，パネル討論を通じて，分野内だけでなく分野間にまたがる境界領域の課題解決と，将来の研究分野の探求を目的として開催されているものである．この分野の研究集会としては国内で最大規模であり，また今回で18回目となり，定評のあるワークショップである．大学の研究者のみならず，企業研究所からの参加も数多く，産学の交流も盛んである．

このワークショップは，回路とシステム関連分野としてアルゴリズム関係，グラフ理論関係の講演も行われているため，関心を持つ聴衆も多く，ここで今回のセッションを企画することは有効だと考えられる．

以下に，関連プログラムを挙げる．

本特定領域研究関連セッション

セッション D2-1 (4/26 9:30-10:15)
動きだした特定領域研究『新世代の計算限界』(1)

- 「プロジェクトの概要 ―計算限界の過去・現在・未来―」伊藤大雄 (京大)
  （概要）本特定領域研究の目的と概要，さらに様々な研究課題に関して紹介された．

セッション D2-2 (4/26 10:30-12:00)
動きだした特定領域研究『新世代の計算限界』(2)

- 「オンライン予測の理論と応用」瀧本英二 (東北大)
  （概要）オンライン予測の理論について，そのモデルと戦略，またそれらの結果について詳しく解説された．さらに，オンライン予測の投資問題や最短路問題などへの応用についても紹介された．

- 「Witt分解を用いたフーリエ解析 ― MOD回路サイズの下限証明のための新しい代数―」築地立家 (東京電機大)
  （概要）Witt分解や関連する代数的背景について紹介された．

本セッションが実施された会場には30人ほどの聴衆が集まり，興味の高さが伺えた．また，実行委員会においても，本セッションは好評であったということで，翌年度の継続して実施することが要請された．

研究集会 (モデル班)

世話役: 瀧本 英二，篠原 歩，徳山 豪 (東北大学)

モデル研究班の各研究グループから，以下のような講演形式で研究紹介や問題提起等の話題を提供していただき，それに基づいてモデル研究の方向性についてディスカッションを行った．

日程：2005 年 5 月 26 日 13:00〜5 月 27 日 12:30
場所：東北大学工学部電子情報システム・応物系
351・353 号室 (26日), 451・453 号室 (27日)
参加者：瀧本英二，酒井義文，天野一幸，徳山豪，篠原歩，西関隆夫，周暁 (以上東北大)，渡辺治 (東工大)，武永康彦 (電通大)，高木一義 (名大)，加藤直樹 (京大)，山下茂 (NAIST)，藤田聡 (広島大)，下園真一 ，坂本比呂志 ，宮野英次 (以上九工大)，他計約 40 名

瀧本:あるルーティングゲームの最適戦略について
ルーティングに関連する問題を零和ゲームとしてモデル化し，オンライン予測とカーネル手法を組み合わせて最適戦略を求めるアルゴリズムを与えた．

高木：ハードウェアアルゴリズムの設計と性能評価について
ハードウェアアルゴリズムの設計と設計支援環境について，現在進めている研究での事例を基に説明し，回路モデルと性能評価に関する問題点を挙げた．

山下：NAIST の量子計算研究グループの紹介
古典スタック付き量子プッシュダウンオートマトンの計算能力，エラーのある量子オラクルの分類を行う量子アルゴリズム，および N 個の関数の論理和を分散環境で効率よく計算する量子プロトコルについて紹介した．

藤田：A Tight Bound on the Number of Mobile Servers to Guarantee the Mutual Transferability among Dominating Configurations
サーバの位置が動的に変化する分散システムのための新しいモデルを提案し，ユーザへのサービスが中断しないようにするためのサーバ数に関する必要十分条件を与えた．

宮野：最小ブロック転送問題に対する近似アルゴリズム
最小ブロック転送問題を，与えられた DAG の頂点を指定されたサイズに分割する問題としてモデル化し，その厳密計算と近似の複雑さについて議論した．

徳山：緩衝地帯のあるボロノイ図問題におけるアルゴリズムとモデル
緩衝地帯のあるボロノイ図の数学的定式化と，その計算アルゴリズムの評価における離散アルゴリズムと数値計算アルゴリズムの融合の問題点について述べた．

加藤：一様三角形分割問題と幾何学的配置問題：新しい結果と未解決問題
建築におけるトラス構造物の最適設計問題や都市工学における道路の最適配置問題を，幾何的最適化問題としてモデル化し，近似アルゴリズムや未解決問題について論じた．

武永：グラフのシンボリック表現とアルゴリズム
区間グラフや比較可能グラフなどのさまざまなグラフクラスに対する種々の問題に対し，OBDD 表現を用いたアルゴリズムとその計算の複雑さについて，最近の研究動向を概観した．

篠原：漸増的最長共通部分列問題について
２つの文字列の最長共通部分列を求める問題を拡張し，どちらかの文字列の前あるいは後ろに文字が１つずつ追加されていくオンライン版の問題を提案し，効率の良いアルゴリズムを与えた．

この研究集会を通して，各研究グループがどのような視点で問題に取り組んでいるか，また，今何が問題となっているかについて，情報やアイディアの交換を行うことができた．また，モデル研究班が極めて幅広い領域をカバーしているにもかかわらず，全体として正しい方向性を持って本特定領域研究に貢献しつつあることが実感できた．

ミニ研究集会 (組合せゲーム・パズル)

世話役： 伊藤 大雄 (京都大学)

組合せゲーム・パズルに関する話題を広くとらえ，最新の研究成果の発表はもちろん，個人的に興味を持っていることなど，普段あまり発表の機会のないものも自由に発表し，意見交換することで，交流の活発化とこの分野の研究の発展への寄与を試みるという目的で，本研究集会は開催された．

構成は１件の特別招待講演と９件の一般講演からなる．特別招待講演は数学者であり組合せゲーム・パズルの研究にも造詣の深い東海大学教育開発研究所の中村義作教授を招いて「ゲームにひそむ数理」というタイトルでチュートリアル講演をお願いした．

一般講演の９件は，理論からプログラミングまで広範囲におよび，活発な意見交換もなされた．さらに終了後に懇親会を催し交流を深めた．詳細は以下の通りである．

日時 2005 年 9 月 12 日（月）　9:30 – 17:40

場所 京都大学工学部情報第一講義室（工学部 10 号館 1 階）

参加者数 31 名（教員 16 名, 学生 15 名）

特別招待講演（チュートリアル）

ゲームに潜む数理：中村義作（東海大学教育開発研究所）

要旨 ゲームを数理的視点から分類すると完全情報ゲームと不完全情報ゲーム，確率的ゲームと確定的ゲームの２×２＝４通りに分類できる．今回は完全情報な確定的ゲームを取り上げ，１人ゲームから，(1) ペグ・ソリテア，(2) ナイトの周遊，２人ゲームから，(3) １つ山くずし，(4) ２つ山くずし，を選び，その背後に潜む数理を紹介する．時間に余裕があれば，２人ゲーム：(5) 銀貨の鋳造（sylver coinage）にも触れたい．

一般講演

1. シャノンのスイッチングゲームにおけるペアリング戦略について：高橋良介，瀧本英二（東北大学 情報科学研究科）

   要旨 HEX というゲームは，$n \times n$ の盤面では最適戦略を求めることが PSPACE 困難であるが，$n \times m$ の盤面（$n \neq m$）ではペアリング戦略と呼ばれる単純な必勝法が存在することが知られている．本研究では，このゲームを一般化したシャノンのスイッチングゲームにおいて，ペアリング戦略が存在するための条件について考察する．

2. Voronoi game on graphs and its complexity：寺本幸生，上原隆平（JAIST）

   要旨 The Voronoi game is a two-person game which is a model for a competitive facility location. The game is done on a continuous domain, and only two special cases (1-dimensional case and 1-round case) are well investigated. We introduce the discrete Voronoi game of which the game field is given as a graph. We first show the best strategy when the game field is a large complete k-ary tree. We also show that the discrete Voronoi game is NP-complete on a given general graph, even if 1-round case.

3. 碁石ゲームに関する考察 — ４目並べ講座：徳山豪（東北大学 情報科学研究科）

   要旨 伊藤による碁石ゲームに関する講演（7 月 26 日）から生じた問題に関する考察を行う．数学的な厳密な話ではなく，どちらかというと，趣味の話ではあるが，ゲームを解析する場合の考え方について討論したいと思う．具体的には，縦４，横 5 のバージョンのパターン生成問題を取り扱う．

4. 囲碁プログラミングの探索における小目標間の依存関係解決に向けて：美添一樹（東京大学 情報理工学研究科）

   要旨 囲碁においては，盤面全体に対する，速く正確な評価関数を作ることは困難である．そのため，小目標ごとのサーチが，囲碁プログラムの間では広く用いられている．ここで問題になるのが小目標間の依存関係である．小目標の勝敗に影響を与える範囲を求めて依存関係を解決するアプローチが研究され始めている．そのような範囲を求める新たな手法を提案し，囲碁の部分問題を解くことを目指す．

5. 逆算法に基づく詰め将棋の列挙:堀山貴史，中塚裕之，岩間一雄（京都大学 情報学研究科）

   要旨 近年の計算機の高速化やメモリ量の増加，洗練されたアルゴリズム設計法の発展により，与えられた条件を満たす解を 1 つだけでなくすべて列挙することが，実用上要請されるようになってきている．本発表では，逆算法による詰将棋の列挙アルゴリズムを提案する．逆算法により詰め手数の少ないものから順に詰将棋を列挙することで，詰将棋解答プログラムを用いることなく，与えられた条件下で可能な詰将棋を高速に列挙することができる．

6. Toward a Polynomial Time Algorithm for 2-Link Puzzle：牧野格三（東京工業大学 数理計算科学専攻）

   要旨 パズル雑誌などに載っているものの中に「ナンバーリンク」と呼ばれるパズルがある．今回，我々はこのパズルをグラフ問題として考え，k-リンクパズルと名づけた．本研究は，そのk-リンクパズルに関する研究の第一歩として，kを 2 に固定した「2-リンクパズル」に対し，解を持つための必要十分条件について考察する．

7. 一般化アマゾンは PSPACE-complete：清見礼（国立情報学研究所）

   要旨 アマゾンは比較的新しいシンプルなルールの完全情報ゲームである．各局面において着手の候補が非常に多いことから，従来の alpha-beta カットに基づく探索のみでは強いプレーヤを作ることが困難なため注目されている．アマゾンを一般化したゲームの勝敗判定は，終盤戦においてすら NP-complte であることが示されているが，一般の局面の勝敗判定の難しさについては未解決であった．我々は一般の局面においての一般化アマゾンの勝敗判定が PSPACE-complete であることを示した．

8. Rogue の脱出判定問題：武永康彦（電気通信大学）

   要旨 Rogue はキャラクタ端末のディスプレイでよく親しまれていた，コンピュータ上のアドベンチャーゲームである．残り体力のないキャラクターが魔物のいる部屋から脱出できるかというパズルがデュードニーの「コンピュータレクリエーション」で紹介されているが，その一般化が NP 完全であることを証明する．

9. 整数計画法を用いたスリザーリンクの解法：杉村 由花（東京大学）

   要旨 ペンシルパズル「スリザーリンク」の類似パズル「スリザーリンクス」の考案，およびその NP 完全性の証明．また，スリザーリンクの整数計画問題としての定式化，およびその実装実験について．

ミニ研究集会 (複雑ネットワーク, ウェブグラフ)

世話役： 宇野 裕之 (大阪府立大学), 巳波 弘佳 (関西学院大学)

日時 2005 年 9 月 13 日 (火)

場所 関西学院大学 神戸三田キャンパス IV 号館

目的 現実社会で自然発生的に形成されるネットワークを総称して複雑ネットワークと呼び, その一つにウェブグラフがある. 近年, この分野における研究の進展は著しいが, 対象となるネットワークの発生する現場が多岐にわたることから, その研究成果が物理学, 数学, 生物学, 情報科学, 社会科学などの分野に分散し, 互いに専門外の分野の成果を把握するのが困難でもある. そこで本集会では, 複雑ネットワーク，ウェブグラフにはじまり，それらに対するデータマイニングの技法やその応用，それらを用いた結果，実験的考察や理論的解析など，少しでも関係のある話題を幅広く対象とする. 必ずしもフォーマルな講演会を目指すものではなく，内容としては，完成した研究でなく研究の途中段階のもの，話題の提供，興味のあること，素朴な疑問，関連分野の研究紹介などを幅広く扱い，それらをもとにディスカッションを行ない，これらのトピックに関する理解を深めることが大きな目的である. なお本集会は, チュートリアル講演と一般講演の 2 部構成とした.

参加者 [順不同] 伊藤大雄 (京大), 渡辺治 (東工大), 増田直紀 (理化学研究所), 浅野泰仁 (東北大), 来見田裕一 (九大), 茨木俊秀, 巳波弘佳, 山崎達志, 藤井佳一, 原田大輔, 佐々木裕介, 荒木麻季子, 暮部裕介, 井坂元彦, 岡田孝, 杉浦一馬 (以上, 関西学院大), 小野廣隆 (九大), 定兼邦彦 (九大), 中野豊 (京大), 上原隆平 (北陸先端科学技術大学院大), 宇野裕之 (大阪府立大), 以上 21 名.

チュートリアル講演:

1. 複雑ネットワーク — 基礎概念から最近の研究動向まで, 増田直紀 (理化学研究所 脳科学総合研究センター)

(概要) 「複雑ネットワークの科学」(産業図書, 今野紀雄氏との共著) の著者でもある講演者が, 題目どおり複雑ネットワークのこれまでの研究を概説した. 研究の興味は, 複雑ネットワークの成り立ちを説明するモデルの提案・解析から, ネットワーク上のダイナミクスへと移行していることが説明された.

2. サイトを単位として用いた Web 上の情報発見手法, 浅野泰仁 (東北大学大学院情報科学研究科)

(概要) ウェブからコミュニティなどの情報を発見する際に, 既存のページ単位のリンク構造からではなく, ディレクトリにもとづくサイトを単位とするリンク構造からの発見を提唱し, 実験にもとづくその効果および優位性の説明があった.

一般講演:

3. 孤立クリークの線形時間列挙, 伊藤大雄, 岩間一雄, 大隅剛史 (京都大学)

(概要) ウェブのコミュニティなどを表現する可能性がある, グラフの中の密な部分構造として, 孤立クリークという概念を導入し, (入力) 線形式時間で列挙するアルゴリズムを提案している.

4. グラフ分割問題 (最大尤度分割問題) の確率伝播法による線形時間解法, 渡辺治 (東京工業大学)

(概要) Belief propagation 法にもとづくグラフ分割問題の解法について論じ, planted solution model によって生成された多くの問題例に対して効率的に動作することを示している.

5. 複雑ネットワークにおける局所情報に基づく探索戦略, 来見田裕一, 緒方司, 小野廣隆, 定兼邦彦, 山下雅史 (九州大学)

(概要) スケールフリー性を持つ現実の大規模なグラフで, 目標頂点を効率的に発見し到達するために, 局所情報にもとづいたランダムウォークによる探索方法を提案している. またシミュレーションにより, その性能などを評価している.

いずれの講演も, 知見や示唆に富むたいへん興味深いものであった. また, 異分野研究者間の交流をはかるという目的も叶う集会となった. その一方で, 研究分野が未成熟で新しい研究成果が次々と生まれていることから, このようなトピックの研究集会を, 今後とも開催する必要があると感じた.

ミニ研究集会 (列挙合宿)

世話役： 中野 眞一 (群馬大学)，宇野 毅明 (国立情報学研究所)，
上原 隆平 (北陸先端科学技術大学院大学)

本研究集会は，最近の列挙アルゴリズム研究に関する情報交換と議論を行うセミナーである．列挙アルゴリズムは科学・産業のさまざまな場面で使われているが，その使用頻度の高さに比べ，アルゴリズム理論からの研究は立ち遅れている．本セミナーは，理論的な前進と現実問題への適用の両面から，列挙アルゴリズム，および列挙に関連する組合せアルゴリズムに関する議論を行い，列挙アルゴリズムの研究を推し進めるものである．

日程: 2005 年 9 月 27 日〜9 月 29 日
場所: 群馬大学伊香保研修所
参加者:

中野 眞一 (群馬大)	上原 隆平 (JAIST)
山崎 浩一 (群馬大)	大舘 陽太 (群馬大)
山中 克久 (群馬大)	岡本 吉央 (豊橋技科大)
清見 礼 (情報研)	松井 泰子 (東海大)
谷 聖一 (日大)	菊地 洋右 (ERATO)
田中 勇樹 (群馬大)	来嶋 秀治 (東大)
元木 光雄 (JAIST)	日吉 久礎 (群馬大)
高埜 博典 (群馬大)	河合 博之 (群馬大)
有村 博紀 (北大)	荒木 徹 (岩手大)
下園 眞一 (九工大)	宇野 裕之 (大阪府立大)
斎藤 寿樹 (JAIST)	

当日は，以下のような発表と議論が行われた．

清見: Enumerating Labeled Chordal Graphs in an Interval Graph
来嶋: Sampling Chordal Graphs
山中: 整数分割の列挙
岡本: ランダム 2 分探索木の高さの期待値
宇野: An Experimental Study on the Web Graph
菊地: A Quantum Protocol to win the Graph Colouring Game on All Hadamard Graphs
有村: 閉集合パターンと極大 2 部クリーク
田中: 即席クラスタ構築法
高埜: 4 連結極大平面グラフの列挙
元木: Test Instance Generation
岡本: Chan's New Algorithm for the All-Pairs Shortest Paths Problem
上原: The Number of Maximum Independent Sets in Biconvex Graph への誘い
菊地: Discrepancy について

清見 (情報研) の発表では，部分インターバルグラフを列挙するアルゴリズムについて解説があった．現在の手法は一般的であり，他のグラフクラスにも適用可能であるが，インターバルグラフの性質を利用し切れておらず，計算量に課題が残っている．

宇野 (大阪府立大) の発表では，Web グラフの様々な構造の列挙に関する大規模な実験の結果の報告をした．クリークや 2 部クリーク以外の，意味のある自然な構造の候補として，サイクルを構成する点集合 (辺の構造は無視) を提唱した．

有村 (北大) の発表では，理論的な裏付けのあるデータマイニング，特に頻出パタン列挙に関する手法の解説をした．現在は列挙アルゴリズムを主に使用しているが，これに対して一様ランダム生成を利用した手法を考えてみるのも面白そうであった．

全体を通して，非常に活発に議論が行われ，各人の研究結果や問題に関して，より新しいモデルや問題，お互いの疑問点に対する情報やアイディアの提供，といった研究者間のコミュニケーションにおいて重要なことがらが多く行われた．このセミナーは参加者の研究を進める大きな力となるであろう．

ミニ研究集会 (Complexity)

世話役： 垂井 淳 (電気通信大学)

計算量の理論という分野を広く捉え、未解決問題や現在解こうとしている問題の議論も積極的に行おうと呼び掛けて研究集会を開いた。博士後期課程学生３名（来嶋・山本・森住）によるものを含む９つの発表があり、約２０名の参加者はインフォーマルな雰囲気の中で自由に質問、議論することができた。発表された複数の問題についてこの集会をきっかけとして共同研究が続いており、ひとつの問題についてはその後ある解決に成功している。

日時：10 月 11 日（火） 9：30 – 17：30
場所:東工大大岡山キャンパス西８号館８０９号室
発表 ：

1. 索引を用いた文字列検索の計算量と未解決問題：定兼邦彦（九大）

文字列中のパタンの検索を高速化するために、あらかじめ索引を付加する手法がとられているが、索引のサイズと検索時間の間にはトレードオフが存在する。本発表では既存の索引について解説し、検索時間の下限に対する予想を立てる。

2. オラクル同定問題に対する量子質問計算量の幾何的な特徴付け：河内 亮周（東工大）

オラクル同定問題とは与えられたブラックボックス関数（オラクル）に質問を行い，候補関数集合の中のどれがオラクルとして与えられているかを同定する問題である．本講演では候補関数集合の幾何的な特徴に着目して同定に必要な量子質問計算量について議論する．

3. 閉ジャクソンネットワークの正規化定数の近似計算法について：来嶋 秀治（東大）

閉ジャクソンネットワークの積形式解の正規化定数に対する近似計算法を提案する。提案するアルゴリズムはマルコフ連鎖モンテカルロ法で、FPRAS を与える。本発表では特にモンテカルロ法に焦点をあて、近似解の精度保証について議論する。

4. MAX2SAT の Average Case 時間計算量について：山本真基（東工大）

これまでに，MAXSAT および MAX-k-SAT に関する Average-Case 時間計算量の研究は,（筆者の知る限り）全くされていない.（SAT に関してはある.）本講演では，MAX2SAT 問題を考え，以下のような性質を持つ例題生成器 RGEN が生成する例題族 F(RGEN) に対して，Average-Case 時間計算量を議論する．1. RGEN が出力する例題と真理値割り当ての対のほとんど（任意のコンスタントの割合 1- ε ）が，例題とその最大充足解の対である．2. RGEN の生成する例題の大きさは小さい．つまり，2CNF 論理式の節の数が，変数の数の（ ε に関する）コンスタント倍である．3. RGEN が出力する全例題上の MAX2SAT 問題が NP-Hard である．F(RGEN) のほどんど（all but o(1)）が，Local Search タイプのアルゴリズムに弱いことの直感的説明をし，それを示すための方法について議論する．

5. 確率伝搬法とその発展形の可能性について：渡辺治（東工大）

統計力学の研究者により再発見され，非常に盛んに研究されている確率伝搬法について，それがどの程度まで有効（そう）なのか，他の局所探索法と比べて，どのように違うのか／同じなのか，を，たとえば SAT 問題（とその variation）に絞り，議論してみたい．

6. 否定数を $\log(n+1)$ に限定した回路計算量の下界について：森住 大樹（京大）

否定数を $\log(n+1)$ に限定した回路における n 入力 2 出力論理関数 (PARITY, ¬PARITY)（ただし，$n+1$ は 2 の累乗）の回路計算量の $5n-c$ の下界の証明について紹介し，そこからの発展の可能性に触れる．否定数を $\lceil \log(n+1) \rceil$ に限定し

た回路において $\omega(n\log(n))$ の下界を示すことができれば，一般の回路における同等の下界を示したことになることが知られており，否定数をその数に限定した回路の回路計算量を調べることは特別な意味を持つ.

7. 単調 DNF 式の幾つかの性質について：天野一幸（東北大）

DNF 式の充足割り当ての個数を数え上げる問題に関係する (可能性のある)，充足割り当ての個数を最小化/最大化する式の構造に関連する問題について議論したいと思います.

8. NP neq coNP を証明するには？垂井淳（電通大）

NP neq coNP であるという前提のもとに、このことの証明がどのような方法では無理そうかということを考えたい。3SAT フォーミュラ F について、それが充足不可能であって、かつ、（普通の数学を展開する公理系としての）ZF での充足不可能性の最短証明が長いことを Long(F) と表すことにする。NP neq coNP であれば Long な F が存在する。（1）ある explicit な F に対して Long(F) であることを、（我々にとって自然である）コンスタントまたは短いサイズの証明で示すことはできない。そのような証明がないことが Long(F) の主張だから。（2）２つの explicit なフォーミュラ F1,F2 に対して「Long(F1)orLong(F2)」のコンパクトな証明がないことも簡単にわかり、少し注意して拡張すれば p=poly(n) 個に対しても同様に「Long(F1)or...orLong(Fp)」のコンパクトな証明がないことがわかる。（3）フォーミュラのうまい確率的生成を定義し、生成されるフォーミュラが確率 1/poly(n) で Long になるという証明法に対しても、complexity-theoretic assumption のもとでの derandomization により、もしそんな証明ができれば多項式個の F1,...,Fp に対して Long(F1)or...orLong(Fp) であることが証明できてしまうことになり矛盾するのでそんなことはできそうにない、という議論を考えたい。以上において充足不可能な 3SAT フォーミュラの代わりに、たとえば、「root(n) のクリークを持たない n 頂点グラフ」を用いても全く同じ議論となる。

9. k-wise almost independent permutations 垂井淳（電通大）

N 置換の集合 P は次の性質を持つとき k-wise (almost) independent であるという：任意の k 点 $x_1,\ldots,x_k$ に関して π を P から一様ランダムに選んだときの $\pi(x_1),\ldots,\pi(x_k)$ の分布が完全にランダムな置換のもとでの分布と一致する・ほとんど一致する。このような P を k が大きいときも Feistel 変換の composition による構成で生成することができることを示す。Reingold によるブレークスルー：USTCONN in LogSpace[STOC05] の Reingold-Trevisan-Vadhan[ECCC05] による拡張が以上の問題に応用できるという Kaplan-Naor-Reingold[RANDOM05] の指摘、すなわち、もとのグラフの expansion factor を維持した zig-zag product による pseudorandom walk の方法の応用についても簡単に説明し、また、以上の問題に関連する未解決問題のリストを提示する。

ミニ研究集会 (暗号理論)

世話役： 櫻井 幸一 (九州大学)，田中 圭介 (東京工業大学)

総括班の櫻井の呼びかけをきっかけに，本特定領域研究における暗号理論の研究者：

太田 和夫 (電気通信大学)
國廣 昇 (電気通信大学)
櫻井 幸一 (九州大学)
高木 剛 (はこだて未来大学)
田中 圭介 (東京工業大学)

とそれぞれの研究グループの研究者を中心にミニ研究集会を開催した．はこだて未来大学の高木が会場世話人となり，田中がプログラムのとりまとめをした．

当日の参加者は講演者を含めて約 20 名だった．講演は下記の概要の通りであるが，1, 3 番目の講演は，各自の研究成果に関する内容が中心であり，2, 4, 5 番目の講演は，研究分野のサーベイに関する内容が中心であった．

参加者が少ないこともことも手伝って自由に質問できる雰囲気があった．実際，発表の最中にも質問がでるなど活発な質疑や討論が行われ，それぞれの専門分野に関する理解を深めることができた．ただ，本研究集会は，参加者の都合により，半日で開催することになったが，そのため，発表および質疑応答の時間が十分だとはいえなかった．

研究集会後に開いた懇親会では，通常の学会主催の研究会では得られない貴重な集まりだったという意見が多く，次年度以降も継続してこのような暗号理論の研究集会を開催したいという意見も多かった．

次年度以降も，継続して，このような暗号理論の研究集会を企画し，班を越えた相互の研究討論を通じて，最新の情報交換，共同研究を促進していく計画である．

日時　2006 年 2 月 16 日 (木) 13:00-17:30

場所　はこだて未来大学 小講義室 585 （〒 041-8655 北海道函館市亀田中野町 116 番地 2）

プログラム

1. 13:00-13:30
   Privacy-preserving Text Mining in Distributed Environment
   ○ Chunhua Su, Kouichi Sakurai (九州大学)

2. 13:30-14:00
   Pairing Implementation using Hyperelliptic Curves
   Colm O hEigeartaigh (Dublin City University)

3. 14:15-15:00
   A Survey about Side Channel Attacks on XTR
   ○ Dong-Guk Han, Tsuyoshi Takagi (はこだて未来大学)

4. 15:00-15:45
   オフライン検証性を満たす追跡不可能な量子現金
   國廣 昇 (電気通信大学)

5. 16:00-16:45
   離散対数問題系に基づく安全で効率的な署名方式
   太田 和夫 (電気通信大学)

6. 16:45-17:30
   匿名性をもつ公開鍵暗号
   ○林 良太郎, 田中 圭介 (東京工業大学)

各発表の概要

1. Privacy-preserving Text Mining in Distributed Environment
   ○ Chunhua Su, Kouichi Sakurai (九州大学)
   概要：プライバシーを考慮したデータマイニングに対する研究のサーベイと今回，テキストデータをとくに扱ったものに関する著者の提案法方式の紹介．キーワードを用いた質疑プロトコルを利用する際に，紛失通信という暗号技術を利用している．

2. Pairing Implementation using Hyperelliptic Curves
   Colm O hEigeartaigh (Dublin City University)
   概要：ID ベース暗号の実現で注目されている楕円曲線ペアリングを，超楕円曲線の場合に適用した場合のサーベイと著者による最新の実装データを報告した．標数が 2,3 の Duursma-Lee 法を改良した η ペアリングは，現在のところ最も高速にペアリング暗号を実装するアルゴリズムである．1024 ビットのセキュリティを持つ埋込み次数 12 の超特異な超楕円曲線を用いて，Pentium 4 + SSE2 において 1.8ms を達成した．

3. A Survey about Side Channel Attacks on XTR
   ○ Dong-Guk Han, Tsuyoshi Takagi (はこだて未来大学)
   概要：拡大次数 6 の有限体上の離散対数問題を利用した XTR という公開鍵暗号系に対する実装攻撃のサーベイ．発表者 (昨年度は九大で博士課程在籍，今年度は未来大でポスドク) を中心とするここ数年の解読法と防御法に関する研究を紹介した．著者等が提案したユークリッド互助法を応用した防御法は，固定パターン持つ耐 SPA 性クラスの中で最速な方式である．この領域は，未だに「攻撃→防御→攻撃」の繰り返しで研究が進行しているのが現状である．

4. オフライン検証性を満たす追跡不可能な量子現金
   國廣 昇 (電気通信大学)
   概要：これまでに提案されている量子現金方式は，オフライン検証性または追跡不可能性のどちらか一方を満たす方式であったが，今回はこの 2 つの性質を同時に満足する量子現金の提案を行った．さらに，提案した量子現金を，古典の電子現金の世界だけで見てみた場合の対応付けを考察し，量子現金方式の安全性評価への方向付けを示した．

5. 離散対数問題系に基づく安全で効率的な署名方式
   太田 和夫 (電気通信大学)
   概要：Schnorr 署名にはじまり，CRYPTO 2005 で発表された最新の Chevallier 署名にいたる離散対数問題系に基づく電子署名の安全性と効率に関するサーベイ．安全性の根拠として，離散対数問題，計算 Deffie-Hellmann 問題，判定 Deffie-Hellmann 問題の困難性を仮定した場合の，署名生成の実現手段，困難な問題を署名偽造に帰着するための帰着効率，計算効率などを比較している．困難な問題の制約を強めると，帰着効率や計算効率が向上していることが，具体例によって確認できた．

6. 匿名性をもつ公開鍵暗号
   ○林 良太郎, 田中 圭介 (東京工業大学)
   概要：暗号文を見ても，それが誰の公開鍵で暗号化されたのかがわからない，という暗号文の受信者の匿名性に関する研究．2001 年ごろ概念が提起・定式化され匿名通信路の実現・電子入札などへの応用をもつ．著者らの開発した技術を含む，4 つの実現テクニックを，RSA 暗号とエルガマル暗号の場合に分けて，比較考察している．今後の課題としては，ランダムオラクルモデルに依存しない標準モデルの場合の考察・匿名性を満たす ID ベース方式の実現などがある．

ミニ研究集会 (ジオメトリ)

世話役： 浅野 哲夫 (北陸先端科学技術大学院大学),
徳山 豪 (東北大学), 加藤 直樹 (京都大学)

計算幾何学は問題が理解しやすい，応用範囲が広い，などの理由からアルゴリズムの教科書でも題材としてよく取り上げられている．多次元の情報検索，地理情報処理などの技術基盤として幅広い応用価値があり，理論的にも多くの興味深い問題がある．にも関わらず，計算幾何学を系統的に教えている大学，大学院は数少ない．そこで，大学院生や若手研究者を対象に計算幾何学の基礎を系統的に講義することを目的とするミニスクールを開催することとなった．講義だけでは物足りない方たちもいるだろうと考えて，未解決問題，現在取り組んでいる問題についても少しだけお話をした．

本年度は3月15日午後から3月17日昼まで京都市右京区「コミュニテイ嵯峨野」において計算幾何学に関するミニスクールを実施した．大学院生や若手研究者を主たる対象として参加者は，講師（浅野哲夫，徳山豪，David Avis，岡本吉央，加藤直樹）も含め33名で，東北大学，東京大学，名古屋大学，北陸先端大，京都大学の学生が参加した．また，研究者で参加された先生方は，永持仁（京都大学），宇野 裕之（大阪府立大学），大西健輔（東海大学），小野孝男（名古屋大学），河村泰之（石川高専）の5名であった．

講義内容は，計算幾何学の基礎概念として，凸包，三角形分割，ボロノイ図，領域探索，パラメトリック探索法，組合せ幾何を中心に講義がおこなわれた．またいくつかの未解決問題についての紹介もおこなわれた．ナイトセッションにおいては講義中に出された問題を解いてもらい，学生の理解を深めることができた．嵐山という観光地であるにも関わらず夜遅くまで熱心な討論ができ，学生交流も図ることができた．

詳細なスケジュールは以下の通りであった．

3月15日
1時00分–1時15分　開会の挨拶と趣旨説明（加藤）
1時30分–2時30分　計算幾何学とは（徳山, 加藤）
2時45分–3時45分　Range Search I（徳山）
4時00分–5時00分　Voronoi図とDelaunay Triangulation（加藤）
ナイトセッション（Open Problem ＋ solution ＋ Q&A）

3月16日
9時00分–10時00分　Advanced Topic 1： Reverse Search（Avis）
10時15分–11時15分　パラメトリック探索（浅野）
11時30分–12時30分　Range Search I ＋ 組み合わせ幾何入門（徳山）
昼食
散策
3時00分–4時00分　幾何学最適化　（加藤）
4時15分–5時15分　組み合わせ幾何 (岡本)
懇親会
ナイトセッション（Open Problem ＋ solution ＋ Q&A）

3月17日
9時00分–10時00分　Angular Voronoi Diagram（浅野）
10時15分–11時15分　Advanced topic（加藤, Avis）
11時15分–12時00分　Solution Session

なお講義資料は以下からダウンロードできる．

`http://www.archi.kyoto-u.ac.jp/~kato-lab/data/geo_min_proj.zip`

電子情報通信学会 COMP-NHC 学生シンポジウム

世話役： 山下 雅史 (九州大学)，田中 圭介 (東京工業大学)，
定兼 邦彦 (九州大学)

平成１８年3月２４日～２７日にかけて国士館大学において，２００６年度電子情報通信学会総合大会が開催された．その情報・システムソサエティ企画として，コンピュテーション研究会と共同で，２６日にCOMP-NHC 学生シンポジウムを開催したので報告する．

シンポジウムの目的は以下の通りである．計算機科学分野では，画期的な研究の多くが若手の研究者によって遂行されており，本領域研究においても，学生を含む若手の研究者が研究を牽引していることは周知である．そこで，計算機科学分野で活躍する学生諸君のためのシンポジウムを企画し，特に優秀な発表を行った学生に優秀発表賞を贈ることにした．

当日は9時に開始し，それぞれ25分の持ち時間で１６名の学生が講演を行い，１７時過ぎに発表を終了した．その後，受賞者を決める会議に移ったが，その間は東北大学の瀧本先生に御講演を頂いた．

参加者からの投票も受け付けて審査した結果，林良太郎君 (東京工業大学) “Generic Conversion for the Anonymity against the Adaptive Chosen Ciphertext Attach” を優秀発表賞に選出し，１７時４０分盛会の内にシンポジウムを終了した．割り当てられた部屋がほとんど埋まる程度の賑わいで十分に目的を達成できたと考えている．

なお，シンポジウム講演および特別講演は，以下の通りである．

[DS-1-1] “Robustness of Greedy Type Minimum Evolution Algorithms,” Takeya Shigezumi (Tokyo Inst. of Tech.)

[DS-1-2] “Packing Squares with Profits into a Rectangle,” Xin Han, Kazuo Iwama (Kyoto Univ.), Guochuan Zhang (Zhejian Univ.)

[DS-1-3] “閉ジャクソンネットワークに対するMCMC 法,” 来嶋秀治, 松井知己 (東大)

[DS-1-4] “スポーツのスケジューリングにおける会場割当問題,” 鈴鹿順美 (筑波大), 宮代隆平 (東京農工大), 吉瀬章子 (筑波大), 松井知己 (東大)

[DS-1-5] “辺の容量が一定のグラフにおける動的なネットワークフローを用いた避難問題に対する効率的なアルゴリズム,” 神山直之, 加藤直樹, 瀧澤重志 (京大)

[DS-1-6] “A Message Passing Algorithm for MAX2SAT,” Osamu Watanabe, Masaki Yamamoto (Tokyo Inst. of Tech.)

[DS-1-7] “クラスタに基づいた動的センサー網における高速なブロードキャストについて,” 稲葉直貴, 内田次郎, 片山喜章 (名工大), 陳慰 (テネシー州立大), 和田幸一 (名工大)

[DS-1-8] “クエリを高速にサポートする方形描画のコンパクトなコード化,” 山中克久, 中野眞一 (群馬大)

[DS-1-9] “大規模データ利用のための圧縮技術,” 岡野原大輔 (東大)

[DS-1-10] “DNA 構造変化の特徴解析,” 塩崎真史, 小野廣隆, 定兼邦彦, 山下雅史 (九大)

[DS-1-11] “Generic Conversion for the Anonymity against the Adaptive Chosen Ciphertext Attack,” Ryotaro Hayashi, Keisuke Tanaka (Tokyo Inst. of Tech.)

[DS-1-12] “No Preshared Key Quantum Secret Communication Protocol,” Yumiko Murakami, Masaki Nakanishi, Shigeru Yamashita, Katsumasa Watanabe (NAIST)

[DS-1-13] “超限ビット列のランダム性について,” 五十嵐寛晃 (中大)

[DS-1-14] “ランダム写像による非線形概念の学習の効率化に向けて,” 渡邊辰也, 瀧本英二, 天野一幸, 丸岡章 (東北大)

[DS-1-15] “指数的に長い手数の一般化詰将棋,” 八登崇之 (東大)

[DS-1-16] “弦グラフおよびその部分クラスの列挙,” 清見礼, 宇野毅明 (NII)

[特別講演] “我が国志向への転換,” 瀧本英二 (東北大)

第19回 回路とシステム軽井沢ワークショップ
講演企画

世話役： 巳波 弘佳 (関西学院大学)

本特定領域研究の活動の広報と他分野の研究者との交流を目的に，電子情報通信学会 回路とシステム軽井沢ワークショップに招待講演セッションを企画した．

本ワークショップは，回路とシステムに関連した分野の研究者や技術者が集い，招待論文や投稿論文，パネル討論を通じて，分野内だけでなく分野間にまたがる境界領域の課題解決と，将来の研究分野の探求を目的として開催されているものである．この分野の研究集会としては国内で最大規模であり，また今回で 19 回目となり，定評のあるワークショップである．大学の研究者のみならず，企業研究所からの参加も数多く，産学の交流も盛んである．

このワークショップは，回路とシステム関連分野としてアルゴリズム関係，グラフ理論関係の講演も行われているため，関心を持つ聴衆も多く，ここで今回のセッションを企画することは有効だと考えられる．

以下に，関連プログラムを挙げる．

第19回 回路とシステム軽井沢ワークショップ

【日程】 2006 年 4 月 24 日 (月), 25 日 (火)

【場所】 軽井沢プリンスホテル・西館・国際会議場

【URL】 http://www.ieice.or.jp/ess/kws/

本特定領域研究関連セッション

セッション D1-3 (4/24 13:30-14:30)
新世代の計算限界 (1)

- 「Extended Skip Graph for P2P File Exploration」藤田聡 (広島大)

セッション D1-4 (4/24 15:00-17:00)
新世代の計算限界 (2)

- 「An experimental study of web structure mining」宇野裕之 (阪府大)
- 「The weakest failure detectors for the stable leader election」小野廣隆 (九大)

2.　研究課題別活動報告

A01: オンライン予測の手法を用いた意思決定モデルに関する研究

瀧本 英二 † 酒井 義文 ‡ 天野 一幸 §

† 東北大学 大学院 情報科学研究科
〒 980-8579 仙台市青葉区荒巻字青葉 6-6-05
t2@ecei.tohoku.ac.jp

‡ 東北大学 大学院 農学研究科
〒 981-8555 仙台市青葉区堤通雨宮町 1-1
sakai@biochem.tohoku.ac.jp

§ 群馬大学 工学部 情報工学科
〒 376-8515 桐生市天神町 1-5-1
amano@cs.gunma-u.ac.jp

1 はじめに

本研究では，意思決定とデータの提示が交互に繰り返されるオンラインでの意思決定過程に関する問題を統一して扱うことのできる普遍的なモデルの構築，および，様々な評価基準のもとで理論的に保証された性能を持つ意思決定手法の設計と解析手法の確立を目指し，次に述べる３つのアプローチを試みている．

１つめは，計算学習理論の分野で開発された様々な手法を手がかりにしようとするもので，この観点から，今年度は以下の４つの成果を得た（２章）．(1) 昨年度，従来の動的資源分配モデルを拡張し，投資の対象となるオプションの損失の範囲（リスク）がオプションごとに異なり，その情報が開示されているとするモデルを提案し，そのモデルのもとでオンライン予測の手法に基づく最適なアルゴリズムを与えた．ここで，各オプションのリスクは固定されており，時間とともに変動しないという強い仮定をおいていたが，今年度は，その仮定を大幅に緩めることに成功した．また，リスク情報を用いないアルゴリズムとの性能の差は，リスクが一様のときに最大になることを示唆する結果を得た．これは，リスク情報が本質的に役に立たないかも知れないことを意味しており，投資戦略に対し，新たな知見を与えるものである．(2) オンラインオークションと呼ばれる商品売買のモデルが，リスク情報つきの動的資源分配モデルに還元できることを示し，妥当な問題設定の下で，従来手法より優れた利得下界を持つアルゴリズムを与えた．(3) 各ノードに否定のない単項式がラベルづけされた単調項決定リストと，複数の単調 DNF 式を排他的論理和で結んだ XOR-MDNF 式が等価となる条件を与え，その結果から，単調項決定リストに対する質問による学習アルゴリズムを導いた．(4) 非線形な幾何概念に対する学習の枠組みとして，ランダム写像に基づく新しい手法を提案した．提案する写像関数は，従来手法よりも対数的に短い長さのランダムシードを用いるもので，インスタンスを特徴ベクトル空間へ写す非線形写像と合成することにより，サポートベクトルマシンと同等の汎化性能を持つ仮説を得ることができる．ここで，この合成関数が，それぞれの写像関数を陽に計算することなく効率よく計算できれば，計算効率の点でサポートベクトルマシンを凌ぐ新しい学習方式が得られることになる．

２つめは，さまざまな分野の問題で，社会的・学術的に求められている品質保証を明らかにし，本研究に還元しようとするものである．この観点から，今年度は以下の２つの成果を得た（３章）．(1) 与えられた３つの系列 X，Y，P に対し，P を部分列として含む X と Y の最長共通部分列を求める問題を一般化し，P の少なくとも長さ r の部分列を含む最長共通部分列を求める問題を提案し，この問題に対する効率の良いアルゴリズムを与えた．これは，特定の機能を持つタンパク質のアミノ酸配列を P としたとき，その機能に関連する２つのアミノ酸配列 X と Y の共通構造を発見する手法として用いることができる．(2) ウェブ検索におけるスコアリング法として，更新の新鮮さを考慮し，検索に用いた単語が最近に現れた

ページを重視するランク関数を提案し，その有効性を実データにより確かめた．

３つめは，意思決定アルゴリズムが保持すべき表現の複雑さに注目し，アルゴリズムの計算量的な限界について考察しようとするものである．この観点から，今年度は論理関数の複雑さに注目し，主に以下の４つの成果を得た（４章）．(1) 任意の二次関数を計算するサイズ最小の単調論理回路は，論理積素子を単層として含むという単層予想と呼ばれる未解決問題を，否定的に解決する重要な手がかりを与えた．(2) 否定素子数を限定した論理回路，２層しきい値回路，および論理式のサイズの下界を導出する新しい手法をそれぞれ与えた．(3) 乗算を計算するほぼ最適な OBDD の設計を行った．(4) ある制約を満たす単調積和形論理式のうち，充足割り当ての個数を最小，あるいは最大にするものを特定することに成功した．

2　計算学習理論からのアプローチ

2.1　リスク情報つき動的資源配分問題

資源配分問題は，オンライン予測の最も適用範囲の広いモデルの１つであり，次のように定式化される．投資の対象（オプション）が K 個あるとし，投資の方法についてアドバイスを行う「エキスパート」が N 人いると仮定する．各時刻 $t = 1, 2, \ldots$ において，各エキスパート i は，投資ベクトル $x_{i,t} = (x_{i,t}(1), \ldots, x_{i,t}(K))$ を提示する．投資ベクトルは，資源をオプション集合にどのように配分するかを表すもので，確率ベクトルでなければならない．これらを受け，投資アルゴリズム（学習者）は，自分の投資ベクトル $p_t = (p_t(1), \ldots, p_t(K))$ を定める．その後，各オプション j のコスト $l_t(j) \geq 0$ が明らかとなる．このとき，学習者は，投資ベクトルとコストベクトルの内積 $p_t \cdot l_t = \sum_{j=1}^{K} p_t(j) l_t(j)$ の損失を被る．同様に，各エキスパート i も損失 $x_{i,t} \cdot l_t$ を被る．学習者の目標は，このプロセスをある時刻 T まで行った後の累積損失 $\sum_{t=1}^{T} p_t \cdot l_t$ を，最適なエキスパートの累積損失 $\min_i \sum_{t=1}^{T} x_{i,t} \cdot l_t$ に比べてそれほど大きくならないようにすることである．従来は，オプションのコスト $l_t(j)$ の上界（リスク）が定数に限定されているモデルしか扱われていなかったが，昨年度は，リスクがオプションごとに異なり，その値 $b_{t,j}$ が開示されているとするモデル（リスク情報つき動的資源配分問題）を提案し，そのモデルの下で，最適性が保証されている Vovk の統合戦略に基づくアルゴリズムを与えた．ただし，この結果は，リスクベクトル $(b_{t,1}, \ldots, b_{t,K})$ が時刻 t によらず一定という条件を必要としていた．今年度はこの条件を大幅に緩め，リスク集合 $\{b_{t,1}, \ldots, b_{t,K}\}$ が多重集合として時刻によらず一定でさえあれば，同様の結果が成立することを示した．また，従来手法の１つであるヘッジアルゴリズムの与える投資ベクトルは，リスク情報をまったく用いないにもかかわらず，我々の与えた投資ベクトルの近似になっており，しかも，リスクのばらつきが大きくなるほどその近似度が良くなることを示した．これは，ヘッジアルゴリズムが，我々のモデルのもとで，より精密な損失上界を持つことを意味しているだけでなく，リスク情報が投資行動において本質的に役に立たないかもしれないことを意味している．

2.2　オンラインオークション

Bar-Yossef らが提案したオンラインオークションモデルは，１種類の商品を次々と来訪する入札者に売るための価格の決定過程をモデル化したものである [1]．このモデルでは，各入札者 $t = 1, 2, \ldots$ について，次のような取引が行なわれる．売り手が商品の価格 r_t を提示した後，入札者の入札金額 $m_t \in [1, h]$ が明かされる．ここでは簡単のため，入札金額の最低額を 1 に規格化し，入札金額の最高額を h と仮定する．このとき，$r_t \leq m_t$ ならば売り手は商品を売り利得 $g_t = r_t$ を得るが，$r_t < m_t$ ならば利得を得られない $(g_t = 0)$．目標は，時刻 T までの累積利得 $G_T = \sum_{t=1}^{T} g_t$ を，最適な価格 $r*$ で売り続けたときの売り上げ OPT に匹敵させることである．

この問題は次のように（利得型の）リスク情報つき動的資源配分問題へと還元される．まず，$[1, h]$ を離散化し，N 個の価格候補 $b(1) > b(2) > \cdots > b(N)$ を定め，これらをオプションと考える．また，各オプション（価格）$b(i)$ に対し，そのオプションにのみ全資源を投資するエキスパートを導入する．すなわち，エキスパート i（$1 \leq i \leq N$）

の与える投資ベクトル $x_{i,t}$ は，常に，第 i 成分が 1 の単位ベクトルであるとする．これらの投資ベクトルを受け，学習者が時刻 t の投資ベクトル p_t を定めたとき，これをオプション集合上の確率分布とみなし，その分布に従って価格 r_t を選ぶ．すなわち，確率 $p_t(i)$ で $r_t = b(i)$ とする．そして，入札者 t の入札額 m_t が提示されると，各オプション i に対し，$b(i) \leq m_t$ ならば $l_t(i) = b(i)$，そうでないならば $l_t(i) = 0$ とおくことにより，コスト（利得）ベクトル l_t を定める．ここで，オプション i のリスク（利得の上界）が $b(i)$ となることに注意されたい．この変換のもとで，時刻 t の利得 g_t の期待値は，投資ベクトルとコストベクトルの内積 $p_t \cdot l_t$ で与えられ，エキスパート i（価格 $b(i)$）の利得も内積 $x_{i,t} \cdot l_t$ で与えられる．従って，価格候補集合を $\{b(1), \ldots, b(N)\}$ に限定したオンラインオークション問題は，この集合をオプション集合とするリスク情報つき動的資源分配問題とみなすことができ，前節で与えた投資アルゴリズムを適用することにより，価格候補集合の中で最適な価格 $b(i^*)$ で売り続けたときの累積利得 G_T^* に匹敵する累積利得を得ることができる．さらに，N を大きくして離散化レベルを十分細かくすることにより，真の最適価格 r^* による利得 OPT と $G_{i^*,T}$ の比を十分小さく抑えることができる．

このとき用いる動的資源配分問題の解析手法は，コストベクトル l_t が直積集合 $\{0, b(1)\} \times \cdots \times \{0, b(N)\}$ の任意の要素を取りうるとして最悪の場合の利得下界を求めるものである．しかし，オークションモデルは，入札金額 m_t 以下の価格を提示すれば必ずその価格で売れるという単調性を持つため，還元によって得られた動的資源配分問題においては，コストベクトル l_t は $\{(0, \ldots, 0, b(i-1), b(i), \ldots, b(N)) \mid 1 \leq i \leq N\}$ の N 通りしか取り得ない．本研究ではこのコストベクトル空間を用いて Vovk の統合戦略を厳密に適用することによって，アルゴリズムのさらなる改良を行い，次に示す期待利得の下界を得た．

便宜的に $b(0) = \infty$ とおき，確率ベクトル r と s を，それぞれ

$$r(j) = \left(\frac{1}{b(j)} - \frac{1}{b(j-1)}\right) b(N),$$
$$s(j) = \left(\frac{1}{\alpha^{b(j)} - 1} - \frac{1}{\alpha^{b(j-1)} - 1}\right) (\alpha^{b(N)} - 1)$$

とおく．ここで，$\alpha > 1$ は適当な定数である．このとき，

$$E[G_T] \geq \frac{b(N) \ln \alpha}{D(r||s) + b(N) \ln \alpha} \left(G_{i^*} - \frac{\ln N}{\ln \alpha}\right).$$

ここに，$D(r||s)$ は，KL ダイバージェンスである．

価格候補集合を適当に定めると，この下界は，$h \leq 10^{100}$ 程度以下ならば，従来手法の下界よりも大きくなることを数値計算により確かめた．これは，現実的な問題設定のもとでの本手法の優位性を示すものである．

2.3 単調項決定リストの学習

決定リストは，ブール関数の最も基本的な表現の 1 つであり，

$$f = ((f_1, a_1), \ldots, (f_d, a_d), (\mathrm{TRUE}, a_{d+1}))$$

のように表される．ここで，各 f_i は積和型論理式（DNF 式），a_i は 0 または 1 であり，一般性を失わず，$a_i \neq a_{i+1}$ とする．d を f の交代数と呼ぶ．決定リスト f は，ベクトル $v \in \{0,1\}^n$ に対し，v が満たす最初の DNF 式が f_i のとき，a_i を値として取る．これまで，決定リストのさまざまな部分クラスの学習可能性が示されているが，本研究では，各項に否定リテラルを含まない単調項決定リストの学習可能性について考えた．単調項決定リストは，任意のブール関数を表現することができるため，決定リストの部分クラスとして，その学習可能性は特に重要である．

我々は，単調項決定リストのクラスと単調 DNF の排他的論理和式（⊕MDNF 式）との密接な関係に着目した．⊕MDNF 式は，ブール関数の単調関数への分解方法の 1 つとして提案されたもので，$f_1 > \cdots > f_d$ なる d (≥ 1) 個の単調 DNF 式を用いて，$f = f_1 \oplus \cdots \oplus f_d$ で表される．ただし，同じ項が式の中に 2 度以上現れることはないとする．ここで，d を式の深さと呼ぶ．⊕MDNF 式のクラスは，学習対象 f の積閉包複雑度と呼ばれる組み合わせ量に比例する時間で，所属質問と等価性質問を用いて学習可能であることが知られている [2]．f の積閉包複雑度 $\mathrm{cl}(f)$ とは，f を構成する各単調 DNF 式 f_i から高々 1 つずつ項を選び，それらを論理積で結ぶことにより得られる項全体から

なる集合の要素数である．我々は，単調項決定リストに対する積閉包複雑度の概念を同様に定義し，任意の⊕MNDF 式 f から，f と等価で積閉包複雑度が等しい単調項決定リスト f' が直ちに得られること，および，交代数が d の任意の単調項決定リスト f' に対し，f' と等価で $cl(f) \leq (cl(f')/d)^d$ を満たす⊕MDNF 式 f が存在することを示した．さらに，これらの結果より，$O(\log n)$ 項単調項決定リストのクラス，および，交代数が定数の単調項決定リストのクラスが，所属質問と等価性質問を用いて多項式時間学習可能であることを導いた．

2.4 ランダムプロジェクションによる非線形概念の学習

ユークリッド空間中のベクトルとそれが正か負かを示すラベルの対の集合がサンプル $S = \{(x_1, y_1), \ldots, (x_m, y_m)\} \subseteq R^n \times \{-1, +1\}$ が与えられており，正と負のベクトルを分離する仮説超曲面を求める問題について考える．いま，ある非線形写像 $\phi : R^n \to R^N$ が存在して，S の像 $\phi(S) = \{(\phi(x_i), y_i)\}$ が原点を通る超平面によって線形分離可能であると仮定する．ここで，各ベクトルの像 $z_i = \phi(x_i)$ を特徴ベクトル，R^N を特徴空間と呼ぶ．この仮定より，以降では，特徴空間において $\phi(S)$ を分離する超平面を求める問題について考える．

サンプルを分離する超平面 $h \in R^N$ に対し，その超平面から一番近い特徴ベクトルまでのユークリッド距離を h のマージンと呼ぶ．マージン理論より，マージンが大きいほど汎化誤差の上界が小さくなる．サポートベクトルマシン（SVM）は，特徴空間において，マージンが最大の分離超平面 h^* の双対表現を求める手法であり，その汎化誤差は，$\tilde{O}(1/(m\ell^2))$ となることが知られている．ここで，ℓ は h^* のマージンである．しかし，SVM では 2 次計画問題として知られる最適化問題を解く必要があり，その計算量を減らすことが，SVM の学習における中心的な課題のひとつとなっている．一方，2 次計画法の計算過程において，特徴ベクトルは内積（$K(x_i, x_j) = \phi(x_i)^{\mathsf{T}}\phi(x_j)$）の形でしか現れないため，カーネル関数 K が効率よく計算可能であれば，計算時間は特徴空間の次元数 N に依存しない．

本研究では，ランダム写像と呼ばれる技術を用いて，特徴空間（R^N）中のサンプルを低次元空間（R^d）に写像し，その低次元空間中で分離超平面を直接求める新しい学習方式について検討している．これまで知られているランダム写像は，各成分が独立なランダム $N \times d$ 行列に基づくもので，ユークリッド距離を高い確率で保存するという性質（Johnson-Lindenstrauss の補題）を持つ．この性質から，次元数を $d = O(1/\ell^2)$ とすると，サンプルの線形分離性（マージン）も高い確率で保存されることを導くことができる．VC 理論より，d 次元空間中でサンプルを線形分離する超平面の汎化誤差は $\tilde{O}(d/m) = \tilde{O}(1/(m\ell^2))$ なので，線形計画法によってそのような超平面を 1 つ求めることにより，SVM と同等の汎化能力を持つ仮説が，2 次計画問題を解くことなく効率よく得られることになる．しかし，従来のランダム写像を用いた場合，サンプルを d 次元空間に変換するのに N に依存する時間がかかってしまう．

本研究では，ランダム写像を与える行列 R を，n の多項式程度のビット数のランダムシード r を用いて構成する（$R = \psi(r)$）という学習の枠組みを提案する．この枠組みで効率のよい学習アルゴリズムを設計するためには，次の 2 つの条件が必要十分である．

条件 1 ランダム性の弱いランダム行列 $R = \psi(r)$ を用いて，サンプルのマージンを保存する性質を持つ低次元空間へのランダム写像を構築すること．

条件 2 各ベクトル x_i に対し，$\phi(x_i)$ と $\psi(r)$ を陽に計算することなく，x_i の像 $z'_i = K'(x_i, r) = R^{\mathsf{T}} z_i = \psi(r)^{\mathsf{T}}\phi(x_i)$（SVM におけるカーネル関数に相当）が効率よく計算できること．

今年度は，条件 1 を満たす 2 種類の新しいランダム写像の手法を与えることに成功した．以下に，そのうちの 1 つの構成法を述べる．

$\{-1, +1\}$ 上の k (≥ 4) 限定独立なランダム $N \times P$ 行列を Q 個 $R_1, \ldots, R_Q$ 選び，各 $1 \leq q \leq Q$ に対し，R^N から R^P への写像 $f_q(x) = R_q^{\mathsf{T}} x / \|R_q^{\mathsf{T}} x\|$ を定義する．ここに，各行列 R_q は k 限定独立であるが，$R_1, \ldots, R_Q$ は互いに独立となるように選ぶ．本研究で与えるランダム写像は，ベクトル $x \in R^N$ を，Q 個の P 次元ベクトル $f_1(x)$，$\ldots$，

$f_Q(x)$ を連結した $d = PQ$ 次元ベクトルへと写すものである．このとき，P と Q と適当に選ぶことにより，

$$d = \tilde{O}(1/\ell^{3+4/k})$$

で，このランダム写像は高い確率で線形分離性を保存する．また，このとき用いるランダムシードのビット数は，$\tilde{O}((\log N)/\ell)$ 程度であり，特徴空間の次元数 N が n の指数程度に大きい場合でも，ランダムシードの大きさは n の多項式で抑えられる．

3 社会的・学術的に要請される品質保証に基づくアプローチ

3.1 弱制約最長共通部分配列問題

複数個の配列（sequence）の間の共通の部分配列（subsequence）の中で長さが最大のものを求める最長共通部分配列問題は，配列の間に存在する類似性や共通構造を見出す問題として，計算機科学や分子生物学など様々な分野での応用が考えられる．この問題に関する研究の一環として，最近，任意に指定された配列 P が部分列として含まれるという条件のもとで，配列 X，Y の最長の共通部分配列を求める制約最長共通部分配列問題が Tsai[4] によって提案され，この問題を解く $O(|X| \cdot |Y| \cdot |P|)$ 時間アルゴリズムが Chin ら [3] によって与えられた．

制約最長共通部分配列問題は，例えば，分子生物学において，アミノ酸配列 X，Y に部分配列として共通に含まれる配列 P が両者から得られるタンパク質に共通する特定の機能に関与していることが解っているときに，この前提のもとで更なる共通構造を見出すことに利用できるものと期待できる．ただし，制約として指定される P が冗長な配列であり，実際には P に含まれるより短い部分配列がタンパク質の機能に関与しているような場合には，制約が強すぎることにより短い共通配列しか得られず、有用な共通構造が見落とされる可能性がある．そこで，制約最長共通部分配列問題を更に一般化して，制約である配列 P の他に，パラメタ $0 \leq r \leq |P|$ を与えて，P の少なくとも長さ r の部分列を部分列として含む X と Y の最長の共通部分配列を求める状況を想定し，これを効率よく解くための手法について考えた．以降では，この問題を，弱制約最長共通部分配列問題ということにする．$r = 0$ のときの弱制約最長共通部分配列問題は，従来の最長共通分配列問題に等しく，$r = |P|$ のときの弱制約最長共通部分配列問題は，制約最長共通分配列問題に等しい．

弱制約最長共通部分配列問題を解く一つの方法は，P の長さ r の部分配列それぞれに対して，これを制約配列としたときの制約最長共通部分配列問題を $O(|X| \cdot |Y| \cdot r)$ 時間で解き，得られた配列の中で最も長いものを選ぶことである．ただし，この方法では，$\binom{|P|}{r}$ 個存在する P の長さ r の部分配列の中から制約最長共通部分配列が最長となるものをしらみつぶしに探さなければならないため，実行時間に関して非常に効率が悪い．そこで，X，Y，P の各長さの接頭辞に対する 3 次元の表を用いる動的計画法に基づく Chin ら [3] の制約最長共通部分配列問題に対するアルゴリズムを，更に P の部分配列の長さ $0 \leq q \leq r$ に関する次元を加えた 4 次元の表を用いるアルゴリズムに変形することによって，$O(|X| \cdot |Y| \cdot |P| \cdot r)$ 時間で弱制約最長共通部分配列問題を解くアルゴリズムを提案した．

また，P の部分配列の長さ $0 \leq q \leq r$ に関する次元を加える代わりに，P の部分配列の長さ $l - r \leq q \leq l$ に関する次元を加えることによって，$O(|X| \cdot |Y| \cdot |P| \cdot (l - r))$ 時間で弱制約最長共通部分配列問題を解くアルゴリズムを提案した．ただし，l は，X，Y，P の最長共通部分配列の長さである．このアルゴリズムは，たとえ $l < |P|$ であっても，$r = l$ に対して $O(|X| \cdot |Y| \cdot |P|)$ 時間で動作するという意味で，Chin ら [3] の制約最長部分配列問題に対する $O(|X| \cdot |Y| \cdot |P|)$ 時間アルゴリズムの機能を，漸近的な時間計算量を変化させることなく拡張したものとなっている．

提案した後者のアルゴリズムは，例えば $l = |P|/2$ の場合に，$\binom{|P|}{|P|/2}$ 個存在する P の長さ $|P|/2$ のどの部分配列が弱制約最長共通部分配列に部分配列として含まれるかに関する事前の知識なしに，$O(|X| \cdot |Y| \cdot |P|)$ 時間で弱制約最長共通部分配列を求める．一方，制約最長共通部分配列問題は，事前にどの配列が含まれるかについての知識が事前に与えられる場合の弱制約最長共通部分配列問題とみなすことができるものの，この問題に対す

る $O(|X|\cdot|Y|\cdot|P|)$ 時間よりも真に高速なアルゴリズムは知られていない．この意味で，共通部分配列に含まれる配列そのものに関する事前の知識がアルゴリズムの漸近的な時間計算量に実質的にどのように影響しているのかを検討することは，今後の課題の一つである．

3.2 新鮮な情報検索のスコアリングの提案

ウェブ検索における新鮮さを重視する文書のスコアリングとしてこれまでに提案した FTF·IDF に関して，改良と実データを用いた性能の評価実験を行った．

文書集合 D における単語 w と文書 d に対する FTF·IDF は，以下のように定義される．TF は，単語 w が文書 d に現れる回数である．IDF は，単語 w が少なくとも 1 回以上現れる D 中の文書の個数の D 中のすべての文書の個数に対する割合の対数である．したがって，頻繁に用いられるありふれた単語ほど小さな値が設定される．多くの検索エンジンにおいて，TF·IDF をスコアとする文書のランク付けが用いられている．FTF は，TF を用いて，

$$\mathrm{FTF}=\sum_{j=1}^{\mathrm{TF}}\exp\left(-\frac{t-t_j}{\alpha}\right)\cdot\mathrm{TF}$$

と定義される．ここで，t は現在の時刻，t_j は文書 d の先頭から j 番目に現れる単語 w が更新などによって文書 d に初めて生じた時刻である．α は，FTF が時刻の経過するにしたがってどの程度減衰するかを指定する因子である．この定義より，単語 w が生じてから時間がたつほど，FTF は小さな値が設定されることになる．したがって，FTF·IDF によるランク付けのもとでは，検索に用いた単語が最近に生じた文書ほど上位にランクされる．なお，上に定義した FTF を正確に計算するには，文書に現れるすべての単語に対してそれぞれタイムスタンプを保存し，また，更新の前後で各単語の対応関係を正確に判定しなければならない．これを検索システムに実装して用いるのはあまり現実的ではないため，実際には，正確ではないものの代わりの定義として，

$$\begin{aligned}\mathrm{FTF}_0 &= \mathrm{TF}_0,\\ \mathrm{FTF}_i &= \mathrm{FTF}_{i-1}\cdot\exp\left(-\frac{t_i-t_{i-1}}{\alpha}\right)\\ &\quad +\mathrm{TF}_i-\mathrm{TF}_{i-1}\\ &\quad (i\geq 1\text{ のとき})\end{aligned}$$

を提案している．ただし，t_0 は文書 d が初めて公開された時刻，t_i は文書 d の i 回目の更新の時刻を表し，FTF_i，TF_i はそれぞれ，時刻 t_i における FTF，TF の値を表す．

上の定義より，単語 w に関する検索に対して FTF·IDF で文書のランク付けをした場合，$\alpha=\infty$ ならば，従来の TF·IDF によるランク付けと同様に，文書中に単語 w が現れる回数が多いものほど上位にランク付けされる．一方，α が 0 に近いならば，最近の更新において単語 w が現れた文書ほど上位にランク付けされるものの，その文書に更新以前から存在している単語 w の個数はランク付けにあまり考慮されない．したがって，単語 w を多く含むという意味で単語 w に対する関連性の高く，かつ，公開されてまだあまり時間が経っていない w に関する内容を含むという意味で新鮮である文書を上位にランク付けするには，α をどのように設定するかが重要である．

そこで，文書集合全体における TF の総和が大きく変化する平均的な周期と，平均的な変化の総和の大きさから適応的に α の値を設定する方法を考案し，更新の周期の異なる実在する 2 つのウェブサイトをそれぞれ文書集合全体とみなして，FTF·IDF のランク付けを試した．この結果，どちらのウェブサイトにおいても，最も新しい文書が最上位にランク付けされる検索単語の種類の個数が飽和する境界の α が，考案した方法によって効率よく得られることを確認した．

4 計算の複雑さからのアプローチ

個々の論理関数を，種々の計算モデルを用いて表現する際に必要なサイズを評価する問題，特にそのサイズに対する下界を導出する問題は，計算量理論における中心的かつ挑戦的課題の一つである．勿論，これら表現のサイズは，対応する概念の学習の困難さを特徴付ける尺度としても使用で

きることから，学習理論の立場からも，基本的研究課題として位置づけられている．

本研究では，前年に引き続き，論理回路，論理式，しきい値回路，順序付き二分決定グラフといった，理論上あるいは，実用上重要な各計算モデルにおいて，種々の論理関数を表現する際に必要なサイズの下界を導出する手法の開発を目指した．また，これらの表現を用いて，実用上有用な様々な論理関数に対するコンパクトな表現を求めることによって，既知の上界を改善する研究も合わせて行った．

4.1 単層予想の否定的解決

論理回路とは，論理積素子，論理和素子および否定素子からなる組み合わせ論理回路である．明示的に与えられた論理関数に対して，これを計算する論理回路のサイズに対する有効な下界を導出する問題は，理論計算機科学分野最大の未解決問題である P≠NP 予想の解決にも直結する重要な課題と位置づけられている．本研究では，この問題の解決の手掛かりを得るために，主に，種々の制約を設けた論理回路における複雑さの下界の導出手法の開発を行うことを目指した．

単調論理回路とは，論理積素子と論理和素子のみからなる組み合わせ論理回路である．単調論理回路は，論理否定素子を用いることのできる一般の論理回路に比べ，表現できる関数が単調制の制約を満たすものに限定されるという制約を受けるものの，実用上現れる多くの関数は，単調性を有しており，それゆえ，汎用的モデルと言うことができる．本研究では，特に二次の論理関数，すなわち，丁度２個の変数の積の論理和として表される論理関数を取り上げ，論理回路の構造的性質と，関数の計算に要する回路サイズとの関係に焦点をあて研究を行った．その結果，任意の二次関数を計算するサイズ最小の単調論理回路は，常に単層回路—入力から出力へ至る任意の道上に論理積素子が高々１個しか出現しない回路—であることを予想した，いわゆる単層予想と呼ばれる十数年来の未解決問題に対し，多出力関数を考えた場合には，この予想が偽であることを示し，部分的に解決した．この予想は，その後，Jukna[5] によって，単出力関数の場合にも偽であることが証明され，完全な解決を見た．本研究における結果は，本予想解決への足がかりとなる有効なものであったと考えられる．

4.2 回路計算量の下界導出手法の開発

単調論理回路と一般の論理回路との中間モデルにあたる，制限された個数の否定素子を用いることのできる，否定数限定論理回路を用いた場合の計算複雑さの下界導出手法の開発をを行った．これについては，NP 完全に属するクリーク関数と呼ばれる論理関数を計算するためには，否定素子の使用を $O(\log\log n)$ 個程度許した場合にも，超多項式的なサイズの論理回路を要することを明らかにし，権威ある欧文雑誌の一つである SIAM Journal on Computing において発表した．否定素子の個数を $\log n$ 個にまで増加させた回路に対しても同様の下界を得ることができれば，直ちに P≠NP を意味することから，この結果は，前述した P≠NP 予想の解決へ向けた一つのステップと位置づけられる．

更には，回路中に現れる各素子の出次数を高々 1 に制限した論理回路に相当する，論理式を用いた際の論理関数の表現サイズの下界導出手法の開発にも取り組んだ．これに対しては，近年，量子回路において論理関数を評価する際に必要なオラクル呼び出しの回数の下界を導出する手法として開発された量子敵対者法が，論理式サイズの下界導出手法としても利用可能であるという最新の報告を受けて，本手法の詳細な解析と更なる拡張の可能性について研究を行った．本手法は，ある種の半正定値問題に対する実行可能解の存在が，ある一定値以下のサイズの論理式の不存在性を保証するという著しい性質を利用したものであり，これによって，論理式サイズの下界の証明を構成的に行うことが可能となる．本研究では，本手法を適用する際に得られる半正定値問題とその双対問題における許容解空間の性質に対するいくつかの性質を明らかにし，本手法の更なる拡張への手掛かりを得た．

しきい値回路とは，線形しきい値素子を用いて構成される非周期的回路である．しきい値回路は，単純化した脳のモデルとして，その計算能力について，古くより盛んな研究が行われている．本研

究では，2 層のしきい値回路に着目し，これを用いて論理関数を計算する際に必要なサイズの下界を導出する手法の開発を目指した．これに対して，与えられた論理関数を計算する 2 層しきい値回路のサイズの下界の導出を，ある法則によって与えられる線形計画問題の目的関数の最適解の導出に帰着する，新たな手法を提案発表した．また，提案手法を，2 層しきい値回路で計算が困難であることが強く予想されている内積関数に実際に適用し，得れらた大規模な線形計画問題を高い計算能力を持った計算機を用いて解くことによって，これまで同種の回路に対して得られていた最良の下界に匹敵する指数関数的下界を導出することに成功した．

4.3 乗算を計算する OBDD の設計

順序付き二分決定グラフ (Ordered Binary Decision Diagram, 以下 OBDD) は，近年活発に研究されている論理関数の表現形式である．OBDD は，各節に論理変数が割り当てられた決定二分木であり，かつ変数の出現する順序が根から各葉に至る道上で一様であるという制約を満たすものをいう．OBDD は，変数の出現順序を固定した場合には，その表現の最小化や，等価性判定が効率良く行うことが出来，この性質を利用して，VLSI の正当性の検証や，学習に際しての知識表現等の場面で幅広く用いられている．

OBDD は，変数順序を上手く選択することによって，数多くの実用上重要な論理関数を，非常にコンパクトに表現することができる一方，基本的な幾つかの関数は，いかなる変数順序の元でも，その表現サイズが指数関数的となることが知られている．二進数で与えられた整数同士の掛け算は，この様な性質を持つ最も代表的な関数である．90 年代初頭に Bryant によって証明されたこの事実は，以来，計算機科学分野において最も多く引用される結果の一つとなったが，掛け算を実現する最小の OBDD のサイズの具体的な値，および，その実現方法については，明らかとなっていなかった．

本研究では，この状況を打破すべく，二進 n 桁同士の掛け算を OBDD で表現する手法について理論と実験の両面から評価した．その結果，ベンチマークとして最も良く用いられる，n 桁同士の二進整数の掛け算の中心の桁を計算する，サイズが $O(2^{6n/5})$ である OBDD の構成手法を与えることに成功した．これは，従来知られる最良の上界を改善するものである．また，比較的小さな入力桁数に対して，掛け算を表現する最適な OBDD を実際に計算機実験により構成することで，上で示した上界の性能を評価した．その結果，n 桁の掛け算の中心桁を実現する最適な OBDD のサイズは $2^{6n/5}$ にほぼ比例すること．すなわち，本研究で得た構成手法は，ほぼ最適なサイズの OBDD を与えることを強く示唆する結果を得た．

4.4 単調 DNF 式の充足割り当て数の評価

ある制約を満たす単調積和型論理式 (MDNF 式) のうち，充足割り当ての個数を最大にする，あるいは最小にするものを特定する問題にも取り組んだ．これは，機械学習における知識表現の際にも広く用いられる MDNF 式に対して，極限的性質を持った式を特徴付けることを通じて，学習の効率化などに貢献しようという試みである．本研究では，極値集合論，あるいは極値グラフ理論といった分野において開発されてきた様々な手法が，この種の問題に適用できることを明らかにし，特に，変数の個数に比べて項の数が少ない，いわゆる疎な MDNF 式に対しては，上記の性質を持つ式を特定することに成功した．

参考文献

[1] Z. Bar-Yossef, K. Hildrum and F. Wu, “Incentive-Compatible Online Auctions for Digital Goods,” SODA 2002, pp. 964–970, 2002.

[2] E. Takimoto, Y. Sakai, and A. Maruoka, “The learnability of exclusive-or expansion based on monotone DNF formulas,” Theoretical Computer Science, **241**, pp. 37–50, 2000.

[3] F.Y.L. Chin, A. De Santis, A.L. Ferrara, N.L. Ho, S.K. Kim, “A simple algorithm for

the constrained sequence problem," Inf. Process. Lett., vol. 90, pp. 175–179, 2004.

[4] Y.T. Tsai, "The constrained longest common subsequence problem," Inf. Process. Lett., vol. 88, pp. 173–176, 2003.

[5] S. Jukna, "Disproving the Single Level Conjecture", SIAM J. Comput. (to appear)

研究業績一覧

学術論文

1. Shigeaki Harada, Eiji Takimoto, Akira Maruoka:
"Online Allocation with Risk Information", Proc. 16th International Conference on Algorithmic Learning Theory, Lecture Notes in Artificial Intelligence, Vol. 3734, 343–355, Oct. 2005.
概要: We consider the problem of dynamically apportioning resources among a set of options in a worst-case online framework. The model we investigate is a generalization of the well studied online learning model. In particular, we allow the learner to see as additional information how high the risk of each option is. This assumption is natural in many applications like horse-race betting, where gamblers know odds for all options before placing bets. We apply the Aggregating Algorithm to this problem and give a tight performance bound. Surprisingly, the Hedge algorithm without seeing risk information performs nearly as well as the Aggregating Algorithm. So the risk information does not help much. We discuss some interesting behaviors of the loss bound.

2. Eiji Takimoto, Naomitsu Aizawa, Akira Maruoka:
"On Proper Learning for Monotone Term Decision Lists from Queries", Proc. Workshop on Learning with Logics and Logics for Learning, 45–51, Jun. 2005.
概要: A monotone term decision list is a decision list where each node is labeled with a conjunction of literals with no negation. We characterize the class of monotone term decision lists in terms of another class of Boolean formulas called the XOR expansions of monotone DNF formulas. The relationships we give imply the proper learnability for some subclasses of monotone term decision lists. In particular, monotone term decision lists with $O(\log n)$ terms and monotone term decision lists with a constant number of alternations are both polynomial time properly learnable from membership and equivalence queries.

3. 酒井義文:
"弱制約最長共通部分配列問題", 電子情報通信学会論文誌, D-I, Vol. J88-D-I, No. 8, 1261–1263, 2005 年 8 月.
概要: 配列 X, Y の共通部分配列（subsequence）の中で，制約として与えられた配列 P の長さ r の部分配列を部分配列として含む，長さが最大の配列の一つを求める $O(|X| \cdot |Y| \cdot |P| \cdot r)$ 時間アルゴリズム及び $O(|X| \cdot |Y| \cdot |P| \cdot (l - r))$ 時間アルゴリズムを提案する．ただし，l は X，Y，P の最長共通部分配列の長さである．

4. Nobuyoshi Sato, Minoru Uehara, Yoshifumi Sakai:
"Evaluation of Freshness Considering Scoring on Fresh Information Retrieval", Journal of Interconnection Networks, Vol. 5, No. 3, 265–282, 2005 年 9 月.
概要: Fresh information is important for real business. In order to realize fresh information retrieval, we need not only to collect documents in a short time, but also to rank the results in the suitable order. However, conventional ranking methods are not suited for fresh information retrieval because they ignore temporal value of information. So, we have proposed the novel

ranking method FTF·IDF for fresh information retrieval. FTF · IDF extends TF · IDF by means of using FTF (Fresh Term Frequency) instead of TF (Term Frequency). FTF differs from TF because FTF decreases as time goes. The speed of decreasing FTF is determined by the dumping factor. The dumping factor is sensitive against small changes of documents. So, we use a threshold to ignore such small changes. In some papers we published, we detect the optimal threshold manually. In this paper, we proposed an adaptive calculating method in order to detect threshold automatically. In this method, the optimal value is determined by iterating to test generated thresholds. In this paper, we describe our method and its evaluation.

5. Kazuyuki Amano, Akira Maruoka:
"On the Monotone Circuit Complexity of Quadratic Boolean Functions", Algorithmica, (掲載予定).
概要: Several results on the monotone circuit complexity and the conjunctive complexity, i.e., the minimal number of AND gates in monotone circuits, of quadratic Boolean functions are proved. We focus on the comparison between single level circuits, which have only one level of AND gates, and arbitrary monotone circuits, and show that there is an exponential gap between the conjunctive complexity of single level circuits and that of general monotone circuits for some explicit quadratic function. Nearly tight upper bounds on the largest gap between the single level conjunctive complexity and the general conjunctive complexity over all quadratic functions are also proved. Moreover, we describe the way of lower bounding the single level circuit complexity and give a set of quadratic functions whose monotone complexity is strictly smaller than its single level complexity.

6. Kazuyuki Amano, Akira Maruoka:
"On Learning Monotone Boolean Functions under the Uniform Distribution", Theoretical Computer Science, 350(1), 3–12, Jan. 2006.
概要: In this paper, we prove two general theorems on monotone Boolean functions which are useful for constructing a learning algorithm for monotone Boolean functions under the uniform distributions. A monotone Boolean function is called fair if it takes the value 1 on exactly half of its inputs. The first result proved in this paper is that a single variable function $f(x) = x_i$ has the minimum correlation with the majority function among all fair monotone functions. This proves the conjecture by Blum, Burch and Langford (1998, Proc. 39th FOCS, pp.408–415) and improves the performance guarantee of the best known learning algorithm for monotone Boolean functions under the uniform distribution they proposed. Our second result is on the relationship between the influences and the average sensitivity of a monotone Boolean function. The influence of variable x_i on f is defined as the probability that $f(x)$ differs from $f(x \oplus e_i)$ where x is chosen uniformly from $\{0,1\}^n$ and $x \oplus e_i$ means x with its i-th bit flipped. The average sensitivity of f is defined as the sum of the influences over all variables x_i. We prove that a somewhat unintuitive result which says if the influence of every variable on a monotone Boolean function is small, i.e., $O(1/n^c)$ for some constance $c > 0$, then the average sensitivity of the function must be large, i.e., $\Omega(\log n)$. We also discuss how to apply this result to the construction of a new learning algorithm for monotone Boolean functions.

7. Kazuyuki Amano, Akira Maruoka:
"A Superpolynomial Lower Bound for a Circuit Computing the Clique Function with at Most $(1/6)\log\log n$ Nega-

tion Gates", SIAM Journal on Computing, 35(1), 201–216, Oct.2005.

概要: In this paper, we investigate the lower bound on the number of gates in a Boolean circuit that computes the clique function with a limited number of negation gates. To derive strong lower bounds on the size of such a circuit we develop a new approach by combining three approaches: the restriction applied to constant depth circuits due to Håstad, the approximation method applied to monotone circuits due to Razborov, and the boundary covering developed in the present paper. We prove that if a circuit C with at most $\lfloor(1/6)\log\log m\rfloor$ negation gates detects cliques of size $(\log m)^{3(\log m)^{1/2}}$ in a graph with m vertices, then C contains at least $2^{(1/5)(\log m)^{(\log m)^{1/2}}}$ gates. No nontrivial lower bounds on the size of such circuits were previously known, even if we restrict the number of negation gates to be a constant. Moreover, it follows from a result of Fischer (Lecture Notes in Comput. Sci., 33 (1974), pp. 71–82) that if one can improve the number of negation gates from $\lfloor(1/6)\log\log m\rfloor$ to $\lfloor 2\log m\rfloor$ in the statement, then we have P $\neq$ NP. We also show that the problem of lower bounding the negation-limited circuit complexity can be reduced to the one of lower bounding the maximum of the monotone circuit complexity of the functions in a certain class of monotone functions.

8. Kazuyuki Amano, Jun Tarui:
"Monotone Boolean Functions with s Zeroes Farthest from Threshold Functions", Proc. of the 3rd European Conf. on Combinatorics, Graph Theory and Applications (EuroComb05), Discrete Mathematics and Theoretical Computer Science, Vol. AE, 11-16, Sep. 2005.

概要: Let T_t denote the t-threshold function on the n-cube: $T_t(x) = 1$ if $|i : x_i = 1| \geq t$, and 0 otherwise. Define the distance between Boolean functions g and h, $d(g,h)$, to be the number of points on which g and h disagree. We consider the following extremal problem: Over a monotone Boolean function g on the n-cube with s zeros, what is the maximum of $d(g,T_t)$? We show that the following monotone function p_s maximizes the distance: For $x \in 0,1^n$, $p_s(x) = 0$ if and only if $N(x) < s$, where $N(x)$ is the integer whose n-bit binary representation is x. Our result generalizes the previous work for the case $t = n/2$ and s=2^{n-1} by Blum, Burch, and Langford [FOCS98], who considered the problem to analyze the behavior of a learning algorithm for monotone Boolean functions, and the previous work for the same t and s by Amano and Maruoka [ALT02].

9. Kazuyuki Amano, Akira Maruoka:
"On the Complexity of Depth-2 Circuits with Threshold Gates", Proc. of the 30th Mathematical Foundations of Computer Science (MFCS05), Lecture Notes in Computer Science 3618, 107-118, Aug. 2005.

概要: The paper investigates the complexity of depth-two circuits with threshold gates and consisting of two parts. First, we develop a method for deriving a lower bound on the size of depth two circuits with a threshold gate at the top and a certain type of gates at the bottom. We apply the method for circuits with symmetric gates at the bottom that compute the "inner product mod 2", and obtain a lower bound of 1.3638^n. Although our lower bound is slightly weaker than the best known lower bound of $\Omega(2^{n/2}/n)$, which was recently proved by Forster et al., our method has unique features: A lower bound is obtained by solving a certain linear program, and solving larger linear programs yield higher lower bounds. We also discuss the gen-

eralization of the proposed method. Second, we develop a simplified simulation of a depth-one threshold circuit with unbounded weights by a depth-two threshold circuit with small weights. Precisely, we give an explicit construction of depth-two circuits with small weights consist of $\tilde{O}(n^5)$ gates that compute an arbitrary threshold function. We also give the construction of such circuits with $O(n^3/\log n)$ gates computing the COMPARISON and CARRY functions, and that with $O(n^4/\log n)$ gates computing the ADDITION function. These improve the previously known constructions on its size and simplicity.

研究会等

1. 原田薫明，瀧本英二，丸岡章:
“リスク情報を用いたオンライン資源分配”, 電子情報通信学会技術研究報告（コンピュテーション）, Vol. 104, No. 743, 105–110, 2005 年 3 月.
概要: 本論文では，動的資源分配問題について，オンライン予測の枠組みで考察を行う．我々は，広く研究されているオンライン学習のモデルを一般化したモデルを提案する．このモデルでは，学習者はそれぞれの投資先のリスクがどれほど高いかという情報を知ることができる．このような仮定はごく自然なもので，多くの例が考えられる．例えば競馬では，投資家は資金を賭ける前にリスク情報として馬の倍率を知ることができ，投資家はその倍率を考慮した投資が許される．本論文ではアグリゲーティングアルゴリズムをこのような問題に適用し，厳密な性能評価を行う．我々の結果は，投資先のリスクが一様である場合と比較して，それぞれの投資先でリスクが異なるほど，アルゴリズムはよりよい性能を持つことを示唆している．

2. Shigeaki Harada, Eiji Takimoto, Akira Maruoka:
“Online Allocation with Risk Information”, Proc. of the 4th Japanese-Hungarian Symp. on Disc. Math. and Its Applications, 84–91, Jun. 2005.
概要: We consider the problem of dynamically apportioning resources among a set of options in a worst-case online framework. The model we investigate is a generalization of the well studied online learning model. In particular, we allow the learner to see as additional information how high the risk of each option is. This assumption is natural in many applications like horse-race betting, where gamblers know odds for all options before placing bets. We apply the Aggregating Algorithm to this problem and give a tight performance bound. The bound we give intuitively implies that the algorithm performs better when faced with options of various risks than when faced with options of the same risk.

3. Tatsuya Watanabe, Eiji Takimoto, Kazuyuki Amano, Akira Maruoka:
“Random Projection and Its Application to Learning”, Proc. 2005 Workshop on Randomness and Computation, 3–4, Jul. 2005.
概要: 任意の 2 点間のユークリッド距離を保存するランダムプロジェクションを用いた線形分離関数の学習について述べる．また，ランダムシードが 4 限定独立のときは弱い距離保存の性質を持つが，3 限定独立のときは距離保存の性質をまったく持たないことを示す.

4. 渡邊辰也，瀧本英二，天野一幸，丸岡章:
“マージンを保存するランダム性を限定したプロジェクションとブール空間への埋め込み”, 電子情報通信学会技術研究報告（コンピュテーション）, Vol. 105, No. 343, 21–28, 2005 年 10 月.
概要: マージンが最大となる仮説を求めることは機械学習の分野における最も重要な問題のひとつである．しかし，与えられたデータを分離する大きなマージンを持った超平面を見つけることは難しい．本稿では，高次元空

間でのマージンをほぼ保存したまま低次元空間へのランダムな写像を行うような，3つのランダムプロジェクションの手法を提案する．これらの手法により写像された低次元空間内でパーセプトロン等のアルゴリズムを用いることで，高速に適切な仮説を探すことができる．我々の手法は，Johnson-Lindenstraussの補題に基づく既存の手法に比べ，マージンの保存という点では，より効果的である．JL補題に基づく手法が任意の2点間の距離を保存するという強い性質を持つのに対し，我々の手法はマージンの保存のみを目的とするからである．具体的には，マージンの保存性能をほぼ維持したままランダムビットを削減する写像を与え，さらに，ブール空間へのマージンを保存した写像も与える．

5. 原田薫明，瀧本英二，丸岡章:
“オンラインオークション型資源配分”, 冬のLA シンポジウム, 2006 年 1 月.
概要: 次々と訪れる入札者に商品を売るにあたり，その都度価格を設定し，総売り上げの最大化を図るオンラインオークション問題を取り上げる．本稿では，この問題が動的資源分配問題へと帰着できることに注目し，Vovkの統合戦略を用いて新しいオークション型の統合アルゴリズムを導出し，その性能評価を与える．

6. 高橋良介，瀧本英二，丸岡章:
“シャノンスイッチングゲームにおけるペアリング戦略の複雑さについて”, 電子情報通信学会技術研究報告（コンピュテーション）, 2006 年 3 月.
概要: 与えられたグラフ上で，特定の2点間を結ぶ道を作ろうとするプレイヤーと，それを阻止しようとするプレイヤーが戦うシャノンスイッチングゲームにおいては，最適戦略を求めることがPSPACE困難であることが知られている．本論文では，後手の戦略をペアリング戦略と呼ばれる単純な戦略に限定した場合，先手の戦略に対応する問題の計算量がNP完全で，後手の戦略に対応する問題が Σ_2^p 完全となることを示す．

7. Kazuyuki Amano, Akira Maruoka:
“Tighter Bounds on the OBDD Size of Integer Multiplication”, Proc. of the 4th Japanese-Hungarian Symp. on Disc. Math. and Its Applications, 9–15, Jun. 2005.
概要: We show that the middle bit of the multiplication of two n-bit integers can be computed by an OBDD of size less than $2.8 \cdot 2^{6n/5}$. This improves the previously known upper bound of $(7/3) \cdot 2^{4n/3}$ by Woelfel (STACS, 2001). The experimental results suggest that our exponent of $6n/5$ is (at least very close to) optimal. A general upper bound of $O(2^{3n/2})$ on the OBDD size of each output bit of the multiplication and some conjecture on the structural properties of multipliers inspired by the experimental results are also presented.

8. 天野 一幸，佐藤 貴之，丸岡 章:
“充足割り当て数を最小化/最大化する単調DNF 式について”, 電子情報通信学会技術研究報告（コンピュテーション）, Vol. 105, No. 344, 21–25, 2005 年 10 月.
概要: 変数の個数，項の数，項の長さ等が固定された中で，充足割り当ての個数が最も少ない，あるいは，最も多い単調DNF式を特定する問題について考える．まず，充足割り当ての個数を最小化する単調DNF式は，項を“辞書順”に並べた式であることが，極値集合論におけるKruskal-Katonaの定理より，容易に導くことができることを述べる．一方，充足割り当ての個数を最大化する単調DNF式は，各項の長さを2に限定し，かつ，項の個数にもある制約を設けた場合には，Bollobásによる完全部分グラフの個数に関する定理から容易に求められるものの，項の長さや項数を一般化した問題は，非常に困難な問題となっている可能性のあることを述べる．

学会大会等

1. 瀧本英二:
“オンライン予測の理論と応用”, 第 18 回 回

路とシステム軽井沢ワークショップ, 595–600, 2005 年 4 月.

2. 渡邊辰也，瀧本英二，天野一幸，丸岡章: “ランダム写像による非線形概念の学習の効率化に向けて”, 電子情報通信学会総合大会 COMP-NHC 学生シンポジウム, 2006 年 3 月 .

3. 瀧本英二: “Path Kernels and Finding the Optimal Strategy for a Routing Game”, Tutorial workshop on game-theoretic probability and related topics, 2006 年 3 月.

4. 天野一幸: “しきい値素子を用いた回路における計算量について”, 日本オペレーションズ・リサーチ学会関西支部研究部会, 2005 年 1 月.

A02: 計算理論的設計による知識抽出モデルに関する研究

徳山　豪　　塩浦　昭義

東北大学 大学院 情報科学研究科
〒 989-3201 仙台市青葉区荒巻字青葉
{tokuyama, shioura, k-keniti}@dais.is.tohoku.ac.jp

1　はじめに

本研究の目的はデータマイニングにおける現在の精度限界を打破するための知識抽出モデルの提案と，それに関する理論研究及び実際のシステムの構築である．特に，研究代表者の持つ先端技術である計算幾何学的手法を中心に，計算理論手法による限界突破を目指す．データマイニングは大規模なデータから情報をコンパクトな知識として抽出する技術であり，近年に情報科学から発信した技術であるにもかかわらず，経済学，経営学，統計学などの学問分野，及び経営コンサルティング，在庫管理や顧客サービスといった実用分野に幅広く応用が期待され，情報化社会における最重点技術の一つである．

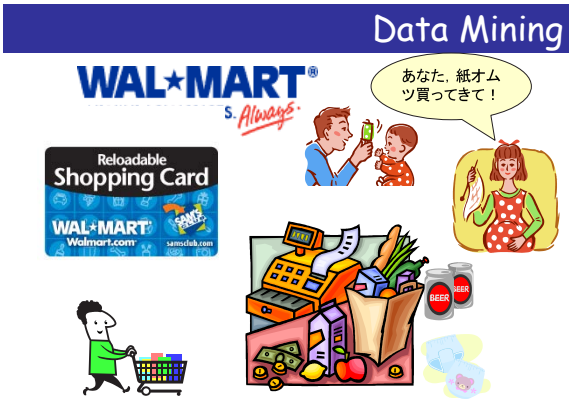


図 2.1: データマイニングのイメージ：紙おむつを買う人は高い確率でビールも同時に買う

自動的に抽出し，表示された知識形態は，ユーザにより意志決定等の補助として用いられる．重要な条件は，抽出した知識形態がシンプルであり（単純性），正確にデータの特性を記述しすること（正確性），知識として（サンプルに依存しない）汎用性を持つ事（学習汎用性）さらにユーザにとって説得力があり，検証が容易であること（透明性）である．単純性と透明性の観点から，結合ルール及びそれを用いた決定木は有力な手法である．これらの手法を用いたデータマイニングの研究はIBM 社アルマデン研究所や米国スタンフォード大学，カナダ国サイモンフレーザー大学，オーストラリア国シドニー大学等で 1980 年代半ばに始まり，主に二値データに対する研究が行われた．スタンフォード大学での研究成果の一例として，スーパーマーケットの売上情報のデータのマイニングでの「紙おむつを買う人はビールを買う」といったルールは広く知られている．これは，どちらかというとネガティブなイメージ（くだらないルールしか発見できない）に捉えられがちだが，「常識からは見出せないルールも発見できる」と見るべきである．現在では，広くデータマイニング技術は用いられており，例えば本のインターネット販売でも，データマイニングを用いた解析により，購買者の過去の履歴から，興味のありそうな書籍のリストを作成して提示するというような事が行われている．

さて一方，実用データマイニングで必須である数値データベースの取り扱いを考えると，数値データの二値化誤差から生じる，正確性と学習汎用性のトレードオフに関する精度限界があり，それを乗り越えるのは技術的に困難と思われていた．日本でのデータマイニングの研究はこれに数年遅れ，研究代表者を含む日本 IBM のチームが 1990 年代後半に行った研究が国際的に最初に認められた成果である．具体的には，結合ルール条件生成時のアダプティブな二値化のアイデアを導入し，二値化誤差最小化の理論的枠組みである最適結合ルールの定式化を与え，データマイニングに計算理論の手法を導入することに世界に先駆けて成功



図 2.2: 書籍販売でのデータマイニング

した（1996-1998 年）．これにより，上記のトレードオフは大きく改善された．世界的に独創的な研究として高く評価され，現在広く関連研究がなされている．しかしながら，最小誤差二値化を用いても誤差には理論的下界があり，上記限界の完全な克服には至っていない．本研究では，透明性を保ちながら，この二値化誤差からくる限界を克服するデータマイニングシステムの設計とその理論的解析を行う．このようなデータマイニングシステムは要望されてはいるが，現実化は難しく，独創的な新しいアイデアが必要とされていた．

本研究により，既存の多くのデータマイニングシステムの重要なコンポーネントである意志決定システムに透明性と高い学習汎用性が与えられると予想される．更に，基本技術として用いるグラフ・計算幾何アルゴリズム理論を中心とした理論計算機科学での理論発展と共に，理論計算機科学技術の知識抽出への応用の新しい進展が期待される．

2　平成１７年度の計画と成果

上述のように本研究では，透明性を保ちながら，二値化誤差からくる限界を克服するデータマイニングシステムの設計とその理論的解析を行う．平成１７年度の具体的な成果目標としては，基礎理論に関する研究と階層化ルールをエキスパートとして用いた柔軟な決定木の実現がメインであり，特にグラフ理論に関する最適化技術，学習理論の先端技術の研究とその利用についての研究を行った．

本年度の具体的な成果としては，下記のものがある．

1. 柔軟な決定木の構築に用いる階層ルールの高次元におけるモデル化と高速アルゴリズムの設計及び最適データ近似の研究．
2. 上記目的のための計算幾何学の最適化理論の研究
3. データマイニングでの主要な道具であるクラスタリングにおいて，クラスタ発見の高濃度部分グラフ問題としての定式化と，計算クラスに関する新しい発見．
4. ヨーロピアン・アジアンオプションの価格付けに対する近似アルゴリズムの設計

3　研究活動

研究活動予定に従い，徳山は基礎理論とモデル化及び計算限界の算定，塩浦は数理最適化とアルゴリズム理論に絞って研究を開始した．システム実装と実験に関しては，全眞嬉学術振興会特別研究員を中心に大学院学生のプロジェクトを構成し実施した．

研究代表者の徳山は研究成果に関連した論文誌・査読付き国際学会論文を 8 本，研究協力者の塩浦は同 4 本 発表している．また、途中から計画に参画した河原林健一（研究室助手）は権威ある国際会議 FOCS での発表を行った。その他，国際学会招待講演，国内学会，研究会等での発表も数多く行った．また，徳山は 7 月に仙台で開催した SMAPIP-NHC 共催の国際ワークショップ「Randomness and Computation」の開催責任者の一人として貢献をおこなった．

理論的な研究が主体であるため，研究活動に必須である国際的活動と，仙台からの国内旅費の必要性から，小規模な備品・消耗品を除き研究費のほとんどは旅費に当てた．特に NHC 国際会議には，プロジェクトに参加する学生を参加させ，国際的な一流研究者との交流経験を積ませたが，その旅費も本研究費から拠出した．また，河原林は IEEE-FOCS 国際会議，徳山は ISAAC 国際会議などのアルゴリズム分野でのシリーズ国際会議で研究成果を発表し，さらに塩浦はドイツ，河原林は米国

やデンマーク等に長中期の訪問を行うことにより，共同研究を行い，広く国際的に活動した．また，特定研究の研究費で O. Cheong, M. Halldorsson ら国際的に一流の研究者に東北大学において講演・共同研究を依頼し，成果をあげている．

4　研究成果の概要

4.1　エキスパート付き決定木の構成と実装

本テーマについては平成 16 年度からの引き続いた研究である．アソシエーションルールを用いた決定木はデータマイニングにおける意思決定システムとして広く用いられている．しかしながら，数値属性を含むデータにおいては，データのカテゴリ属性への変換による情報損失があり，この損失と決定木における過学習のバランスを取る事が重要になる．そのために，数値属性の情報をエキスパートとして付加した決定木を構成する．エキスパート付き決定木に関しては主に学習理論の見地から理論的な研究は行われているが，現実のエキスパートの作成を階層化ルールを用いて実現し，数値データベースでのデータマイニングへの応用を意識した実装実験を行ったのは世界でも初めてのものである．

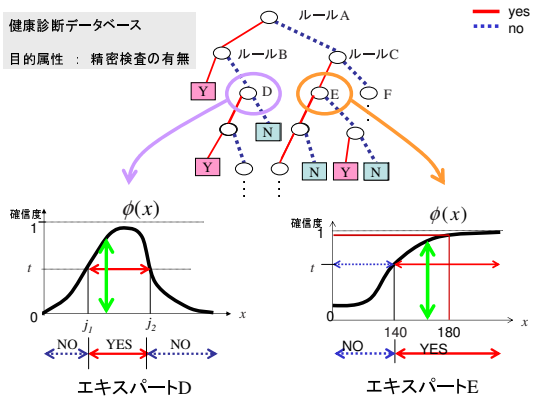


図 2.3: エキスパート付き決定木

最適ピラミッドを用いた決定木構成アルゴリズムは以下のようになっている．

step1 学習データ T を読み込む．

step2 T のすべての事例が同一クラスならば葉とする．

そうでなければ，各属性に対して次の 1〜4 を行う．

1. 各属性値における確信度を求める．
2. 求めた確信度を元に最適ピラミッドを構築する．
3. 全ての高さに対して分割を行い，相互情報量を計算する．
4. 得られた各属性の相互情報量を比較する．
   (a) 閾値 g_ℓ 以上かつ最も大きな相互情報量が得られた属性があるならば，それをノードとし，T を T_1，T_2 に分割する．同時に，T_1，T_2 の確信度を求めておく．
   (b) もし，どの属性の相互情報量も g_ℓ 未満であるならば，T に最も多く現れるクラスラベルの葉とする．
5. 分割頂点に最適ピラミッドから構成したエキスパートを配備する

step3 分割された事例集合に対し，全てが葉になるまで **step1**，**step2** を繰り返す．

生成された決定木の各ノードでは分割テストが行われる．例えば，根である属性 A テストは，全学習データ T の，属性 A について求められた確信度のヒストグラム f を持つ．また，f から求められた最適ピラミッド ϕ，そして，分割された T_1，T_2 の確信度 $conf(T_1)$，$conf(T_2)$ をそれぞれ持っている．この確信度はテストデータが分類され，枝を通るときに各テスト事例に対して与えられる．分割された事例集合 T_1，T_2 は，子ノードに入力され，子ノードも同様な構造を持つ．

また，決定木の末端である葉には，クラスラベルが与えられる．その葉に振り分けられた学習データの事例数 $|T_{11}|$，その中でクラスが C でない事例数 $|E_{11}|$ (エラー数) も記録してある．

エキスパートは，決定木構築アルゴリズムの **step2**.4 の後に生成され，該当ノードにおける学習データ数 $|T|$，及び，T より構築された最適ピラミッド関数 $\phi(T)$ を持つ．エキスパートは決定木の各ノードに配置される．入力されたデータ i に

対し，ノード A のエキスパートは，学習データ数 $|T|$，及び $\phi(T)$ におけるデータ i の確信度 $\alpha_T(i)$，を与える．そして，与えられた確信度と事例数のセットにより，データ i のクラスを決定できるかどうか判断する．平成 16 年度に設計したシステムでは，あるノード A の情報の信頼性が大きいと判断し，そこでデータ i にラベルを与え，テストを終了する判断を行う．即ち，ノード A, B 間で枝刈りを行うことになる．ここで，比較に用いた $\alpha_T(i)$ の値は各データによって値が異なる．つまり，エキスパートは，個々のデータに依存した，データことに柔軟かつインプリシットに決定木の枝刈りを行う．

平成 17 年度には，更にスペシャリストモデルを用いたオンライン学習理論を適用し，従来よりも高い理論保証を持つシステム構築を行った．ここで，スペシャリストモデルでのオンライン学習は，A01 班の研究テーマと関連し，多くの決定システムを統合する理論的な枠組みである．各スペシャリストは決定を行うことも，決定を保留することも出来，最適なスペシャリストグループの統合した決定と同等の判定を，(その最適なグループを知らずに）自動的に行う学習システムである．理論的な保証の導出と，実験による検証を行い，従来のシステムに比べての優位性を見出した．

4.2 高濃度部分グラフを用いたクラスタリングに関する研究

本テーマも平成 16 年度からの引き続いたテーマである．知識抽出システムでは重複を許した非排他的クラスタリングが重要な tool である．そこでは，データを分割するのではなく，クラスタを一つづつ発見していくというアプローチが採られる．代表的なアルゴリズムとしてしられる Agrawal らのアプリオリアルゴリズムは，データと（カテゴリ）属性の作る二部グラフを考え，データ部分の大きい 2 部クリーク（完全二部グラフ）を全て列挙するという方針をとっている．しかしながら，この手法では属性数の多いクリークを求める事は計算爆発により不可能である．改良として極大 2 部クリーク列挙アルゴリズムも提案されているが，計算爆発を完全には克服できない．一方，枝数が最大のクリークを求める問題，もしくは指定した属性数に対する最大クリークを求める問題は NP 完全であり，近似する事も計算量理論的に困難である．従って，本研究では，クリークではなく,(サイズを指定した）最大濃度部分グラフ問題を用いてクラスタ発見を行うという新しいアプローチを採る．最大濃度部分グラフ問題は古くから研究されている．従来の計算理論の研究においては，U. Feige によってランダム 3SAT 判定からの帰着が示されており，計算量は近似困難問題のクラスに入り多項式時間アルゴリズム設計は（計算階層が崩壊しない限り）不可能であった．知られている最良の近似比は $O(n^{1/3})$ を少し改良したもの（Feige–Kortsarz–Peleg, Algorithmica 1993）であり，これを越えることは非常に難しいとされていた．多項式時間の定数近似アルゴリズム設計が可能な既知の場合は，Arora–Karger–Karpinski らによる部分グラフが $\Omega(n^2)$ の辺数を持つ場合（STOC95）の PTAS があるが，これは実用的に利用できない．また，朝廣–岩間–玉木–徳山によるグリーディーアルゴリズムの解析（J. Algorithms 2000）では，定数近似を達成するのは頂点数が $\Omega(n)$ の場合に限られていた．一方，本研究では，最大濃度部分グラフの濃度に注目し，この濃度が高い（クリークに比べて定数倍の辺を持つ）場合は，高速な近似アルゴリズムの設計が可能であることを示した．この高濃度条件は，データマイニングのようにクリークに近い部分グラフのみを必要とする場合には実用的に妥当な条件である．

成果としては，二部グラフに対しては $O(n^\epsilon)$ 近似アルゴリズムおよび擬多項式時間近似スキームを与え，この近似スキームが多項式時間近似スキームになるための条件の明確な提示を行った．これらは，新しい見地から最大濃度部分グラフ問題の計算量を追求したものであり，世界的にも新規性の高い成果である．更に一般の重み付きグラフに対してもこの理論を拡張し，$O(n^\epsilon)$ 近似の多項式時間アルゴリズム及び 2 近似を達成する擬多項式時間アルゴリズムを考案している，本年度は国際会議 ISAAC 等で成果を発表し，更に一般の組み合わせ最適化問題に対しての同様のアプローチの検討を行った．subdense なインスタンスでの計算困難性の追求という観点から，世界的にも大きな貢献であるといえる．

4.3 ヨーロピアン・アジアンオプションの価格付けに対する近似アルゴリズムの設計

本研究では，パス依存型オプションの一種であるヨーロピアン・アジアンオプションの価格付けという問題に対し，高速かつ近似誤差が小さい近似アルゴリズムを提案した．

オプションの購入日から満期までの平均株価を A，行使価格を X とおいたとき，ヨーロピアン・アジアンオプションのペイオフは $\max\{A - X, \}$ と表される．二項木モデル上でパス依存型オプションの価格を厳密に求めることは，一般に#P 困難であることが知られている．ゆえに，効率的かつ理論的に近似精度が保証された近似アルゴリズムの設計が望まれており，これまでに様々な近似手法が開発された．

ヨーロピアン・アジアンオプションの厳密な価格を計算する単純な方法として，二項木のすべてのパスを列挙するという，全パス法と呼ばれる方法がある．しかし，最悪の場合，二項木のパスの数は指数個であり，ゆえに全パス法は指数時間を要する．

Aingworth, Motwani, Oldham (AMO) (2000) は，近似誤差を理論的に保証した最初の多項式時間近似アルゴリズムを提案した．この近似アルゴリズムでは，理論的な近似誤差はボラティリティに依存しないという利点をもつ．このアルゴリズムは動的計画法とバケッティングに基づいたものであり，高いペイオフをもつ指数個のパスを数式を使って枝刈りする，というアイディアを用いることで計算効率を高めている．このアルゴリズムの各ステップにおいて生じる誤差は X/k により押さえられる．ここで k は二項木の各頂点において使用されるバケットの数を表す．ゆえに，アルゴリズムの総ステップ数を n としたとき，AMO アルゴリズムの誤差は nX/k で押さえられる．またアルゴリズムの実行時間は $\mathrm{O}(kn^2)$ となることが示されている．のちに，AMO アルゴリズムの近似誤差は Dai, Huang, Lyuu (2002) および我々の研究グループ (2005) により改善された．AMO アルゴリズムでは，二項木の各頂点において同じ数のバケットが使用されているのに対し，Dai, Huang, Lyuu のアルゴリズムでは各頂点ごとに異なる数のバケットを使用する．近似アルゴリズムの計算時間を $\mathrm{O}(kn^2)$ に保ちつつ，各頂点でのバケットの数を適切に調整することにより，$\mathrm{O}(\sqrt{n}X/k)$ という近似誤差を実現している．ここで k は各頂点で用いられるバケットの数の平均値を表す．一方，我々が提案したアルゴリズムは，AMO アルゴリズムに「ランダム丸め」の技法を適用したものであり，$\mathrm{O}(n^{1/4}X/k)$ という近似誤差を実現した．

本研究では，計算時間がこれまでと同じ $\mathrm{O}(kn^2)$ であり，かつより小さい近似誤差 $\mathrm{O}(X/k)$ をもつランダム化アルゴリズムを提案した．AMO アルゴリズムおよび過去に提案された改良版アルゴリズムと異なり，このアルゴリズムの理論的な近似誤差は二項木の深さ n と独立である，という利点をもつ．提案するアルゴリズムでは，過去の 2 つのアルゴリズムで用いられたアイディアを同時に利用している．まず，我々のグループ (2005) が以前提案したアルゴリズムと同様に，今回提案したアルゴリズムでは，適切な確率変数を導入することにより，アルゴリズムの動きを $\mathrm{O}(n^2)$ 段階のマルチンゲール過程と見なす．そして，アルゴリズムの出力の期待値が厳密な値と等しいことを証明するとともに，各ステップで生じる近似誤差が二項木の頂点で用いられるバケット数の関数により抑えられることを示した．したがって，上記で述べたマルチンゲール過程に Azuma の不等式を適用することが可能となり，これにより近似誤差の理論的な解析が可能となった．ここで，二項木の各頂点でちょうど k 個のバケットを用いた場合，我々のグループ (2005) が以前提案した近似アルゴリズムと同一のものが得られる．このアルゴリズムの近似誤差を出来る限り小さくするために，二項木の各頂点で用いられるバケットの数を調整し，$\mathrm{O}(X/k)$ という近似誤差を得ることに成功した．ここで k は各頂点で用いられるバケットの数の平均値を表す．X/k という値は，二項木の各頂点で生じる近似誤差の「平均値」と見なすことが出来るので，我々のアルゴリズムの近似誤差は，AMO アルゴリズムの枠組みの中で最良といえる．また，本研究では提案する近似アルゴリズムおよび過去に提案された近似アルゴリズムをコンピュータ上で実装し，実際の計算により得られるオプション価格の近似値の精度についても評価を行った．

研究業績一覧

学術論文

1. Jinhee Chun, Kunihiko Sadakane, Takeshi Tokuyama:
"Linear Time Algorithm for Approximating a Curve by a Single-peaked Curve", Algorithmica, Vol.44, No.2, 103-115, 2006年2月.
概要: Given a function $y = f(x)$ in one variable, we consider the problem of computing the single-peaked (unimodal) curve $y = \phi(x)$ minimizing the L_2-distance between them. If the input function f is a histogram with $O(n)$ steps or a piecewise linear function with $O(n)$ linear pieces, we design algorithms for computing ϕ in linear time. We also give an algorithm to approximate f with a function consisting of the minimum number of unimodal pieces under the condition that each unimodal piece is within a fixed L_2-distance from the corresponding portion of f.

2. Jinhee Chun, Kunihiko Sadakane, Takeshi Tokuyama:
"Efficient Algorithms for Constructing a Pyramid from a Terrain", IEICE Transactions, Vol.E89-D, No.2, 783-788, 2006年2月.
概要: Given nonnegative valued functions ρ and μ in d variables, we consider the optimal pyramid maximizing the total parametric gain of ρ against μ. The pyramid can be considered as the optimal unimodal approximation of ρ relative to μ, and can be applied to hierarchical data segmentation. In this paper, we give efficient algorithms for a couple of two-dimensional pyramid construction problems.

3. Jinhee Chun, Kunihiko Sadakane, Takeshi Tokuyama, Masato Yuki:
"Peak-Reducing Fitting of a Curve under the L_p Metric", Interdisciplinary Information Sciences, Vol.11, No.2, 191-197, 2005年9月.
概要: Given a function $y = f(x)$ in one variable, we consider the problem of computing a k-peaked curve $y = \phi(x)$ minimizing the L_p distance between them. In other words, $\phi(x)$ has at most k local peaks and minimizes the area bounded by the curves $f(x)$ and $\phi(x)$. This gives extension of the authors' previous work on the unimodal (i.e., single-peaked) approximation for the L_2 distance.

4. Jinhee Chun, Kunihiko Sadakane, Takeshi Tokuyama:
"Construction of Expert Guided Decision Tree on Numeric Database", 8th Japan-Korea Workshop on Algorithm and Computation, WAAC05, 27-34, 2005年8月.
概要: In this paper, we propose the technique for constructing a decision tree with high prediction accuracy. There is over fitting as a problem at the time of constituting a decision tree. If the optimal decision tree is used to training data, trade-off that the prediction accuracy over unknown data will fall will arise. In this paper, we propose a new method for removing these drawbacks. Indeed, we give optimized numeric association rules with multi attributes, and give layered-structure numeric association rules. We use layered-structure numeric association rules as expert of decision tree.

5. A. Suzuki, T. Tokuyama:
"Dense Subgraph Problems with Output-Density Conditions", Proceedings of The 16th Annual International Symposium on Algorithms and Computation, LNCS3837, 266–276, 2005年12月.
概要: We consider the dense subgraph problem that extracts a subgraph with a prescribed number of vertices that has the maximum number of edges (total edge

weight in the weighted case) in a given graph. We give approximation algorithms with improved theoretical approximation ratios assuming that the density of the optimal output subgraph is high, where density is the ratio of number of edges (or sum of edge weights) to the number of edges in the clique on the same number of vertices. Moreover, we investigate the case where the input graph is bipartite, and design a pseudo-polynomial time approximation scheme that can become a PTAS even if the size of the optimal output graph is comparatively small. This is a significant improvement in a theoretical sense, since no constant-ratio approximation algorithm was known previously if the output graph has $o(n)$ vertices.

6. T. Tokuyama:
" Minimax parametric optimization problems and multidimensional parametric searching", Interdisciplinary Information Sciences, 11-1, 1–9, 2005年4月.
概要: The parametric minimax problem, which finds the parameter value minimizing the weight of a solution of a combinatorial maximization problem, is a fundamental problem in sensitivity analysis. Moreover, several problems in computational geometry can be formulated as parametric minimax problems. The *parametric search* paradigm gives an efficient sequential algorithm for a convex parametric minimax problem with one parameter if the original non-parametric problem has an efficient parallel algorithm. We consider the parametric minimax problem with d parameters for a constant d, and solve it by using multidimensional version of the parametric search paradigm. As a new feature, we give a feasible region in the parameter space in which the parameter vector must be located. Typical results obtained as applications are: (1) Efficient solutions for some geometric problems, including theoretically efficient solutions for the minimum diameter bridging problem in d-dimensional space between convex polytopes. (2) Solutions for parametric polymatroid optimization problems, including an $O(n \log n)$ time algorithm to compute the parameter vector minimizing k-largest linear parametric elements with d dimensions.

7. K. Ohta, K. Sadakane, A. Shioura, T. Tokuyama:
"A Fast, Accurate and Simple Method for Pricing European-Asian and Saving-Asian Options", Algorithmica, 42, 141–158, 2005年4月.
概要: We propose an efficient and accurate randomized approximation algorithm for computing the price of European-Asian options. Our algorithm can be seen as a modification of the approximation algorithm developed by Aingworth et al. (2000) into a randomized algorithm, which improves the accuracy theoretically as well as practically. We also propose a new option named the Saving-Asian option which enjoys advantages of both the European-Asian and American-Asian options. It is shown that our approximation algorithm also works for pricing Saving-Asian options.

8. A. Shioura, T. Tokuyama:
"Efficiently Pricing European-Asian Options: Ultimate Implementation and Analysis of the AMO Algorithm", Proc. of 1st International Conference on Algorithmic Applications in Management (AAIM 2005), LNCS 3521, 291–300, 2005年6月.
概要: We propose an efficient and accurate randomized approximation algorithm for pricing a European-Asian option on the binomial tree model. For an option with the strike price X on an n-step binomial tree and any positive integer k, our algorithm runs in $\mathrm{O}(kn^2)$ time with the error bound

$O(X/k)$ which is independent of n. Our algorithm is a modification of the approximation algorithm developed by Aingworth, Motwani, and Oldham (2000) into a randomized algorithm, which improves the accuracy theoretically as well as practically.

9. K. Murota, A. Shioura:
"Substitutes and Complements in Network Flows Viewed as Discrete Convexity", Discrete Optimization, 2, 256–268, 2005年9月.
概要: We study combinatorial properties of the optimal value function of the network flow problem. It is shown by Gale–Politof [Substitutes and complements in networks flow problems, Discrete Appl. Math. 3 (1981) 175–186] that the optimal value function has submodularity and supermodularity w.r.t. problem parameters such as weights and capacities. In this paper we shed a new light on this result from the viewpoint of discrete convex analysis to point out that the submodularity and supermodularity are naturally implied by discrete convexity, called M-convexity and L-convexity, of the optimal value function.

10. A. Shioura, N. Sun, Z. Yang:
"Efficient Strategy Proof Fair Allocation Algorithms", Journal of Operations Research Society of Japan, (掲載予定).
概要: We study a fair division problem with indivisible objects like jobs, houses, and one divisible good like money. Each individual is to be assigned with one object and a certain amount of money. The preferences of individuals over the objects are private information but individuals are assumed to have quasi-linear utilities in money. It is shown that there exist efficient algorithms for eliciting honest preferences and assigning the objects with money to individuals efficiently and fairly.

11. E. Demaine, M. Hajiaghayi, K. Kawarabayashi:
"Algorithmic Graph Minor Theory: Decomposition, Approximation, and Coloring", Proceedings of IEEE Symposium on Foundation of Computer Science, 46, 637 － 646, 2005年10月.
概要: At the core of the seminal Graph Minor Theory of Robertson and Seymour is a powerful structural theorem capturing the structure of graphs excluding a fixed minor. This result is used throughout graph theory and graph algorithms, but is existential. We develop a polynomial-time algorithm using topological graph theory to decompose a graph into the structure guaranteed by the theorem: a clique-sum of pieces almost-embeddable into bounded-genus surfaces. This result has many applications. In particular, we show applications to developing many approximation algorithms, including a 2-approximation to graph coloring, constant-factor approximations to treewidth and the largest grid minor, combinatorial polylogarithmic-approximation to half-integral multicommodity flow, subexponential fixed-parameter algorithms, and PTASs for many minimization and maximization problems, on graphs excluding a fixed minor.

研究会等

1. 全眞嬉, 定兼邦彦, 徳山豪:
"データ分布の近似を用いたエキスパート付き決定木構築", 日本応用数理学会, JSIAM05, 2005年9月.
概要: 本論文では，予測精度の高い決定木を構築するための手法の提案を行う．決定木を構成する際の問題点として過学習がある．学習データに対して最適な決定木を用いると，未知データに対する予測精度が落ちてしまうといったトレードオフが生じる．そのため決定木の枝刈りが必要となるが，どのように枝刈りを行えば最適であるかはわからない．予

測精度の高い決定木を生成するためには，学習データの分割をできるだけ小さな誤差で行い，そして適切な枝刈りを行うことが必要である．従来の数値データの 1 点分割手法は，分割時にデータの誤差問題がある．また，最適サポートルールの区間を用いた分割手法では，誤差の少ない区間分割は可能であるが，適切な枝刈りは困難である．本論文では，分割時の誤差をより小さくするために，数値データを最適ピラミッド近似を利用して整理し，構築されたピラミッドをエキスパートとして用いた，個々のデータに依存する柔軟な枝刈り手法を提案する．

2. 浅野哲夫, Jiri Matousek, 徳山豪:
“中立地帯を持ったボロノイ図に関する考察”, 情報処理学会アルゴリズム研究会, 巻号, 掲載ページ, 200 年 5 月.
概要: 中立地帯のあるボロノイ図の概念の提案を与える。従来のボロノイ図が空間の分割だったのに対し、中立地帯のあるボロノイ図では、空間内の母点に対応する領域は互いに隣接せず、様々なパターンの生成を可能にする。数学的な定義を与え、その存在性と幾何学的性質、及び構築アルゴリズムに関して議論する。

3. 関野剛永　徳山豪:
“ヨーロピアン・アジアンオプションの価格付けに関する近似的解法”, 電子情報通信学会 COMP 研究会, 105 － 344　COMP2005-46 , 13 － 18, 2005 年 10 月.
概要: アジアオプションの価格決定において、金利や株価のボラティリティーに変動があるモデルで理論保証のあるアルゴリズムを提案する

学会大会等

1. Akiko Suzuki, Takeshi Tokuyama:
“Approximation Algorithms for Computing a Highly Dense Subgraph”, Japan-Hungary Conference (Invited talk), 2005 年 6 月.

2. Akiko Suzuki, Takeshi Tokuyama:
“Dense Subgraph Problem Revisited”, Proceedings of 2005 Workshop on Randomness and Computation, 21-22, 2005 年 7 月.

3. Takeshi Tokuyama:
“Semi-Balanced Colorings of Graphs”, Proceedings of 2005 Workshop on Randomness and Computation, 23-24, 2005 年 7 月.

4. Takeshi Tokuyama:
“Distance Trisector and Voronoi Diagram with Neutral Zone”, NHC Workshop on Discrete Algorithms(Invited talk), 2006 年 3 月.

A03: 論理関数表現のモデルとシンボリックアルゴリズム

武永 康彦

電気通信大学 電気通信学部 情報工学科
〒 182-8585 調布市調布ヶ丘 1-5-1
takenaga@cs.uec.ac.jp

1 はじめに

分岐プログラムは有向グラフによる論理関数の表現法であり、古くから主に理論的研究が行われていた。近年になって、分岐プログラムに強い制限を加えた二分決定グラフ（OBDD：Ordered Binary Decision Diagram）と呼ばれる表現法が注目され、論理設計支援などの分野で論理関数の内部表現として多く用いられている。そのため、二分決定グラフや、それに類したいくつものモデルについて、論理関数の処理手法やその計算複雑さについて、理論・応用の両面から研究が盛んに行なわれるようになった。

二分決定グラフを用いたアルゴリズムは、基本的に、問題をすべて符号化して論理関数の形で表現し、二分決定グラフ上で論理関数処理を行うことによって問題を解くという形をとっている。このようなアルゴリズムはシンボリックアルゴリズムと呼ばれ、最近では、その実用性から従来広く利用されてきた論理設計支援の分野だけでなく、グラフアルゴリズムなどにおいてアルゴリズム理論の立場からも興味深いシンボリックアルゴリズムの研究が行われるようになりつつある。

本研究では、第一に、シンボリックアルゴリズムに関して、アルゴリズムの入力となる二分決定グラフやそれに類する論理関数表現による様々な問題の表現方法、具体的なアルゴリズムの設計と、その評価方法に関する研究を行なう。具体的な対象としては、まずはグラフ問題を中心に扱う。また、これらの研究成果をもとに、具体的なシンボリックグラフアルゴリズム、それに関連する一般的なグラフアルゴリズムの設計も行なう。

第二に、分岐プログラムや二分決定グラフなど、グラフによる論理関数の表現の基本的性質や複雑さに関する研究、論理関数のグラフ表現と他の表現との関連など、論理関数やその表現法そのものに関する研究を行なう。論理関数表現の基本的性質や複雑さに関する研究は、前述の入力データの二分決定グラフ表現の研究と密接に関連しており、その表現の複雑さを中心に研究を進める。また、グラフ表現と他の表現との関連については、論理関数の主項と二分木表現との対応をもとに定義された正論理関数のクラスである、tree-shellable 論理関数について研究を行う。

本年度は、具体的には以下の研究を行なった。まず、二分決定グラフ等によるグラフの表現およびシンボリックアルゴリズムに関する研究として、重みつきグラフの二分モーメントグラフを用いた表現方法について研究を行い、規則的な重みを持つグラフについて有効な場合があることを示した。また、基本的グラフ問題のアルゴリズムに関する研究として、比較可能グラフから k 本の辺を除いた、比較可能-ke グラフの頂点彩色問題について研究を行い、k が 1 の場合には多項式時間アルゴリズムが存在することを示し、比較可能グラフの制限つき彩色問題との関係を明らかにした。

グラフによる論理関数の表現については、論理関数の形に制限を加えた場合の (ordered) tree-shellable 論理関数の性質および、その判定問題の計算複雑さについて研究を行なった。各リテラルの出現回数が定数でおさえられる場合には、tree-shellable になる関数の積項数や分岐の深さに上限があることを明らかにし、これを用いて出現回数が定数の場合には多項式時間で判定可能であることを示した。また、各積項のリテラル数に制限がある場合については、リテラル数が最大 4 の場合に、ordered tree-shellable 論理関数の判定が NP 完全であることを示した。

これらの他に、本特定領域研究のミニ研究集会などを通じ、組合せゲーム・パズルについても研

究を行った。

以下の各章で、これらの研究成果について説明を行なう。

2 二分モーメントグラフを用いた重み付きグラフの表現

2.1 概論

Ordered Binary Decidion Diagram(OBDD)[1]とは論理関数の有向非巡回グラフによる表現法であり、多くの実用的な論理関数を効率的に表現でき、変数順序を決めれば関数の表現が一意に定まるなどの利点から、論理設計支援の分野を中心に広く用いられるようになっている。また、最近ではグラフアルゴリズムなど幅広い分野のシンボリックアルゴリズムについて理論的研究が行われるようになりつつある。

一方、OBDD を用いてさまざまな問題を解く中で、目的に応じて OBDD の定義を変化させたり拡張したものがいくつも考案されている。それらを用いると、特定の対象に対しては通常の OBDD を用いるより効率よい表現が可能になる。そのような表現法の 1 つに Binary Moment Diagram (BMD) がある。また、これを改良したものとして、multiplicative BMD (*BMD) が考案されている [2]。ここではこれらをまとめて二分モーメントグラフと呼ぶ。二分モーメントグラフは論理変数に対し整数値を返す関数を表現するためのデータ構造であり、特に乗算などの OBDD では効率的に表現できない算術演算を効率的に表現することができるという特長を持つ。

本研究では、この二分モーメントグラフを用いて重みつきのグラフを表現する方法について研究を行った。グラフを OBDD によって表現する場合には、グラフの頂点を二進数で符号化し、辺集合と頂点集合をその特性関数により表現する方法が用いられる。重みつきグラフについても重みの二進数表現を用いて同様に表現が可能である。このような表現により、特に、規則的な構造を持つグラフに対して、効率的な表現が可能であり、そのようなグラフに対して高速に動作するシンボリックアルゴリズムが設計可能であることが明らかにされつつある [8]。しかし、規則的な構造を持つ重みつきグラフにおいて、重みの与え方も規則的である場合には、二分モーメントグラフを用いることにより、より効率的な表現が可能な場合があると考えられる。そこで、二分モーメントグラフを用いた重みつきグラフの表現法を提案し、効率的な表現が可能なグラフの例を示した。

2.2 二分モーメントグラフ

二分モーメントグラフとは、$f : \{0,1\}^n \to Z$ となる関数を表す有向非巡回グラフである。基本的構造は OBDD と類似しているが、以下の点で異なる。

二分モーメントグラフは次のような関数の展開に基づいている。

$$f = f|_{x_i=0} + x_i(f|_{x_i=1} - f|_{x_i=0})$$

この式の $f|_{x_i=0}$ を定数モーメントと呼び、$f|_{x_i=1} - f|_{x_i=0}$ を線形モーメントと呼ぶ。x_i でラベル付けされた頂点の 0 枝は定数モーメントを指し、1 枝は線形モーメントを指す。そして、定数頂点は整数でラベル付けされている。二分モーメントグラフで与えられた関数の関数値は、開始頂点から変数の値に従って、値が 0 なら 0 枝、値が 1 なら 0 枝と 1 枝両方を辿り、到達した終端頂点のラベルの値の総和で与えられる。*BMD では各枝に重みを与えることができ、その枝を通る際には、枝の重みがその枝の指す頂点の値に掛けあわされる。

2.3 辺に重みの付いたグラフの表現

辺重み付きグラフを表現する方法として、まず頂点の組を入力とし、その 2 頂点間に辺があればその辺の重みを返す関数を用いたグラフ表現を考える。辺 $E \subseteq V \times V$ は、両端の頂点のビット列を並べた長さ $2l$ のビット列として符号化し、辺を符号化したビット列からその辺の重みを求める関数 $w(x,y)$ を二分モーメントグラフで表現する。このとき、辺の有無の区別がつけられるように、$(\forall (x,y) \in E)(w(x,y) < w_{up})$ となる定数 w_{up} を定義し、2 頂点間に辺があればその重みを返し、無ければ w_{up} を返す。

$|V| = n,\ |E| = m$ とし、頂点の重みが k ビットで表現可能な場合、OBDD を用いた通常の表

現のサイズは $O(m \log n + mk)$ となるのに対し、二分モーメントグラフで表したときは、辺の数にかかわらず $O(n^2)$ となる。

次に、辺の本数にかかわらず効率的に表現するために、二分モーメントグラフと OBDD を併用して表現する方法を提案する。辺を、2 頂点間に辺があれば 1 を返す OBDD と、辺を符号化したものからその辺の重みを求める*BMD で表現する。OBDD は、辺の重みを持たないグラフで辺の有無を与える OBDD と同じものである。辺を符号化したビット列からその辺の重みを求める関数 $w(x, y) \in \mathrm{Z}$ を二分モーメントグラフで表現する。この二分モーメントグラフは、辺を持たない頂点の組み合わせに対しても何らかの値を返す。

この表現の OBDD のサイズは $O(m \log n)$ となる。二分モーメントグラフのサイズは、一般的には $O(n^2)$ となり効率よく表現できないが、w が $|x| + |y|, |x| * |y|, 2^{|x|}$ 等の算術演算を用いて表される場合は $O(\log n)$, $|x|^2$ などを用いて表される場合は $O(\log^2 n)$ となる。

2.4 2 次元メッシュへの応用

二分モーメントグラフと OBDD を用いた表現が有効と考えられるグラフの例として、[8] でも取り上げられている 2 次元メッシュの各辺に、規則的な重みを付加したグラフを考える。このグラフに対して、辺の重みだけでなく、長さ k の経路の重みも二分モーメントグラフを用いて効率的に表現できることを示す。

2 次元メッシュのサイズは簡単のため $n \times n$ とし、$l = \lceil \log n \rceil$ とする。$x, y \in \{0,1\}^l, |x| = \sum_{i=0}^{l-1} 2^i x_i$ とする。頂点 V は、その位置の座標により $V = (x, y),\ 0 \le |x|, |y| < n$ で表される。辺は $((x, y), (x', y'))$ と表され、$(|x| = |x'|) \wedge (|y'| - |y| = 1)$ または、$(|y| = |y'|) \wedge (|x'| - |x| = 1)$ のとき $((x, y), (x', y')) \in E$ となる。また、ここでは辺 $((x, y), (x', y'))$ の重みを $w(x, y, x', y') = |x'||y'|$ と定義する。

経路に x 軸方向に向かう辺が含まれていれば 0、y 軸方向に向かう辺が含まれいるなら 1 となる変数を用意し、経路に含まれる順番に $(i_1, i_2, \ldots, i_k)$ とする。始点 (x, y) から長さ j の経路でたどり着く頂点を (x^j, y^j) とすると、経路の j 番目の辺の重さは、$w(x^{j-1}, y^{j-1}, x^j, y^j) = (x + (1 - i_1) + \cdots + (1 - i_j))(y + i_1 + \cdots + i_j)$ となる。

これをもとに、頂点 (x, y) を始点とする長さ k の経路の重さ $W(x, y, i_1, \cdots, i_k)$ を表す二分モーメントグラフを考える。変数順序を $(i_k, \ldots, i_1, x_0, \cdots, x_{l-1}, y_0, \cdots, y_{l-1})$ とすると、二分モーメントグラフのサイズは $O(kl + l^2)$ となることを示した。

3 比較可能-ke グラフの彩色問題

3.1 概論

一般の入力に対して NP 完全である問題への取り組みの 1 つとして、問題の入力の一部をパラメータとして特定の値 k に固定して、特定の k の値の元では容易に解けるかどうかを考えるアプローチがある。

本研究では、グラフの頂点彩色問題を扱う。頂点彩色問題は次で定義される。

Input: グラフ $G = (V, E)$、正の整数 $t \le |V|$

Question: G は t 彩色可能か。つまり、すべての G の辺 (u, v) に対して $f(u) \neq f(v)$ を満たす関数 $f : V \to \{1, 2, \ldots, t\}$ が存在するか。

t 彩色可能である t のうち最小のものを彩色数 $\chi(G)$ という。頂点彩色問題は彩色数を 3 に固定しても NP 完全である。

しかし、特定の性質を持つグラフだけを対象とした場合には、頂点彩色問題が多項式時間で解けることがある。このとき、そのグラフに「ある程度近い」グラフについても多項式時間で解ける可能性がある。

このように、あるグラフ族に近いグラフとして、ここでは以下のようなグラフ族を考える。$\mathcal{F}$ をあるグラフ族とすると、$\mathcal{F}$ グラフに辺を高々 k 本加えたグラフからなるグラフ族を $\mathcal{F}$+ke グラフ、$\mathcal{F}$ グラフから辺を高々 k 本取り除いたグラフからなるグラフ族を $\mathcal{F}$-ke グラフと呼ぶ。$\mathcal{F}$ - ke グラフ $G = (V, E)$ のモジュレータとは、$\mathcal{F}$ グラフから取り除かれた辺集合のことで、$\mathcal{F}$-ke グラフにモジュレータに含まれる辺を加えると $\mathcal{F}$ グラフが得られる。

一般に、頂点彩色問題が多項式時間で解けるグラフクラス $\mathcal{F}$ について、$\mathcal{F}$ が非隣接頂点の identification に関して閉じている場合、$\mathcal{F}$ + ke グラフの頂点彩色問題は固定パラメータ容易であり、$\mathcal{F}$ が辺の縮退に関して閉じている場合、$\mathcal{F}$ - ke グラフの頂点彩色問題は固定パラメータ容易であることが知られている [4]。

本研究では、比較可能+ke, -ke グラフの彩色問題について研究を行う。グラフ G が比較可能グラフであるとは、G の各無向辺を適当な方向の有向辺にしたときに、そのグラフが推移的グラフになるものが存在するときをいう [3]。ただし、推移的グラフとは辺 (u,v), (v,w) が存在するならば辺 (u,w) も存在するような有向グラフのことである。推移的グラフはハッセ図によって表すことができる。推移的グラフにおいて頂点 u から v への辺が存在するとき、$u \prec v$ と表す。

比較可能グラフに対しては頂点彩色問題が多項式時間で解けることが知られている [5]。しかし、上記の $\mathcal{F}$ + ke, -ke グラフの彩色問題が固定パラメータ容易となる条件はともに満たさない。これまでの研究により、比較可能+ke グラフの彩色問題は $k = 1$ の場合には多項式時間で解けるが、$k \leq 2$ に対しては NP 完全となることが明らかになっている。

そこで、今回は比較可能-ke グラフの頂点彩色問題について研究を行った。その結果、$k = 1$ の場合には多項式時間で解けることを明らかにした。また、彩色方法に簡単な制約を加えた、比較可能グラフの頂点彩色問題と比較可能-ke グラフの頂点彩色問題の関係を明らかにした。

3.2 比較可能-1e グラフの彩色問題

比較可能グラフ G において、その彩色数 $\chi(G)$ と、クリーク数（最大クリークのサイズ）$\omega(G)$ が同じであることが知られている。比較可能グラフを彩色する場合、それから得られる推移的グラフの頂点のレベル付けを行うことにより、色数最小の頂点彩色が得られる。推移的グラフ G の頂点 u, v について、辺 (u,v) が存在するとき $f(u) < f(v)$ を満たすような関数 $f : V \to \{1, 2, \ldots, \omega(G)\}$ を G のレベル付けといい、このとき $f(u)$ を u のレベルという。同じレベルの頂点を同じ色で彩色すれば、$\omega(G)$ 色での頂点彩色が得られる。

以下では、与えられた比較可能-1e グラフを G、G にモジュレータの辺 (a,b) を追加して得られる比較可能グラフを G_c とする。G においては、モジュレータの両端の頂点を同じ色で彩色することにより、G_c より少ない色数で彩色できる可能性がある。両者のクリーク数を比べた場合、G のクリーク数 $\omega(G)$ は $\omega(G_c)$ と同じか、あるいはそれより 1 少ないことは明らかであり、$\omega(G)$ がこのいずれになるかも容易に判定することができる。しかし、G は比較可能グラフとは限らないため、$\omega(G) = \omega(G_c) - 1$ であったとしても、クリーク数と同じ色数で彩色可能とは限らない。

この場合、まず彩色数を変えないグラフの変形を行なう。ハッセ図表現において頂点 w, x, y, z において辺 $(w,x), (y,x), (w,z)$ を持ち、w と x が同じ $(\omega(G_c) - 1)$-クリークに含まれるとき、ハッセ図において辺 (y,z) を付加する。この操作によって彩色数が増えないことから、上の条件を満たす頂点の組がなくなるまでこの操作を繰り返し、得られたグラフを G_+ とする。

ハッセ図においてモジュレータ (a,b) が a から b への有向辺となるとき、V_a, V_b をそれぞれ、G_+ のハッセ図において頂点 a からのパスを持つ頂点の集合、頂点 b へのパスを持つ頂点の集合とする。このとき、以下の補題が成り立つ。

Lemma 1 モジュレータの両端の頂点を同時に含まず、また全ての頂点が $V_a \cup V_b$ に含まれるような $(\omega(G_c) - 1)$-クリークが存在するとき、G_+ は $(\omega(G_c) - 1)$ 色で彩色可能である。

これらをまとめると、比較可能-ke グラフの彩色問題に対する以下の多項式時間アルゴリズムが得られる。

[アルゴリズム COLOR-1E]
入力: 比較可能-1e グラフ $G = (V, E)$, モジュレータ $E_1 = \{(a,b)\}$
出力: G の彩色数

1. $G_c = (V, E \cup E_1)$ の推移的な方向付けを求め (ハッセ図 $H = (V, E_H)$ により表現する)、$\chi(G_c)$ を計算する。

2. 新たな辺を追加できなくなるまで、以下の操作を繰り返す。
   以下の条件を満たす頂点の組 w, x, y, z を探す: w と x は G_c の同じ $(\omega(G_c)-1)$-クリークに属し、$(w,x),(y,x),(w,z)$ がすべて E_H に含まれる。そのような頂点の組があれば、辺 (y,z) を E_H に追加する。
   以上により得られたグラフを G_+ とする。

3. $V_a = \{v \mid a \prec v \text{ in } H_+\}$ および $V_b = \{v \mid v \prec b \text{ in } H_+\}$ を求める。

4. $V_a \cup V_b - \{a, b\}$ により誘導される H_+ の部分グラフを求める。

5. この誘導部分グラフが長さ $\chi(G_c)-1$ のパスを含めば $\chi(G_c)$ を、含まなければ $\chi(G_c)-1$ を出力する。

3.3 比較可能グラフの制限付き彩色問題との関係

パラメータ化グラフの彩色問題が、PRECOLORING 問題など、制限を加えた頂点彩色問題と密接な関係を持つ場合が多いことが明らかにされつつある。ここでは、頂点彩色問題に制限を加えた、以下の問題を考える。

PAIR COLORING
入力：グラフ $G = (V, E)$、頂点の対の集合 $P \subseteq V^2$ および正整数 k.
出力：各 $(u, v) \in P$ に対し、u, v を同じ色で彩色するとき、v は k 彩色可能か。

比較可能-ke グラフの彩色問題が、比較可能グラフの PAIR COLORING 問題に帰着可能であることを示した。ただし、この帰着はパラメータ化帰着ではないため、パラメータ化計算量に関する結果を得ることはできない。

4 Tree-Shellable 論理関数の性質と判定複雑さ

4.1 概論

論理関数の特性を理解し、明らかにすることは、計算機科学の様々な分野において重要なことである。積和形論理式 (Disjunctive Normal Form Boolean Formula：DNF) は、論理関数の代表的な表現法の 1 つである。それぞれの積項は論理関数の内項に相当し、特に主項は、論理関数の最小形を表すなど、非常に重要な概念である。特に、正論理関数は非冗長な積和形正論理式 (Positive DNF：PDNF) により一意に表現される。一方、二分決定木も論理関数のグラフによる表現法として広く用いられている。

Tree-shellable 論理関数 [7] とは、正論理関数において関数の主項とその関数を表す二分決定木の 1 ノードへたどるパスの数が等しい論理関数である。また、Ordered tree-shellable 論理関数は tree-shellable 論理関数の一種であり、関数を表す二分決定木が順序付き二分決定木となっているものである。論理関数 f が (oedered) tree-shellable であれば、f の双対関数 f^d を求めるのは容易であり、f の DNF 表現から f^d の非冗長な DNF 表現を多項式時間で求めることが可能である。また、各変数が 1 となる確率が与えられたとき、$f = 1$ となる確率を求める問題はある種のシステムの信頼性計算に対応しており、f が shellable であれば、この問題も容易に解くことができる。

Tree-shellable 論理関数の判定複雑さを明らかにし、また効率的に tree-shellability の判定が行える論理関数の条件を示すことが重要である。tree-shellable 論理関数、ordered tree-shellable 論理関数の判定問題の複雑さについては以下の結果が知られている。Tree-shellable 論理関数については、1 つの主項に含まれるリテラル数の最大値 k が定数の場合は多項式時間で判定可能である [6]。Ordered tree-shellable 論理関数に対しては判定問題は NP 完全であり、特に $k \geq 5$ のとき NP 完全である [9]。全ての項が 2 つの変数からなる quadratic 論理関数に対しては tree-shellable 論理関数は必ず ordered tree-shellalble 論理関数となり、多項式時間で判定可能である。

本研究では、各変数の出現回数に制限を加えた場合と積項の長さに制限を加えた場合の、tree-shellable 論理関数の性質や判定複雑さについて考察する。Union of Product 問題を、変数で表される各条件が満たされる確率からシステムの全体の信頼性を求める問題と考えると、前者は各条件が影響を及ぼすサブシステムの範囲が限られている

場合、後者は各サブシステムが正常に動作するための条件の数が限られている場合に対応する。

本研究では、第一に、積和形論理関数で表した場合の各リテラルの出現回数と関数の tree-shellability の関係について考察した。同一リテラルの出現回数が高々i回である tree-shellable 論理関数 f が tree-shellable であるためには、積項数が高々i^2 でなければならないことを示した。また、f が tree-shellable であることを示す二分木の分岐の深さについても明らかにした。第二に、積項の長さが制限された場合の ordered tree-shellable 論理関数の判定複雑さについて、$k = 4$ の ordered tree-shellable 論理関数判定問題は NP 完全であることを、3 集合打問題からの帰着によって示した。以下では、リテラルの出現回数を制限した場合について説明を行う。

4.2 Tree-Shellable 論理関数

二分決定木は論理関数を表す、ラベル付けされた木である。二分決定木の根ノードから値が 1 である葉ノードまでのパスを 1 パスと呼ぶ。特に、変数の全順序 π が存在し、二分木の全てのパスにおいて、現れる変数の順序が π に矛盾なく従っている場合、その二分木を順序付き二分決定木という。π を順序付き二分決定木の変数順序と呼ぶ。

Definition 1 [7] f は *PDNF* $f = \bigvee_{k=1}^{m} \bigwedge_{i \in I_k} x_i$ で表されているとする。f を表す *(*順序付き*)* 二分決定木で m 個の *1* パスを持つものが存在するとき、f は *(ordered) tree-shellable* であるという。

Theorem 1 [7] $f = \bigvee_{k=1}^{m} \bigwedge_{i \in I_k} x_i$ が *tree-shellable* であるとき、以下を満たす二分決定木 T を構成できる。

1. T は $P_1, \cdots, P_m$ の m 個の *1* パスを持つ。

2. 各々の $P_k (1 \leq k \leq m)$ は $i \in I_k \leftrightarrow x_i \in P_k$ を満たす項 I_k に対応する。

4.3 リテラルの出現回数を制限した場合の性質

非冗長な積和形論理式において、各リテラルの出現回数に制限を加えた tree-shellable 論理関数の判定複雑さについて考える。中心となる結果として、次の定理が示すように、リテラルの出現回数に制限がある場合、tree-shellable となる関数の積項数にも上限があることを示した。

Theorem 2 各リテラルの出現回数が高々i 回の *PDNF* で表される論理関数 f で、項を $i^2 + 1$ 個以上持つものは *tree-shellable* ではない。

リテラルの出現回数を高々i 回に制限すると、f が tree-shellable であることを示す f の二分決定木は根のラベル x_s を含む 1 パスを高々i 個しか持たない。また x_s を含む項 1 つに対して定理 1 の条件を満たす x_s を含まない項は高々$i - 1$ 個であることがわかる。よってこの場合、tree-shellable 論理関数の積項数は高々i^2 個となる。

この結果をもとに、tree-shellable となる二分木の根に選べる変数の条件や、i 回以上出現するリテラルが少数存在するときの tree-shellable 論理関数の積項数の上限についても明らかにした。

また、実際に各リテラルの出現回数が高々i 回かつ積項数が i^2 の PDNF で表される tree-shellable 論理関数が無数に存在することも明らかにした。つまり、i^2 は最適な値である。具体的には、以下にそのような関数の例を示す。A, B をそれぞれ変数の積とする。ただし A、B は共通の変数を含まず、また変数 $x_1, \cdots, x_{2i-2}$ も含まないものとする。$f = \sum_{j=2}^{i}(x_1 x_j + x_j B + \sum_{k=i+1}^{2i-2} x_j x_k) + \sum_{k=i+1}^{2i-2} A x_k + x_1 A + AB$ とする（ただし $i > 1$）。この f は図 2.1 の二分木で表される。ただし図の A、B と書かれている部分はそれぞれ A、B を表す二分決定木とする。

Tree-shellability の判定は、一般には、与えられた論理関数のすべての可能な木を調べることになる。その際、判定アルゴリズムの計算時間は木のどの深さまでパスの分岐があるかに依存する。i^2 個の項を持てば、分岐の深さは最大 $i^2 - 1$ となり得るが、関数が tree-shellable である場合には、このように大きな分岐の深さを持たないことがわかる。二分木の根ノードから、根ノードを含めて

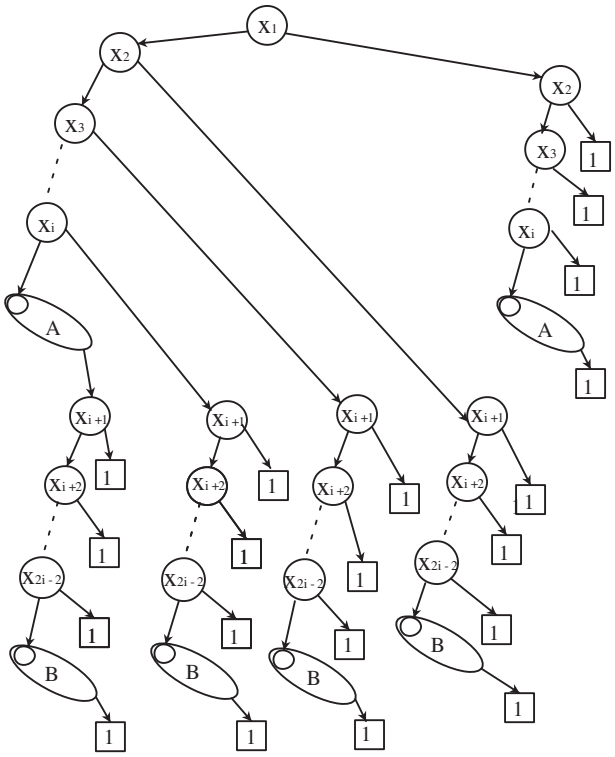


図 2.1: f が tree-shellable であることを示す二分木

0 枝のみで辿れるノードの列を street とすると、以下の結果が成り立つことを示した。

Theorem 3 各リテラルの出現回数が高々i 回の *PDNF* で表される *tree-shellable* 論理関数を f とすると、f が *tree-shellable* であることを示す二分決定木 T の *street* のノード数は $2i-1$ 以下である。

長さ $2i-1$ の street を持つ関数も存在するため、この値も最適であることがわかる。

この結果を判定アルゴリズムに適用すると、関数が tree-shellable 論理関数であるかどうかは $O(n^{4i-1}i^5)$、また関数が ordered tree-shellable 論理関数であるかどうかは $O(n^{3i}i^5)$ で判定可能であることがわかる。したがって、各リテラルの出現回数が定数であれば、多項式時間で (ordered) tree-shellable であるかどうかが判定可能となる。特に、多項式の次数も i に関して線形となり、効率的に判定が可能であることがわかる。

参考文献

[1] R.E. Bryant, “Graph-Based Algorithms for Boolean Function Manipulation”, IEEE Trans. Comput. Vol.C-35, No.8 (1986).

[2] R.E. Bryant and Y.A. Chen, “Verification of arithmetic circuits with binary moment diagram” In Proc. 32nd ACM/IEEE Design Automation Conference, 535-541, 1995.

[3] M.C. Golumbic, *A*lgorithmic Graph Theory and Perfect Graphs 2nd Ed., Elsevier, 2004.

[4] Leizhen Cai, “Parameterized Complexity of Vertex Colouring”, Discrete Applied Mathematics, 127, No.3, 415-429, 2003.

[5] Grotschel, M., Lovasz, L. and Schrijver, A., “Polynomial Algorithms for Perfect Graphs.”, Annals of Discrete Mathematics, 21, 325-356, 1984.

[6] Y.Takenaga, “Complexity of Recognizing Tree-Shellable Functions” 信学技報 COMP2001-62, 71-77, 2001.

[7] Y. Takenaga, K. Nakajima and S. Yajima, “Tree-Shellability of Boolean Functions”, Theoret. Comput. Sci. 262, 633-647, 2001.

[8] P. Woelfel, “Symbolic Topological Sorting with OBDDs”, Mathematical Foundations of Computer Science 2003, LNCS 2747, 671-680, 2003.

[9] E. Boros, Y. Crama, O. Ekin, P. L. Hammer, T. Ibaraki and A. Kogan, Boolean Normal Forms, Shellability and Reliability Computations, SIAM J. Discrete Mathematics, vol.13, no.2, 212-226, 2000.

研究業績一覧

学術論文

1. 東出賢一, 武永康彦:
“比較可能+ke グラフの彩色問題”, 京都大学

数理解析研究所講究録, 1426, 153–158, 2005 年 4 月.
概要: 一般には NP 完全である頂点彩色問題は、比較可能グラフに対しては多項式時間で解くことができる。そのため、比較可能グラフに近いグラフについても多項式時間で解ける可能性がある。本論文では、比較可能グラフに辺を k 本加えた比較可能 $+ke$ グラフを考える。まず、比較可能 $+1e$ グラフの彩色問題が多項式時間で解けることを示す。次に、3SAT 問題からの帰着により、比較可能 $+2e$ グラフの彩色問題が NP 完全であることを示す。

2. Yasuhiko Takenaga:
"Coloring Comparability-ke Graphs", 京都大学数理解析研究所講究録, (掲載予定).
概要: $\mathcal{F}+k$e and $\mathcal{F}$-ke graphs are classes of graphs close to graphs in a graph class $\mathcal{F}$. They are the classes of graphs obtained by adding or deleting at most k edges from a graph in F. In this paper, we consider vertex coloring of comparability$-k$e graphs. We prove that vertex coloring of comparability-1e graphs is solved in polynomial time. We also show that vertex coloring of comparability$-k$e graphs is closely related with vertex coloring of comparability graphs with restrictions that some pairs of vertices must have the same color.

3. 松金輝久、武永康彦:
"組合せ最適化問題としてのぷよぷよの連鎖数判定問題", 電子情報通信学会論文誌, Vol.J89-D, No.3, 405–413, 2006 年 3 月.
概要: ゲームやパズルの計算量や解法に関する研究は古くから行われている。特に最近ではテトリスのようなゲームが注目を集めている。本論文では、対戦型ゲームとして広く知られるぷよぷよを、入力として初期盤面と落下してくるピース列が与えられ、ピースを落下させることにより特定の目的を達成するパズルゲームとして定式化し、その連鎖数判定問題を考える。連鎖はぷよぷよにおける特徴的な性質であり、最大の連鎖を発生させる連鎖数判定問題が NP 完全であることを証明する。

研究会等

1. 加藤木直, 武永康彦:
"リテラルの出現回数に制限を加えた関数の tree-shellablity 判定問題", 電子情報通信学会技術研究報告, COMP2005-12, 25–30, 2005 年 5 月.
概要: Tree-shellable 論理関数とは、根のノードから 1 にラベル付けされた葉ノードへのパスの数が、主項の数と同じになるような二分木表現を持つ正論理関数である。本稿では、積和形論理式で与えられた関数中の同一変数の出現回数と tree-shellability に関する性質を明らかにする。またそれを用い、リテラルの出現回数に制限を加えた場合の、(ordered) tree-shellable であるか否かを判定する問題の複雑さ明らかにする。本稿のアルゴリズムにより、同一リテラルの出現回数が高々定数の場合、tree-shellable 論理関数、ordered tree-shellable 論理関数の判定がともに多項式時間で実行できる。

2. 加藤木直, 武永康彦:
"種々の制限を加えた ree-shellable 論理関数判定問題の複雑さ", 電子情報通信学会技術研究報告, COMP2005-67, 31–37, 2006 年 3 月.
概要: Tree-shellable 論理関数とは、根のノードから 1 にラベル付けされた葉ノードへのパスの数が、主項の数と同じようになるような二分決定木表現をもつ正論理関数である。また二分決定木が順序付きであるならば、ordered tree-shellable 論理関数であるという。本稿では、関数内の積項に含まれるリテラルの最大数が 4 以上の場合、ordered tree-shellable 論理関数判定問題は NP 完全問題であることを明らかにする。また同一変数の出現回数に制限を加えた場合の (oredered) tree-shellable 論理関数判定問題の性質を明らかにし、その結果より (oredered) tree-shellable 論理関数判定問題の計算複雑さを明らかにする。

A04: 組み合わせ最適化における指数サイズ・多項式時間近傍の設計

玉木　久夫　　井口　幸洋

明治大学　理工学部　情報科学科
〒 214-8517 川崎市多摩区東三田 1-1-1
{tamaki,iguchi}@cs.meiji.ac.jp

1　はじめに

本課題では、組み合わせ最適化問題に対する指数サイズの近傍のアプローチをテーマにしている。おもに、次の３つの方向から研究を進めている。

(A) 一般的、基礎的な技法およびそのための理論

(B) 具体的な問題に対する近傍と解法の設計と実装

(C) 解法のハードウェア化ないし準ハードウェア化

(A) に関する活動については 2 節において、(B) に関する活動については 3 節において、(C) に関する活動 4 節において述べる。

2　技法の基礎

本研究では、近傍内最適化においてグラフやハイパーグラフの再帰的分割に基づいた動的計画法を基本的な技法として用いている。この目的のために、与えられたグラフに対して幅の小さい木分割 [5, 6] や分枝分割 [7] を効率的に求めることが重要になる。特にこの研究では、実装のしやすい動的計画法の基礎となる分枝分割を多用している。一般のグラフの場合には、最適の木分割や分枝分割を求める問題はＮＰ困難であるが、平面グラフの場合には、分枝分割を求める $O(n^4)$ 時間のアルゴリズムが知られていた [8]。昨年度の研究で、海外研究協力者である Qiangping Gu 教授と共にこの計算時間を $O(n^3)$ に改良することに成功した。今年度は、８月に同教授を明治大学に招き、また、３月には同教授を訪問して引き続き共同研究を行った。８月の議論は主に、木分割と分枝分割の関係に集中した。特に、最適な木分割が容易に求まる弦グラフのクラスに対して、分枝分割の多項式時間アルゴリズムの可能性を探った。また、３月の訪問では、上記の平面グラフ分枝分割アルゴリズムの論文のジャーナル版を完成し、また分枝分割および分枝幅アルゴリズムの効率的実装について検討した。これまでにも、分枝分割および分枝幅アルゴリズムの実装と実験を行ってきているが、この訪問で得られたいくつかのアイディアの有効性を、今後の実験により確認して行く予定である。なお、分枝分割アルゴリズムの実験においては、学部４年吉武由実の協力を得た。

2.1　弦グラフの分枝分割

弦グラフ（chordal graph) は、長さ４以上の閉路は必ず弦（閉路上で隣り合わない２頂点を結ぶ辺）を持つという性質を持ったグラフである。弦グラフにおいては、極大クリークの個数が高々n個であり、それらを容易に列挙することができる。また、最適な木分割を容易に構成することができる。しかしながら弦グラフの最適な分枝分割を求めるあるいは分枝幅（最適な分枝分割の幅）を決定する多項式時間アルゴリズムは知られていない。そこで、このテーマではそのような多項式時間アルゴリズムの可能性を検討した。

木分割と分枝分割の関係としては、Robertson と Seymour により、一般のグラフ G に対して、その木幅（最適な木分割の幅）$\mathrm{tw}(G)$ と、分枝幅 $\mathrm{bw}(G)$ の間には、$\mathrm{bw}(G) \leq \mathrm{tw}(G)+1 \leq \lfloor 3\mathrm{bw}(G)/2 \rfloor$ が成り立つことが示されている。左側の等号は完全グラフに対して、また右側の等号

は、$K_{n,n}$ からひとつの完全マッチングを取り除いたグラフに対して成り立つ。Hicks は、弦グラフでありかつ $\mathrm{tw}(G)+1 = \lfloor 3\mathrm{bw}(G)/2 \rfloor$ が成り立つようなグラフ G の例を与えた。我々はこの例を一般化し、$\mathrm{tw}(G)+1$ と $2(\mathrm{tw}(G)+1)/3$ の間の任意の整数値に対して、$\mathrm{bw}(G)$ がその値をとるような弦グラフの例を構成した。

下の証明では、Robertson と Seymour によるタングルの概念と定理を用いる。

定義 1 グラフ G に対する位数 k のタングルとは、G の辺集合の集合 $A \subseteq 2^{E(G)}$ で、次の条件を満たもののことを言う。

1. $E(G)$ の 2 分割 (E_1, E_2) で、幅が k 以下である（E_1 と E_2 の共有頂点集合の大きさが k 以下である）ような任意のものに対して、E_1 か E_2 のどちらか一方は A に属す。
2. すべての $e \in E(G)$ に対して、$\{e\}$ は A に属す。
3. A のどの 3 要素 E_1、E_2、E_3 をとっても、$E_1 \cup E_2 \cup E_3$ は $E(G)$ と等しくない。

定理 1 *(Robertson と Seymour)* グラフ G に対する位数 k のタングルが存在することと $\mathrm{bw}(G) > k$ は同値である。

$m \le n \le 2m$ を満たす正整数 n、m に対して $H_{n,m}$ を次のように定義する。

1. $H_{n,m}$ の頂点集合は $\{1, \ldots, n\}$ である。
2. $H_{n,m}$ の辺集合は、$\{\{i,j\} \mid 1 \le i < j \le m\} \cup \{\{i,j\} \mid 1 \le i \le m, m < j \le n, i \ne j\}$ である。

上記の Hicks の例は、$H_{2m,m}$ に相当する。

定理 2 $\mathrm{bw}(H_{n,m}) = \min\{m, \lceil 2n/3 \rceil\}$

証明: $H_{n,m}$ は、$n-m+1$ 個のクリーク $\{1, \ldots, n\}$, $\{1, \ldots, n\} \cup \{i+m\} \setminus \{i\}$, $1 \le i \le n-m$, に分解される。第一のクリークを親とし、残りのクリークをその直接の子とする木分割の幅は $n-1$ である。従って、$\mathrm{bw}(H_{n,n}) \le \mathrm{tw}(H_{n,m}) + 1 \le n$ が成り立つ。また、完全グラフ K_n に対して幅 $\lceil 2n/3 \rceil$ の分枝分割が知られているので、$\mathrm{bw}(H_{n,n}) \le \lceil 2n/3 \rceil$ も成り立つ。次に $\mathrm{bw}(H_{n,m}) \ge \min\{m, \lceil 2n/3 \rceil\}$ であることを示す。k を $2 \le k < \min\min\{m, \lceil 2n/3 \rceil\}$ なる任意の正整数として位数 k のタングルを構成すれば、定理 1 より目的は達せられる。共有頂点集合が C、$|C| \le k$ であるような $E(G)$ 任意の 2 分割 (E_1, E_2) において、C が $\{1, \ldots, n\}$ を包含しないことより、E_1 か E_2 のどちらか一方は必ず G の C によって誘導される部分グラフに完全に包含される。そのような一方を我々のタングル A に含めるこにする。明らかに、A はすべての単元集合を含む。また、条件 $k < \lceil 2n/3 \rceil$ より、A がタングルの 3 番目の条件も満たすことを示すことができる。[]

また、上で目標とした一般の問題への一歩として、「与えられたグラフ G が、その最大クリークサイズ $\omega(G)$ より真に小さい分枝幅を持つか」という決定問題を考えた。アルゴリズムのアプローチと、NP 完全性の証明のアプローチをともにいくつも考案して試みたが解決に至っていない。

2.2 平面グラフの分枝分割

昨年度開発した、$O(n^3)$ 時間の平面グラフ分枝分割アルゴリズムを、卒業研究生の協力により実装した。約５００頂点程度までの例題について実験し、Seymour と Thomas によるもとのアルゴリズムより高速であることを確認した。その他に、理論的な解析は難しい、いくつかの改善技法の実験を行い、効果のあることを確認した。

実験規模が小さいのは、これらのアルゴリズムの使用している、分枝幅決定アルゴリズムのメモリ消費量が大きいことに主に起因している。現在、このメモリ消費量を抑える実装を検討している。$O(n^2)$ の作業領域を必要とするデータの使用にはある程度局所性があることがわかったので、キャッシュを用いることにより、実行時間の極端な増大をきたすことなくメモリ消費量を抑えることが可能ではないかと期待している。来年度は、このアプローチを実装して、数万頂点の例題に対しても実行できるようにしたい。

3 具体的な問題

3.1 巡回セールスマン問題

平面巡回セールスマン問題における無効辺の除去

巡回セールスマン問題（TSP) のベンチマークインスタンスの多くは、平面上のユークリッド距離に基づくものである。これを平面 TSP と呼ぶことにする。一方我々の技法は、グラフ上の TSP に対して特化している。平面 TSP インスタンスからグラフ上の TSP インスタンスを得るために、これまでは主に、他の手法で良い巡回路を多数得て、それらを併合したグラフを用いて来た。我々は他の手法に頼らずに、もとの平面 TSP インスタンスから、最終的な解に至るまででのすべての過程を巨大近傍アプローチによって構成することを目指している。そのための最初のステップとして、最適性を損なわずに平面インスタンスから平面グラフインスタンスに変換する方法を開発して来た。ふたつの頂点を結ぶ辺のうち、直観的に決して最適な巡回路に含まれることがないと思われるものが多数あるが、この直観を裏付けるための十分な理論は文献に見当たらない。かなり多くの場合に当てはまる、下の定理を証明した。2 点 p, q の距離を $d(p,q)$ で表す。

定理 3 平面上の有限点集合 S が与えられたとする。S 中の相異なる 4 点 p, q, t_1, t_2 が次の条件を満たすならば、辺 pq は、S に対する最適巡回路に決して含まれることはない。この条件の記述において、c は十分大きな普遍的定数である。

1. 線分 pq と線分 t_1t_2 は交差する。
2. 線分 pq と線分 t_1t_2 の交点を r とおくと、$d(p,r)) \geq cd(t_1,t_2)$ かつ $d(q,r)) \geq cd(t_1,t_2)$
3. 線分 t_1t_2 を線分 pq に射影した結果の線分の長さを h, t_i、$i = 1,2$、と線分 pq との距離を v_i とおく。このとき、直線 pq に関して t_1 と同じ側にあるどの点 $s \neq t_1$ に対しても $d(t_1,s) > \max\{h, v_1\}$ が成り立つ。また、直線 pq に関して t_2 と同じ側にあるどの点 $s \neq t_2$ に対しても $d(t_2,s) > \max\{h, v_2\}$ が成り立つ。

証明:（概略）最適な巡回路 T を固定する。T が辺 pq を含むと仮定して矛盾を導く。T は、点 p の直後に q を訪れると仮定する。一般に p_1、p_2、q_1、q_2 が相異なる S の点であり、T が p_1 の直後に p_2 を訪れ、q_1 の直後に q_2 を訪れるとき、「p_1 の直後に q_1 を訪れ、その後 T と逆の順に点をたどって p_2 にいたり、次に q_2 から T と同じ順に点をたどって p_1 に至る」という巡回路を、$\mathrm{flip}(T, p_1, p_2, q_1, q_2)$ と呼ぶことにする。

t_i から pq に降ろした垂線の足を f_i とするとき、一般性を失うことなく、f_1 の方が f_2 よりも p に近いか、または f_1 と f_2 は等しいと仮定する。T において t_1 の直前の点を s_1、t_2 の直後の点を s_2 とおく。T の最適性より、線分 pq は線分 s_1t_1 とも線分 t_2s_2 とも交差しない。また、有向直線 s_1t_1 と、有向直線 pq のなす角を 0 と π の間で表した値は $\frac{2}{3}\pi$ 以上である。もしそうでなければ、$\mathrm{flip}(T, p, q, s_1, t_1)$ の長さは T より短く、T の最適性に矛盾する。（ここで、c が十分に大きいことと、条件 $d(t_1,s) > v_1$ を用いる。）同様に、有向直線 t_2s_2 と、有向直線 pq のなす角を 0 と π の間で表した値は $\frac{2}{3}\pi$ 以上である。T から 3 辺 pq、s_1t_1、t_2s_2 を取り除いたときにできる 3 つの経路のうち、q を始点とするものを P_1、p を終点とするものを P_2、残りのひとつを P_3 と呼ぶことにする。P_1、P_2、および P_3 の逆転をつなげてできる巡回路が T よりも短い。（ここでは、c が十分に大きいことと、条件 $d(t_i,s) > h$、および上で示した角度の条件を用いる。）[]

平面グラフ TSP に対する解法エンジンの実装

平面グラフ TSP に対する動的計画法アルゴリズムは、既に本研究の開始時点で試験的な実装を持っていたが、解放エンジンとして配布できるパッケージの作成を目指している。今年度は、その基本的な部分が完成した。その過程のなかで、下で述べる技法上の改良を発見し、実験を行った。なお、解法エンジンの実装と下記手法の開発においては、修士課程 1 年土屋裕樹の協力を得た。

平面グラフ TSP に対する動的計画法の表管理

平面グラフ TSP に対する動的計画法アルゴリズムでは、動的計画法の表をどのように管理するかが重要なポインタになる。今年度の研究では、以下に述べるような改良を発見した。

平面グラフ TSP の、グラフ分割に基づいた動的計画法に現れる部分問題は、次のように定義される、非交差マッチングによって表現される。

定義 2 有限集合 V 上の マッチングとは、V 上の

非順序対（無向辺）の集合 M でグラフ (V, M) における各頂点の次数がちょうど 1 であるようなもののことを言う。全順序集合 $V = \{v_1 < v_2 < v_3 < \cdots < v_n\}$ 上の マッチング M が非交差であるとは、V のどのような 4 要素 v_i 、v_j 、v_k 、v_h、$i < j < k < h$ に対しても M が $\{v_i, v_k\}$ と $\{v_j, v_h\}$ の両方を持つことはないことを言う。

定義 3 M_1 を $U = \{u_1 < u_2 < \cdots, u_n\}$ 上の非交差マッチング M_2 を $V = \{v_1 < v2 < \cdots, v_m\}$ 上の非交差マッチングとするとき、$0 \leq k \leq \min(n, m)$ なる整数 k に対して、グラフ $G(M_1, M_2, k)$ を、頂点集合が $U \cup V \setminus \{v_1, v_2, \ldots v_k\}$ であり、辺集合が $M_1 \cup \{\{f(v_i), f(v_j)\} \mid (v_i, v_j) \in M_2\}$ であるようなグラフとして定義する。ただし、関数 f は、$1 \leq i \leq k$ に対しては $f(v_i) = u_i$, $k < i \leq m$ に対しては $f(v_i) = v_i$ によって定義される。

$G(M_1, M_2, k)$ の各連結成分は経路か閉路であることに注意する。

定義 4 M_1 を $U = \{u_1 < u_2 < \cdots, u_n\}$ 上の非交差マッチング M_2 を $V = \{v_1 < v2 < \cdots, v_m\}$ 上の非交差マッチングとするとき、M_1 と M_2 が k-貼り付け可能であるとは、$G(M_1, M_2, k)$ が閉路を持たないか、あるいはただひとつの閉路だけからなることを言う。後者は $m = n = k$ のときにのみ起こりうる。M_1 と M_2 が k-貼り付け可能であるとき、$\mathrm{paste}_k(M_1, M_2)$ によって $G(M_1, M_2, k)$ の経路を辺とみなして得られる $\{u_n < u_{n-1} < \ldots < u_{k+1} < v_{k+1} < \ldots < v_{m-1} < v_m\}$ 上のマッチングを表す。

$2n$ 個の頂点集合上の非交差マッチングは、n 組の括弧からなる wfp （well-formed parenthesis) によって表現される。W_n によって n 組の括弧からなる wfp 全体からなる集合を表す。$p \in W_m$ が非交差マッチング M_p を表し、$q \in W_n$ が非交差マッチング M_q を表を表すとき、$\mathrm{paste}_k(M_p, M_q)$ を表現する W_{m+n-k} の要素を $\mathrm{paste}_k(p, q)$ と表す。

定義 5 $2n$ 次の *DP* 表とは、W_n から非負実数への写像を言う。t_1 が $2m$ 次の *DP* 表、t_2 が $2n$ 次の *DP* 表であるとき、t_1 と t_2 の k-合成とは、$2(m+n-k)$ 次 の *DP* 表 t でありそのエントリは、各 $p \in W_{m+n-k}$ に対して

$$t[p] = \min\{t_1[q] + t_2[r] \mid q \in W_m, r \in W_n, p = \mathrm{paste}_k(q, r))\}$$

によって定義される。

DP 表の合成を素朴に行った場合、W_m と W_n に関する 2 重ループを実行することになり、時間は C_n をカタラン数として、$O(C_m C_n)$ を要することになる。この合成操作を、2 段階に分けて効率的に実行する次のような手法を開発した。

定義 6 p、q を *well-formed* とは限らない任意の括弧列とするとき、$p + q$ で p と q の連結を表し、$\mathrm{pref}_k(p)$ によって p の長さ k の接頭辞を、$\mathrm{suf}_k(p)$ によって p の長さ k の接尾辞を表す。$\mathrm{rv}(p)$ によって、p のなかの括弧の順番と同時に括弧の向きを反転してできる括弧列を表す。また、$\mathrm{lp}(p)$ によって、p の中にある開き括弧の個数、$\mathrm{rp}(p)$ によって、p の中にある閉じ括弧の個数を表す。また、$\mathrm{open}(k)$ によって k 個の開き括弧からなる括弧列を、$\mathrm{close}(k)$ によって k 個の閉じ括弧からなる括弧列を表す。最後に、$\mathrm{trim}_k(p)$ によって、$\mathrm{pref}_k(p) + \mathrm{close}(\mathrm{lp}(\mathrm{pref}_k(p)) - \mathrm{rp}(\mathrm{pref}_k(p)))$ を表す。

定義 7 $p + \mathrm{close}(i)$ が W_m に属す括弧列であり、q が W_n に属す括弧列であると仮定する。このとき、$\mathrm{lftPlug}(p, q)$ によって、p の開き括弧のなかで対応する閉じ括弧のないものを $\mathrm{pref}_i(q)$ の要素で置き換えてできる列の後に $\mathrm{suf}_{n-i}(q)$ をつなげてできる括弧列を表す。また。$\mathrm{rgtPlug}(p, q)$ によって $\mathrm{rv}(\mathrm{lftPlug}(reverse(q), reverse(p))$ を表す。

定理 4

$$\begin{aligned}
&\mathrm{paste}_k(p, q) \\
&= \mathrm{lftPlug}(\mathrm{pref}_{m-k}(\mathrm{rv}(p)), \mathrm{paste}_k(\mathrm{trim}_k(p), q)) \\
&= \mathrm{lftPlug}(\mathrm{pref}_{m-k}(\mathrm{rv}(p)), \\
&\quad \mathrm{rgtPlug}(\mathrm{paste}_k(\mathrm{trim}_k(p), \mathrm{trim}_k(q))), \\
&\quad \mathrm{suf}_{n-k}(q)))
\end{aligned}$$

この定理を用いて、DP 表の合成を 2 段階で行うことができる。各 $p \in W_{m+n-k}$

に対して、$t[p]$ の定義式の右辺は、$\min\{t_1[q]] + t_2[q] \mid q \in W_m, r \in W_n, p = \mathrm{lftPlug}(\mathrm{pref}_{m-k}(\mathrm{rv}(q)), \mathrm{paste}_k(\mathrm{trim}_k(q), r))\}$ と表すことができる。ここで、$\mathrm{trim}_k(q) = s$ と $\mathrm{paste}_k(trim_k(q), r)) = u$ を固定すると t_2 の表エントリのみに基づいて、一部の最適化が可能であることに注目する。各 $s \in \{\mathrm{trim}_k(q) \mid q \in W_m\}$ と $u \in W_h$ に対して $a[s,u]$ を $\min\{t_2[r] \mid r \in W_n, u = \mathrm{paste}_k(s,r)\}$ によって定義すると、$t[p]$ の値は、$\min\{t_q[q] + a[s,u] \mid q \in W_m, s = \mathrm{trim}_k(q), p = \mathrm{lftPlug}(\mathrm{pref}_{m-k}(\mathrm{rv}(q)), u\}$ によって表すことができる。$a[s,u]$ の計算は表 t_2 のみに基づいているため、全体の表アクセス回数の削減が期待できる。実際、予備的に行った実験においては、m, n の値を２０程度まで大きくした場合に、１５パーセント程度の高速化が得られることを確認した。

3.2 クリーク被覆問題

論理回路のテストパターン圧縮への応用の見地からクリーク被覆問題の解法を研究した。実際のテストパターン圧縮においては、純粋なクリーク被覆問題として扱うのではなく、付加的な回路情報を用いて高度の圧縮を目指すことが多い。この研究の意義は、回路情報を用いずに、テストパターンそのものだけを見て圧縮する方法の限界を明確に示すことであると考えて、厳密解のアルゴリズムを中心に研究した。その過程で、極大クリークの列挙が必要になったために、文献から得たアルゴリズムを実装した。これらのアルゴリズムの実装、実験においては、学部４年八木澤圭の協力を得た。また、下で述べるように、極大クリークの列挙の効率を改善する試みも行った。

3.3 極大クリークの列挙

極大クリークの列挙のアルゴリズムは築山らによる遅延時間 $O(n^3)$ のものが古くから知られているが、最近牧野と宇野によって遅延時間 $O(n^{2.376})$ に改良された [4]。我々は、木分割に基づいた効率化が可能ではないかと考えて、そのアプローチを検討した。どのクリークも必ず木分割のあるひとつのノードに所属するので、この方向は有望に思われた。現状では、木分割は用いないが、計算量が木幅を用いて表される次のような結果を得ている。

定理 5 与えれらたグラフ G の頂点数を n、辺の数を m、最大次数を d、クリーク数 *(*最大クリークの大きさ*)* を ω、木幅を w、極大クリークの個数を M とするとき、G のすべての極大クリークを $O(m \log n + M\omega(\omega d + (\min\{d, w\})^{2.376}))$ 時間で列挙することができる。

アルゴリズムは次のような単純なアイディアに基づく。$V(G)$ 上の全順序 $<$ を固定したとき、頂点 v の前方近傍 $\Gamma^+(v)$ を v の隣接点 u で $v < u$ なるものの集合とする。アルゴリズムは、各 v に対して $G[\Gamma^+(v)]$ の極大クリークを列挙し、得られた各クリーク K について、もし K のすべての頂点と隣接する v より小さい頂点が存在しなければ、$K \cup \{v\}$ を出力する。出力の有無にかかわらず列挙されるクリークの総数はたかだか ωM である。また、これらのクリークひとつひとつの列挙に要する時間は、前方近傍の大きさの最大値を d^+ とするとき、$O((d^+)^{2.376})$ である。列挙されたクリークを出力すべきかどうかのテストは、$O(\omega d)$ 時間で行うことができる。最後に、d^+ を最小化する全順序は、貪欲法により $O(m \log n)$ 時間で求めることができる。明らかに $d^+ \leq d$ であり、最小化された d^+ は G の木幅以下であることは、G の最適木分割に基づく三角化グラフの完全除去順序を考えれば自明である。

3.4 集合被覆問題

集合被覆問題はさまざまな組み合わせ最適化問題へ応用される重要な問題である。巨大近傍アプローチの前段階として、柳浦らによる３反転近傍のアルゴリズム [9] を学部４年平川宗則の協力を得て実装した。論文で報告された実装と比べて幾分性能が劣るものとなっているが、今後巨大近傍を取り入れて実験をしていく基礎としては十分と考えている。

4 ハードウェア化の検討とツールの準備

大規模な組合せ問題を解く専用ハードウェアは，シミュレーションによる評価だけでなく，実際にシステムを構築し稼動する予定である．これを限られた予算内で行うために，我々は，パーソナルコンピュータにハイエンドの FPGA (Field Programmable Gate Array) を搭載したボードを組込み，その上にシステムを載せることにした．

LUT (Look-Up Table) を直列多段に接続することで所望の論理回路が LUT カスケード法として提案されているが [1]，これを FPGA 内部の組込みメモリを用いて実装するツールの開発と実際の応用例として FIR フィルタの実装に用いて性能評価を行った [2].

また，高速な演算を FPGA で実現可能かどうかを確認するために Walsh 変換の専用ハードウェアを実現することで Pentium M 上で C 言語で記述したソフトウェア実現に比較して 1000 倍以上高速になることも確認している [3].

これらのハードウェアの記述には，Verilog-HDL を用いている．これを直に記述する手間とバグが混入する可能性が高くなるので，仕様から直に Verilog-HDL 記述を生成するようなソフトウェアツールの開発も行い実際に使用している．この場合，仕様をメニューなどで与えて，開発したツールを用いて Verilog-HDL 記述を生成し，最後に FPGA 開発システムで論理合成・配置配線を行い，実装することになる．これと並行して，一度，Verilog-HDL を生成するのではなく，C 言語で動作を記述することで EDIF と呼ばれるネットリストに直接論理合成するシステムを購入し，性能評価を現在行いシステムの実装の準備を進めている．

参考文献

[1] Y. Iguchi, T. Sasao, and M. Matsuura , ”Realization of multiple-output functions by reconfigurable cascades, ” International Conference on Computer Design :VLSI in Computers & Processors (ICCD-2001), Austin, TX, Sept. 23-26, 2001. pp. 388-393.

[2] T. Sasao, Y. Iguchi, and T. Suzuki, “On LUT cascade realizations of FIR filters,” *DSD2005, 8th Euromicro Conference on Digital System Design: Architectures, Methods and Tools*, Porto, Portugal, Aug. 30 - Sept. 3, 2005, pp.467-474.

[3] Y. Iguchi and T. Sasao, ”Hardware to compute Walsh coefficients,” ISMVL-2005, pp.75-81.

[4] K. Makino and T. Uno, New Algorithms for Enumerating All Maximal Cliques, Prod. SWAT 2004, LNCS 3111, 260-272, 2004.

[5] N. Robertson and P.D. Seymour, Graph minors I. Excluding a forest, Journal of Combinatorial Theory, Series B, 35: 39-61, 1983

[6] N. Robertson and P.D. Seymour, Graph minors. II. Algorithmic aspects of tree-width, Journal of Algorithms, 7: 309-322, 1986

[7] N. Robertson and P.D. Seymour, Graph minors. X. Obstructions to tree-decomposition, Journal of Combinatorial Theory, Series B, 52: 153-190, 1991

[8] P.D. Seymour and R. Thomas, Call Routing and the Ratcatcher. Combinatorica, 14(2), 217-241, 1994

[9] M. Yagiura and M. Kishida and T. Ibaraki, A 3-flip Neighborhood Local Search for the Set Covering Problem, manuscript, 2003.

研究業績一覧

学術論文

1. H. Qin, T. Sasao, and Y. Iguchi:
“An FPGA design of AES encryption circuit with 128-bit keys”, Proc. of GLSVLSI 2005, pp.147–151, April 17, 2005.
概要: This paper addresses a pipelined partial rolling (PPR) architecture for the AES encryption. The key technique

is the PPR architecture, which is suitable for FPGA implementation. Using the proposed architecture on the Altera Stratix EP1S20F780C5 FPGA, the AES-4SM achieves a throughput of 5.61 Gbps by using 20 M4Ks, and the AES-8SM achieves a throughput of 10.49 Gbps by using 40 M4Ks. Compared with the unrolling implementation that achieves a throughput of 20.48 Gbps by using 80 M4Ks on the same FPGA, implementations with the PPR architecture reduce the amount of memory up to 75(i.e., throughput divided by the size of memory for core) up to 9.6and rolling architectures, and fits on less expensive FPGAs.

2. K. Nakamura, T. Sasao, M. Matsuura, K. Tanaka, K. Yoshizumi, H. Qin, and Y. Iguchi:
"Programmable logic device with an 8-stage cascade of 64K-bit asynchronous SRAMs", Proc. of Cool Chips VIII, IEEE Symposium on Low-Power and High-Speed Chips, April 20, 2005.
概要: The first implementation of a new programmable logic device using LUT(Look-Up Table) cascade architecture is developed in 0.35um CMOS logic process. Eight 64Kb asynchronous SRAMs are simply connected to form an LUT cascade with a few additional circuits. Benchmark results show that it has a competitive performance to FPGAs.

3. Y. Iguchi and T. Sasao:
"Hardware to compute Walsh coefficients", Proc.of ISMVL-2005, pp. 75–81, May 19, 2005.
概要: This paper presents a method to compute a fragment of the Walsh coefficients of logic functions using hardware. First, it introduces the Walsh transformation tree, and shows a method to compute Walsh coefficients using the Walsh transformation tree. Next, it shows the hardware realization for the Walsh tree. The amount of hardware to compute a coefficient and the entire coefficients are O(2n) and O(n2・2n), respectively. FPGA implementations show their feasibility up to n = 14. The FPGA realization is at least 1253 times faster than a software implementation on a microprocessor for n = 14.

4. T. Sasao, Y. Iguchi, and T. Suzuki:
"On LUT cascade realizations of FIR filters", Proc. of 8th Euromicro Conference on Digital System Design: Architectures, Methods and Tools, pp. 467–474, Aug. 30, 2005.
概要: This paper first defines the n-input q-outputWS function, as a mathematical model of the combinational part of the distributed arithmetic of a finite impulse response (FIR) filter. Then, it shows a method to realize theWS function by an LUT cascade with k-input q-output cells. Furthermore, it 1) shows that LUT cascade realizations require much smaller memory than the single ROM realizations; 2) presents new design method for a WS function by arithmetic decomposition, and 3) shows design results of FIR filters using FPGAs with embedded memories.

5. T. Sasao, Y. Iguchi, and M. Matsuura:
"LUT cascades and emulators for realizations of logic functions", RM2005, pp. 63–70, Sept. 5, 2005.
概要: Two types of programmable logic devices using LUTs (Look-Up Tables) are presented. An LUT cascade directly implements logic functions by a series connection of LUTs, while an emulator emulates an LUT cascade by sequentially accessing LUTs. The LUT cascade is faster, but has a limited logic capability, while the emulator is slower, but has a higher logic capability. LUT cascades and emulators can be directly generated from the BDDs of tar-

get functions. Their performances are easy to estimate. The C-measure that show the complexity of LUT cascades are also presented. Functions with small C-measures have efficient LUT cascade and emulator realizations. Classes of functions that are suitable for LUT cascade and emulator realizations are also presented.

6. Qiangping Gu, Hisao Tamaki:
"Optimal branch-decomposition of planar graphs in $O(n^3)$ time", Proc. 32nd International Conference on Automata, Languages, and Programming, LNCS 3580, 373-384, 2005 年 7 月.
概要: n 頂点の平面グラフ G が与えられたとき、G の分枝分割で幅が最小であるようなものを求める $O(n^3)$ 時間のアルゴリズムを与える。これはこれまでの最良の Seymour と Thomas による $O(n^4)$ 時間アルゴリズムを改良するものである。

研究会等

1. 笹尾勤, 井口幸洋, 鈴木隆広:
"FIR フィルタの算術分解を用いた LUT カスケードによる実現", 電子情報通信学会 リコンフィギャラブルシステム研究会, 2005 年 9 月 15 日.
概要: FIR フィルタの分散演算の組合せ論理回路の数学モデルとして n 入力 m 出力 WS 関数を定義する. 次に WS 関数を k 入力 q 出力のセルを用いた LUT カスケードで実現する方法を示す. 更に, 次の 3 点を明らかにする：(1) 単一の ROM で実現する場合に比べ, LUT カスケードを用いた実現は, 必要メモリ量を大幅に削減できる. (2) 算術分解を用いて WS 関数を実現する新しい方法を提案する. (3) FIR フィルタを組込みメモリを用いて FPGA 上に実現した結果を示す.

A05: ハードウェアアルゴリズムの性能評価に関する研究

高木 直史　高木 一義

名古屋大学 大学院 情報科学研究科
〒 464-8603 名古屋市千種区不老町
{ntakagi,ktakagi}@is.nagoya-u.ac.jp

1　はじめに

集積回路技術の進展に伴い、これまでソフトウェアでは実現できなかった高度の実時間処理を、専用回路を構成して実現することが可能になってきている。すなわち、専用回路を構成することにより、処理時間に関わる計算限界を打破することが可能となってきている。このような専用回路を開発する場合、並列処理による高速計算や集積回路化に適した規則正しい回路構造等を意識した、ハードウェア実現向きのアルゴリズム、すなわち、「ハードウェアアルゴリズム」を設計することが重要である。

ハードウェアアルゴリズムの性能は、従来、アルゴリズムに基づく回路の、組合せ回路モデル上での段数や素子数、VLSI モデル上での面積等で評価してきた。しかし、集積回路技術の進展に伴い、これらのモデルおよび評価基準は、現実に即さなくなってきている。たとえば、回路の微細化に伴い、論理素子間を結ぶ配線における遅延が論理素子における遅延に対して無視できなくなってきており、回路の段数のみで計算時間を見積もることができなくなってきている。また、携帯機器等に用いられる回路の重要な性能要件である消費電力を見積もるための評価基準が定められていない。

本研究は、ハードウェアアルゴリズムの性能の、より現実に即した評価基準の確立を目的としている。具体的には、配線遅延や消費電力の評価を可能とする回路モデルを定め、配線遅延を考慮した計算時間の評価基準、および、消費電力の評価基準を確立することを目指している。

平成 17 年度は、前年度に提案した乗算および除算の新しいハードウェアアルゴリズムを含む、算術演算のためのいくつかのハードウェアアルゴリズムについて、これらに基づく回路の設計を行い、シミュレーションによる評価を行った。また、このうち乗算器については、詳細設計を行い、現在ＬＳＩを試作中である。さらに、これまでの回路設計資産および新たに設計した回路について、回路の性質と回路シミュレーション上の性能を分析し、最新技術の諸側面を反映した新しい回路モデルを構築すべく検討を行った。また、情報セキュリティの向上に不可欠な公開鍵暗号で用いられる、大きな整数を法とする乗算剰余算について、並列計算を可能とする画期的な計算法を開発した。具体的には、以下の研究を行った。

1. 前年度に提案した Karatsuba の方法に基づく新しいアルゴリズムに基づく乗算器の詳細設計を行った。現在、ＬＳＩを試作中である。

2. 前年度に提案した冗長２進表現の絶対値計算を用いた新しいハードウェアアルゴリズムに基づく整数除算器を設計し、回路設計支援ソフトウェアを用いて論理合成と配置配線を行い、スタンダードセル方式のＬＳＩ上に実現した場合の計算時間および面積の評価を行い、市販の演算器ＩＰライブラリ中の整数除算器と比較した。

3. 前年度に開始した、算術演算のための減算シフト型ハードウェアアルゴリズムの自動合成システムの開発を進めた。

4. 暗号処理で用いられる乗算剰余算について、並列処理を可能にした、二分乗算剰余算法と呼ぶ、新しいハードウェアアルゴリズムを開発した。

以下、これらの研究の詳細を述べる。

2 Karatsubaの方法に基づく乗算器の設計

スタンダードセル方式のVLSIにおいては、配線層数の増加により配線の複雑化による面積の増加量が小さくなり、セルの総面積が回路面積に直接反映されるようになってきた。

本研究では、昨年度、多倍長乗算のソフトウェア実装においてしばしば用いられるKaratsubaの方法[1]に基づく、配線が複雑であるが素子数の少ない乗算器を設計し、小面積の並列乗算器が実現可能であることを示した[2]。今年度は、この乗算器の詳細設計を行った。現在、ＬＳＩを試作中である。

2.1 Karatsubaの方法に基づく並列乗算器

Nビット符号なし2進整数の乗算について考える。被乗数Xと乗数Yを上位$k_H = \lceil N/2 \rceil$ビットと下位$k_L = \lfloor N/2 \rfloor$ビットにわけ、それぞれ$X_H, X_L, Y_H, Y_L$と表す（$X = 2^{k_L}X_H + X_L, Y = 2^{k_L}Y_H + Y_L$）。これらを用いて積$XY$を表すと、$XY = 2^{2k_L}X_HY_H + 2^{k_L}(X_HY_L + X_LY_H) + X_LY_L = 2^{2k_L}P_1 + 2^{k_L}(P_3 - P_1 - P_2) + P_2$となる。ここに$P_1 = X_HY_H$、$P_2 = X_LY_L$、$P_3 = (X_H + X_L)(Y_H + Y_L)$である。

Karatsubaの方法では、上式に従いP_1, P_2, P_3を計算する約$N/2$ビットの乗算3回と、加算、減算、シフトでNビットの乗算を行う。本研究ではアルゴリズムを再帰的に適用せず、一度だけ適用した乗算器を設計する。一般的な並列乗算器はおよそN^2個の全加算器が必要であるが、Karatsuba乗算器では$N/2$ビットの乗算3回におよそ$\frac{3}{4}N^2$個の全加算器ですむため、素子数が少なくなる。

2.2 乗算器の詳細設計

32ビット符号なし整数乗算器の詳細設計を行った。P_1とP_2の計算に配列型乗算器、P_3の計算にDadda乗算器を用いた。P_3を求める際に桁上げ伝搬加算器を使用せず、P_3の部分積とP_1、P_2をともに足し合わせるようにした。

乗算器をVerilog-HDLで記述し、論理合成を行い、さらに配置配線を行った。現在、東京大学大規模集積システム設計教育センター（ＶＤＥＣ）を通して、ローム$0.18\mu m$ ＣＭＯＳプロセスでＬＳＩを試作中である。

3 冗長２進表現の絶対値計算を用いた整数除算のハードウェアアルゴリズムの評価

整数除算は、基本算術演算の一つであり、いくつかの整数除算器が市販のＩＰライブラリに登録されている[3]。整数除算は、プロセッサにおいて多くのクロックサイクルを要する演算であり、サイクル数は演算数の値によって可変となる。

本研究では、昨年度、冗長2進表現の絶対値計算を用いた整数除算のハードウェアアルゴリズムを提案した[4]。今年度は、このハードウェアアルゴリズムに基づく整数除算器を設計し、回路設計支援ソフトウェアを用いて論理合成と配置配線を行い、スタンダードセル方式のＬＳＩ上に実現した場合の計算時間および面積を見積ることにより、アルゴリズムの評価を行った[5]。

3.1 整数除算のハードウェアアルゴリズム

nビット2の補数表示2進整数である被除数Xと除数Y $(\neq 0)$から、$X = Y \times Z + R$を満す、nビット2の補数表示2進整数の商Zと剰余Rを求めるものとする。ただし、RはXと同じ符号になるようにする。

提案アルゴリズムは、基数2の非回復型整数除算法に基づいている。商の各桁q_jは部分剰余R_{j+1}の符号から決定する。構造の規則性を増すために、途中で 部分剰余が0となっても$q_j = 1$として計算を続ける。数列$\hat{R}_j = sign(R_{j+1}) \cdot R_j$を導入し、$\hat{R}_j$を冗長2進表現（基数2の符号付きディジット表現）で表す。定義より、$|\hat{R}_j| = |R_j|$、
$sign(\hat{R}_j) = sign(R_{j+1}) \cdot sign(R_j)$ $(R_j \neq 0)$、
$sign(\hat{R}_j) = +1$ $(R_j = 0)$
が成り立つ。よって、元のR_jの符号は、
$sign(R_j) = sign(R_{j+1}) \cdot sign(\hat{R}_j)$ $(R_j \neq 0)$、
$sign(R_j) = +1$ $(R_j = 0)$
となる。$sign(R_{j+1}) = -1$のとき$R_j = R_{j+1} + 2^j \cdot D$、他のとき$R_j = R_{j+1} - 2^j \cdot D$であるから、

$\hat{R}_j = |\hat{R}_{j+1}| - 2^j \cdot D$ である。ただし、$D = |Y|$ である。この計算は、桁上げの伝搬なしに高速に行う。$|\hat{R}_{j+1}|$ は、$\hat{R}_{j+1}$ を最上位桁から順に調べることにより、上位桁から順に求めることができる。したがって、$\hat{R}_j$ は $sign(R_{j+1})$ と独立に計算できる。すなわち、$\hat{R}_j$ と $|\hat{R}_j|$ の計算を $R_{j+1}(\hat{R}_{j+1})$ の符号がわかる前に開始でき、漸化式の繰返し計算を高速に行うことができる。

アルゴリズムに基づく除算器の組合せ回路モデル上での段数は演算数の長さに比例し、素子数は演算数の長さの平方に比例する。また、ＶＬＳＩモデル上での面積は演算数の長さの平方に比例する。

3.2 ハードウェアアルゴリズムの評価

アルゴリズムに基づく整数除算器をいくつか設計した。これらを Verilog-HDL で記述し、Synopsys Design Compiler により論理合成を行った。また、Synopsys 社の DesignWare ＩＰライブラリ [3] の整数除算器を同様に合成した。スタンダードセルのライブラリとして、東京大学大規模集積システム設計教育センター（ＶＤＥＣ）提供のローム 0.35μm CMOS の京大 3.3V 高速版を用いた。

表１ (a) と (b) に、32 ビット整数除算器のセル面積、遅延、クロックサイクル数、計算時間（遅延×サイクル数）の見積りを示す。表 (a) 中の「$k = 2$」および「$k = 4$」はそれぞれ、内部でクロックサイクル毎に商の２および４ビット分ずつ計算を行う順序回路実現を示し、「comb」は組合せ回路実現を示している。表 (b) 中の「div_seq」は順序回路の除算器で、「div (rpl)」と「div (cla)」はそれぞれ加算器として順次桁上げ加算器と桁上げ先見加算器を用いた組合せ回路の除算器である。

表 2.1: 32 ビット除算器の見積り

(a) 提案除算器

divider	area $[mm^2]$	delay $[ns]$	#cycle	time $[ns]$
$k = 2$	0.69	4.67	21	98.07
$k = 4$	0.91	7.74	11	85.14
comb.	4.33	77.54	1	77.54

(b) Synopsys DesignWare の除算器

divider	area $[mm^2]$	delay $[ns]$	#cycle	time $[ns]$
div_seq	0.28	8.20	16	131.20
	0.39	13.40	8	107.20
div (rpl)	0.65	246.20	1	246.20
div (cla)	1.49	65.42	1	65.42

4 算術演算のための減算シフト型ハードウェアアルゴリズムの自動合成システムの開発

プロセッサ等の開発において、種々の信号処理やコンピュータグラフィックス等のために、より高い演算性能を実現するためには、処理に頻出し、時間のかかる算術演算のための専用回路を開発することが有効であると考えられる。このような演算の例として、平方根の逆数計算や立方根計算等が挙げられる。

本研究では、昨年度に、算術演算のための減算シフト型ハードウェアアルゴリズム [6] の自動合成システムを構想し [7]、その開発に着手した。今年度は、このシステムの開発を進めた [8]。

4.1 システムの概要

アルゴリズムの自動合成システム全体としては、以下の機能を実現する必要がある。

1. 算術式から漸化式を生成する部分
2. 漸化式や基数、桁集合などからある程度の自由度を持つ桁選択関数を出力する部分
3. いくつかの実現方法の中から用途に応じてよい実現方法を選ぶ部分

本年度は、２について、いくつかの自由度を持つ桁選択関数を出力するツールの構築を行った。今回構築したツールは、設計に手間がかかる桁選択関数の生成を支援することを目的としており、桁選択関数の大まかな見積りを得るための利用を想定している。具体的には、桁選択関数の生成において、桁 s_{j+1} として k を選んでもよい $rW[j]$ の下限 $L_k[j]$ 及び上限 $U_k[j]$ から、桁選択関数の生成に必要なパラメータの値を決定する処理を行

う。桁選択関数の実現方法はテーブルによる実現と仮定する。本ツールは、除算、開平、平方根の逆数計算、立方根計算のアルゴリズムのための桁選択関数の生成に適用できる。

以降、$L_k[j]$ 及び $U_k[j]$ に含まれる各変数（オペランド、中間結果、中間変数）の個数を l とし、各変数を $P_1[j], P_2[j], \cdots P_l[j]$ と表す。

4.2 桁選択関数生成ツールの入出力

本ツールでは、入力として、$L_k[j]$ 及び $U_k[j]$ の式、$W[j]$ の満たすべき範囲の下限 $\underline{B}[j]$ 及び上限 $\overline{B}[j]$ の式、$W[j]$ の表現方法、各 $P_i[j](i = 1, 2, \cdots, l)$ の範囲の下限 $\underline{P_i}[j]$ 及び上限 $\overline{P_i}[j]$、各 $P_i[j]$ の表現方法、基数 r の値、桁集合の最大の要素 a の値、反復回数 j の初期値、$l+2$ 個の出力パラメータ（後述）の探索範囲の上限を与える。

$L_k[j]$、$U_k[j]$、$\underline{B}[j]$、$\overline{B}[j]$ の式は、基数 r の一般形で与える。$W[j]$ 及び各 $P_i[j]$ の表現方法については、非冗長表現か桁上げ保存形のどちらかを与える。$P_i[j]$ は全て符号なしで表現され、正の範囲をとるものとする。$P_i[j]$ の範囲が j や他の変数などに依存する場合も考えられるが、今回のツールではこれらに依存しない実数として $\underline{P_i}[j]$ 及び $\overline{P_i}[j]$ を与えるものとする。r は 2 のべきとし、a は $\frac{r}{2} \leq a \leq r-1$ を満たす正の整数であるとする。

このとき、桁選択関数の設定に必要な以下のパラメータの値を決定する。

- 共通の桁選択関数が設定可能な反復回数の下限 J
- その関数の入力に必要な $rW[j]$ の小数点以下のビット数 t、及び、$P_i[j]$ の小数点以下のビット数 $d_i(i = 1, 2, \cdots, l)$

これらはトレードオフの関係にあり、いくつかの取り得る値の組合せが存在する。ここでは、J の値と桁選択関数の入力ビット数の和の関係に着目し、以下の組合せを求める。

- 取り得る最小の J に対し、桁選択関数への入力ビット数の和が最小となる組合せ
- 取り得る最小の入力ビット数の和に対し、J の値が最小となる組合せ

また、これらの組合せに対する、選択の境界となる値 $m_k(k = -a+1, \cdots, -1, 0, 1, \cdots, a)$ の下限及び上限を求める。

4.3 桁選択関数生成ツールの処理手順

まず、$l+2$ 個のパラメータ J, t, d_i（$i = 1, 2, \cdots, l$）に対し、探索範囲の下限 $\underline{J}$、$\underline{t}$、$\underline{d_i}$ を設定する。$\underline{J}$ の値は反復回数 j の初期値である。$\underline{d_i}$ の値は $\underline{P_i}[j]$ 及び $\overline{P_i}[j]$ から適切に定める。$\underline{t}$ の値は $\underline{B}[j]$ 及び $\overline{B}[j]$ から、r 及び a の値などを考慮して適切に定める。

この探索範囲の中から、各パラメータにそれぞれある値を設定し、その値で桁選択関数が設定可能かどうか判定する処理 [ANALYSIS] を行う。この処理をパラメータの値を変化させて行う。その後、設定可能なパラメータの組合せの中から、前述の条件を満たす組合せを選ぶ。選ばれた各組合せに対し、パラメータの値及び選択の境界となる値 m_k の下限及び上限を出力する。

以降、処理 [ANALYSIS] について説明する。パラメータの値 J, t, d_i $(i = 1, \cdots, l)$ を与え、以下の手順により桁選択関数が設定可能かどうか判定する。

[Step 1]

各変数 $P_i[j]$ について、$\underline{P_i}[j]$ 及び $\overline{P_i}[j]$ から、取り得る全ての見積り値 $\widehat{P_i}[j]$（2^{-d_i} の倍数）を求める。ここで、取り得る見積り値がただ一つとなる場合は、その変数が桁選択関数の入力として不要であるということを表す。

[Step 2]

各変数について、取り得る $\widehat{P_i}[j]$ の中から一つを選び（c_i とする）、その値が見積り値となる $P_i[j]$ の最小値 $\underline{P_i}[j]_{c_i}$ 及び最大値 $\overline{P_i}[j]_{c_i}$ を定める。$P_i[j]$ が非冗長表現ならば、

$$\begin{aligned} \underline{P_i}[j]_{c_i} &= \max\{c_i, \underline{P_i}[j]\} \\ \overline{P_i}[j]_{c_i} &= \min\{c_i + 2^{-d_i}, \overline{P_i}[j]\} \end{aligned}$$

であり、$P_i[j]$ が桁上げ保存形ならば、

$$\begin{aligned} \underline{P_i}[j]_{c_i} &= \max\{c_i, \underline{P_i}[j]\} \\ \overline{P_i}[j]_{c_i} &= \min\{c_i + 2^{-d_i+1}, \overline{P_i}[j]\} \end{aligned}$$

である。

[Step 3]

各 k（$k = -a+1, \cdots, a$）について、$\underline{P_i}[j]_{c_i} \leq P_i[j] \leq \overline{P_i}[j]_{c_i}$ 及び $j \geq J$ としたときの、$L_k[j]$ の最大値 $\max(L_k[j])$ 及び $U_{k-1}[j]$ の最小値 $\min(U_{k-1}[j])$ を求める。

[Step 4]

各 k について、選択の境界 $m_k(\widehat{P}_i[j])$ の下限 $\underline{m_k}(\widehat{P}_i[j])$ 及び上限 $\overline{m_k}(\widehat{P}_i[j])$ を求め、値を比較する。$m_k(\widehat{P}_i[j])$ は 2^{-t} の倍数となる必要があるので、残余の表現方法が非冗長表現ならば、

$$\begin{aligned} \underline{m_k} &= 2^{-t}\lceil 2^t \max(L_k[j])\rceil \\ \overline{m_k} &= 2^{-t}\lfloor 2^t \min(U_{k-1}[j])\rfloor \end{aligned}$$

であり、桁上げ保存形ならば、

$$\begin{aligned} \underline{m_k} &= 2^{-t}\lceil 2^t \max(L_k[j])\rceil \\ \overline{m_k} &= 2^{-t}\lfloor 2^t (\min(U_{k-1}[j]) - 2^{-t})\rfloor \end{aligned}$$

である。$\underline{m_k} > \overline{m_k}$ となる場合が一つでもあれば、与えたパラメータの値では桁選択関数を設定することができない。

[Step 5]

取り得る見積り値の全ての組合せに対して、[Step 2] から [Step 4] を行う。

[Step 6]

以上のステップにおいて、設定不可とならなければ、与えたパラメータの値で桁選択関数を設定できる。

上述のツールをC言語により実装した。

5 二分乗算剰余算法

乗算剰余算は、暗号処理に用いられる基本的な演算である。ＲＳＡ等の公開鍵暗号システムで必要な剰余系指数計算は、非常に大きな整数を法とする乗算剰余算の繰返しにより実現されている。

本研究では、乗算剰余算の並列処理を可能にした、二分乗算剰余算法と呼ぶ、新しい計算法を提案する [9]。

この計算法では、剰余系の乗算をＫＴ剰余という体系で行う。法 M は基数 r で n 桁の整数とし、$r^{n-1} < M < r^n$ および $\gcd(M, r) = 1$ を満たすものとする。U を $[0, M-1]$ の範囲の整数とするとき、U のイメージ（ＫＴ剰余）X を $X = U \cdot r^{\alpha n} \bmod M$ と定義する。ここに α は、$0 < \alpha < 1$ で、αn が整数となるような有理数である。

これらイメージの集合はＫＴ剰余系と呼ぶ剰余系を形成する。二つのイメージ X と Y が与えられたとき、ＫＴ剰余系における M を法とする乗算を、

$$X * Y = X \cdot Y \cdot r^{-\alpha n} \bmod M$$

と定義する。$r^{\alpha n}$ と M が互いに素であれば、$r^{-\alpha n} \bmod M$ は必ず存在する。暗号においては、M は奇数であるから、$r = 2^k$ とすれば、互いに素であるという条件が満たされる。

整数の元の表現から新しい剰余系への変換は、その整数と定数 $r^{\alpha n}$ との通常の乗算剰余算により行える。新しい剰余系から元の表現への逆変換は、イメージと定数 $r^{-\alpha n}$ との乗算剰余算で行え、モンゴメリアルゴリズムにより計算できる。

元の整数集合 Z_M とその上で定義された通常の乗算剰余算と、ＫＴ剰余系 Z'_M とその上で定義された演算 $*$ との間には、同型の関係が成り立つ。

提案する計算法では、乗数を二つの部分に分け、並列に処理する。すなわち、ＫＴ剰余系におけるイメージ X と Y の M を法とする乗算は、乗数 Y を $Y = Y_H \cdot r^{\alpha n} + Y_L$ となるように Y_H と Y_L の二つの部分に分けると、以下の式により、効率よく計算できる。

$$\begin{aligned} X * Y = (&X \cdot Y_H \bmod M \\ &+ X \cdot Y_L \cdot r^{-\alpha n} \bmod M) \bmod M \end{aligned}$$

$X \cdot Y_H \bmod M$ の項はインターリーブ法等、通常の乗算剰余算アルゴリズムにより計算でき、$X \cdot Y_L \cdot r^{-\alpha n} \bmod M$ の項はモンゴメリアルゴリズム [10] により計算できる。分割後の演算数 Y_H と Y_L は Y より短いので、$X \cdot Y_H \bmod M$ および $X \cdot Y_L \cdot r^{-\alpha n} \bmod M$ の計算は、それぞれ、分割しない演算数で通常の乗算剰余算あるいはモンゴメリ乗算を行う場合に比べ、高速に行える。

この二つの計算がほぼ同じ計算速度で行え、乗数を同じ大きさの二つの部分に分割すれば、分割しない演算数に対してそれぞれのアルゴリズムを単独で用いる場合に比べ、理論的に最大二倍の高速化が可能である。さらに、モンゴメリ法に比べ、元の剰余系とＫＴ剰余系との間の変換が最大二倍高速になり、変換に必要な定数の事前計算も不要

になる。

提案手法では、中で行う通常の乗算剰余算およびモンゴメリ乗算の計算がどのようなアルゴリズムで実現されても構わない。さまざまなアルゴリズムを組合せることが可能であり、また、それぞれを高速化する方法が、独立に適用可能である。二つの計算の速度が異なる場合は、分割の割合 α を調節すればよい。例えば、後者が前者より２倍高速であれば、$\alpha \approx \frac{2}{3}$ とすればよい。

本手法は、ハードウェアばかりでなく、マルチプロッセ環境でソフトウェアで実現することもできる。

さらに、部分積の生成は独立に並列に行い、累算は統合して行うことも可能である。これをパイプライン化したハードウェアアルゴリズムも提案している [11]。

6　まとめ

前年度に提案した Karatsuba アルゴリズムに基づく新しいハードウェアアルゴリズムに基づく乗算器、および、冗長２進表現の絶対値計算を用いた新しいハードウェアアルゴリズムに基づく整数除算器の設計を行い、シミュレーションによる評価を行った。このうち乗算器については、詳細設計を行い、現在ＬＳＩを試作中である。これらから得られた回路データを解析し、ハードウェアアルゴリズムの性能の、より現実に即した評価基準の確立を目指して、研究を進めている。

今年度は、さらに、前年度に開始した、算術演算のための減算シフト型ハードウェアアルゴリズムの自動合成システムの開発を進めるとともに、情報セキュリティの向上に不可欠な公開鍵暗号で用いられる、大きな整数を法とする乗算剰余算について、並列計算を可能とする画期的な計算法を開発した。

参考文献

[1] A. Karatsuba and Yu. Ofman: ‘Multiplication of multidigit numbers on automata,’ Sov. Phys. Dokl., 7, pp.595-596, 1963.

[2] 柴岡雅之，高木直史，高木一義：「Karatsuba アルゴリズムに基づく小面積並列乗算器」，2005 年電子情報通信学会総合大会，A-3-1，2005 年３月．

[3] Synopsys Inc.: ‘DesignWare Building Block IP,’ 2003.

[4] 門脇俊介，高木直史，高木一義：「冗長２進数の絶対値計算を用いた整数除算回路」，信学技報，VLD2004-3，2004 年５月．

[5] N. Takagi, S. Kadowaki, K. Takagi: ‘A hardware algorithm for integer division,’ Proc. 17th IEEE Symposium on Computer Arithmetic, pp. 140–146, June 2005.

[6] M.D. Ercegovac and T. Lang, Division and Square Root – Digit-Recurrence Algorithms and Implementations, Kluwer Academic Publishers, 1994.

[7] 熊澤文雄，高木直史：「算術演算のための減算シフト型ハードウェアアルゴリズムの自動合成」，信学技報，VLD2004-90，2004 年 12 月．

[8] 熊澤文雄，高木直史：「算術演算のための減算シフト型ハードウェアアルゴリズムの自動合成ツールの構築」，情報処理学会ＤＡシンポジウム 2005 論文集，231〜236 頁，2005 年８月．

[9] M. E. Kaihara, N. Takagi: ‘Bipartite modular multiplication,’ Springer LNCS 3659: Proc. 7th International Workshop on Cryptographic Hardware and Embedded Systems - CHES 2005, pp. 201–210, August 2005.

[10] P. L. Montgomery: ‘Modular multiplication without trial division,’ Mathematics of Computation, vol. 44, no. 170, pp. 519–521, April 1985.

[11] M. E. Kaihara, N. Takagi: ‘Pipelined bipartite modular multiplication,’ 信学会技報，VLD2005-67，2005 年 12 月

研究業績一覧

学術論文

1. N. Takagi, S. Kadowaki, K. Takagi:
"A hardware algorithm for integer division", Proceedings of the 17th IEEE Symposium on Computer Arithmetic, pp. 140–146, June, 2005.
概要: A hardware algorithm for integer division is proposed. It is based on the digit-recurrence, non-restoring division algorithm. Fast computation is achieved by the use of the radix-2 signed-digit representation. The algorithm does not require normalization of the divisor, and hence, does not require area-consuming leading one (or zero) detection nor shifts of variable-amount. Combinational (unfolded) implementation of the algorithm yields a regularly structured array divider, where pipelining is possible for increasing the throughput. Sequential implementation yields a compact divider.

2. M. E. Kaihara, N. Takagi:
"Bipartite modular multiplication", Springer LNCS3659: Proceedings of 7th International Workshop on Cryptographic Hardware and Embedded Systems - CHES 2005, pp. 201–210, August, 2005.
概要: This paper proposes a new fast method for calculating modular multiplication. The calculation is performed using a new representation of residue classes modulo M that enables the splitting of the multiplier into two parts. These two parts are then processed separately, in parallel, potentially doubling the calculation speed. The upper part and the lower part of the multiplier are processed using the interleaved modular multiplication algorithm and the Montgomery algorithm, respectively. Conversions back and forth between the original integer set and the new residue system can be performed at speeds up to twice that of the Montgomery method without the need for precomputed constants. This new method is suitable for both hardware implementation and software implementationin a multiprocessor environment. Although this paper focusing on the application of the new method in the integer field, the technique used to speed up the calculation can also easily be adapted for operation in the binary extended field $GF(2^m)$.

3. M. E. Kaihara, N. Takagi:
"A hardware algorithm for modular multiplication/division based on the extended Euclidean algorithm", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E88-A, No. 12, pp. 3610–3617, December, 2005.
概要: A hardware algorithm for modular multiplication/division which performs modular division, Montgomery multiplication, and ordinary modular multiplication is proposed. The modular division in our algorithm is based on the extended Euclidean algorithm. We employ our newly proposed computation method that consists of processing the multiplier from the most significant digit first to calculate Montgomery multiplication. Finally, the ordinary modular multiplication is based on shift-and-add multiplication. Each of these three operations is carried out through the iteration of simple operations such as shifts and additions/subtractions. To avoid carry propagation in all additions and subtractions, the radix-2 signed-digit representation is employed. A modular multiplier/divider based on the algorithm has a linear array structure with a bit-slice feature and carries out n-bit modular multiplication/division in $O(n)$ clock cycles, where the length of the clock cycle is constant and independent of n. This multiplier/divider can be implemented us-

ing a hardware amount only slightly larger than that of the modular divider.

研究会等

1. 熊澤文雄，高木直史:
“算術演算のための減算シフト型ハードウェアアルゴリズムの自動合成ツールの構築”, 情報処理学会 DA シンポジウム 2005 論文集, pp. 231–236, 2005 年 8 月.
概要: プロセッサ等の開発において、より高い演算性能を実現するためには、頻出する算術演算のための専用回路を開発することが有効であると考えられる。本報告では、以前示した考察に基づく、算術演算の専用回路のための減算シフト型ハードウェアアルゴリズムの自動合成ツールについて述べる。本報告で説明するツールは、減算シフト型アルゴリズムのための桁選択関数の生成を支援する。漸化式から導出される選択領域、基数、桁集合などを与え、アルゴリズムの性能の見積りを基に桁選択関数の生成に必要なさまざまなパラメータを決定する。

2. カイハラ マルセロ，高木直史:
“Pipelined bipartite modular multiplication”, 電子情報通信学会技術研究報告, VLD2005-67, pp. 37–42, 2005 年 12 月.
概要: We propose a fast hardware algorithm for calculating modular multiplication. The algorithm is based on the recently proposed bipartite modular multiplication method. The calculation of modular multiplication is performed in the KT-residue system which enables the splitting of the multiplier into two parts which can then be processed in parallel. In the hardware algorithm that we propose, the addition of the partial products to the intermediate accumulated product is pipelined in order to reduce the critical path delay. A radix-4 version of the hardware algorithm is given and its hardware implementation is discussed.

A06: 幾何的配置問題の計算量限界と近似可能性の研究

加藤 直樹　大崎 純　瀧澤 重志

京都大学 大学院 工学研究科
〒 615-8540 京都市西京区京都大学桂 C クラスター
{naoki,ohsaki,kukure}@archi.kyoto-u.ac.jp

1　はじめに

建築におけるトラス構造物の最適設計問題や，都市工学における通路，道路，鉄道などの配置問題および道路網などにおける配送問題は，数理的にはユークリッド幾何構造の上での最適化問題として特徴付けられる。また，これらの問題の多くは，実現可能な解集合を考慮すると本質的に離散構造を有する。たとえば，建築構造物の設計では，実現できる部材長や部材断面積は，あらかじめ与えられたサイズ集合から選択されるのが望ましい。通路，道路の配置問題，配送問題でも実現可能な幾何学的単位は限定される。本研究では，これらの問題を幾何的配置問題としてモデル化し，個々の問題の計算量限界を明らかにするとともに，離散組合せ手法や計算幾何学を用いて実用的に解ける近似アルゴリズムの開発することにより近似可能性について解析をおこなう。今年度において得られた主要な成果の概略は以下の通りである。

1. 選択可能な節点と部材の集合から，安定性を満たす最小の部材と節点を選択し，そこから 1 つの部材を取り除いてリンク機構を作成する。このような機構を全列挙して，最適な解を求める際のその計算量限界を明らかにする。

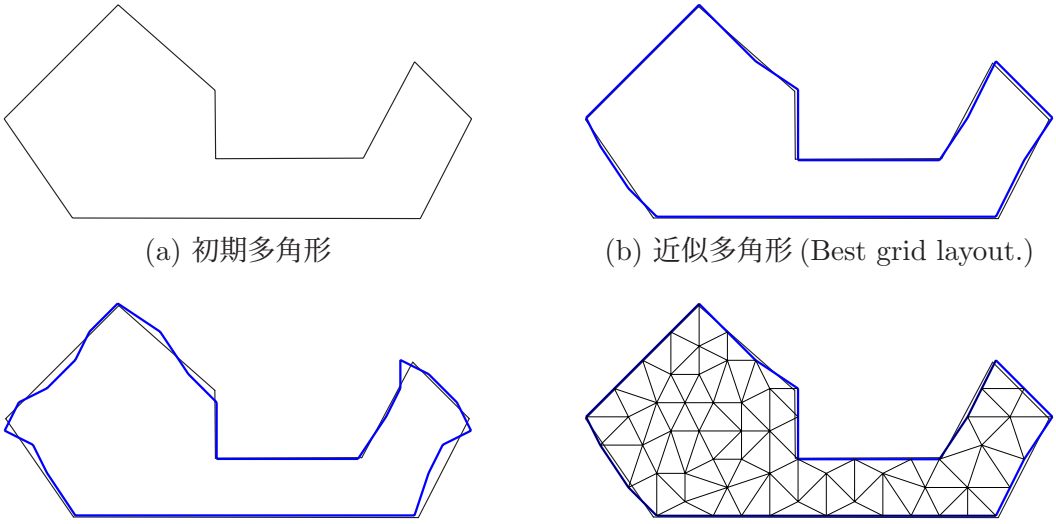
2. 昨年度は異なる部材長の数を最小にするトラスの設計問題を，その数を最小化する二次元平面上の三角形メッシュ生成問題としてモデル化し，計算量限界，近似性能比を明らかにしたが，今年度は境界を正方形グリッドの点を用いて近似する方法を提案し，内部領域の三角形メッシュの良さを定量的に評価した。また，最適な正方形グリッドの配置アルゴリズムも開発した。

3. 木構造ネットワーク，格子状ネットワークにおける最適避難計画問題を動的なネットワークフロー問題として定式化し，以下の研究成果を得た。(1) 木構造ネットワークにおいてシンクが 1 および 2 の場合，避難完了時間最小化問題を解く $O(n \log n)$ 時間アルゴリズムを開発した。(2) 枝容量，枝移動時間が一定の格子状ネットワークにおいて避難完了時間最小化問題を解く $O(n \log n)$ 時間アルゴリズムを開発した。

4. 昨年度において，平面上に存在する利用者間の交通量が与えられている時，総和が一定の長さの線分集合で表現される道路（または鉄道）を配置することにより増大する利用者の利便性を最大化する交通網を設計する問題を幾何的最適化問題としてモデル化したが，今年度はこの問題の計算量限界を明らかにし，いくつかのヒューリスティックについて近似性能比も明らかにする。

5. また，配送問題では，積込み，配送の 2 種類の荷物を有する場合について，とくに需要点が木構造ネットワークに配置されている場合について，計算量限界，近似性能比に関する研究をおこなった。

6. テンセグリティの実現可能性と安定性を，釣合い行列のランクを用いて明確に定義し，節点位置と張力に関する要求を満たす安定な構造を求めるための最適化手法を提案するとともに，その計算量限界を明らかにする。



(a) 初期多角形　(b) 近似多角形 (Best grid layout.)

(c) 近似多角形 (Worst grid layout.)　(d) 三角形分割

図 2.1: 近似多角形とその三角形分割。異なる辺長種類数は 7。($\underline{l} = 50, \alpha = 0.5$ and $\beta = 2.0$)

2　異なる辺長種類数制約下における平面三角形分割

異なる部材長の数が制約されている条件化において三角形トラスを設計する問題は，異なる辺長の種類数制約下における二次元平面上の三角形メッシュ生成問題としてモデル化することが可能である。一般に，任意に与えられた境界多角形内部を定数種類の辺長のみを用いて三角形分割を行うことは，非常に難しい問題と考えられる。そこで本研究では，与えられた境界多角形を僅かにずらす (別の近似多角形を考える) ことによって，異なる辺長種類数が一定である三角形分割を求めるアルゴリズムを提案した。具体的には，以下のように問題を定式化することができる。

入力:各辺長の長さが $\underline{l}$ 以上，$2\underline{l}$ 以下で与えられた頂点数 n の x-単調多角形 P。

出力:各辺長が $\underline{l}$ 以上，$\beta\underline{l}$ 以下の P の近似多角形 Q と，Q 内部の異なる辺長種類数が一定である三角形分割。

アルゴリズムのアイデアは，近似多角形 Q の頂点及び，メッシュ生成のために Q 内部に追加する Steiner 点をすべて幅 $\alpha\underline{l}$ で与えられた正方形グリッド G の頂点上に配置することである。そのことによって，得られる三角形分割の辺長の上限値が定数ならば，異なる辺長種類数も定数となる。

まず P を G の頂点のみを用いた多角形 Q へと近似を行う問題を考え，Hausdorff distance 最小となる近似多角形を $O((n/\alpha^4)\log(n/\alpha))$ 時間で求めるアルゴリズムを提案した。次に，Q の内部に逐次的に Steiner 点を G の頂点上にのみ追加していき，Q の頂点と Steiner 点に対する Delaunay 三角形分割を求めることで得られる三角形分割が，辺長及び，角度に関して以下を満たしていることを示した。

- 得られた三角形分割の辺長は $\underline{l}$ 以上，$(2+\sqrt{2}\alpha)\underline{l}$ 以下である。
- 得られた三角形分割の各三角形の内角は $\min\{\arccos(\beta/2), \arcsin(1/(2+\sqrt{2}\alpha))\}$ 以上である。

このことにより，アルゴリズムによって得られる三角形分割の異なる辺長種類数は $3\pi/8\alpha^2 + o(1/\alpha^2)$ となる。

図 2.1 にこのアルゴリズムを実装した結果を示す。図 2.1(a) を初期多角形，$\alpha = 0.5$ とした時，図 2.1(b),(c) が多角形近似の結果，図 2.1(d) は図 2.1(b) の三角形分割である。三角形分割の辺長種類数は 7 種類という結果が得られた。

また図 2.1(b) と (c) は，同じグリッド幅であっても，グリッドの位置によって得られる近似多角形の近似精度が大きく異なる例である。そこで新たな問題設定としてグリッドの最適配置問題を考え，グリッドの最適配置と近似多角形を同時に求める $O((n^3/\alpha^{12})\log(n/\alpha))$ 時間のアルゴリズムを提案した。

3 辺の容量が一定のネットワークにおける動的なフローを用いた避難計画問題に対する効率的なアルゴリズム

本論文では，辺に容量と移動時間が付されたネットワークにおける最速フロー問題を扱い，シンクを一つ持つ辺の容量が一定のグリッドネットワークにおける最速フロー問題に対する $O(n \log n)$ 時間アルゴリズムを提案する。

任意の点がサプライを持つネットワークが与えられたとき，最速フロー問題は全てのサプライを最も早くシンクに流すことのできる最適なフローを求める問題と定義される。任意のネットワークにおける最速フロー問題に対しては，多項式時間アルゴリズムが存在するが，その計算時間は高次元の多項式となるので，一般的には実用的ではない。それゆえ，構造を限定した現実への応用に有益な問題に対する高速なアルゴリズムの開発が必要となる。そこで本論文では，現実の道路や廊下が一定の規格に沿っていることを考慮し，辺の容量は一定，さらに都市のモデル化の際頻出する構造としてグリッドネットワークに扱うネットワークを限定した。

ここで，本論文で提案するアルゴリズムの概要を説明する。提案するアルゴリズムは，グリッドネットワークの構造の特徴を利用している。まず，与えられるネットワークを $\mathcal{N}$，そして $\mathcal{N}$ のシンクを r とする。また，r の子を u_1, u_2, u_3, u_4 とする。グリッドネットワークの辺は全てシンクへ近づく方向に向き付けられているので，$\mathcal{N}$ の点集合を八つの集合 U_1, U_2, U_3, U_4，W_1, W_2, W_3, W_4 に分解することが出来る (図 2.2)。U_i はサプライが全て辺 (u_i, r) を通ってシンクへ流れこむ点の集合であり，W_i はサプライが (u_i, r) または (u_{i+1}, r) を通ってシンクへ流れ込む点の集合である。ここで，任意の点 $v \in W_i$ の (u_i, r) を通過してシンクに流れるサプライと (u_{i+1}, r) を通過してシンクに流れるサプライへの分配が決定すれば，任意の実行可能なフロー f を，それぞれが (u_i, r) を通過してシンクに流れ込むサプライを表す四つのフロー $f_i, i = 1, 2, 3, 4$ に分解出来ることに注意する。本論文ではこの $f_i, i = 1, 2, 3, 4$ に関して，以下の二つの主張を証明した。

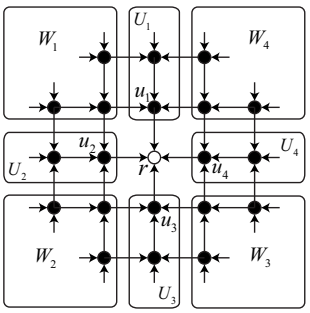


図 2.2: $\mathcal{N}$ の分解の例

主張 1 f_i と $f_j, i \neq j$ が辺を共有しない実行可能なフロー f の中に最適なフローが存在する

主張 2 f_i と $f_j, i \neq j$ が辺を共有しない任意の実行可能なフロー f の最速避難完了時間は等しい

以上の二つの主張とグリッドネットワークが図 2.3 のように分解できることにより，

本論文で扱う最速フロー問題は，任意の点 $v \in W_i, i = 1, 2, 3, 4$ の (u_i, r) と (u_{i+1}, r) へのサプライの最適な分配を求めればよいことが証明された。さらに，本論文ではこの任意の点 $v \in W_i, i = 1, 2, 3, 4$ の (u_i, r) と (u_{i+1}, r) へのサプライの最適な分配を求める問題は，効率的なアルゴリズムが存在する min-max 型の目的関数を持つネットワーク制約下の資源配分問題へ帰着できることを証明することにより，辺の容量が一定のグリッドネットワークにおける最速フロー問題に対する $O(n \log n)$ 時間アルゴリズムの開発に成功した。

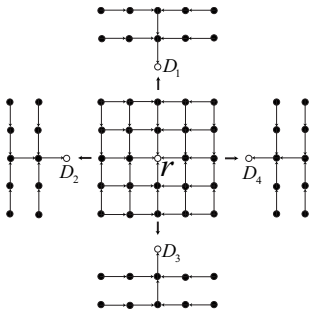


図 2.3: グリッドネットワークの分解

4 テンセグリティの形状設計

図 2.4 に示すような，互いに接触しない棒材（ストラット）と，張力の導入される連続なケーブル

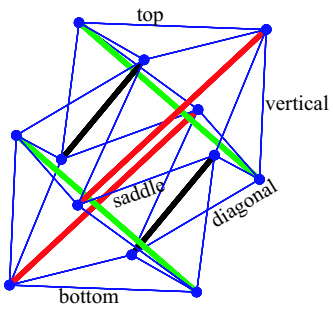


図 2.4: 2 層テンセグリティ構造

で構成されるピン接合構造物を，テンセグリティ構造という。このような張力構造物に対して，外力の作用しない自己釣合い状態での形状を求めることを，釣合い形状解析という。

部材 i の軸力を N_i, 長さを L_i としたとき，$q_i = N_i/L_i$ を軸力密度（force density）といい，そのベクトルを $\mathbf{q}$ とする。n 個の節点の x, y, z 座標をまとめたベクトルを，それぞれ $\mathbf{X}, \mathbf{Y}, \mathbf{Z}$ とし，それらに関する釣合い行列を $\mathbf{E}$ で定義すると，構造物の自己釣合方程式は $\mathbf{EX} = \mathbf{EY} = \mathbf{EZ} = \mathbf{0}$ のように書ける。ここで，$\mathbf{E}$ は $\mathbf{q}$ の関数であり，実対称行列である。また，形状が退化しないためには，条件 $\mathrm{rank}\mathbf{E} = n - 4$ を満たす必要がある。

$\mathbf{E}$ の固有ベクトルを並べた行列 $\mathbf{U}$ と，固有値を対角成分に持つ対角行列 $\mathbf{S}$ を用いて，$\mathbf{E}$ は $\mathbf{E} = \mathbf{USU}^\top$ のようにスペクトル分解できる。したがって，$\mathbf{S}$ の最小の 4 個の固有値をゼロにした行列 $\bar{\mathbf{S}}$ を用いて $\bar{\mathbf{E}}$ を $\bar{\mathbf{E}} = \mathbf{U}\bar{\mathbf{S}}\mathbf{U}^\top$ のように再構成する。以上より，繰返し計算によって釣合い条件と非退化条件満たす $\mathbf{q}$ を得ることができる。

ところで，上記の方法で得られるテンセグリティは，釣合い条件は満たすが，安定であるとは限らない。接線剛性行列 $\mathbf{K}$ は，線形剛性行列 $\mathbf{K}^\mathrm{E}$ と幾何剛性行列 $\mathbf{K}^\mathrm{G}$ の和として $\mathbf{K} = \mathbf{K}^\mathrm{E} + \mathbf{K}^\mathrm{G}$ のように定義できる。$\mathbf{K}^\mathrm{E}$ と $\mathbf{K}^\mathrm{G}$ の r 次固有値，固有ベクトルを，それぞれ λ_r^E, $\boldsymbol{\Psi}_r^\mathrm{E}$ 及び λ_r^G, $\boldsymbol{\Psi}_r^\mathrm{G}$ で表す。λ_i^E 及び λ_i^G のなかで，$\lambda_i^\mathrm{E} = 0$ 及び $\lambda_i^\mathrm{G} < 0$ がそれぞれ成立する添字（次数）の集合を J^E 及び J^G で表す。また，テンセグリティは，一般に張力が存在しないとき剛体モード以外の不安定な変形モードが存在するので，J^E は空でないものとする。このとき，安定性に関して，次のような条件が成立する。

1. $\lambda_r > 0, (r = 1, \ldots, f)$ のとき安定である。
2. $\boldsymbol{\Psi}_i^\mathrm{E}$ $(i \in J^\mathrm{E})$ が $\boldsymbol{\Psi}_i^\mathrm{G}$ $(i \in J^\mathrm{G})$ の線形結合で表されるとき，不安定である。
3. 安定な構造において張力の符号を全て入れ替えると，不安定になる。
4. $\lambda_{\min}^\mathrm{E} = \min_{i \notin J^\mathrm{E}} \lambda_i^\mathrm{E}$, $\lambda_{\min}^\mathrm{G} = \min_{i \notin J^\mathrm{E}} \lambda_i^\mathrm{G}$ とする。次の 2 つの条件が成立するとき安定である。
   (a) 全てのベクトル $\boldsymbol{\Psi}_i^\mathrm{E}$ $(i \in J^\mathrm{E})$ が $\boldsymbol{\Psi}_i^\mathrm{G}$ $(i \notin J^\mathrm{G})$ の線形結合で表され，少なくとも 1 つの正の固有値 λ_j^G に関する固有モードの成分が 0 でない。
   (b) 張力は十分に小さく，$\lambda_{\min}^\mathrm{E} + \lambda_{\min}^\mathrm{G} > 0$ が成立する。

以上，本研究では，テンセグリティ構造に対して，釣合い条件と非退化条件を満たす軸力密度ベクトルを，釣合い行列のスペクトル分解を用いた繰返し計算によって求める方法を提案した。

さらに，線形剛性行列と幾何剛性行列の固有値と固有ベクトルを用いて，テンセグリティの安定性条件を導いた。

5 バイステーブル・コンプライアントメカニズムの設計

コンプライアントメカニズムとは，構造物の適切な位置に柔軟性を付加することにより構造一体で機能を実現するメカニズムである。医療部品やマイクロメカニクスの分野で積極的に利用されている。バイステーブル構造物は，2 つの自己釣合い状態を持つ構造である。

本研究では，座屈現象を積極的に利用したバイステーブル・コンプライアントメカニズムを，最適化手法によって生成する。本構造は，建築構造や宇宙構造物での展開構造などで利用できる。

以下のような条件の下で，最適化問題を定式化する。

1. スナップスルーを利用して，小さい外力で大変形を発生させる。

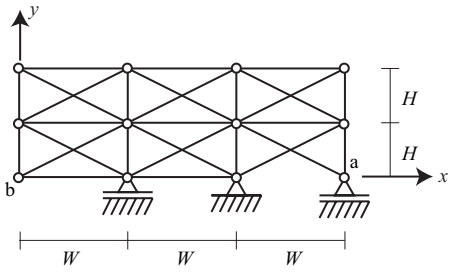


図 2.5: 平面トラスモデル

2. 最終状態での外力は 0 であり，強制変位を与える点に微小な外力を与えて拘束すれば安定化できる。

3. 全部材体積を最小化。

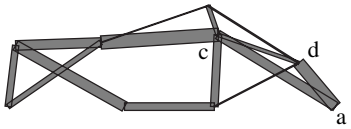
4. 初期剛性が指定値以上。

5. 最終状態で拘束した構造物の剛性が指定値以上。

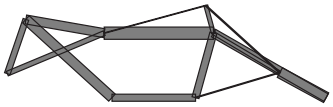
6. 最終状態で拘束を解除して微小な外乱を与えれば初期状態が回復される。

例えば，図 2.5 に示すような平面トラスを初期解として，節点位置と断面積を変数として最適化し，断面が 0 となる部材を除去して最適な節点位置とトポロジーを求める。節点 a を x 軸方向に変位させたときに，節点 b が y 軸方向に移動するメカニズムを生成する。最適化によって得られた形状を図 2.6 に示す。この解での入力節点 a の変位と外力の関係は図 2.7 にようであり，スナップスルーが実現されている。また，初期解を変更して最適化すると，図 2.8 のような解が得られる。

以上，本研究では，スナップスルーを用いたバイステーブル・コンンプライアントメカニズムの形状とトポロジーを，非線形最適化によって求めるアルゴリズムを提案した。



(a) 初期状態



(b) 最終状態

図 2.6: 最適解 Type-1 ($V = 1.2858 \times 10^{-4}$ m^3)

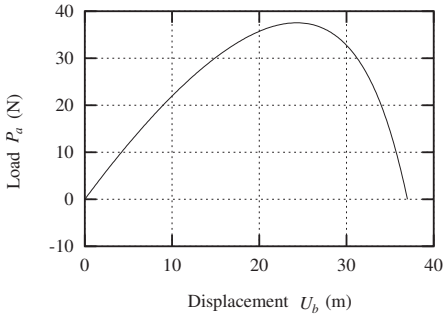
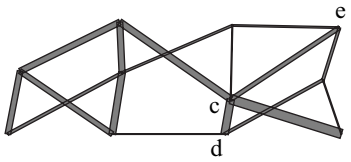
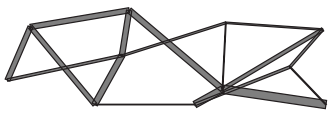


図 2.7: 最適解 Type-1 の U_a と P_a の関係



(a) 初期状態



(b) 最終状態

図 2.8: 最適解 Type-2 ($V = 8.7875 \times 10^{-5}$ m^3)

研究業績一覧

著書

1. 日本建築学会編:
   “建築最適化への招待”, 日本建築学会, 2005.4.
   概要: 本書は主に建築を学ぶ学生を対象に最適化技術の魅力を理解してもらうための啓蒙書として，建築に関する平易な事例を通して最適化理論の初歩が学べるように工夫されている。また，取り扱う建築分野も都市計画，建築計画，構造形状，構造設計，熱環境，内外装計画の多岐にわたっている。

学術論文

1. Tetsuo Asano, Mark de Berg, Otfried, Cheong, Hazel Everett, Herman Haverkort, Naoki Katoh, and Alexander Wolff:
   “Optimal Spanners for Axis-Aligned Buildings”, Computational Geometry: Theory and Applications, Vol.30(1), 59-77, 2005.
   概要: We consider the following problem: We wish to connect buildings using bridges or tunnels, such that people can pass between the buildings without having to step outside. We want to place the bridges such that the dilation of the resulting network is minimum, where the dilation is the maximum ratio between distance within the network and L_1 distance over all pairs of points in the given buildings. Given n axis-parallel rectangular buildings and a set of pairs of buildings that are to be connected by axisparallel bridges, we can find a minimum dilation bridge placement in $O(n^2)$ time if the building-bridge graph is a path. For the case that the graph is a tree, we give a pseudo-polynomial solution based on an LP-formulation of the problem. We show that the problem is NP-hard if the graph has cycles.

2. X. Gandibleux, H. Morita, N. Katoh:
   “Population-based heuristic for solving assignment problems with two objectives”, Journal of Mathematical Modelling and Algorithms, 掲載予定.
   概要: A population-based heuristic for computing an approximation of the efficient solution set for the assignment problem with two objectives is presented. It is based on an intensive use of three operators performed on a population composed only of elite solutions. The operators are a local search, a crossover and a path-relinking. The initial population is a subset of supported solutions. A genetic information is derived from elite solutions. A lower bound set defined in the objective space provides an acceptable limit for performing a local search. Results of extensive numerical experiments show that the heuristic is able to find quickly a very good approximation of the efficient frontier and outperforms the previous results published.

3. Naoki Katoh and Taihei Yano:
   “An Approximation Algorithm for the Pickup and Delivery Vehicle Routing Problem on Trees”, Discrete Applied Mathematics, 掲載予定.
   概要: This paper presents an approximation algorithm for a vehicle routing problem on a tree-shaped network with a single depot where there are two types of demands, pickup demand and delivery demand. Each customer has a positive demand of pickup and/or delivery. Demands of customers are served by a fleet of identical vehicles with unit capacity. Each vehicle can serve pickup and delivery demands. It is assumed that the demand of a customer is splittable, i.e., it can be served by more than one vehicle. The problem asks to find a set of tours of the vehicles with minimum total lengths. In each tour, a vehicle begins at the depot with certain amount of goods for delivery, visits a subset of the customers in order to de-

liver and pick up goods and returns to the depot. At any time during the tour, a vehicle must always satisfy the capacity constraint. We propose a 2-approximation algorithm for the problem.

4. 具 源龍，横田 隆志，瀧澤 重志，加藤 直樹:
“建築画像からの建築構成要素の認識手法に関する研究 ベイズ判別によるガラス開口部の認識”, 日本建築学会総合論文誌, 第 4 号 情報化の視点からみた建築・都市のフロンティア, 123–127, 2006.2.
概要: 本研究では，デジタルカメラで撮影した住宅のファサード画像から，ガラス開口部を判別するモデルを構築し，その判別精度を検証するものである。ガラス開口部は，建物火災の延焼シミュレーションや，環境防犯設計において重要な因子となるものであるが，大量に存在するので, その位置を自動的に認識する必要がある。ガラスは透明性や反射性などの素材の持つ特徴から，他の建築部位と比較して色分布が安定しておらず，既往研究で対象とした畳や格子と比較して判別が難しいと考えられる。そこで，色情報だけでなく開口部が出現しやすい位置情報を加味するとともに，Naive Bayes を非独立な確率変数を扱えるように拡張した手法を新たに開発して判別モデルを構築した。

5. 神山直之，瀧澤重志，加藤直樹:
“フロアプランの列挙に基づく 2 階建て住宅の室配置アルゴリズム”, 日本建築学会環境系論文集, 第 601 号, 65–72, 2006.3.
概要: 本研究は，2 階建て住宅の LDK 形式で表現される室配置を対象として，列挙アルゴリズムと最適化アルゴリズムを併用して，その配置を決定するアルゴリズムを提案するものである。概要を説明すると，まず，中野によって提案された高速なフロアプラン列挙アルゴリズムを用いてフロアプランを生成し，それらから隣接関係と方位条件，階を貫く室（階段室）の整合性を満たす室配置を抽出する。そして，タブー探索法を用いて室の大きさと形状を最適化し，要求に沿う室配置を複数求めようとするものである。2 階建て住宅を対象とし，吹き抜けなどの複数階で共有する空間の制約を利用して，列挙解の組み合わせを減少させる工夫をしている点にアルゴリズム面の特徴がある。

6. M. Ohsaki and N. Katoh:
“Topology optimization of trusses with stress and local constraints”, Structural and Multidisciplinary Optimization, 29, 190–197, 2005.
概要: A truss topology optimization problem under stress constraints is formulated as a Mixed Integer Programming (MIP) problem with variables indicating existence of nodes and members. The local constraints on nodal stability and intersection of members are considered, and a moderately large lower bound is given for the cross-sectional area of an existing member. An upper-bound solution is obtained as a solution of NonLinear Programming (NLP) problem for the topology satisfying the local constraints. It is shown in the examples that upper- and lower-bound solutions with small gap in the objective value can be found by the branch-and-bound method, and the computational cost can be reduced by using the local constraints for obtaining a practically optimal solution.

7. M. Ohsaki and S. Nishiwaki:
“Shape design of pin-jointed multistable compliant mechanisms by utilizing snapthrough behavior”, Structural and Multidisciplinary Optimization, 30, 327–334, 2005.
概要: A general approach is presented for generating pin-jointed multi-stable compliant mechanisms utilizing snapthrough behavior. An optimization problem is formulated for minimizing the total structural volume under constraints on the displacements at the specified nodes, stiffnesses at initial and final states, and load factors to lead to snapthrough behavior.

The design variables are cross-sectional areas and the nodal coordinates. It is shown in the numerical examples that several mechanisms can be naturally found as a result of optimization starting from randomly selected initial solutions. It is also shown that no local bifurcation point exists along the equilibrium path, and the obtained mechanism is not sensitive to initial imperfections.

8. J. Zhang and M. Ohsaki:
"Form-finding of self-stressed structures by an extended force density method", J. Int. Assoc. for Shell and Spatial Struct., 46(3), 159–166, 2005.
概要: A numerical method for the form-finding problem of self-stressed structures is presented as an extension of the basic idea and formulations of the force density method, which is initially developed for cable nets. Singular value decomposition of the equilibrium matrix with respect to nodal coordinates is utilized to find the feasible set of force densities for satisfying the non-degeneracy condition of the structure. A unique configuration of the structure can be obtained by specifying an independent set of nodal coordinates. The proposed method can have some, although not exact or direct, controls over the geometrical and mechanical properties of the structure. Its strong ability of searching new configurations and the good convergence properties are demonstrated by several numerical examples.

9. J. Zhang, M. Ohsaki and Y. Kanno:
"A direct approach to design of geometry and forces of tensegrity structures", Int. J. Solids and Struct., 43(7), 2260–2278, 2006.
概要: In the process of designing a tensegrity system, some constraints are usually introduced for geometry and/or forces to ensure uniqueness of the solution, because the tensegrity systems are underdetermined in most cases. In this paper, a new approach is presented to enable designers to specify independent sets of axial forces and nodal coordinates consecutively, under the equilibrium conditions and the given constraints, to satisfy the distinctly different requirements of architects and structural engineers. The proposed method can be used very efficiently for practical applications because only linear algebraic equations are to be solved, and no equation of kinematics or material property is needed. Some numerical examples are given to show not only efficiency of the proposed method but also its ability of searching new configurations.

10. J. Zhang and M. Ohsaki:
"Adaptive force density method for form-finding problem of tensegrity structures", Int. J. Solids and Struct., （掲載決定）.
概要: A numerical method is presented for form-finding of tensegrity structures. Eigenvalue analysis and spectral decomposition are carried out iteratively to find the feasible set of force densities that satisfies the requirement on rank deficiency of the equilibrium matrix with respect to the nodal coordinates. The equilibrium matrix is shown to correspond to the geometrical stiffness matrix in the conventional finite element formulation. A unique and non-degenerate configuration of the structure can then be obtained by specifying an independent set of nodal coordinates. A simple explanation is given for the required rank deficiency of the equilibrium matrix that leads to a non-degenerate structure. Several numerical examples are presented to illustrate the robustness as well as the strong ability of searching new configurations of the proposed method.

研究会等

1. Shin-ichi Tanigawa and Naoki Katoh:
"Finding a triangular mesh with a constant number of different edge lengths", Proc. of 17th Canadian Conference of Computational Geometry, 271-274, 2005.8.
概要: The problem of triangulating a specified domain is a basic problem in computational geometry and has numerous applications. We consider the problem of finding an almost uniform triangular mesh for a given x-monotone polygon with a constant number of different edge lengths. This problem is motivated by constructing structure truss such as a dome with a limited number of different elements to reduce its construction cost. Though it is difficult in general to find a triangular mesh for any polygon with a constant number of different edge lengths, we give an algorithm for finding such a triangular mesh by approximating a given boundary using square grid points.

2. Shin-ichi Tanigawa and Naoki Katoh:
"Polygonal Curve Approximation Using Grid Points with Application to a Triangular Mesh Generation with Small Number of Different Edge Lengths", Proc. of the Second International Conference on Algorithmic Aspects in Information and Management, Hong Kong, （発表予定）.
概要: We consider approximating an x-monotone polygonal curve with n vertices by another x-monotone curve using points of a given square grid. Our algorithm finds an approximate polygonal curve as well as an optimal grid placement simultaneously in $O((n^3/\alpha^{12})\log^2(n/\alpha))$ time.

3. Naoyuki Kamiyama, Naoki Katoh and Atsushi Takizawa:
"An Efficient Algorithm for Evacuation Problem in Dynamic Network Flows with Uniform Arc Capacity", Proc. of the Second International Conference on Algorithmic Aspects in Information and Management, Hong Kong, （発表予定）.
概要: In this paper, we consider the quickest flow problem in a network which consists of a directed graph with capacities and transit times on its arcs, and present an $O(n \log n)$ time algorithm for the quickest flow problem in a network of grid structure with uniform arc capacity which a single sink where n is the number of vertices in the network. In this paper, by using the fact that we can decompose a grid network as four arc-disjoint networks and the property of a layered network with uniform arc capacity we prove that the quickest flow problem for a grid network with uniform arc capacity can be reduced to a resource allocation problem which can be solved efficiently.

4. M. Ohsaki, J. Zhang and S. Kimura:
"An Optimization Approach to Design of Geometry and Forces of Tensegrities", Proc. IASS Symposium 2005, Bucharest, Romania, Int. Assoc. Shell and Spatial Struct., 603–610, 2005.9.
概要: Ageneral method is presented for direct design of member directions, force vectors and nodal locations of tensegrities with given topology, which is defined as a directed graph. The system of equilibrium equations is written in terms of the components of the member force vectors by using the incidence matrix. Since the number of the total components of the force vectors is usually larger than the rank of the equilibrium matrix, some force components can be arbitrary specified. The target values are given here to formulate an optimization problem to obtain a set of force components that satisfies equilibrium conditions. By using the proposed method, the designers can directly control the axial forces and the configuration simultaneously, which is considered a major advantage of the method. A

new configuration can also be obtained by changing the target values of the forces and geometrical constraints.

5. J. Zhang and M. Ohsaki:
"Form-finding of Self-stressed Structures by an Extended Force Density Method", Proc. IASS Symposium 2005, Bucharest, Romania, Int. Assoc. Shell and Spatial Struct., 93–100, 2005.9.
概要: The force density method is extended to find the feasible set of force densities, based on singular value decomposition of equilibrium matrix, and an algorithm for specifying an independent set of nodal coordinates is proposed. The force densities is first formulated in terms of elements of the equilibrium matrix, where constraints on force densities with desired values can be included at the same time. The least square solution of the force densities is then given based on this formulation. Singular value decomposition is next applied to the equilibrium matrix and its smallest elements with the specified number are set to be zero in order to attain the required rank. The equilibrium matrix is reconstructed for calculation of force densities by the equations formulated previously. By iteratively carrying out the above processes of calculating force density vector and equilibrium matrix with the updated ones, a feasible set of force densities is derived. The last step of the method is to specify an independent set of nodal coordinates to achieve a unique geometrical configuration of the structure.

6. M. Ohsaki and N. Katoh:
"Topology optimization of trusses with stress and local constraints", Proc. 5th Int. Conf. on Computation of Shell and Spatial Structures, Salzburg, IASS-IACM, 2005.6.
概要: A mixed integer programming formulation is presented for the truss topology optimization with stress and local constraints. Linear programming problems are successively solved based on a branch-and-bound method, where an upper-bound solution is obtained by solving nonlinear programming problems. It is shown in the examples that upper- and lower-bound solutions with small objective gap can be found, and the computational cost can be reduced by utilizing the local constraints.

7. T. Kinoshita and M. Ohsaki:
"Multistable compliant mechanisms for spatial structures using snapthrough behavior", Proc. IASS Symposium 2006, Beijing, China, Int. Assoc. Shell and Spatial Struct., (発表予定).
概要: Contrary to conventional mechanisms, which are usually achieved by the rotations around hinges and/or sliding supports, a compliant mechanism uses the elastic deformation of structural parts to realize the mechanism for shape transformation of the entire structure. We investigate the applicability and effectiveness of compliant mechanism to realize shape transformation of spatial structures. Conventional mechanism achieves stability at undeformed and deformed states by applying additional forces or constraints. However, our compliant mechanism can keep stability at undeformed and deformed states through its own stiffness, because it has multiple stable states without any additional constraint. To achieve practically useful multistable compliant mechanism, structural optimization technique is used. The design variables of the optimization problem are the cross-sectional areas of structural members and the nodal coordinates. Design conditions are given on the magnitude of deformation, the stability before and after deformation. The total structural volume is minimized as the objective function. Optimization problem is formulated so that snapthrough buckling is naturally

generated. Numerical tests are carried out to several types of spatial structures. It is shown that the mechanism which achieves the expected deformation can be obtained by solving the optimization problem.

学会大会等

1. 谷川眞一，加藤直樹:
“異なる辺長種類数制約下における一様三角形メッシュ生成アルゴリズム”, 形の科学会誌, 第 20 巻 第 1 号, 97–98, 2005.

2. 谷川眞一，加藤直樹:
“必要部材種類数制約下における平面三角形分割手法に関する研究”, 日本建築学会大会学術講演梗概集, A-2, 483–484, 2005.

3. 谷川眞一，加藤直樹:
“グリッド点を用いた多角形近似と三角形メッシュ生成”, 日本応用数理学会 2005 年度会講演予稿集, 318-319, 2005.

4. 川口史恵，塚本智久，加藤直樹，瀧澤重志:
“都市内鉄道の最適ネットワークの形”, 形の科学会誌, 第 20 巻 第 1 号, 81–82, 2005.

5. 塚本智久，加藤直樹，瀧澤重志:
“都市における線的施設配置問題に関する研究”, 日本建築学会大会学術講演梗概集, A-2, 557–558, 2005.

6. 加藤直樹，大原有祐，瀧澤重志:
“幾何学的迂回率最小化問題に関する研究”, 日本建築学会大会学術講演梗概集, A-2, 479–480, 2005.

7. 大原有祐，加藤直樹，瀧澤重志，川口史恵:
“幾何学的迂回率最小化問題に関する研究-迂回率の小さな街路設計への応用-”, 日本応用数理学会 2005 年度会講演予稿集, 316–317, 2005.

8. 木村 駿，大崎 純，張景耀:
“最適化手法によるテンセグリティ構造の軸力・形状決定”, 日本建築学会大会学術講演梗概集 (近畿), B-1, 941–942, 2005 年 8 月.

9. 張 景耀，大崎 純:
“釣合行列の固有値解析によるテンセグリティ構造の形状決定法”, 日本建築学会大会学術講演梗概集 (近畿), B-1, 943–944, 2005 年 8 月.

10. 大崎 純，張 景耀:
“テンセグリティの形状決定と安定性条件”, 日本応用数理学会 2005 年度年会講演予稿集, 78–79, 2005.

11. 大崎 純，張 景耀:
“固有値解析によるテンセグリティの形状設計と安定性条件”, 第 55 回理論応用力学講演会講演論文集, 121-122, 2006.

A07: 現実的な状況下での量子計算の能力に関する研究

山下 茂　中西 正樹

奈良先端科学技術大学院大学 情報科学研究科
〒 630-0192 奈良県生駒市高山町 8916-5
{ger, m-naka}@is.naist.jp

1　はじめに

計算機科学の視点での量子計算の研究は，量子チューリングマシンと呼ばれる非常に理想的な量子計算機のモデルの上で，計算ステップ数の漸近的な評価をしているものが多い．本研究では，より現実的な状況を考慮して，量子計算の一部分が古典的な計算資源で置き換えられたり，量子計算の一部分がエラーを含む場合に，量子計算の計算能力の解析を行なうことを目的としている．また，計算の大部分を古典計算機で行なわなければならないような現実的な状況において，量子計算機を利用すれば，古典計算だけの場合よりもより高速に解ける問題やその状況，およびその具体的な利用方法についての知見を得ることも目標としている．さらに，現実的な量子計算の利用方法を考えた時，計算に限定せずに古典通信では実現が困難な性質を持つ通信プロトコルへの応用も考えられるため，量子プロトコルに関しても新しい知見を得ることを目標としている．以上の目標に対して，本研究では多角的に研究を進めており，本年度の主要な研究成果の概要は以下の通りである．

量子情報を複数に秘密を分散して管理する手法

安全な情報の管理のために，パスワードなどの重要な秘密情報を複数に分散し，そのうちのいくつかが集まれば秘密が復元でき，しかも集まってきた情報のうち不正なものが何かを識別することができる手法を閾値秘密分散法と言う．秘密が量子情報の時に，直交配列とスタビライザ符号を用いて秘密分散を安全に行う手法を考案した．

公開する情報に「封」をする手法

封筒にいれた手紙などに紋章などの封をすることのように，データを途中で誰も見ていないことを保証する「封」の役割を実現する手法を考案した．考案した手法は，既に提案されている手法よりも不正がよりしにくい性質を持つと期待される．

リング状のネットワークでの量子分散アルゴリズム

量子計算機がリング状のネットワークでつながれた状況で，Distinctness と呼ばれる関数を計算する場合の通信量の下限を示した．また下限にほぼ一致する上限を持つ 2 つの量子プロトコルも設計した．得られた上下限は，各計算機に与えられる入力の可能性の数が計算機の数と同じオーダーの時には等しくなるので，設計したプロトコルはほぼ最適であると考えられる．

量子情報を送信可能な量子秘密通信プロトコル

量子暗号プロトコルとしては量子鍵配布が有名であるが，本手法では，鍵の配布だけでなく任意の量子ビットを安全に送信できるプロトコルを考案した．

エラーのある量子オラクルによるロバストな計算

量子バイアス付オラクルとは，各質問に対し確率 $1/2+\epsilon$ 以上で正しい答えを返すような量子オラクルである．そのようなオラクルが与えられたとき，そのオラクルへの $O(1/\epsilon)$ 回の質問を用い

て，確率 2/3 以上で正しい答えを返すようなオラクルへの 1 回の質問をシミュレートするアルゴリズムを考案した．考案したアルゴリズムと既知の結果を用いると，オラクルがエラーを持つ場合の探索問題に関して既知の下限と一致する最適なアルゴリズムを得ることができた．

量子ネットワーク上での効率的な情報の伝送

バタフライネットワークと呼ばれるネットワークでは，s_1 から t_1 及び s_2 から t_2 という 2 つのフローパスが容量 1 のチャンネルを共有している．古典の場合，このボトルネックとなるチャンネルの存在にも拘らず，2 つのパスに沿って 2 ビットを同時に送ることができる．量子の場合，量子状態の非直交性がこのボトルネックをはるかに困難なものにする．しかし，工夫したプロトコルにより，以下の結果を得た．(i) 任意の量子状態 $|\psi_1\rangle$ を s_1 から t_1 に，$|\psi_2\rangle$ を s_2 から t_2 に，それぞれフィデリティが真に 1/2 より大きくなるように同時に送る事ができる．(ii) $|\psi_1\rangle$ か $|\psi_2\rangle$ の一方が古典情報なら，フィデリティが 2/3 となるように同時に送ることができる．(iii) もし，$|\psi_1\rangle$ と $|\psi_2\rangle$ がいくつかの既知の有限個の状態であれば，フィデリティを更に改善することができる．これにより，s_1 から t_1 への古典的な情報を 2 ビット（同時に s_2 から t_2 への 2 ビット）のうちの任意に（通信の後で）選ばれた 1 ビットを復号するようなランダムアクセスコーディングが可能であることを示した．

以上の研究成果のうち 4 つの項目について，以下でより詳細に述べる．

2 量子情報を複数に秘密を分散して管理する手法

2.1 はじめに

秘密情報を分散して管理する方法として，(k,n)-閾値秘密分散法 [10] が知られている．これは，秘密 S を n 個の分散情報に符号化し，k 個以上の分散情報を集めると，元の秘密 S を復元できるが，k 個未満の分散情報からは，S に関する情報は全く得られないというものである．

近年，量子情報処理を用いて秘密分散法を実現する量子秘密分散法に関する研究が盛んに行われており [2, 3, 4, 6, 7, 8]，盗聴者の検出や量子通信を行うことによる通信効率の改善が議論されている．

本研究では，さらに進んだ機能として，不正者識別機能を量子秘密分散法に付加する．つまり，不正者識別が可能な (k,n)-閾値量子秘密分散法を提案する．古典情報処理においては，黒沢らにより不正者識別が可能な秘密分散法が提案されている [9]．本研究で提案する手法は，この黒沢らの手法を量子秘密分散法に拡張したものである．黒沢らの手法においては，メッセージ認証を用いて分散情報の改竄を検出しているが，この認証法は量子メッセージには適用できない．そのため，我々の手法では，無条件安全であることが知られているスタビライザーコードを用いた量子メッセージ認証を利用する．我々が提案する手法においては，$t(k \geq 3t+1)$ 人までの不正者を識別可能である．

2.2 不正者識別可能な量子秘密分散法

諸定義

以下に，提案プロトコルを説明するために必要な諸定義を行う．

Definition 1 **t-不正者識別可能 (k,n)-閾値量子秘密分散法**

S を量子メッセージとする．分配者 D は S から n 個の分散情報 $\{v_1,\ldots,v_n\}$ を生成し，それぞれを n 人の参加者 $P_1,\ldots,P_n$ に配布する．ここで，*(i)* 分配者は不正を行わない．*(ii)* 不正者は高々 t 人しかいない． という二点を仮定する．このとき，以下の性質を持つ場合，そのプロトコルを t-不正者識別可能 (k,n)-閾値量子秘密分散法と呼ぶ．

完全性 不正者を除いて k 人以上の参加者が集まれば，元の秘密を高確率で復元できる．

健全性 k 人以下の参加者が集まっても，元の秘密に関する情報は全く得られない．

不正者識別性 k 人以上の参加者が集まれば，その中に存在する不正者を高確率で識別するチューリング機械 M が存在する．

□

Definition 2 不正者識別性

一般性を失うことなく，$P_1, \ldots, P_t$ を不正者とし，それぞれ，$\hat{v_1}, \ldots, \hat{v_t}$ を開示するとする．次のいずれかの条件を満たすとき，不正が成功したと見なす．

Case 1 不正者の存在が検出されたにもかかわらず，M が不正者を識別できない，かつ，秘密の復元に失敗する．

Case 2 参加者が分散情報 $\{\hat{v_1}, \ldots, \hat{v_t}, v_{t+1}, \ldots, v_m\}$ から誤った秘密を復元してしまう．ただし，$m \geq k$.

□

提案手法

提案手法の概略は以下の通りである．

元となる (k, n)-閾値量子秘密分散法として，クリーブらのスタビライザーコードを用いた量子秘密分散法 [2] を用いる．分配者はランダムに量子秘密分散法 Q を選択する．つまり，使用するスタビライザーコードをランダムに選択することになる．Q を用いて量子秘密 S を n 個の分散情報に符号化する．改竄を検出するため，各分散情報を量子メッセージ認証 [1] を用いて符号化する． これらの操作は，黒沢らの手法 [9] の量子メッセージへの拡張となっている．参加者はさらに古典情報である量子メッセージ認証の鍵と，「Q としてどの符号化 (スタビライザーコード) が使われたか」という情報を共有する．このとき，量子メッセージ認証の鍵は不正者を高々 t 人含んでいたとしても，k 人以上の参加者が集まった時，かつその時のみ復元できるように符号化する．これは，線形符号を用いて可能である．また，「Q としてどの符号化が使われたか」という情報は，古典 (k, n)-閾値秘密分散法を用いて共有する．これにより，k 人以上の参加者が集まれば，量子メッセージ認証の鍵を復元でき，各分散情報が改竄されていないかどうかを確認できる．改竄されていないことが確認できれば，クリーブらの手法に従って，元の量子秘密を復元できる．

Theorem 1 上記の手法は t-不正者識別可能 (k, n)-閾値量子秘密分散法である．ただし，$k \geq 3t + 1$ である．

□

2.3 むすび

本研究では，t-不正者識別可能 (k, n)-閾値量子秘密分散法を提案した．提案した手法において，不正者の人数の上界を得ることができれば，それによりスタビライザーコード $[n, 1, K]$ が存在するような n と K の関係について明らかになる可能性がある．また，不正者による攻撃の成功確率の詳細な解析等が今後の課題として挙げられる．

3 リング状のネットワークでの量子分散アルゴリズム

量子分散計算における通信量を解析することは，将来の量子ネットワークの利用の仕方を考える上で重要な理論研究であり，現在さまざまな角度から研究されいる．現在までのほとんどの研究は 2 者間の通信のモデルを扱っているが，インターネットなどのネットワークの形状を考えると，必ずしも現実的なネットワークのモデルを扱っているとはいえない．そこで，本研究では，より現実的な状況に近いネットワーク形状における通信量の研究のために，ネットワークの構造を考慮した通信量の解析を行った．具体的には，n 個の量子プロセッサがリング状の量子ネットワーク上に配置された状況を考え，以下の **Distinctness** と呼ばれる問題を解く量子分散プロトコルの通信量に関する下限と上限を解析した．以下で，プロトコルはすべて定数エラーを持つものを考える．

Definition 3 (Distinctness) リング状の量子ネットワーク上に配置された各量子プロセッサ P_i $(0 \leq i \leq n-1)$ が，整数 $x_i \in \{0, \ldots, L-1\}$ $(n \leq L)$ を入力として持つ．この時，$i \neq j \longrightarrow x_i \neq x_j$ が成り立つかどうかを決定する問題．

以下では，最終的に各プロセッサが **Distinctness** の問題の 1 ビットの結果を得るために各リンクで通信される量子ビットの合計を解析する．

下限の導出のために，以下を用いる．

Lemma 1 長さ n のビット列 x と y が，任意のネットワークでつながっているプロセッサ P_i と P_j に与えられるとする．この時，s を P_i と P_j の間の最短パスの長さ，w を与えられたネットワークのグラフの P_i と P_j の間の最大のカット数とする．この時，ブール関数 $f(x,y)$ を計算するためのすべてのリンクにおける合計通信量は，$\Omega(s(Q_2(f(x,y)) - \log n)/\log w)$ となる．ただし，$Q_2(f(x,y))$ は，$f(x,y)$ を計算する 2 者間プロトコルで必要となる通信量とする．

証明は，量子プロトコルにおける puclic coin プロトコルの private coin プロトコルへの変換 [11] を利用して，古典の場合 [12] と同様に示すことができる．

下限を示す定理は以下の通りである．

Theorem 2 (Lower Bound) Distinctness の通信量は，$\Omega(n^{\frac{3}{2}})$ である．

証明：$(n-2(cn-1))$（c は $c\,(\leq 1/4)$ であるような定数）個のプロセッサによるリング状のネットワークにおいて，プロセッサ P_A と P_C がちょうど対極に位置しているとする．P_A と P_C が長さ cn のビット列 x と y を入力として持つとする．この時，x と y の関数 $\mathbf{DISJ} = \bigwedge_{i=1}^{cn} \overline{x_i y_i}$ を計算する問題を $\mathbf{DISJ}_{\text{ring}}$ と呼ぶことにする． Lemma 1 において，$w = 2$ および $s = (n-2(cn-1))/2 = O(n)$ とすれば，$\mathbf{DISJ}_{\text{ring}}$ を解くプロトコルがすべてのリンクにおいて通信する通信量の合計は $\Omega(n\sqrt{n})$ であることがわかる．そのため，$\mathbf{DISJ}_{\text{ring}}$ から **Distinctness** へのリダクションが示せれば定理を証明できることになる．

リダクションは以下の通りである．まず，**Distinctness** におけるリング状の n プロセッサを，サイズが cn である A と C，サイズが $(n/2 - cn)$ である B と D の 4 つのグループに分ける．ここで A と C は対極に位置するとする．次に，$L = (1+c)n$ とし，3 つの整数の集合 $I_1 = \{0, 1, \ldots, cn-1\}$，$I_2 = \{cn, \ldots, 3cn-1\}$ および $I_3 = \{3cn, \ldots, L-1\}$ を考える．$\mathbf{DISJ}_{\text{ring}}$ の任意のインスタンスから以下の手順により **Distinctness** のインスタンスを生成すれば，両者の解が一致することは容易にわかる．

1. P_A（P_C）への入力の i（$i = 1, \ldots, cn$）ビット目が 1 ならば，グループ A（C）の i 番目のプロセッサの入力を $(i-1) \in I_1$ とする．そうでないならば，I_2 の中から重なりが起こらないように選んだ整数をグループ A（C）の i 番目のプロセッサの入力とする．

2. C と D のグループの各プロセッサの入力は，I_3 の中から重なりが起こらないように選んだ整数とする．

以上のリダクションは $L \geq (1+c)n$ の時に有効であり，$c \to 0$ とすれば，$L > n$ において定理が成立することがわかる．

次に上限の定理を示す．

Theorem 3 (Upper Bound) Distinctness の通信量は，

$$\min\{O(n\sqrt{n}(\log\log L + \log n), O(n\sqrt{L})\}$$

証明：以下では，通信量が $O(n\sqrt{n}(\log\log L + \log n)$ および $O(n\sqrt{L})$ であるアルゴリズムをそれぞれ示す．

Algorithm 1:

解くべき問題は，以下の探索問題と本質的に同じである．「P_i と P_j $(j \neq i)$ が同じ入力を持っているような i は存在するか？」

もし，入力 i に対して，P_i と同じ入力を持つ $P_j (\neq P_i)$ が存在するときのみ 1 を返すオラクルがあれば，上記の探索問題は，Grover Search により $O(\sqrt{n})$ 回のオラクル呼び出しで解く事が可能である．そこで，ある決められたプロセッサ（便宜上，Alice と呼ぶ）が上記の Grover Search をするようにすれば問題が解ける．そのため，上記のオラクルを Alice がどのように模倣できるかを示せば良い．i に対するオラクルの出力を，Alice は以下のプロトコルで模倣できる．

1. Alice は，最初の L^t 個の素数の中からランダムに一つの素数 p を選ぶ．(t は定数とする．そのため素数定理より，p のビット長は $O(\log\log L)$ となることに注意.）

2. Alice は，$(i,\ p)$ が書かれたトークンをリング上に一周させる．この時，各プロセッサは受け取ったトークンの中の番号が自分のプロ

セッサ番号と一致する時，自分の持っている値 x_i に対して $(x_i \bmod p)$ をトークンに書き込む．

3. Aliceは，$(x_i \bmod p)$ を知った後，新たなトークン $(p, (x_i \bmod p), c)$ をリング上に一周させる．この時，各プロセッサはトークンを受け取ったら，自分の入力 x に対して $(x \bmod p)$ を計算し，受け取ったトークンの中の $(x_i \bmod p)$ と比較して等しい場合には，c を1増やす．c の初期値は0であり，c が2以上の場合は値を増やさないようにする．（補助ビットを使うことにより可逆計算でこの操作は可能である．）そのため，c は2ビットあれば十分である．

このプロトコルの最後で $c = 2$ となっていれば，オラクルの出力は1で $c = 1$ ならばオラクルの出力は0とすればよい．上記のプロトコルでは，各プロセッサは補助ビットを用いて計算するので，最後にトークンを逆周りに回して逆計算を行い，プロトコル中に使用した全ての補助ビットのクリアを行う．上記において，p と $x_i \bmod p$ のビット長は $O(\log\log L)$，i のビット長は $O(\log n)$ なので，プロトコル全体では $O(n(\log\log L + \log n))$ の通信量を必要とする．また，上記のプロトコルではオラクルの出力にエラーがあるが，オラクルが定数エラーの場合にはRobust Grover Searh[22] を用いることにより，Grover Searhと同様の $O(\sqrt{n})$ 回のオラクル呼び出しで探索問題が解ける．以上より，全体の通信量は $O(n\sqrt{n}(\log\log L + \log n))$ となる．

Algorithm 2:

解くべき問題は，以下の探索問題と本質的に同じである．「少なくとも2つ以上のプロセッサがその値を持っているような $x \in \{0, \ldots, L-1\}$ が存在するか?」

入力 x に対して，x を入力値としてもつプロセッサが2つ以上あるときに1を返すオラクルを考える．AaronsonとAmbainisによるDisjointnessを計算する量子プロトコル[13]同様に，このオラクルを $O(\sqrt{L})$ 回呼ぶことによって上記の問題を解く事が可能である．Aaronson と Ambainis による Disjointness を計算する量子プロトコル [13] では，上記のオラクルを実際に呼ぶときには（再帰的に分割して行う手法で，x の可能性が定数個になった時点で初めてオラクルを呼ぶため），x の値を各プロセッサに伝えるのに定数ビットしか必要としない．そのためオラクルのシミュレートは $O(n)$ ビットの通信ですむ．以上より，アルゴリズム全体の通信量は $O(n\sqrt{L})$ となる．

上記の通信量は $L = O(n)$ のときは下限と一致するのでほぼ最適な手法であると考えられる．

今後の課題としては，他のネットワーク形状や他の問題に対して量子プロトコルの通信量の上下限を求めることが考えられる．

4 量子情報を送信可能な量子秘密通信プロトコル

4.1 はじめに

1994年にショアによって多項式時間因数分解アルゴリズムが発表されたことにより，現在の公開鍵暗号は量子計算機によって解読可能であることが知られている．このため，量子計算機による攻撃に対しても安全なものとして，1984年にベネットらによって提案された量子鍵配布プロトコル (BB84)[15] が注目されている．このプロトコルは，秘密通信を行いたい二者間で無条件安全に乱数を共有する手法である．このプロトコルの発表以降，ここ20年の間，さまざまな量子暗号プロトコルに関する研究が行われてきた．B92[14], E91[17], GV95[18] は BB84[15] と同様量子情報技術を応用して安全に鍵配布を行うプロトコルである．また，岡本らにより量子公開鍵暗号 [20] も提案されており，量子計算機を使っても解くのが困難と予想される問題に安全性を帰着している．さらに，河内らによって量子状態の判別の困難さとそれを応用した計算量的に安全な量子秘密通信プロトコルの提案が行われている [19]．さらに近年，鍵配布ではなく，二者間で直接秘密情報を通信するプロトコルが研究されている [16]．本研究では，新しい量子直接秘密通信プロトコルを提案する．提案プロトコルは，古典情報だけでなく量子情報も送信可能であり，また，光子数分割攻撃に強い，エンタングルメントを使用しないといった特徴を持つ．

4.2 提案プロトコル

以下に，提案プロトコルを示す．
$U_\theta = \begin{pmatrix} cos\theta & sin\theta \\ -sin\theta & cos\theta \end{pmatrix}$ とする．

プロトコル

1. アリスは秘密量子ビット $|\psi_s\rangle$ と $k-1$ 個の囮量子ビット $|\phi_1\rangle, \ldots, |\phi_{k-1}\rangle$ を用意し，ランダムな順に並べる．ここで，囮ビットの状態はランダムに決める．アリスが用意した状態を一般性を失うことなく，$|\psi_0\rangle = |\psi_s \phi_1 \ldots \phi_{k-1}\rangle$ と書くことにする．

2. アリスはユニタリ変換 $U_{\hat{\theta_A}} = U_{\theta_A} \otimes U_{\alpha_1} \otimes \cdots \otimes U_{\alpha_{k-1}}$ をランダムに用意する．ここで，θ_a，$\alpha_1, \ldots, \alpha_{k-1}$ はランダムに選んだ回転角である．$d_A = \alpha_1 \ldots \alpha_{k-1}$ とし， また，$U_{d_A} = U_{\alpha_1} \otimes \cdots U_{\alpha_{k-1}}$ とする．アリスは $|\Psi_1\rangle = U_{\hat{\theta_A}} |\Psi_0\rangle$ をボブに送る．

3. ボブはアリスと同様にユニタリ変換 $U_{\hat{\theta_B}} = U_{\theta_B} \otimes U_{\beta_1} \otimes \cdots \otimes U_{\beta_{k-1}}$ をランダムに用意する．ここで，d_B および U_B を d_A，U_A と同様に定める．$|\Psi_2\rangle = U_{\hat{\theta_B}} |\Psi_1\rangle$ をアリスに送る．

4. アリスはボブに何番目のビットが秘密ビットであったかを教える．これに対してボブは，囮ビットに適用した操作，つまり d_B をアリスに教える．アリスは囮ビットに対して $U^\dagger_{d_A}$ および $U^\dagger_{d_B}$ を適用した後，囮ビットが初期状態 $|\phi_1\rangle, \ldots, |\phi_{k-1}\rangle$ に戻っているかどうかを調べる．この時点での量子状態を $|\Psi'_2\rangle$ とする．アリスは $|\Psi_3\rangle = (U^\dagger_{\theta_A} \otimes I^{\otimes k-1}) |\Psi'_2\rangle$ という状態を用意し，ボブに送る．このとき，ビットの順序をランダムに入れ替えて送信する．

5. ボブは $|\Psi_3\rangle$ を受け取った後，アリスにビットの順序および各囮ビットの初期状態を問い合わせる．この情報を元に，ボブは囮ビットに改竄がないことを確かめる．改竄がなければ，$U^\dagger_{\theta_B}$ を秘密ビットに適用し，元の秘密情報 $|\psi_s\rangle$ を得る．

ここで，U_θ は可換であることに注意されたい．そのため，$U_{\theta^\dagger_B} U_{\theta^\dagger_A} U_{\theta_B} U_{\theta_A} = I$ となり，ボブは正しく秘密情報を復号できる．また，$U_{\theta_A}, U_{\theta_B}$ は秘密鍵の役割をなしており，このため，盗聴者が通信路を盗聴しても情報を得ることができない．さらに，これら秘密鍵をアリスとボブで交換する必要がないことも提案手法の特徴である．

以下に，盗聴者 (イブ) が存在した場合の提案プロトコルの振る舞いについて説明する．今，イブは受動的攻撃者であるとする．イブは通信路を流れる量子ビットのうち，どれが囮ビットであるかを知らない．そのためイブができることは，通信路を流れる量子ビットをランダムに抽出して観測するだけである．しかし，仮に秘密ビットを抽出して観測したとしても，秘密ビットの状態はイブにとっては最大混合状態であるため，元の秘密に関する情報は全く得られない．また，仮に囮ビットを観測したとすると，そのことが 1/2 の確率で検出される．

次にイブが能動的攻撃者である場合を考える．このときイブはステップ 2 において，$|\Psi_1\rangle$ を奪い，ステップ 3 でのボブからアリスへの通信時に，奪った $|\Psi_1\rangle$ を送り返すことができる．しかし，この場合，ステップ 4 でアリスは送られてきた量子ビットがボブからのものであるかどうかを確認するため，イブがこの確認をすり抜けるためには，ステップ 2 において，秘密ビットのみを奪う必要がある．これが成功する確率は $1/k$ である．この確率をさらに下げるためにはボブが $|\Psi_2\rangle$ を送信する際にビットの並び順を置換すればよい．これにより，イブの攻撃の成功確率は $1/k^2$ になる．さらに，アリスとボブの間で提案プロトコルを繰り返すことにより，イブの攻撃の成功確率を指数的に下げることが可能である．

4.3 結び

本研究では，量子状態を送信できる量子直接秘密通信プロトコルを提案した．安全性についての証明や，多量子ビットの通信への拡張などが今後の課題として挙げられる．

5 エラーのある量子オラクルによるロバストな計算

現在までに知られている量子アルゴリズムは，エラー（物理的なノイズのエラーのことではない）を含むものが多い．そのような量子アルゴリズムをサブルーチンとして呼び出しながら全体の計算を設計することを考えた時には，以下のような量子オラクル O_f^ε を考えてそれへの質問量を議論することが自然である．

Definition 4 ε バイアスでブール関数 f 計算する量子オラクルは，O_f^ε と表記され，以下のユニタリー変換として定義される．

$O_f^\varepsilon |x\rangle \left|0^{m-1}\right\rangle |0\rangle$
$= |x\rangle (\alpha_x |w_x\rangle |f(x)\rangle + \beta_x |w'_x\rangle \left|\overline{f(x)}\right\rangle)$ ここで，$|\alpha_x|^2 = 1/2+\varepsilon_x \geq 1/2+\varepsilon$ $(x \in [N])$ かつ $\varepsilon_{min} = \min_x \varepsilon_x$ とする．

なお，すべての x に対して $0 < \varepsilon \leq \varepsilon_{min} \leq \varepsilon_x \leq 1/2$ に注意する．通常，ε は明示的に与えられてアルゴリズムを設計するが，ε_{min} や ε_x は与えられないと仮定するのが一般である．

入力値が上記のオラクルのモデルで与えられた時に，N-bit OR の関数を $O(\sqrt{N}/\varepsilon)$ の質問量で計算するアルゴリズムを以下に示す．このアルゴリズムの質問量は，$\varepsilon = \varepsilon_{min}$ の場合には，知られている下限と一致するので最適である．

以下では，オラクル O_f^ε を以下の Lemma に示すオラクル $\tilde{O}_f^\varepsilon$ に変換して考える．なお，変換の構成方法は，文献 [21] の Lemma 1 と同様である．

Lemma 2 O_f^ε と $O_f^{\varepsilon\dagger}$ を *1* 回ずつ用いて，以下の変換: $\tilde{O}_f^\varepsilon$ を実現可能である．

$$\tilde{O}_f^\varepsilon |x, 0^m, 0\rangle = (-1)^{f(x)} 2\varepsilon_x |x, 0^m, 0\rangle + |x, \psi_x\rangle . \tag{2.1}$$

ここで，$|x, \psi_x\rangle$ はノルムが $\sqrt{1-4{\varepsilon_x}^2}$ で，$|x, 0^m, 0\rangle$ と直交する．

以下の Lemma は，Amplitude Estimation が量子並列に動作可能であることを意味する．

Lemma 3 $\mathcal{O}$ を観測を用いない以下のように表される量子オラクルとする．

$\mathcal{O} |x\rangle |\mathbf{0}\rangle = |x\rangle \mathcal{O}_x |\mathbf{0}\rangle = |x\rangle |\Psi_x\rangle = |x\rangle (\left|\Psi_x^1\right\rangle + \left|\Psi_x^0\right\rangle)$.

ここで，状態 $|\Psi_x\rangle$ は，ブール関数 χ により望む状態 $\left|\Psi_x^1\right\rangle$ か望まない状態 $\left|\Psi_x^0\right\rangle$ かを判別できるとする．また，$\sin^2(\theta_x) = \langle\Psi_x^1|\Psi_x^1\rangle$ $(0 \leq \theta_x \leq \pi/2)$ を $\mathcal{O}_x |\mathbf{0}\rangle$ の成功確率と考える．（望む状態が観測で得られれば正しい答えが得られたことに相当すると考える．）この時，以下のような状態の変換を行う量子 $Par\_Est\_Phase(\mathcal{O}, \chi, M)$ を $\mathcal{O}$ とその逆変換を $O(M)$ 回利用して構成することができる．

$|x\rangle |\mathbf{0}\rangle |\mathbf{0}\rangle \longmapsto$
$|x\rangle \otimes \sum_{j=0}^{M-1} \delta_{x,j} |v_{x,j}\rangle \left|\theta \tilde{Par\_Est\_Phase}(\mathcal{O}, \chi, M)_{x,j}\right\rangle$.

ここで，任意の x に関して $\sum_{j:|\theta_x - \tilde{\theta}_{x,j}| \leq \frac{\pi}{M}} |\delta_{x,j}|^2 \geq \frac{8}{\pi^2}$ が成立し，任意の i, j に対して $|v_{x,i}\rangle$ と $|v_{x,j}\rangle$ は互いに直交する．

以上の準備により，以下の Lemma を示すことができる．

Lemma 4 $O_f^{1/6}$ の変換を $O(1/\varepsilon)$ 回の O_f^ε への質問によりシミュレートする量子アルゴリズムが存在する．

証明： O_f^ε を $O(1/\varepsilon)$ 回用いて，以下のような状態の変換を行う量子アルゴリズムが構築可能であることを示す．

$$|x\rangle |\mathbf{0}\rangle |0\rangle \longmapsto |x\rangle (\alpha_x |w_x\rangle |f(x)\rangle + \beta_x |w'_x\rangle \left|\overline{f(x)}\right\rangle).$$

（すべての x に対して $|\alpha_x|^2 \geq 2/3$ が成立するとする．）

アルゴリズムは以下の通りである．

以下では，$\sin\theta = 2\varepsilon$ かつ $\sin\theta_x = 2\varepsilon_x$ $(0 < \theta, \theta_x \leq \pi/2)$ とする．この時，$0 \leq \theta \leq \pi/2$ の時 $\sin\theta \leq \theta \leq \frac{\pi}{2}\sin\theta$ のため，$\Theta(\theta) = \Theta(\varepsilon)$ であることに注意する．また，$M_1 = \left\lceil \frac{3\pi(\pi+1)}{\theta} \right\rceil$ とし，χ を式 (2.1) にあらわれる状態の中で，望ましい状態 $(-1)^{f(x)} 2\varepsilon_x \left|0^{m+1}\right\rangle$ と望ましくない状態 $|\psi_x\rangle$ を区別するブール関数であるとする．χ は単に状態が $\left|0^{m+1}\right\rangle$ であるかないかをチェックするものなので，実装は容易である．Lemma 3 より，$Par\_Est\_Phase(\tilde{O}_f^\varepsilon, \chi, M_1)$ により以下の変換ができる．

$$|x\rangle |\mathbf{0}\rangle |\mathbf{0}\rangle |\mathbf{0}\rangle \longmapsto |x\rangle \otimes \sum_{j=0}^{M-1} \delta_{x,j} |v_{x,j}\rangle \left|\tilde{\theta}_{x,j}\right\rangle |\mathbf{0}\rangle .$$

ここで，すべての x に対して $\sum_{j:|\theta_x-\tilde{\theta}_{x,j}|\leq\frac{\theta}{3(\pi+1)}} |\delta_{x,j}|^2 \geq \frac{8}{\pi^2}$ であり，$|v_{x,i}\rangle$ と $|v_{x,j}\rangle$ は任意の i,j に関して互いに直交する．上記の状態の第 3 レジスタには，高い確率で良い精度の θ_x の近似値が得られている．第 4 レジスタ $|\mathbf{0}\rangle$ は以降の手順に使われるのに十分な大きさがあるとする．

以降の手順では，基本的には推定した $\tilde{\theta}_{x,j}$ の値を用いて Amplitude Amplification を行う．文献 [21] と同様の手法で，まず $m^*_{x,j} = \left\lceil \frac{1}{2}\left(\frac{\pi}{2\tilde{\theta}_{x,j}} - 1\right)\right\rceil$, $\theta^*_{x,j} = \frac{\pi}{4m^*_{x,j}+2}$, $p^*_{x,j} = \sin^2(\theta^*_{x,j})$ および $\tilde{p}_{x,j} = \sin^2(\tilde{\theta}_{x,j})$ を量子並列で計算し，最後の量子ビットに Hadmard 変換を行う．以上により以下の状態を得る．

$$|x\rangle \left(\sum_{j=0}^{M-1} \delta_{x,j} |v_{x,j}\rangle \left|\tilde{\theta}_{x,j}\right\rangle \left|m^*_{x,j}\right\rangle \left|\theta^*_{x,j}\right\rangle \left|p^*_{x,j}\right\rangle |\tilde{p}_{x,j}\rangle \otimes \left|0^{m+1}\right\rangle |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \right).$$

次に，回転 $\mathbf{R} : \left|p^*_{x,j}\right\rangle |\tilde{p}_{x,j}\rangle |0\rangle \rightarrow \left|p^*_{x,j}\right\rangle |\tilde{p}_{x,j}\rangle \left(\sqrt{\frac{p^*_{x,j}}{\tilde{p}_{x,j}}} |0\rangle + \sqrt{1-\frac{p^*_{x,j}}{\tilde{p}_{x,j}}} |1\rangle \right)$ およびオラクル $\mathbf{O} = \tilde{O}^{\varepsilon}_f \otimes \mathbf{R}$ を考える．

$M_2 = \left\lceil \frac{1}{2}\left(\frac{3\pi(\pi+1)}{2(3\pi+2)\theta} + 1\right)\right\rceil$, $\mathbf{Q} = -\mathbf{O}(\mathbf{I}\otimes\mathbf{S}_0)\mathbf{O}^{-1}(\mathbf{I}\otimes\mathbf{S}_\chi)$ とし，$\mathbf{O}$ と $\Lambda_{M_2}(\mathbf{Q})$ をこの順番で適用する．ここで，Λ_{M_2} はレジスタ $\left|m^*_{x,j}\right\rangle$ で制御される変換であり，最後の量子ビットが $|1\rangle$ だと $\mathbf{Q}$ がレジスタ $|x\rangle$ と $\left|0^{m+1}\right\rangle|0\rangle$ に適用される．次に $\mathbf{O}_x$ を $\mathbf{O}|x\rangle\left|0^{m+1}\right\rangle|0\rangle = |x\rangle\mathbf{O}_x\left|0^{m+1}\right\rangle|0\rangle$ という変換を行うユニタリ変換とする．$\mathbf{Q}_x = -\mathbf{O}_x\mathbf{S}_0\mathbf{O}_x^{-1}\mathbf{S}_\chi$ かつ任意の x,j に対して $m_{x,j} = \min(m^*_{x,j}, M_2)$ とすると，以下のように状態を表現できる．(以下では，簡単のため最後の 3 レジスタのみを表記する．)

$$\sum_{j=0}^{M-1} \frac{\delta_{x,j}}{\sqrt{2}} \left(\left|0^{m+1}\right\rangle|0\rangle|0\rangle + \mathbf{Q}_x^{m_{x,j}}\mathbf{O}_x\left(\left|0^{m+1}\right\rangle|0\rangle\right)|1\rangle\right), \tag{2.2}$$

式 (2.2) は以下のように書き直せる．

$$\sum_{j=0}^{M-1} \frac{\delta_{x,j}}{\sqrt{2}} \left(\left|0^{m+1},0\right\rangle|0\rangle + \left((-1)^{f(x)}\gamma_{x,j}\left|0^{m+1},0\right\rangle + |\varphi_{x,j}\rangle\right)|1\rangle \right)$$

ここで，$|\varphi_{x,j}\rangle$ は $\left|0^{m+1},0\right\rangle$ と直交しノルムが $\sqrt{1-\gamma^2_{x,j}}$ である．

ここで，第 3 レジスタ $\left|\tilde{\theta}_{x,j}\right\rangle$ が $|\theta_x - \tilde{\theta}_{x,j}| \leq \frac{\theta_x}{3(\pi+1)}$ を満たしているとする．この時，もし $|\theta_x - \tilde{\theta}_{x,j}| \leq \frac{\theta_x}{3(\pi+1)}$ ならば，$m_{x,j} \leq M_2$ であることは容易にわかる．そのため，$\mathbf{Q}_x$ は $m^*_{x,j}$ 回，すなわち第 4 レジスタで指定された回数だけ適用される．この時，文献 [21] の Lemma 2 と同様に，$\gamma_{x,j} \geq \sqrt{1-\frac{1}{9}}$ であることが示せる．

最後の量子ビットに Hadmard 変換を行うと，状態は以下のようになる．

$$\sum_{j=0}^{M-1} \frac{\delta_{x,j}}{2} \Bigg((1+(-1)^{f(x)}\gamma_{x,j})\left|0^{m+2}\right\rangle|0\rangle + (1-(-1)^{f(x)}\gamma_{x,j})\left|0^{m+2}\right\rangle|1\rangle + |\varphi_{x,j}\rangle(|0\rangle - |1\rangle) \Bigg) .$$

ここで，最後の量子ビットを観測して $|f(x)\rangle$ を得る確率は，

$$\sum_{j=0}^{M-1} \left(\left|\frac{\delta_{x,j}(1+\gamma_{x,j})}{2}\right|^2 + \left|\frac{\delta_{x,j}\sqrt{1-\gamma^2_{x,j}}}{2}\right|^2 \right) \geq \frac{1}{2} \sum_{j:|\theta_x-\tilde{\theta}_{x,j}|\leq\frac{\theta}{3(\pi+1)}} |\delta_{x,j}|^2 (1+\gamma_{x,j}) \geq \frac{2}{3}$$

となる．よって，最終の量子状態を

$$|x\rangle(\alpha_x|w_x\rangle|f(x)\rangle + \beta_x\left|w'_x\right\rangle\left|\overline{f(x)}\right\rangle$$

と表現したとき，任意の x に対して，$|\alpha_x|^2 \geq 2/3$ が成立する．

以上の量子アルゴリズムが用いるオラクルへの質問量は，Amplitude Estimation M_1 と Amplitude Amplification M_2 に関するものである．よって，オラクル質問量は $O(\frac{1}{\theta}) = O(\frac{1}{\varepsilon})$ である．

Lemma 4 と文献 [22] により，$O(\sqrt{N}/\varepsilon)$ 回 O^{ε}_f を用いて，N-bit OR の関数を成功確率 2/3 以上で計算することが可能である．

同じ問題に対して，下限 $\Omega(\sqrt{N}/\varepsilon_{min})$ が文献 [21] の Theorem 6 より示せるため，上記のアルゴリズムは最適であることがわかる．

参考文献

[1] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp, "Authentication of Quantum Messages," Proc. 43rd Annual IEEE Symposium on the Foundations of Computer Science, pp. 449-458, IEEE Press, 2002.

[2] R. Cleve, D. Gottesman, and H. L. Lo, "How to Share a Quamtum Secret," Phys. Rev. Lett., 83, 648, 1999.

[3] C. Crepeau, D. Gottesman, and A. Smith, "Secure Multi-party Quantum Computation," Proc. 34th Annual ACM Symposium on Theory of computing, pp.643–652, 2002.

[4] C. Crepeau, D. Gottesman, and A. Smith, "Approximate Quantum Error-Correcting Codes and Secret Sharing Schemes," EUROCRYPT 2005, May, 2005.

[5] D. Gottesman, "Stabilizer Codes and Quantum Correction," quant-ph/9705052.

[6] G. P. Guo and G. C. Guo, "Quantum Secret Sharing without Entanglement," Phys. Lett. A, vol. 310/4, pp.247–251, 2003.

[7] M. Hillery, C. Buzek, and A. Berthiaume, "Quantum Secret Sharing," Phys. Rev. A., 59, 1829, 1999.

[8] A. Karlsson, M. Koashi, and N. Imoto, "Quantum Entanglement for Secret Sharing and Secret Splitting," Phys. Rev. A., 59, 162, 1999.

[9] K. Kurosawa, S. Obana, and W. Ogata, "t-Cheater Identifiable (k, n) Threshold Secret Sharing Schemes," Proc. of CRYPTO'95, LNCS, 963, pp.410–423, 1995.

[10] A. Shamir, "How to Share a Secret," Commun. ACM 22, 612, 1979.

[11] S. Tani and M. Nakanishi and S. Yamashita, A quantum protocol for the list-nonequality function. In *Proceedings of the Eleventh Quantum Information Technology Symposium (QIT11)*, QIT2004-51, pages 21–25, IEICE, 2004.

[12] P. Tiwari. Lower Bounds on Communication Complexity in Distributed Computer Networks. Journal of the ACM, 34(4):921–938, 1987.

[13] S. Aaronson and A. Ambainis, Quantum Search of Spatial Regions. In *Proceedings of the 44th Symp. on Foundations of Computer Science*, pp.200–209, 2003.

[14] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett. 68, 3121 (1992).

[15] C. H. Bennett, and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," In Proc. IEEE International Conf. Computers, Systems, and Signal Processing, pp. 175–179, (1984).

[16] K. Boström and T. Felbinger, "Deterministic Secure Direct Communication Using Entanglement," Phys. Rev. Lett. 89, 187902 (2002)

[17] A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. 67, 661 (1991).

[18] L. Goldenberg and L. Vaidman, "Quantum cryptograph based on orthogonal states," Phys. Rev. Lett. 75, 1239 (1995).

[19] A. Kawachi, T. Koshiba, H. Nishimura, and T. Yamakami, "Computational indeistinguishability between quantum states and its cryptographic application," Proc. EuroCrypt 2005, LNCS 3494, pp. 268–284, (2005).

[20] T. Okamoto, K. Tanaka, and S. Uchiyama, "Quantum public-key cryptosystems," Proc. of CRYPTO 2000, LNCS 1880, pp.147–165, (2000).

[21] K. Iwama and R. Raymond and S. Yamashita, "General bounds for quantum biased oracles", IPSJ Journal, Vol. 46, No. 10, pp. 1234–1243, 2005.

[22] P. Høyer, M. Mosca, and R. de Wolf, "Quantum search on bounded-error inputs," ICALP, pp.291–299, 2003.

研究業績一覧

学術論文

1. M. Nakanishi, K.Hamaguchi, T.Kashiwabara:
"Expressive power of quantum pushdown automata with classical stack operations under the perfect-soundness conditions", IEICE Transactions on Information and Systems, Vol. E89-D, no. 3, pp. 1120–1127, 2005 年 3 月.
概要: One important question for quantum computing is whether a computational gap exists between models that are allowed to use quantum effects and models that are not. Several types of quantum computation models have been proposed, including quantum finite automata and quantum pushdown automata (with a quantum pushdown stack). It has been shown that some quantum computation models are more powerful than their classical counterparts and others are not since quantum computation models are required to obey such restrictions as reversible state transitions. In this paper, we investigate the power of quantum pushdown automata whose stacks are assumed to be implemented as classical devices, and show that they are strictly more powerful than their classical counterparts under the perfect-soundness condition, where perfect-soundness means that an automaton never accepts a word that is not in the language. That is, we show that our model can simulate any probabilistic pushdown automata and also show that there is a non-context-free language which quantum pushdown automata with classical stack operations can recognize with perfect soundness.

2. K. Iwama, A. Kawachi, S. Yamashita:
"Quantum Sampling for Balanced Allocations", IEICE Transactions on Information and Systems, Vol. E89-D, no. 1, pp. 39–46, 2005 年 1 月.
概要: When we put N balls into N bins uniformally at random, we obtain the highest bin which contains $\Theta(\ln N/\ln\ln N)$ balls with high probability. This problem has a practical meaning such as load balancing. In this paper, we investigate to use a quantum sampling for this problem, based on Grover's quantum search algorithm. We show that our quantum algorithm creates a bin which has $\Omega(\sqrt{\ln N/\ln\ln N})$ balls with high probability. However, it is known that the highest bin contains only $O(\ln\ln N)$ if we choose two bins at random for each ball and put it into the one which is less full. This simple randomized algorithm significantly outperforms the quantum algorithm.

3. M. Adcock, R. Cleve, K. Iwama, R. Putra, S. Yamashita:
"Quantum Lower Bounds for the Goldreich-Levin Problem", Information Processing Letters, Vol.97(5), pp. 208–211, 2006 年 3 月.
概要: At the heart of the Goldreich-Levin Theorem is the problem of determining an n-bit string a by making queries to two oracles, referred to as IP (inner product) and EQ (equivalence). The IP oracle, on input x, returns a bit that is biased towards $a \cdot x$ (the modulo two inner product of a with x) in the following sense. For a random x, the probability that $IP(x) = a \cdot x$ is at least $\frac{1}{2}(1+\varepsilon)$. The EQ oracle, on input

x, returns a bit specifying whether or not $x = a$. It has been shown that a quantum algorithm can solve this problem with $O(1/\varepsilon)$ IP and EQ queries, whereas any classical algorithm requires $\Omega(n/\varepsilon^2)$ such queries. Also, the quantum algorithm requires only $O(n/\varepsilon)$ auxiliary one- and two-qubit gates in addition to its queries. We show that the above quantum algorithm is optimal in terms of both EQ and IP queries. Specifically, $\Omega(1/\varepsilon)$ EQ queries are necessary, and $\Omega(1/\varepsilon)$ IP queries are necessary if the number of EQ queries is $o(\sqrt{2^n})$.

4. Y. Kawano, S. Yamashita, and M. Kitagawa:
"Explicit implementation of quantum circuits on a quantum-dot-cellular-automata-like architecture", Physical Review A, Vol. 72, No. 1, 012301, 2005 年 7 月.
概要: We present an efficient strategy to translate a normal quantum algorithm into a sequence of operations on the unidirectional periodic structure (UPS) originally proposed by S. Lloyd. The UPS assumes arrays of weakly coupled quantum systems where an interaction exists only between neighboring qubits, and can only perform the same quantum operation onto all the qubits. The sequence obtained by the strategy proposed by S. Lloyd needs at most $12n$ operations, where n is the number of qubits for the original circuit. The sequence obtained by our strategy needs at most $6n$ operations. We also clarified the relations between the upper bound of the number of translated operations and the period of the UPS, and between the upper bound of the number of qubits and the period of the UPS.

5. K. Iwama, R. Raymond, and S. Yamashita:
"General Bounds for Quantum Biased Oracles", Journal of IPSJ, Vol. 46, No. 10, pp. 2481–2491, 2005 年 10 月.
概要: An oracle with bias ϵ is an oracle that answers queries correctly with probability at least $1/2 + \epsilon$. In this paper, we study the upper and lower bounds of quantum query complexity of oracles with bias ϵ. For general upper bounds, we show that for any quantum algorithm solving some problem with high probability using T queries of perfect quantum oracles, i.e., oracles with $\epsilon = 1/2$, there exists a quantum algorithm solving the same problem, also with high probability, using $O(T/\epsilon)$ queries of the corresponding biased quantum oracles. As corollaries we can show robust quantum algorithms and gaps between biased quantum and classical oracles, e.g., by showing a problem where the quantum query complexity is $O(N/\epsilon)$ but the classical query complexity is lower bounded by $\Omega(N \log N/\epsilon^2)$. For general lower bounds, we generalize Ambainis' quantum adversary argument to biased quantum oracles and obtain the first lower bounds with explicit bias factor. As one of its applications we can provide another proof of the optimality of quantum algorithms for the so-called quantum Goldreich-Levin problem which was proved before by Adcock et al. using different and more complicated methods.

6. K. Iwama, A. Kawachi and S. Yamashita:
"Quantum Biased Oracles", Journal of IPSJ, Vol. 46, No. 10, pp. 2400–2408, 2005 年 10 月.
概要: This paper reviews researches on quantum oracle computations when oracles are not perfect, i.e., they may return wrong answers. We call such oracles *biased* oracles, and discuss the formal model of them. Then we provide an intuitive explanation how quantum search with biased oracles by Høyer et. al works. We also review the method, by Buhrman et. al, to obtain all the answers of a quantum biased oracle without

any overhead compared to the perfect oracle case. Moreover, we discuss two special cases of quantum biased oracles and their interesting properties, which are not found in the classical corresponding cases. Our discussion implies that the model of quantum biased oracle adopted by the existing researches is natural.

7. Y. Murakami, M. Nakanishi, S. Yamashita and K. Watanabe:
"Quantum versus Classical Pushdown Automata in Exact Computation", Journal of IPSJ, Vol. 46, No. 10, pp. 2471–2480, 2005 年 10 月.
概要: Even though quantum computation is useful for solving certain problems, classical computation is more powerful in some cases. Thus, it is significant to compare the abilities of quantum computation and its classical counterpart, based on such a simple computation model as automata. In this paper we focus on the quantum pushdown automata which were defined by Golovkins in 2000, who showed that the class of languages recognized by quantum pushdown automata properly contains the class of languages recognized by finite automata. However, no one knows the entire relationship between the recognitive abilities of quantum and classical pushdown automata. As a part, we show a proposition that quantum pushdown automata can deterministically solve a certain problem that cannot be solved by any deterministic pushdown automata.

8. M. Nakanishi:
"Automata with quantum and classical resources", Journal of IPSJ, Vol. 46, No. 10, pp. 2384–2391, 2005 年 10 月.
概要: Quantum automata have been studied as simple quantum computation models. They can be considered models of small (or restricted) quantum computers. In this paper, we give descriptions of several kinds of quantum automata and show their power in comparison to their classical counterparts. We also give descriptions of quantum automata that have additional classical computational resources. Introducing classical computational resources can enhance the power of quantum automata, since this approach relaxes such restrictions as reversible state transitions.

9. S. Tani, M. Nakanishi, S. Yamashita:
"Quantum Communication Complexity for the Distinctness Function on a Ring", Workshop on Theory of Quantum Computation, Communication, and Cryptography 2006, pp. 10–11, 2006 年 2 月.
概要: This paper considers the problems of computing functions that depend on distributed inputs on a network whose underlying toplology is not necessarily a complete graph. We first establish a lower bound technique for the communication complexity of computing any Boolean function that depends on the inputs given to two parties on the network of any topology. Next we apply the technique to lower-bound the communication complexity of computing the Distinctness problem on an n-party ring, and also give two quantum algorithms for the problem to upper-bound the complexity. When the set of possible input is of size $O(n)$, our bound is tight.

研究会等

1. 岩間一雄, 河内亮周, Rudy Raymond, 山下茂:
"オラクル同定問題に対するロバストな量子アルゴリズム", 電子情報通信学会 量子情報技術研究会, QIT2005-11, pp. 42–47, 2005 年 5 月.
概要: The oracle identification problem (OIP) was introduced by Ambainis et al., which is given as a set S of M oracles and

a blackbox oracle f. Our task is to figure out which oracle in S is equal to the blackbox f by making queries to f. OIP includes several problems such as the Grover Search as special cases. In this paper, we design *robust* algorithms, i.e., those which are tolerant against noisy oracles, for OIP. Our results include: (i) For any oracle set S such that $|S|$ is polynomial in N, $O(\sqrt{N})$ queries are enough to identify the blackbox oracle, which is obviously optimal since this OIP includes the Grover Search as a special case. (ii) For the case that $|S| \leq 2^{N^d}$ $(d < 1)$, we design an algorithm whose query complexity is $O(\sqrt{N \log M / \log N})$ and matches the known lower bound. (iii) We can furthermore design a robust algorithm whose complexity changes smoothly between the complexity of (ii) and the complexity of recovering all information about the blackbox oracle whose complexity is $O(N)$ as showed by Buhrman et al. Thus our new algorithms are not only robust but also better than the previous noiseless case in terms of query complexity.

2. Y. Murakami, M. Nakanishi, S. Yamashita, K.Watanabe:
"Cheater Identifiable Quantum Secret Sharing Schemes", 情報セキュリティ研究会, vol. 105, pp. 90–92, 2005 年 7 月.
概要: In this paper, we show that there exists a cheater identifiable (k, n) threshold secret sharing scheme for a quantum secret. Suppose that there are at most t cheaters $(k \geq 3t + 1)$, k or more participants can identify who are cheating. Our scheme utilizes authentication codes based on an orthogonal array and stabilizer codes, which are unconditionally secure. Moreover, we discuss the relation between n and t.

3. T. Katsumata, M. Nakanishi, S. Yamashita, K. Watanabe:
"Quantum sealing schemes against collective measurement attacks", 電子情報通信学会 量子情報技術研究会, QIT2005-90, pp. 229–232, 2005 年 11 月.
概要: A quantum seal is a way of encoding a classical message into quantum states, so that everyone can read the message with no or little error, while authorized verifiers can detect that someone has read the message and broken the seal. We present two schemes that are more impervious to collective measurement than the Bechmann-Pasquinucci scheme. Both schemes have an advantage that the longer a classical message is encoded, the more difficult a collective measurement perform in practice. Moreover one of them, *scheme 2*, may make it impossible to try collective measurement depending on an encoded classical message.

4. K. Iwama, H. Nishimura, R. Raymond, S. Yamashita:
"Transmitting classical information on the quantum network efficiently", 電子情報通信学会 コンピュテーション研究会, vol. 105, pp. 15–20, 2005 年 12 月.
概要: The question in this paper is whether the quantum random access (QRA) coding, given by Ambainis et al., on the *network* is possible. This question is motivated by the network coding introduced by Ahlswede et al., which enables us to send classical information much more efficiently on the network by coding at intermediate nodes. We demonstrate that quantum network coding is possible for the QRA coding, by using a simple network model called the Butterfly network. In this network, there are two flow paths, s_1 to t_1 and s_2 to t_2, which shares a single bottleneck channel of capacity one. In the classical case, we can send two bits simultaneously, one for each path, in spite of the bottleneck. However, the quantum case makes this bottleneck much more se-

vere than in the classical case because of the non-orthogonality of quantum states. We resolve this bottleneck and design a protocol which can send two classical bits from s_1 to t_1 (similarly from s_2 to t_2) but only one of them should be recovered.

5. 林正人, 岩間一雄, 西村治道, Rudy Raymond, 山下茂:
"量子ネットワーク上での効率的な情報の伝送", 冬のＬＡシンポジウム, 2006 年 1 月.
概要: Since quantum information is continuous, its handling is sometimes surprisingly harder than the classical counterpart. A typical example is cloning; making a copy of digital information is straightforward but it is not possible exactly for quantum information. The question in this paper is whether or not *quantum* network coding is possible. Its classical counterpart is another good example to show that digital information flow can be done much more efficiently than conventional (say, liquid) flow. Our answer to the question is similar to the case of cloning, namely, it is shown that quantum network coding is possible if approximation is allowed, by using a simple network model called Butterfly. In this network, there are two flow paths, s_1 to t_1 and s_2 to t_2, which shares a single bottleneck channel of capacity one. In the classical case, we can send two bits simultaneously, one for each path, in spite of the bottleneck. We show that We can send any quantum state $|\psi_1\rangle$ from s_1 to t_1 and $|\psi_2\rangle$ from s_2 to t_2 simultaneously with a fidelity strictly greater than 1/2.

6. 鈴木智哉, 山下茂, 中西正樹, 渡邉勝正:
"誤り率を考慮したバイアス付量子オラクル計算量", 冬のＬＡシンポジウム, 2006 年 1 月.
概要: This paper considers the quantum query complexity of *ε-biased oracles* that return the correct value with probability only $1/2 + \varepsilon$. In particular, we show a quantum algorithm to compute N-bit OR functions with $O(\sqrt{N}/\varepsilon)$ queries to ε-biased oracles. This improves the known upper bound of $O(\sqrt{N}/\varepsilon^2)$ and matches the known lower bound; we answer the known conjecture affirmatively. We also show a quantum algorithm to cope with the situation in which we have no knowledge about the value of ε. This contrasts with the corresponding classical situation, where it is almost hopeless to achieve more than a constant success probability without knowing the value of ε.

7. Geometric Characterization of Quantum Oracle Identification:
"河内亮周, 山下茂", 冬のＬＡシンポジウム, 2006 年 1 月.
概要: We geometrically characterize the query complexity of the oracle identification problem in this paper. By defining an inner product between two oracles, we construct a quantum algorithm, which generalizes Bernstein-Vazirani and Grover algorithms, for a certain class of the oracle identification problem characterized by the inner product. We also show the optimality of this quantum algorithm.

学会大会等

1. Y. Murakami, M.Nakanishi, S.Yamashita, K.Watanabe:
"No preshared key quantum secret communication protocol", 電子情報通信学会２００６年総合大会講演論文集, DS-1-12, 2006 年 3 月.

A08: 動的な構造をもつネットワーク上の資源割当て問題の研究

藤田 聡　中野 浩嗣　森本 康彦

広島大学 大学院 工学研究科
〒 739-8527 東広島市鏡山 1-4-1

1　はじめに

本研究課題の目的は、動的な構造をもつネットワーク上の資源割当て問題の数理的な構造を明らかにし、その根本的な解決のための道筋を示すことである。本研究の柱は以下の 3 つである：

1) 動的ネットワーク上の資源割当て問題のモデル化と特徴づけ

2) 実時間性を考慮した新たな評価基準の考案とその妥当性の検証

3) 考案した評価基準のもとで最適なアルゴリズムの提案とその有効性の評価

昨年度までの研究成果を踏まえて研究を進めた結果、本年度は以下のような成果をあげることができた。

a) 参加ノードが動的に変化する無線通信ネットワーク上で通信品質を保証するための各端末への通信機会 (TXOP) 割当て問題を定義し、この問題に対する解法の提案を行った。

b) 構造が動的に変化する P2P ネットワーク上での共有資源の効率的な管理を目的として、スキップグラフに基づく新しいオーバーレイネットワークの提案を行った。

c) DHT 型 P2P 上で効率よく連言検索を行うための手法の提案を行った。提案手法の基本アイデアは、検索の部分結果を保持するリザルトキャッシュの使用と、ブルームフィルタによる効率的な情報共有である。

以下では、上記の a), b) について、背景と研究の位置づけを含めて、本研究課題の成果として得られた結果の概要を述べる。

2　無線 LAN における TXOP 割当て問題

2.1　背景

無線 LAN におけるメディアアクセス制御は、アクセスポイント (AP) がポーリングによって集中制御を行う PCF (Point Coordination Function) と、各端末が CSMA/CA により分散的に送信を試みる DCF (Distributed Coordination Function) を適切に組み合わせることで実現される。ただし、マルチメディア通信などのように通信品質 (QoS) の保証が求められる用途においては、ポーリングによる制御をいかにうまく行うかが重要となる。

QoS 保証を前提とした無線 LAN の規格のひとつである IEEE802.11e では、PCF を拡張した HCCA(HCF Controlled Channel Access) と呼ばれる方式が採用されている。HCCA の基本アイデアは、通信を希望する各フローからそのフローの満たすべき要件 (具体的には遅延と転送速度) をあらかじめ収集した上で、各フローに対して、それらの要件を満たすような通信機会 (Transmission Opportunity: TXOP) の割当てを行うことである。HCCA で実際に採用されている TXOP の割当て方法は、次のようなものである：1) 各フローが要求する遅延時間の中で最も厳しい値を、各フローに対して通信機会が割当てられる共通のサービスインターバル (SI) とする。2) 各 SI ごとに、各フローが要求する転送速度を実現するような TXOP 割当てを行う。この方式には、各フローに対する遅延時間の保証が容易になるという利点がある一方で、遅延時間の長いフローに対しても均一な SI で TXOP の割当てがなされるため、効率が悪いという欠点がある。以下では、HCCA の上記の問題点を解決するための、新しい TXOP 割当て手法の提案を行う。

2.2 モデル

以下ではQoS制御機能をもつAPをQAP (QoS Access Point) と呼び、QAPに接続している各端末をQSTA(QoS STAtion) と呼ぶ。HCCAの具体的な手続きは以下の通りである：

1. 各QSTAがQAPに対して、送信を希望するフローの情報を送る。
2. QAPは受け取ったフローの受け入れが可能かどうかを判定し、もし可能であればフローに対するTXOPの割当てと送信タイミングの決定を行い、そうでなければそのことをQSTAに通知する。
3. QAPによって受け入れられたフローに対するアクセス制御は、“QoS CF-Poll” と呼ばれるフレームを、該当するQSTAに対して送ることで実現される。このフレームを受け取ったQSTAは、フレーム内に記述された時間の間だけフローの送信を行うことができる。

2.3 提案手法

QAPからすべての端末に向けて定期的に発せられるビーコンの時間間隔をT_bとし、通信を希望するフローの集合を$S = \{q_1, q_2, \ldots, q_k\}$とする。フロー$q_i$が要求する最大遅延時間 (RSI) を$r(q_i)$と記す。提案手法では、要求される最大遅延時間の厳しさに応じたクラス分けをS中のフローに対して行った後、要求される転送速度に応じたTXOPの割当てを各フローに対して行っていく。

Step 1 (フローのクラス分け): Sに含まれるフローの中で最も厳しい遅延時間をr^*とする。r^*が、任意の$q \in S$に対して$r^* \leq r(q)$を満たすような最大の値であることに注意しよう。集合Sに関する最小サービスインターバル (MSI) を$T^* \stackrel{\text{def}}{=} T_b/2^i$のように定義する。ここで$i$は、$T_b/2^i \leq r^* < T_b/2^{i-1}$を満たす整数である。以下では、$r(q)$が$2^j \times T^* \leq r(q) < 2^{j+1} \times T^*$を満たすとき、フロー$q$のクラスは$j$であると呼ぶことにする。

Step 2 (TXOPの計算): 次に、各フローに対して、RSIの厳しさに応じたSIを割り当てる。具体的には、クラスjに属する各フローのSIは、$T_j \stackrel{\text{def}}{=} 2^j \times T_0$のように決定される。SIを決定した後、各クラスごとにTXOPの割当てを行う。具体的には、各フローがそのフローに対して与えられたSIの間に転送しなくてはならない平均フレーム数を求め、その数だけのフレームを送るのに必要な時間を物理層の転送速度から求めた上で、その値をTXOPとしてフローに割り当てる。

Step 3 (アドミッションコントロール): TXOPが割り当てられたフローに対するアドミッションコントロールは、以下のように行われる。基本アイデアは、各フローに対してそのフローの属するクラスに応じた重み付けを行い、その総和がHCCAに与えられた時間を越えないかどうかで受け入れ可能性を判断することである。第i番目のフローに割当てられたTXOPをt_iとし、そのフローに割当てられたSIをT_iとする (そのフローのクラスが$\log_2(T_i/T_0)$で与えられることに注意しよう). このとき、k番目のフローが受け入れられるための条件は、以下のように与えられる：

$$\sum_{i=1}^{k} \left(\frac{t_i}{T_i} \right) \leq \alpha$$

ここでα (≤ 1) はビーコンインターバルT_bの中で提案手法のために用いることのできる時間の割合を示す値であり、すべての時間を提案手法のために用いることができるとき1となる.

2.4 スケジューリング

フローのスケジューリングは、QSTAから新しいフローの送信要求が送られてきたときに実行される。スケジューリングの目的は、各フローのTXOPを、以下の条件を満たすように時間軸に割当てることである：1) あるフローに割当てられたSIの中で、そのフローのTXOPがいつも同じ場所から開始されていること。2) 複数の異なるTXOPがオーバーラップしないこと。ここで前述のアドミッションコントロールが、フローの開始時刻の周期性を想定しない理想的な状況に対応していることに注意しよう (したがって、上述のアドミッションコントロールで受け入れが拒否されたフローは、どのような方法を用いてもスケジューリングすることはできない)。

本研究ではこの問題に対し、以下のようなスケジューリング方式を提案する。提案手法の基本アイデアは、以下のようなフローの順序付けにしたがって、貪欲に TXOP の時間軸への割り当てを行うことである：1) フローの割当ては、より短い SI が割当てられたフローから順番に行われる。2) もし同じ SI が割当てられたフローが複数存在する場合は、そのフローに割当てられた TXOP の長い順にフローの割り当てがなされる。加えて、スケジューリングの公平性を保つため、新しいフローの受け入れが決定されたときは、すでに受け入れているフローの割り当てが終わった後で、新しいフローの割り当てを行うものとする。ここで、上記のフローの順序付けには、時間軸の断片化を防ぐ狙いがあることに注意されたい。

提案手法における具体的な割当てアルゴリズムは以下の通りである：

Step 1: まずクラス 0 に属する各フローの TXOP を、時間軸上の連続した区域に、任意の順番で割当てる (ここでクラス 0 がもっとも遅延要求の厳しいクラスであることに注意)。次にビーコンインターバル上でクラス 0 のフローが割当てられていない時間軸上の連続した領域を考え、それらを左から順に、$P_1, P_2, \ldots, P_k$ のようにラベル付けする。ここで定義より、k が 2 のべき乗であり、各連続領域の長さがすべて等しいことに注意されたい。

Step 2: 次に、各クラスの CTP (corresponding time periods) をそれぞれ定義する。具体的には、クラス j (≥ 1) の CTP は、$P_{i\times 2^j - 2^{j-1}}$ のように定義される。ここで i は $1 \leq i \leq k/2^j$ を満たす整数である。したがってたとえば、クラス 1 の CPT は $P_1, P_3, P_5, \ldots, P_{k-1}$、クラス 2 の CPT は $P_2, P_6, P_{10}, \ldots, P_{k-2}$、などのように定義される。

Step 3: 変数 j を 1 に初期化する。

Step 4: クラス j に属するフローの TXOP をクラスクラス j' ($\leq j$) の CPT に割当てる。このとき、パッキングされていないアイテムの総和を最小化するような、異なるサイズのビンに対する一種のビンパッキング問題が解かれていることに注意されたい。もしそれらの TXOP が与えられた CTP に収まりきらないときは、残った TXOP はより大きなクラスの CPT にパッキングされる (構成法よりあきらかに、より大きなすべてのクラスの CPT のユニオンは、クラス j の CPT と同一の構造をもつことに注意)。なお、より大きなクラスの CTP を使ってパッキングをしたときは、各連続領域の長さを使用した領域の長さの分だけ短くする。

Step 5: もしまだ TXOP の割当てが完了していないフローが存在すれば、変数 j の値を 1 増やして Step 4 へ。そうでなければ、アルゴリズムを終了する。

3 検索コストの最小化をめざした P2P オーバーレイ

3.1 背景

情報管理を集中的に行うサーバの存在を仮定しない「ピュア型 P2P システム」のためのオーバーレイネットワークは、その構成法によって、構造型と非構造型とに大別される。非構造型オーバーレイを用いた P2P システムの具体例として、Gnutella や Freenet などが知られている。非構造型オーバーレイのノード次数は一般に定数であり、生存時間 (TTL) で制御されるクエリのフラッディングによって、求めるべきコンテンツの検索が行われる。一方の構造型オーバーレイの具体例としては、分散ハッシュテーブル (Distributed Hash Table: DHT) が広く知られており、これまでに様々な座標空間に基づいた DHT 型 P2P システムが提案されている。DHT に基づく構造型オーバーレイ上でのインデックス検索には、非構造型オーバーレイの場合とは異なり、もし目的とするインデックスがシステム上に保存されていればそれを必ず取得することができるという大きなメリットがある。しかし一般に DHT 型オーバーレイでは、ノード次数と平均ルーティング時間との間にトレードオフの関係があり、したがってたとえば多項対数 (polylog) 時間でのクエリのルーティングを実現するためには、ノード次数を $\log\log N$

や $\log N$ などの “N に依存した値” に設定する必要がある。

本研究では、各ノードの平均次数が定数で、しかも多項対数時間でのクエリのルーティングを可能とするような、新しい構造型オーバーレイネットワークの提案を行った。提案するオーバーレイネットワークは、Aspnes と Shah によって提案されたスキップグラフの拡張となっている。スキップグラフは、順序関係のあるデータ集合に対する効率的なキー検索を実現するために提案された分散データ構造の一種であり、基本となる線形リストに対して平均次数が $O(\log N)$ となるようにショートカットリンクを付加して得られる構造をもっている。以下では、スキップグラフで用いられていたノードあたり $O(\log N)$ 本のショートカットリンクのうち、定数本のみをランダムに選択することで、$O(\log^2 N)$ ステップの平均ルーティング時間が実現できることを証明する。定理の証明には、Kleinberg が提案したグリッドグラフのためのショートカット手法と同様のアイデアが用いられる。実際、本稿で提案するオーバーレイネットワークは、スキップグラフのショートカット選択に対して Kleinberg の手法を近似的に応用したものとなっている。

3.2 スキップグラフ

スキップグラフ (以下、SG) は、順序関係のあるデータ集合に対する効率的な検索を実現するために提案された分散データ構造の一つである。N 個のノードからなるノード集合 V を考える。V 中の各ノード u には、固有の識別子のほかに、整数値 $key(u)$ がキーとして割り当てられているものとする。加えて各ノードには、ランダムかつ独立に選択された無限長のビット列が**メンバーシップベクトル**として割り当てられる。以下では、ノード u に割り当てられたメンバーシップベクトルを $m(u)$ と記す。

ある与えられたキー k を保持しているノードを V の中から探し出す問題を考える。この問題を効率よく解くために SG で用いられている基本アイデアの一つは、集合 V を、そこで保持されているキーの大きさに関して整列 (sorting) することである。整列の結果は、隣り合った要素をキーとしてもつ 2 ノード間を双方向リンク (無向辺) で結んで得られる線形リストの形で保存される。以下では、このリストのことを**基本リスト**と呼び、記号 C で表現する。キーの探索効率を高めるために SG で採用されているアイデアの二つ目は、基本リストに対して効果的なショートカットを付加することである。あるリスト L の**部分リスト** L' とは、L 中の要素のいくつか (もしくは全部) を、L 中で出てくる順番に、双方向リンクで結んで得られるリストのことである。また基本リスト C の**レベル i の部分リスト**とは、C の部分リストの中で、メンバーシップベクトルの「長さ i のプレフィックス」が同一であるようなノードたちのみを結んで得られるもののことをいう (レベル 0 の部分リストが C そのものであることに注意しよう)。ただしここでは部分リストとして、長さが 2 以上のリストのみを考えることにする[1]。無限の長さをもつビット列の長さ i の異なるプレフィックスの個数は 2^i であるから、レベル i の部分リストが、任意の C に対して高々 2^i 個存在しうることに注意しよう。また各ノードは任意の i について高々一つのレベル i の部分リストにしか含まれず、しかもここでは各部分リストの長さが少なくとも 2 以上であると仮定しているので、レベル i の部分リスト数の上限は、値 $\lfloor N/2 \rfloor$ によっても与えることができる。

いま、リスト C のレベル i の (長さ 2 以上の) 部分リスト全体で用いられている辺の集合を E_i としよう。ここで各辺にはその辺の所属している部分リストのレベルがラベルとして付与されており、同一のノード対を結んでいても、ラベルが異なるものは別の辺と見なすことにする。このときスキップグラフ G は、

$$G \stackrel{\text{def}}{=} \langle V, \bigcup_{i=0}^{\infty} E_i \rangle \tag{2.3}$$

のように定義される。文献では、N 個のノードをもつ SG の平均次数と直径の期待値がともに $O(\log N)$ であることが示されている。

[1] 長さ 1 のリストはショートカットとしての意味をなさないため。

3.3 提案手法

提案手法では、各ノードは集合 D $(=\{1,2,\ldots,\log N\})$ から δ 個の要素を (重複なく) 等確率で選択し、選択された要素のそれぞれをショートカット生成のためのプレフィックス長として用いる (δ は生成されるオーバーレイの次数になる)。具体的には、選択された要素が ℓ のとき、そのノードは「長さ ℓ のプレフィックス」が同一となるような基本リスト上の次のノード v を特定し、そのノードに向けてショートカットリンクを張ることになる。

$k=\log N$ をメンバーシップベクトルの長さとし、$\delta=1$ とする。以下では簡単のために、メッセージのルーティング方向は一方向とし、終点ノード t は基本リスト上の端点に位置するとする。したがって、各ノードは選択したプレフィックスによってその方向のみのショートカットを生成する。また、終点ノードとの距離によってノード集合を以下のように分ける: 1) 集合 B_0 を t からの距離が 1 となる 2^0 $(=1)$ 個のノード集合とし、2) 各 $1\le j\le \log N-1$ について、集合 B_j を t からの距離が $2^{j-1}+1$ から 2^j までの 2^{j-1} 個のノード集合とする (基本リスト上で存在しうる最長の距離が $2^{\lceil \log N\rceil}-1$ であることに注意しよう)。

ノード u が ℓ $(\in D)$ をプレフィックス長として選択したとしよう。他のノード v が u と同じ長さ ℓ のプレフィックスを持っている確率は $1/2^\ell$ であるから、ノード u から集合 $\{t\}\cup\bigcup_{i=0}^{j}B_i$ 内のあるノードにショートカットが張られている確率は、

$$P_\ell = \left(1-\frac{1}{2^\ell}\right)^{x-1}\left\{1-\left(1-\frac{1}{2^\ell}\right)^{2^j}\right\}$$

となる。ここで、x は u から B_j までの距離である。$y=2^j$ のとき $1\le x\le 2^j$ であるから、一般性を失うことなく、$x-1=2^{j-1}=y/2$ と仮定することができる。このとき、

$$\begin{aligned} P_\ell &= \left(1-\frac{1}{2^\ell}\right)^{y/2}\left\{1-\left(1-\frac{1}{2^\ell}\right)^{y}\right\} \\ &= \left(1-\frac{1}{2^\ell}\right)^{y/2}-\left(1-\frac{1}{2^\ell}\right)^{y+y/2} \\ &> \left(1-\frac{1}{2^\ell}\right)^{y/2}-\left(1-\frac{1}{2^{\ell-1}}\right)^{y/2} \end{aligned}$$

となるが、いま、各プレフィックスは確率 $1/k$ で選択されるため、u から $\{t\}\cup\bigcup_{i=0}^{j}B_i$ 内のあるノードにショートカットが張られている確率 P は、

$$\begin{aligned} P &> \left(\frac{1}{k}\right)(P_k+P_{k-1}+\cdots+P_1) \\ &> \left(\frac{1}{k}\right)\left\{\left(1-\frac{1}{2^k}\right)^{2^{j-1}}-\left(\frac{1}{2}\right)^{2^{j-1}}\right\} \\ &\simeq \left(\frac{1}{k}\right)\left(\frac{1}{e}\right)^{1/2^{k-j+1}} \end{aligned}$$

となり、不等式の右辺は、ある定数 α を用いて α/k のように表現することができる。実際、

- $j=\log N$ のとき $P>0.6065/\log N$、
- $j=\log N-1$ のとき $P>0.7788/\log N$、
- $j\le \log N-2$ のとき $P>0.8825/\log N$

となる。したがって、部分集合 B_{j+1} 内でのルーティング時間の期待値は、

- $j=\log N$ のとき $1.65\log N$、
- $j=\log N-1$ のとき $1.29\log N$、
- $j\le \log N-2$ のとき $1.14\log N$

となる。このような部分集合は高々$\log N$ 個であるため、ルーティング時間の期待値は高々$1.65\log^2 N$ となる。

δ の値を増やした場合は、上記の解析の中で各ノードが行っていたベルヌーイ試行の数が 1 から δ に増加するため、走査するノード数の期待値は、単純に $1/\delta$ に減ることになる。したがって、ルーティング時間の期待値は、高々$(1.65/\delta)\log^2 N$ となる。

3.4 拡張

前節では、各ノードの次数を定数に抑えたままで多項対数時間でのルーティングを実現するためのスキップグラフの拡張方法を述べた。以下ではスキップグラフのもうひとつの拡張として、より多くの次数を用いることで、二重対数時間でのルーティングを実現する方法を示す。ここで、各ノードの次数が $n-1$ のとき、定数時間のルーティン

グが自明に達成されることに注意しておこう。したがって以下では、次数をできるだけ抑えたままで二重対数時間のルーティングを行うことを具体的な目標とする。

基本アイデアは、$\lg\lg N$ 段のレベルをもつ再帰的な構造を用いることである (このような構造は、たとえば PRAM 上の中央値選択アルゴリズムなどで用いられている)。再帰の基本ステップは、与えられたサイズ M の集合をサイズ $\sqrt{M}$ の $\sqrt{M}$ 個の部分集合に分割し、再帰のより深いレベルに受け渡すことである。与えられた集合のサイズが N のとき、上記のステップを繰り返し適用することで、各レベルの部分集合のサイズは

$$N^{1/2}, N^{1/4}, N^{1/8}, N^{1/16}, \ldots$$

のように縮小していくことになる。したがって、部分集合のサイズが定数になるレベルの深さは $i = \lg\lg N$ となる。

メンバーシップの考え方を用いることで、そのような再帰的な分割を、以下のように行うことができる：1) 各ノードにそれぞれ長さ $\lg N$ のメンバーシップベクトルを与える。2) i 番目のレベルの部分集合を、メンバーシップベクトルの長さ $\sum_{j=1}^{i}(\lg N)/2^j$ のプレフィックスが同一のノードたちからなる集合として定義する。ここで $\sum_{j=1}^{i}(\lg N)/2^j = (\lg N)\left(\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{2^i}\right) = \lg N - \left(\frac{1}{2^i}\right)\lg N$ であることに注意しておこう。もし同一のレベルに属するすべてのノードを互いに (完全結合で) 結ぶことができれば、同一のレベルに属するノード間の通信をそれぞれ定数ステップで実現することができるから、任意の 2 ノード間のメッセージ転送を平均 $O(\log\log n)$ ステップで実現できるようなネットワークが構成されることになる (結合がランダムに与えられたメンバーシップベクトルに基づいて行われることに注意しよう)。したがって、平均通信時間をスキップグラフの $O(\log n)$ から $O(\log\log n)$ に大幅に減少することができる。ただしこのような直接的な方法では、根に最も近いレベルの部分集合のサイズが $\sqrt{N}$ であることから、ノードあたりの次数は、

$$\sum_{i=1}^{\lg\lg N} N^{1/2^i} = \sqrt{N} + O(N^{1/4})$$

にまでしか抑えることができない。

しかし上述のノード次数は、ステップ数をわずかに増加させることで、次のような方法を用いて減少させることが可能である。基本アイデアは、最も高いレベルのショートカットリンクを (同様の手法を最適的に用いることで) $\lg\lg N - 1$ ステップでシミュレートすることである。再帰の最も高いレベルのリンクが、同一部分集合に属する $N^{1/2}$ 個のノードを完全結合していたことに注意しよう。前述の手法が N 個のノード間のルーティングを平均 $O(\log\log n)$ ステップで実現していたことに注意すると、同様の手法を最も高いレベルに適用することで、ノードあたりの平均次数を

$$2\sum_{i=2}^{\lg\lg N} N^{1/2^i} = 2N^{1/4} + O(N^{1/8}).$$

にまで減少させることができる。さらにこのような再帰的な手法を k 回適用することで、平均ルーティング時間を $2^k \lg\lg N$ に抑えたままで、ノードの次数を

$$2^k N^{1/2^k} + O(N^{1/2^{k+1}})$$

に減少させることができる。したがって、たとえば k の値を $k = \lg\lg\lg N$ のように設定すれば、ノード次数が $(\lg\lg N) \times N^{1/\lg\lg N}$ であるようなネットワーク上で平均 $(\lg\lg N)^2$ ステップのルーティングを実現することが可能となる。

研究業績一覧

学術論文

1. H. Osada, S. Fujita:
   “CHQ: A Multiagent Reinforcement Learning Scheme for Partially Observable Markov Decision Processes”, IEICE Trans. Information and Systems, E88-D(5), 1004–1011, (2005).
   概要: In this paper, we propose a new reinforcement learning scheme called CHQ that could efficiently acquire appropriate policies under partially observable Markov decision processes (POMDP) involving probabilistic state transitions, that frequently occurs in multi-agent systems in which each agent

independently takes a probabilistic action based on a partial observation of the underlying environment. A key idea of CHQ is to extend the HQ-learning proposed by Wiering *et al.* in such a way that it could learn the activation order of the MDP subtasks as well as an appropriate policy under each MDP subtask. The goodness of the proposed scheme is experimentally evaluated. The result of experiments implies that it can acquire a deterministic policy with a sufficiently high success rate, even if the given task is POMDP with probabilistic state transitions.

2. S. Tagashira, S. Shirakawa, S. Fujita:
"Proxy-Based Index Caching for Content-Addressable Networks", IEICE Trans. Information and Systems, E89-D(2), 555–562, (2006).
概要: Content-Addressable Network (CAN) provides a mechanism that could retrieve objects in a P2P network by maintaining indices to those objects in a fully decentralized manner. In the CAN system, index caching is a useful technique for reducing the response time of retrieving objects. The key points of effective caching techniques are to improve cache hit ratio by actively sharing caches distributed over the P2P network with every node and to reduce a maintenance and/or routing overhead for locating the cache of a requested index. In this paper, we propose a new caching technique based on the notion of proxy-type caching techniques which have been widely used in WWW systems. It can achieve active cache sharing by incorporating the concept of proxy caching into the index access mechanism and locate a closer proxy cache of a requested index with a little routing overhead. By the result of simulations, we conclude that it can improve the response time of retrieving indices by 30conventional caching techniques.

3. H. Ochi, S. Tagashira, S. Fujita:
"A Localization Scheme for Sensor Networks Based on Wireless Communication with Anchor Groups", IEICE Trans. Information and Systems, （掲載予定）.
概要: In this paper, we propose a new localization scheme for wireless sensor networks consisting of a huge number of sensor nodes equipped with simple wireless communication devices such as wireless LAN and Bluetooth. The proposed scheme is based on the Point-In-Triangle (PIT) test proposed by He *et al.* The scheme is actually implemented by using Bluetooth devices of Class 2 standard, and the performance of the scheme is evaluated in an actual environment. The result of experiments indicates that the proposed scheme could realize a localization with an error of less than 2 m.

4. D. Takemoto, S. Tagashira, S. Fujita:
"A Fault-Tolerant Content Addressable Network", IEICE Trans. Information and Systems, （掲載予定）.
概要: In this paper, we propose a new method to enhance the fault-tolerance of the Content Addressable Network (CAN), which is known as a typical pure P2P system based on the notion of Distributed Hash Table (DHT). The basic idea of the proposed method is to introduce redundancy to the management of index information distributed over the nodes in the given P2P network, by allowing each index to be assigned to several nodes, which was restricted to be one in the original CAN system. To keep the consistency among several copies of indices, we propose an efficient synchronization scheme based on the notion of labels assigned to each copy in a distinct manner. The performance of the proposed scheme is evaluated by simulation. The result of simulations indicates that the proposed scheme significantly enhances the

fault-tolerance of the CAN system.

5. S. Tagashira, M. Mito, S. Fujita:
"A Generic Solver based on Functional Parallelism for Solving Combinatorial Optimization Problems", IEICE Trans. Information and Systems, （掲載予定）.
概要: This paper proposes a new class of parallel branch-and-bound (B&B) schemes. The main idea of the scheme is to focus on the functional parallelism instead of conventional data parallelism, and to support such a heterogeneous and irregular parallelism by using a collection of autonomous agents distributed over the network. After examining several implementation issues, we describe a detail of the prototype system implemented over eight PC's connected by a network. The result of experiments conducted over the prototype system indicates that the proposed parallel processing scheme significantly improves the performance of the underlying B&B scheme by adaptively switching exploring policies adopted by each agent participating to the problem solving.

6. 藤田聡:
"分散ネットワーク上の故障診断問題について", 電子情報通信学会論文誌 A,（掲載予定）.
概要: Preparata らによって 1967 年に提案された分散システムのための自律的な故障診断モデルである PMC モデルは、近年、アルゴリズム理論や計算複雑さに関する研究者たちをまきこんで、新しい展開を見せている。本解説では、この問題の重要さと面白さについて、最新の成果を交えてわかりやすく解説する。

7. J. L. Bordim, T. Hunziker, K. Nakano:
"Adaptive Carrier Sensing and Packet Sending- An Alternative to Boost the Performance in Directional Communications", Proc. of 6th International Conference on PDCAT, 274–278, (Dec. 2005).
概要: Despite the efforts to leverage the network performance through the use of Directional Communications, most protocols still rely on the basic mechanisms employed by the IEEE802.11 standards. While this might be desirable facilitate compatibility, nodes empowered with directional antennas should be able to explore the benefits of directional communications whenever possible. With that in mind we propose two mechanisms, termed Adaptive Carrier Sensing and Adaptive Packet Sending, aiming to allow nodes equipped with directional antennas to exploit the advantages of such systems to improve network performance.

8. H. Ochi, S. Tagashira, S. Fujita:
"A Localization Scheme for Sensor Networks Based on Wireless Communication with Anchor Groups", Proc. the 11th Int'l Conf. on Parallel and Distributed Systems (ICPADS05), 299–305, (2005).
概要: In this paper, we propose a new localization scheme for wireless sensor networks consisting of a huge number of sensor nodes equipped with simple wireless communication devices. The proposed scheme is based on the Point-In-Triangle (PIT) test proposed by He *et al.* The scheme is actually implemented by using Bluetooth devices of Class 2 standard, and the performance of the scheme is evaluated in an actual environment. The result of experiments indicates that the proposed scheme could realize a localization with an error of less than 2 m.

9. S. Fujita, S. Tagashira, C. Qiao, and M. Mito:
"Distributed Branch-and-Bound Scheme for Solving the Winner Determination Problem in Combinatorial Auctions", Proc. Int'l Conf. on Advanced Information Networking and Applications (AINA05), 661–666, (2005).

概要: In this paper, we propose a new class of parallel branch-and-bound (B&B) schemes. The main idea of the scheme is to focus on the *functional parallelism* instead of conventional *data parallelism*, and to support such a heterogeneous and irregular parallelism by using a collection of autonomous agents distributed over the network. After examining several design issues toward the implementation of a prototype of the distributed B&B system, we illustrate the result of our preliminary experiments conducted to estimate the performance of the proposed scheme. The result shows that it could cause a significant performance improvement if each agent autonomously changes its function type according to the change of the underlying environment.

10. T. Tang, S. Tagashira, S, Fujita:
"LQ-Routing Protocol for Mobile Ad-Hoc Networks", Proc. Int'l Conf. on Computer and Information Science (ACIS-ICIS 2005), 441–446, (2005).
概要: In this paper, we propose a new routing protocol for mobile ad-hoc networks (MANET), which have attracted considerable attentions in recent years as a tool to realize flexible and robust communication environments in many critical application fields. The proposed protocol, called LQ-routing, is a proactive routing protocol based on the Q-routing protocol which was originally proposed for conventional wired networks. In order to reflect the mobility of hosts to the routing decision, which would cause frequent connection and disconnection of communication links between nearby hosts, we introduce the notion of lifetime to represent the stability of routes connecting to the destination. The performance of the proposed routing scheme is experimentally evaluated by using NS-2. The result of simulation indicates that by introducing the notion of lifetime to a simple combination of previous proactive routing scheme DSDV and the Q-routing, we could improve the performance of DSDV in terms of the packet loss rate and the average packet delay.

11. S. Fujita:
"On the relation between average and maximum cuts in linear arrangements of graphs", 2005 Korea-Japan Joint Workshop on Algorithms and Computation, 191–198, (2005).
概要: This paper studies the relationship between the average and the maximum cut of linear arrangement of graphs.

12. S. Tagashira, M. Mito, S. Fujita:
"Towards Generic A Branch-and-Bound Solver of Combinatorial Optimization Problems with Autonomous Agents in P2P Networks", Proc. Int'l Symp. on High Performance Computing (ISHPC'05), CD-ROM, (2005).
概要: In this paper, we propose a new class of parallel branch-and-bound (B&B) schemes. The main idea of the scheme is to focus on the *functional parallelism* instead of conventional *data parallelism*, and to support such a heterogeneous and irregular parallelism by using a collection of autonomous agents distributed over the network. After examining several design issues toward the implementation of a prototype of the distributed B&B system, we illustrate the result of our preliminary experiments conducted to estimate the performance of the proposed scheme. The result shows that it could cause a significant performance improvement if each agent autonomously changes its function type according to the change of the underlying environment.

13. D. Takemoto, S. Tagashira, S. Fujita:
"A Fault-Tolerant Content Addressable

Network", Proc. Int'l Symp. on Parallel and Distributed Processing and Applications (ISPA'2005), Lecture Notes in Computer Science 3758, 792 – 803, (2005).
概要: In this paper, we propose a new method to enhance the fault-tolerance of the Content Addressable Network (CAN), which is known as a typical pure P2P system based on the notion of Distributed Hash Table (DHT). The basic idea of the proposed method is to introduce a redundancy to the management of index information distributed over the nodes in the network, by allowing each index to be assigned to several nodes, which was restricted to be one in the original CAN system. To keep the consistency among several copies of indices, we propose an efficient synchronization scheme based on the notion of labels assigned to each copy in a distinct manner. The performance of the proposed scheme is evaluated by simulation. The result of simulations indicates that the proposed scheme really enhances the fault-tolerance of the CAN system.

14. S. Umezane, S. Fujita:
"On Linkage Identification in EC for Solving Combinatorial Optimization Problems", Proc. The International Conference on Systems, Man and Cybernetics (SMC2005), CD-ROM, (2005).
概要: This paper proposes a new linkage identification method based on the notion of evolution of linkages, that is designed for evolutionary computation schemes to solve combinatorial optimization problems. Linkage identification is a task to identify an appropriate fragment of genes contained in a chromosome that is expected to significantly increase the fitness of the overall individuals. As a concrete target problem of the proposed scheme, we focus on the traveling salesman problem (TSP) that is known as a typical combinatorial optimization problem. The performance of the scheme is experimentally evaluated by using TSPLIB, and is compared with the performance of previous schemes. The result of experiments shows that the proposed scheme really improves the performance of the previous scheme, and the amount of improvement is 42.7% in the best case.

15. S. Fujita, A. Ohtsubo, M. Mito:
"Extended Skip Graphs for Efficient Key Search in P2P Environment", Proc. the 8th International Symposium on Parallel Architectures, Algorithms, and Networks (I-SPAN 2005), (2005).
概要: In this paper, we propose three techniques to improve the cost/performance of the skip graph that was recently proposed by Aspnes and Shah in 2003. More concretely, the skip graph, in which each node is connected with exactly $\log_2 N$ neighbors among N nodes contained in the system, is extended in the following two directions: 1) proposal of a subgraph of the skip graph which realizes a graceful degradation of the routing performance when the number of neighbors reduces from $\log_2 N$, and 2) proposal of a supergraph of the skip graph which realizes a significant performance improvement when the number of neighbors increases from $\log_2 N$. The performance of those extended graphs will be evaluated analytically with concrete numerical results.

16. S. Fujita:
"A Tight Bound on the Number of Mobile Servers to Guarantee the Mutual Transferability among Dominating Configurations", Proc. lgorithms and Computation, 16th International Symposium, ISAAC 2005, Proceedings (Xiaotie Deng, Ding-Zhu Du Eds.). Lecture Notes in Computer Science, 563–572, (2005).
概要: In this paper, we propose a new framework to provide continuous services to

users by a collection of mobile servers distributed over an interconnection network. We model those mobile servers as a subset of host computers, and assume that a user host can receive the service if at least one adjacent host computer (including itself) plays the role of a server; i.e., we assume that the service could not be routed via the interconnection network. The main results obtained in this paper are summarized as follows: For the class of trees with n hosts, $\lceil (n+1)/2 \rceil$ mobile servers are necessary and sufficient to realize continuous services by the mobile servers, and for the class of Hamiltonian graphs with n hosts, $\lceil (n+1)/3 \rceil$ mobile servers are necessary and sufficient.

学会大会等

1. 伊達和宏，中野浩嗣:
“トラフィック分散を考慮したアドホックルーティングプロトコル”, 情報科学ワークショップ論文集, 10–11, 2005 年 9 月.

2. 山地敦大，中野浩嗣:
“モバイルアドホックネットワークにおける Localized Power Aware Routing”, 情報科学ワークショップ論文集, 12–13, 2005 年 9 月.

3. 山本亮平，中野浩嗣:
“指向性アンテナを用いたルーティングプロトコル”, 情報科学ワークショップ論文集, 14–15, 2005 年 9 月.

4. 松野博之，中野浩嗣:
“動的なアドホックネットワークにおけるクラスタリングアルゴリズム”, 情報科学ワークショップ論文集, 16–17, 2005 年 9 月.

A09: 非明示的表現に対するアルゴリズムの開発

篠原　歩 †　竹田　正幸 ‡　下薗真一 §　坂本　比呂志 §

† 東北大学 大学院情報科学研究科
〒 980-8579 仙台市青葉区荒巻字青葉 6-6-05
ayumi@ecei.tohoku.ac.jp

‡ 九州大学 大学院 システム情報科学研究院
〒 812-8581 福岡市東区箱崎 6-10-1
takeda@i.kyushu-u.ac.jp

§ 九州工業大学 情報工学部 知能情報工学科
〒 820-8502 福岡県 飯塚市 大字川津 680-4
{sin,hiroshi}@ai.kyutech.ac.jp

1　研究の概要

本研究は，非明示的に表現されたオブジェクトに対するアルゴリズムの開発とその計算量の解析を行うことを目的し，また同時に，効率のよいアルゴリズムの開発に適した非明示的な表現法を文字列やグラフなどの離散構造を対象として研究を展開している．

まず，文字列の類似性を測るためによく用いられている，最長共通部分列の漸増的計算方法について議論した．有限アルファベット Σ 上の文字列 $A = a_1a_2 \ldots a_n$ に対し，$|A|$ はその長さ n を表し，$A[i] = a_i$ とする．列 $A[i_1]A[i_2] \ldots A[i_k]$ は，$1 \leq i_1 < i_2 < \ldots < i_k \leq n$ のとき，A の長さ k の部分列という．文字列 A と B に共通して現れる部分列の中で，長さが最長のものを最長共通部分列 *(Longest Common Subsequence)* とよび，その長さを $LCS(A, B)$ と表す．$LCS(A, B)$ は，動的計画法を用いて $O(nm)$ 時間で求められることが知られている [1]．ここに n と m はそれぞれ A と B の長さを表す．我々は，$LCS(A, B)$ が既に求まっているときに，A や B の前または後に文字 c が追加された文字列に対して，$LCS(cA, B)$, $LCS(A, cB)$, $LCS(Ac, B)$, $LCS(A, Bc)$ を効率よく求める問題を考える．$LCS(A, B)$ が計算済みであるとき，$LCS(cA, B)$ と $LCS(A, cB)$ はそれぞれ $O(L)$ 時間と $O(n)$ 時間で計算できる．$LCS(Ac, B)$ と $LCS(A, Bc)$ は，それぞれ $O(L)$ 時間と $O(n)$ 時間で容易に計算できる．ここに $L = LCS(Ac, B)$ である．

また，文字列とそれに関連付けられた数値属性値との対の集合から最適パターンを発見する問題を扱った．パターンの「良さ」として，個々の文字列におけるパターンの生起回数とその文字列に関連付けられた数値属性値との間の相関を用い，接尾辞木に基づく二つのアルゴリズムを提示した．これらのアルゴリズムは，最適部分文字列パターンをそれぞれ $O(Nn)$ 時間と $O(N^2)$ 時間で求めることができる．ここに，n は文字列の個数であり，N は文字列長の総和である．また，より複雑なパターン族を扱う際に用いることのできる一般的な分枝限定手法をを示した．さらに，上述の $O(N^2)$ 時間アルゴリズムと分枝限定法を組み合わせることにより，著しく効率が良くなることを示した．

さらに，これまで主に対象を文字列として開発してきた照合技術を木パターンへ応用した．木パターン照合問題とは，二つのラベル付木 P と T（それぞれパターン木、ターゲット木とよぶ）が与えられて，T における P のすべての生起を見つける問題である．この問題に対して，順序木と無順序木の両方の場合について多くの研究がなされている．柔軟な照合を行うために，一種の VLDC が導入されている．XML 文書の部分を指し示すための言語である XPath においては，経路 VLDC が用いられている．本研究では，水平方向の VLDC を導入した．この VLDC は，順序木において連続した兄弟を根にもつ部分木の系列にマッチする．我々は，パターンが水平方向の VLDC をもつ場合の木パターン照合問題を扱った．この設定では，ターゲット木は，XML データストリームのように，タグを含む文字列として与えられる．この問題を $O(mn)$ 時間，$O(mh)$ 領域で解くアルゴリズムを提案した．ここに，m と n は，それぞれ，P と T の長さであり，h は T の高さである．さら

に，ビット並列化技法を用いることにより、実用的に高速なアルゴリズムを得ることができた．

また，XQuery に関して，文字列検索技術を応用した単純で高速な処理手法を提案した．XML データから Aho-Corasick 法を拡張した XML データ走査器によって高速にタグやキーワードの検出を行い，パスに応じた処理を行うことで XQuery の質問式を処理した．特にパスの照合を高速に処理するために，XML データから得られるパススキーマを用いることで決定性有限オートマトンを構築するパスプルーニングを提案し，その効果を計算機実験によって検証した．

さらに，半構造データに対する高速な XPath 処理法を提案した．本研究では，算術符号化を半構造データの検索に応用した逆算術符号化にノード間の先祖子孫関係を判定可能な範囲ラベルを導入することにより，より複雑な問い合わせ処理を高速に実現するための手法を提案した．評価実験の結果，300MB 程度の XML データに対してテキストを直接処理する既存の手法と比較し，数十から百倍の高速化を達成した．

また，畳み込みカーネルのアイディアに基づいた，ラベル付き順序木に対する新しいカーネル関数を提案した．畳み込みカーネルの枠組みにおいてラベル付き順序木に対して任意の部分グラフを部分構造として用いた場合の，効率の良いカーネル計算のアルゴリズムを提案し，曖昧なラベルや構造を取り込むような拡張を行い，より一般的な木構造として，順序のないラベル付き根付き木に対するカーネルを考えた場合には，カーネルの計算が#P-完全問題であることを示した．

最後に，最も基本的な文字列照合アルゴリズムである，素朴なアルゴリズムについて，その平滑化解析を行った．文字列照合は文字列処理のなかでも最も基本的な問題の一つである．照合を行うテキスト T の長さが n，パターン P の長さが m であるとき，文字列照合アルゴリズムの中でも最も基本的なアルゴリズムである素朴なアルゴリズムに於いて，最悪計算時間は $O(mn)$ であることがよく知られている．しかしながら，テキストやパターンが一様分布にしたがって完全にランダム選ばれたと仮定すると，このアルゴリズムの平均計算時間は，パターン長と無関係に $O(n)$ となる事も同時に知られている．すなわち，最悪時の計算時間と，平均時の計算量の間に大きなギャップが存在する．そこで，本研究において我々は，Spielman と Teng [4] によって提唱された，平滑化解析 (smoothed analysis) を文字列処理アルゴリズムの評価に適応させ，そのギャップを埋める解析を行った．

以下，最長共通部分列の漸増計算と，文字列照合アルゴリズムの平滑化解析について，より詳しく述べる．

2 最長共通部分列の漸増計算

文字列 A と B に対し $(m+1)\times(n+1)$ の二次元配列 DP を次のように帰納的に定義する．

$$DP[i,j] = \begin{cases} 0 & i=0 \text{ or } j=0 \\ \max\{DP[i-1,j], DP[i,j-1]\} & A[j]\neq B[i] \\ DP[i-1,j-1]\} & A[j]=B[i] \end{cases}$$

このとき，$DP[m,n] = LCS(A,B)$ であり，これは $O(mn)$ 時間と領域で計算できる（図 2.1 上）．

2.1 Landau らのアルゴリズム

Landau ら [3] は，$L = LCS(A,B)$ が計算済みであるとき，任意の文字 c に対して $LCS(cA,B)$ を効率よく計算するアルゴリズムを提案した．彼らのアルゴリズムは，DP 全体を再計算するのではなく，次のように定義される分割点の集合 P のみを計算するため，従来の手法より高速かつ省領域で動作する．$A[j] = B[i]$ のとき，対 (i,j) を A と B の間の一致点という．また，$DP[i,j] = DP[i-1,j]+1$ が成り立つとき，対 (i,j) を DP の分割点とよぶ．DP のすべての分割点からなる集合を P で表す．$DP[i,j] = v$ となる分割点 $(i,j)\in P$ に対し，$P[v,j] = i$ と定義する．すなわち，$P[v,j]$ は DP の第 j 列において，初めて v になる行を表す（図 2.1）．

定理 1 (Landau ら [3]) $L = LCS(A,B)$ が計算済みであるとき，任意の文字 c に対して，$LCS(cA,B)$ を $O(L)$ 時間で計算できる．

		a	d	b	d	c	d
b		0	0	**1**	1	1	1
c		0	0	1	1	**2**	2
b		0	0	**1**	1	2	2
b		0	**1**	1	**2**	2	**3**

	b	a	d	b	d	c	d
b	**1**	1	1	**1**	1	1	1
c	1	1	1	1	1	**2**	2
b	**1**	1	1	**2**	2	2	2
b	1	1	**2**	2	**3**	3	**3**

図 2.1: $A =$ adbdcd, $B =$ bcbd のときの DP（上図）と，A の先頭に b を追加したときの DP^{Ah}（下図）．簡単のため，$i > 0$, $j > 0$ の部分のみ記載する．一致点を太字で表し，分割点を□で囲み，DP^{Ah} で新たに分割点になったところを灰色で塗っている．

2.2 $LCS(A, cB)$ の計算

$LCS(A, B)$ が計算済みであるとし，そのときの DP 表を DP とし，分割点の集合を P とおく．B の先頭に文字 c が追加されたときの $LCS(A, cB)$ に対する DP 表を DP^{Bh} とし，分割点の集合を P^{Bh} とする．この変化に着目するために，$k = \min\{j \mid A[j] = c\}$ とする．k は DP^{Bh} の最初の行のなかの一致点を表す列である．

補題 1 任意の列 $j \geq k$ に対し，次式を満たす行 E_j が存在する．

$$DP^{Bh}[i, j] = \begin{cases} DP[i, j] + 1 & (i < E_j), \\ DP[i, j] & (i \geq E_j). \end{cases}$$

補題1より，P を P^{Bh} に更新する際，各列 $j \geq k$ で行 E_j のみに着目すればよいことがわかる．ここで (E_j, j) は P を P^{Bh} に更新する際に，列 j において削除される分割点である．次に示す補題 2 と補題 3 より，削除すべき分割点 (E_j, j) を効率よく求めることができる．

補題 2 分割点集合 P を P^{Bh} に更新する際に *j-1* 列および j 列で削除される分割点をそれぞれ

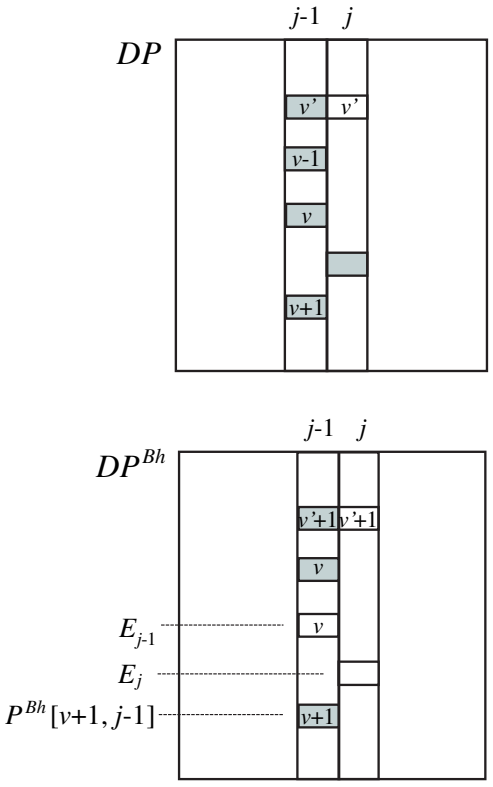


図 2.2: P を P^{Bh} に更新する際に第 j 列の分割点 E_j が存在する範囲．灰色で表した点が分割点を表す．

$(E_{j-1}, j-1)$ および (E_j, j) とし，$DP^{Bh}[E_{j-1}, j-1] = v$ とする．このとき，$E_{j-1} \leq E_j \leq P^{Bh}[v+1, j-1]$ が成り立つ．(図 *2.2* 参照)．

補題 3 分割点集合 P を P^{Bh} に更新する際に $j-1$ および j 列で削除される分割点をそれぞれ $(E_{j-1}, j-1)$ および (E_j, j) とし，$DP^{Bh}[E_{j-1}, j-1] = v$ とする．このとき，$P^{Bh}[v, j-1] < x \leq Ej-1$ を満たす一致点 (x, j) が存在するときは，$E_j = E_{j-1}$, そうでなければ $E_j = P[v+1, j]$ が成り立つ．

補題 4 $k = \min\{j \mid A[j] = c\}$ とする．DP の j 列に分割点が存在するときは $E_k = null$, そうでなければ $E_k = P[1, k]$ である．

以上をまとめて，次の定理が得られる．

定理 2 $L = LCS(A, B)$ が計算済みであるとき，任意の文字 c に対して，$LCS(A, cB)$ を $O(n)$ 時間で計算できる．

		動的計画法	KP 法	提案手法
計算時間	$LCS(cA, B)$	$O(mn)$	$O(m+n)$	$O(L)$
	$LCS(Ac, B)$	$O(m)$	$O(m)$	$O(L)$
	$LCS(A, cB)$	$O(mn)$	$O(m+n)$	$O(n)$
	$LCS(A, Bc)$	$O(n)$	$O(n)$	$O(n)$
作業領域		$O(mn)$	$O(mn)$	$O(nL+m)$

表 2.1: 計算量の比較．KP 法は文献 [2] を応用したものである．$|A| = n$, $|B| = m$ であり，$L = LCS(A, B) \leq \min(n, m)$ が常に成り立つことに注意．

表 2.1 に本論文の提案手法と従来手法の計算時間の比較結果を示す．$LCS(A, B)$ が計算済みであるとき，$LCS(cA, B)$ と $LCS(A, cB)$ はそれぞれ $O(L)$ 時間と $O(n)$ 時間で計算できる．$LCS(Ac, B)$ と $LCS(A, Bc)$ は，それぞれ $O(L)$ 時間と $O(n)$ 時間で容易に計算できる．

3 文字列照合アルゴリズムの平滑化解析

文字列照合は文字列処理のなかでも最も基本的な問題の一つである．照合を行うテキスト T の長さが n，パターン P の長さが m であるとき，文字列照合アルゴリズムの中でも最も基本的なアルゴリズムである素朴なアルゴリズム (naïve matching algorithm) に於いて，最悪計算時間は $O(mn)$ であることがよく知られている．しかしながら，テキストやパターンが一様分布にしたがって完全にランダム選ばれたと仮定すると，このアルゴリズムの平均計算時間は，パターン長と無関係に $O(n)$ となる事も同時に知られている．すなわち，最悪時の計算時間と，平均時の計算量の間に大きなギャップが存在する．(もちろん，最良時の計算時間も $O(n)$ であることは明かであるが，このことはあまり重要ではない.) そこで，本研究において我々は，Spielman と Teng [4] によって提唱された，平滑化解析 (smoothed analysis) を文字列処理アルゴリズムの評価に適応させ，そのギャップを埋める解析を行うことにした．平滑化解析は，アルゴリズムの最悪計算時間と平均時間の不一致を説明するための比較的新しい手法である．解析の方法としては，最悪時間となる入力を与えたり，完全にランダムな入力を与える代わりに，最悪時間を与える入力にランダムな部分摂動を行う．この解析法は，最悪計算時間と平均計算時間の間を補完する事ができるだけでなく，実際のアプリケーションなどの高速化のヒントにもなり得るという点でとても有用である．実際，Spielman と Teng らは，線形計画法を実用的によく用いられている，シンプレックス法（単体法）の平滑化解析を行い，その実用性を裏付ける理論的結果を得ている．シンプレックス法は，最適解が多面体の頂点に現れることを利用し，最適解に達するまで多面体の辺をたどってより高い目的関数の値を次々にたどることで線形計画問題を解く．このアルゴリズムは実際にかなり効率がよいことが知られており，巡回していないかに注意を払えば大域的最適解を見つけることが保証される．しかしながら，シンプレックス法は，最悪時には指数時間かかってしまう．一方，内点法や射影変換法など，最悪時でも多項式時間で動作することが保証されているアルゴリズムもあるが，実装のしやすさや，実際の問題に適用した際の実行時間の計測により，依然としてシンプレックス法はよく用いられている．Spielman と Teng は，新たに導入した摂動モデルを用いて，最悪時の入力に対しても，ほんの少しだけ摂動をかけることによって，実行時間が劇的に改善されることを示した．このことから，素朴な文字列照合アルゴリズムは，最悪時の実行時間は $O(nm)$ 時間であるものの，実質的にそのような「悪い」入力となるインスタンスは，問題空間の中で「孤立」していることが明かとなった．すなわち，実質的にはそのような例はほとんど発生しないため，素朴な文字列照合アルゴリズムは，実用的にも十分有用であることの理論的な裏付けが得られたことになる．

$\sigma = |\Sigma|$ とし，文字列 $w \in \Sigma^*$ と二つの整数 i, j 対して，$w[i, j]$ を w の $w[i]$ から $w[j]$ までの**部分文字列**とする．**文字列照合問題**は，長さ n のテキスト文字列 T と長さ m のパターン文字列 P が入力として与えられたとき，T の中に P が出現する全ての位置を求める問題である．

素朴な文字列照合アルゴリズムは 2 重構造のループからなるとても単純なアルゴリズムで，外側のループでテキストの全ての位置を訪れ，内側のループでそこから始まる部分文字列とパターンが等しいかを一文字ずつ検証する．不一致が見つ

かった時点で内側のループは終了する．よく知られているように，このアルゴリズムの計算時間が最悪となるのは $T = aaaa\cdots aaaa$, $P = aa\cdots aab$ のような入力に対してである．このとき，$O(mn)$ であるが，一様ランダムな文字列に対しては，平均計算時間は $O(n)$ である．

4 平滑化解析

文字列 $w \in \Sigma^*$ の各位置において，確率 p で Σ から一様ランダムに選ばれた文字に置換する，**部分摂動**を行う．$p = 0$ の時，変異は起こらず w そのままになり，$p = 1$ の時は w とは関係のない完全なランダム文字列になる．$|w|$ と $|w'|$ のハミング距離の期待値は $|w|p(1 - \frac{1}{\sigma})$ となる．

$\mu(i, j)$ を，テキスト T の i 番目の文字 $T[i]$ と，パターン P の j 番目の文字 $P[j]$ が一致する確率と定義する．また，l を $1 \leq l \leq |P|$ である整数，i の範囲をそれぞれ $1 \leq i \leq |T|$ とする．この時，長さ $l-1$ のテキスト T の部分文字列 $T[1, l-2]$ にパターン P のプレフィックス $P[1, l-1]$ が一致し，かつテキスト中の文字 $T[i+l-1]$ とパターン中の文字 $P[l]$ が一致しない確率 $P_F(i, l)$ は次式で表される．

$$\begin{aligned} &P_F(i,l) = \\ &\quad (\mu(i,1)\cdot\mu(i+1,2)\cdots\mu(i+l-2,l-1)) \\ &\quad \cdot(1-\mu(i+l-1,l)) \end{aligned} \tag{2.4}$$

また，パターン P がテキスト T の i 番目からの部分文字列と完璧に一致するときの確率 $P_S(i, l)$ は，次式で表される．

$$\begin{aligned} &P_S(i,l) = \\ &\quad \alpha(i,1)\cdot\alpha(i+1,2)\cdots\alpha(i+l-2,l-1) \\ &\quad \cdot\alpha(i+l-1,l) \end{aligned} \tag{2.5}$$

テキストとパターンが一様ランダムに選ばれたとき，素朴な文字列照合アルゴリズムの総計算時間の期待値 $Ex(T, P)$ は次式で表される．

$$\begin{aligned} &\mathrm{Ex}(T,P) = \\ &\quad \sum_{i=1}^{n}\left(\sum_{l=1}^{m}\left(P_F(i,l)\cdot l\right) + P_S(i,m)\cdot m\right) \end{aligned} \tag{2.6}$$

特に，$\Sigma = \{\mathtt{a}, \mathtt{b}\}$ の場合，$P_F(i, l) = P_S(i, l) = \frac{1}{2^l}$ より式 (2.6) は以下のようになる．

$$\mathrm{Ex}(T,P) = \sum_{i=1}^{n}\left(\sum_{l=1}^{m}\frac{l}{2^l} + \frac{m}{2^m}\right) \tag{2.7}$$

ここで，$\sum_{l=1}^{m}\frac{l}{2^l}$ について，

$$a_m = \sum_{l=1}^{m}\left(\frac{l}{2^l}\right) = \frac{1}{2} + \frac{2}{2^2} + \frac{3}{2^3} + \cdots + \frac{m}{2^m} \tag{2.8}$$

とする．(2.8) の両辺に $\frac{1}{2}$ をかけると，

$$\frac{1}{2}a_m = \frac{1}{2^2} + \frac{2}{2^3} + \cdots + \frac{m-1}{2^m} + \frac{m}{2^{m+1}} \tag{2.9}$$

となる．ここで (2.8) の両辺から (2.9) の両辺の差をとると，

$$\frac{1}{2}a_m = \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots + \frac{1}{2^m} - \frac{m}{2^{m+1}}$$

となるので，a_m は

$$\begin{aligned} a_m &= 1 + \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^{m-1}} - \frac{m}{2^m} \\ &= \frac{1-\frac{1}{2}^m}{1-\frac{1}{2}} - \frac{m}{2^m} \\ &= 2\cdot\left(1 - \frac{1}{2^m}\right) - \frac{m}{2^m} \end{aligned}$$

と表せる．a_m を (2.7) に代入すると，

$$\mathrm{Ex}(T,P) = 2n\cdot\left(1 - \frac{1}{2^m}\right) \tag{2.10}$$

となる．

4.1 最悪時の入力に部分摂動を行った場合の期待値

p を T と P の各文字に対して置換が起こる確率とする．$0 \leq p \leq 1$ である．特に，$p = 0$ の時は入力文字列に変化はなく，$p = 1$ の時は入力に関係ない完全にランダムな文字列になる．ここで，$\Sigma = \{a_1, \cdots, a_\sigma\}$, $|\Sigma| = \sigma$ であるとき，Σ に含まれる a_1 のみからなる文字列 w があるとする．こ

の文字列に含まれる各文字が，p の確率で Σ 内の文字のどれかに置き換わった文字列を w' とする．この時，a_1 のみの元の文字列と w' とのハミング距離の期待値，すなわち w' 内の文字で a_1 ではない文字の数は $p \cdot \frac{\sigma-1}{\sigma} \cdot |S(p)|$ で表される．

これと同じ事を素朴なアルゴリズムの入力 T と P についても考える．a_1 のみで構成される長さ n のテキスト T と，長さ m のパターン P それぞれについて前述のように置換を行うと，T の i 番目の文字 $T[i]$ と，P の j 番目の文字 $P[j]$ が一致するのは次の 3 つの場合に分けられる．

(1) $T[i]$ と $P[j]$ が両方とも置換されない

(2) $T[i]$ と $P[j]$ がが両方とも置換され，かつ両方とも同じ文字になる

(3) $T[i]$ と $P[j]$ の片方のみが置換され，かつもう一方の文字と同じ文字になる

まず (1) について，テキストとパターン双方において，文字が置換されない確率は $(1-p)$ であるため，(1) の確率は $(1-p)\cdot(1-p)$ である．

次に (2) について，文字が置換される確率は p であるため，文字が等しくなるためには置換され，かつ同じ文字にならなければならない．$|\Sigma| = \sigma$ であるとき，条件を満たす確率は $p\frac{1}{\sigma} \cdot p\frac{1}{\sigma} + p\frac{1}{\sigma} \cdot p\frac{1}{\sigma} + \cdots = p \cdot p\frac{1}{\sigma}$ となる．

最後に (3) について，片方が置換されもう片方が置換されず文字が等しくなる確率は $p\cdot(1-p)\frac{1}{\sigma}$ である．置換されるのがテキストの場合とパターンの場合 2 通りあるため求める確率は $2\cdot p\cdot(1-p)\frac{1}{\sigma}$ となる．

この 3 つをまとめると，$T[i]$ と $P[j]$ が一致する確率 $\alpha(i,j)$ は以下のように表される．

$$\begin{aligned}
&\alpha(i,j)\\
&= (1-p)(1-p) + p\cdot p\frac{1}{\sigma} + 2\cdot(1-p)\cdot p\frac{1}{\sigma}\\
&= 1 - p(2-p)\left(1-\frac{1}{\sigma}\right)\\
&= 1 - \left(1-(1-p)^2\right)\left(1-\frac{1}{\sigma}\right) \qquad (2.11)
\end{aligned}$$

ここで $\alpha(i,j)$ について，σ は定数であり，$\alpha(i,j)$ は i, j によらない p の関数であるので $\alpha(i,j)$ を α_p と表すことにする．これを用いると $P_F(i,l)$ と $P_S(i,l)$ は以下のようになる．

$$\begin{aligned}
P_F(l) &= \alpha_p^{l-1}\cdot(1-\alpha_p) \qquad (2.12)\\
P_S(l) &= \alpha_p^{l} \qquad (2.13)
\end{aligned}$$

これらと式 (2.11) を式 (2.6) に代入し式 (2.10) と同じように式変形を行うと，期待値 $\mathrm{Ex}(T,P)$ は

$$\begin{aligned}
&\mathrm{Ex}(T,P)\\
&= \sum_{i=1}^{n}\left(\sum_{l=1}^{m}\left(\alpha_p^{l-1}\cdot(1-\alpha_p)\cdot l\right) + \alpha_p^m\cdot m\right)\\
&= \frac{1-\alpha_p^m}{1-\alpha_p}\cdot n\\
&= \frac{n\cdot\left(1-\left(1-p\,(2-p)\left(1-\frac{1}{\sigma}\right)\right)^m\right)}{\left(1-(1-p)^2\right)\left(1-\frac{1}{\sigma}\right)}
\end{aligned}$$

と表される．

例えば $\sigma = 2$ の時は $\alpha_p = 1 - p + \frac{1}{2}p^2$ となるため，$\mathrm{Ex}(T,P)$ は

$$\mathrm{Ex}(T,P) = \frac{n}{p-\frac{p^2}{2}}\cdot\left(1-\left(1-\left(p-\frac{p^2}{2}\right)\right)^m\right)$$

となる．

またこれより，

$$\lim_{m\to\infty}\frac{\mathrm{Ex}(T,P)}{n} = \begin{cases}\frac{2}{p(2-p)} & (0 < p \le 1)\\ \infty & (p = 0)\end{cases}$$

となる．この式を図 2.3 に表す．最悪計算時間時の入力ににほんの少しノイズを混ぜただけで，計算時間は劇的に速くなる事がわかる．

4.2 $p \neq q$ の時の平滑化関数の導出

前節まではテキスト T とパターン P に対し摂動の起こる確率が等しいとして考えてきたが，次は T と P それぞれに対し，摂動が起こる確率が違う場合について考える．T の各文字に摂動が起こる確率を p，P の各文字に摂動が起こる確率を q とする．p, q 共に $0 \le p \le 1$, $0 \le q \le 1$ である．

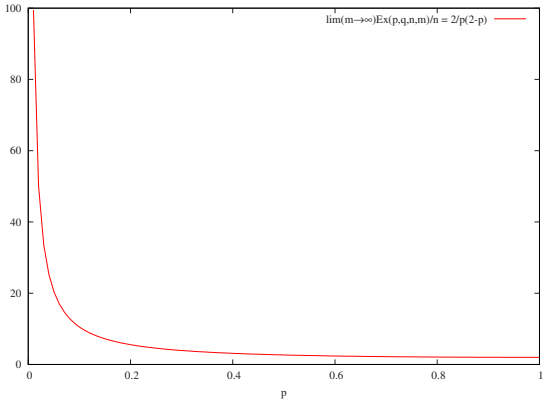


図 2.3: 最悪時の入力に部分摂動を行った場合の平滑化解析 ($\sigma = 2$)

この時，前節の (2.11) と比較して $T[i]$ と $P[j]$ が一致する確率 $\alpha(i,j)$ は以下のようになる．

$$\begin{aligned}
&\alpha(i,j) \\
&= (1-p)(1-q) + p\cdot q\cdot\frac{1}{\sigma} \\
&\quad +(1-p)\cdot q\cdot\frac{1}{\sigma} + p\cdot(1-q)\cdot\frac{1}{\sigma} \\
&= (1-p)(1-q)(1-\frac{1}{\sigma}) + \frac{1}{\sigma} \qquad (2.14)
\end{aligned}$$

よって，式 (2.6) に式 (2.12) と (2.13), (2.14) を代入すると求める期待値 $\mathrm{Ex}(T,P)$ は

$$\mathrm{Ex}(T,P) = \frac{n\cdot\left(1-\left(1-\frac{1}{\sigma}\right)^m\left((1-p)(1-q)+\frac{1}{\sigma-1}\right)^m\right)}{(1-(1-p)(1-q))(1-\frac{1}{\sigma})}$$

となり，また $\lim_{m\to\infty}\frac{\mathrm{Ex}(T,P)}{n}$ は，

$$\lim_{m\to\infty}\frac{\mathrm{Ex}(T,P)}{n} = \begin{cases} \frac{1}{(1-(1-p)(1-q))(1-\frac{1}{\sigma})} & (0<p\le 1) \\ \infty & (p=0) \end{cases}$$

となる．この式を図 2.4 に表す．

図より，T と P に摂動の起こる確率が異なる場合でも少しノイズを混ぜただけで計算時間は劇的に速くなっている．p または q が 0.15 付近で計算時間はほぼ平均時間となっている．

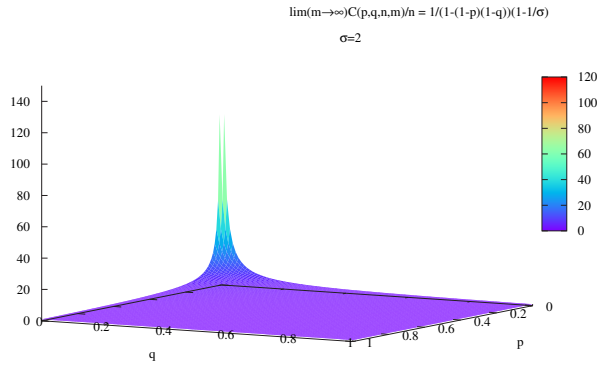


図 2.4: T と P に置換が起こる確率が異なる時の平滑化解析 ($\sigma = 2$). T と P に摂動の起こる確率が異なる場合でも少しノイズを混ぜただけで計算時間は劇的に速くなることがわかる．

5 今後の課題

前年度までに蓄積してきた，主に文字列を対象とした技術を，今年度は木構造へと応用していった．また，漸増的な手法についての議論や，平滑化解析といった新しい手法の開発を行った．今後は，ここで得られた知見に基づきながら，グラフ構造など高次のデータ構造に対する拡張の可能性を探っていく予定である．また，文字列のみならず数値列に対してもその適用範囲を広げ，画像処理などの応用も目指す．

参考文献

[1] A. Apostolico. String editing and longest common subsequences. *Handbook of Formal Languages*, Vol. 2, pp. 361–398, 1997.

[2] S.R. Kim and K. Park. A dynamic edit distance table. In *Proc. 11th Ann. Symp. on Combinatorial Pattern Matching*, Vol. 1848 of *Lecture Notes in Computer Science*, pp. 60–68. Springer-Verlag, 2000.

[3] G.M. Landau, E. Myers, and M. Ziv-Ukelson. Two algorithms for LCS consecutive suffix alignment. In *Proc. 15th Ann.*

Simp. on Combinatorial Pattern Matching, Vol. 3109 of *Lecture Notes in Computer Science*, pp. 173–193. Springer-Verlag, 2004.

[4] Daniel A. Spielman and Shang-Hua Teng. Smoothed analysis of algorithms: Why the simplex algorithm usually takes polynomial time. In *Proc. of the 33rd Ann. ACM Symp. on Theory of Computing (STOC)*, pp. 265–305, 2001.

研究業績一覧

学術論文

1. Shunsuke Inenaga, Ayumi Shinohara, and Masayuki Takeda:
"A Fully Compressed Pattern Matching Algorithm for Simple Collage Systems", International Journal of Fundations of Computer Science, Vol. 16, No. 6, pp. 1155–1166, December 2005.
概要: We study the fully compressed pattern matching problem (FCPM problem): Given $\mathcal{T}$ and $\mathcal{P}$ which are descriptions of text T and pattern P respectively, find the occurrences of P in T without decompressing $\mathcal{T}$ or $\mathcal{P}$. This problem is rather challenging since patterns are also given in a compressed form. In this paper we present an FCPM algorithm for simple collage systems. Collage systems are a general framework representing various kinds of dictionary-based compressions in a uniform way, and simple collage systems are a subclass that includes LZW and LZ78 compressions. Collage systems are of the form $\langle \mathcal{D}, \mathcal{S} \rangle$, where $\mathcal{D}$ is a dictionary and $\mathcal{S}$ is a sequence of variables from $\mathcal{D}$. Our FCPM algorithm performs in $O(||\mathcal{D}||^2 + mn \log |\mathcal{S}|)$ time, where $n = |\mathcal{T}| = ||\mathcal{D}||$ and $m = |\mathcal{P}|$. This is faster than the previous best result of $O(m^2 n^2)$ time.

2. Zdeněk Troníček and Ayumi Shinohara:
"The Size of Subsequence Automaton", Theoretical Computer Science, Vol. 341, Issue 1–3, pp. 379-384, September 2005.
概要: Given a set of strings, the subsequence automaton accepts all subsequences of these strings. We derive a lower bound for the maximum number of states of this automaton. We prove that the size of the subsequence automaton for a set of k strings of length n is $\Omega(n^k/(k+1)^k k!)$ for any $k \geq 1$. It solves an open problem because only the case $k \leq 2$ was shown before.

3. Yusuke Ishida, Shunsuke Inenaga, Ayumi Shinohara, and Masayuki Takeda:
"Fully Incremental LCS Computation", Proc. The 15th International Symposium of Fundamentals of Computation Theory (FCT2005), Lecture Notes in Computer Science 3623, pp. 563–574, August 2005.
概要: Sequence comparison is a fundamental task in pattern matching. Its applications include file comparison, spelling correction, information retrieval, and computing (dis)similarities between biological sequences. A common scheme for sequence comparison is the longest common subsequence (LCS) metric. This paper considers the fully incremental LCS computation problem as follows: For any strings A, B and characters a, b, compute $LCS(aA, B)$, $LCS(A, bB)$, $LCS(Aa, B)$, and $LCS(A, Ba)$, provided that $L = LCS(A, B)$ is already computed. We present an efficient algorithm that computes the four LCS values above, in $O(L)$ or $O(n)$ time depending on where a new character is added, where n is the length of A. Our algorithm is superior in both time and space complexities to the previous known methods.

4. Heikki Hyyrö, Yoan Pinzon, and Ayumi Shinohara:
"New Bit-Parallel Indel-Distance Algorithm", Proc. 4th International Workshop

on Efficient and Experimental Algorithms (WEA2005), Lecture Notes in Computer Science 3503, pp. 380–390, May 2005.
概要: The task of approximate string matching is to find all locations at which a pattern string p of length m matches a substring of a text string t of length n with at most k differences. It is common to use Levenshtein distance, which allows the differences to be single-character insertions, deletions, substitutions. Recently, the IndelMYE, IndelWM and IndelBYN algorithms where introduced as modified version of the bit-parallel algorithms of Myers, Wu&Manber and Baeza-Yates&Navarro, respectively. These modified versions where made to support the indel distance (only single-character insertions and/or deletions are allowed). In this paper we present an improved version of IndelMYE that makes a better use of the bit-operations and runs 24.5 percent faster in practice. In the end we present a complete set of experimental results to support our findings.

5. Hideo Bannai, Kohei Hatano, Shunsuke Inenaga, and Masayuki Takeda:
"Practical Algorithms for Pattern Based Linear Regression", Proc. 8th International Conference on Discovery Science (DS 2005), Lecture Notes in Computer Science 3735, pp. 44–56, October 2005.
概要: We consider the problem of discovering the optimal pattern from a set of strings and associated numeric attribute values. The goodness of a pattern is measured by the correlation between the number of occurrences of the pattern in each string, and the numeric attribute value assigned to the string. We present two algorithms based on suffix trees, that can find the optimal substring pattern in $O(Nn)$ and $O(N^2)$ time, respectively, where n is the number of strings and N is their total length. We further present a general branch and bound strategy that can be used when considering more complex pattern classes. We also show that combining the $O(N^2)$ algorithm and the branch and bound heuristic increases the efficiency of the algorithm considerably.

6. Hisashi Tsuji, Akira Ishino, and Masayuki Takeda:
"A Bit-Parallel Tree Matching Algorithm for Patterns with Horizontal VLDC's", Proc. 12th International Conference on String Processing and Information Retrieval (SPIRE 2005), Lecture Notes in Computer Science 3772, pp. 388–398, November 2005.
概要: The tree pattern matching problem is, given two labeled trees P and T, respectively called pattern tree and target tree, to find all occurrences of P within T. Many studies have been undertaken on this problem for both the cases of ordered and unordered trees. To realize flexible matching, a kind of variable-length-don 't-care 's (VLDC 's) have been introduced. In particular, the path-VLDC 's appear in XPath, a language for addressing parts of an XML document. In this paper, we introduce horizontal VLDC 's, each matches a sequence of trees whose root nodes are consecutive siblings in ordered trees. We address the tree pattern matching problem for patterns with horizontal VLDC 's. In our setting, the target tree is given as a tagged sequence such as XML data stream. We present an algorithm that solves the problem in $O(mn)$ time using $O(mh)$ space, where m and n are the sizes of P and T, respectively, and h is the height of T. We adopt the bit-parallel technique to obtain a practically fast algorithm.

7. 石野 明, 竹田 正幸:
"パスプルーニングによる決定性有限オート

マトンを用いたXQuery処理の提案", DBSJ Letters, Vol. 4, No. 4, (受理印刷中), 2006.
概要: 本稿では，文字列検索技術を応用した単純で高速なXQuery処理手法を提案する．XMLデータからAho-Corasick法を拡張したXMLデータ走査器によって高速にタグやキーワードの検出を行い，パスに応じた処理を行うことでXQueryの質問式を処理する．特にパスの照合を高速に処理するために，XMLデータから得られるパススキーマを用いることで決定性有限オートマトンを構築するパスプルーニングを提案する．また，実際に本手法の実装を行い，その実験結果について述べる．

8. 鹿島 久嗣, 坂本 比呂志, 小柳 光生:
"木構造データに対するカーネル関数の設計と解析", 人工知能学会論文誌, Vol. 21, No. 1, pp. 113–121, 2006.
概要: 本研究では，畳み込みカーネルのアイディアに基づいた，ラベル付き順序木に対する新しいカーネル関数を提案する．まず，畳み込みカーネルの枠組みにおいてラベル付き順序木に対して任意の部分グラフを部分構造として用いた場合の，効率の良いカーネル計算のアルゴリズムを提案し，曖昧なラベルや構造を取り込むような拡張を行った．さらに，より一般的な木構造として，順序のないラベル付き根付き木に対するカーネルを考えた場合には，カーネルの計算が#P-完全問題であることを示した．

研究会等

1. 小林　隼人，井上　淳，石野　明，篠原 歩:
"スクリプト言語Luaを用いたロボカップ四足ロボットリーグシミュレータ", 人工知能学会第21回SIG-Challenge研究会, 2005年5月.
概要: In RoboCup four-legged robot league, no modifications or additions to the robot hardware are allowed; hence, there is no difference between teams without software. For optimum results, to improve the software development process is critical. In this paper, we introduce a method of using the scripting language Lua in soccer robots, and we show the soccer simulator, in which Lua scripts are executed as in robots. Using the scripts in both the environments has made it easy to develop soccer robots.

2. 柳町　修平，大崎　嗣豊，小林　隼人，石野　明，篠原　歩:
"実ロボットによる揺動運動のスキル獲得", 人工知能学会第62回人工知能基本問題研究会, 2006年3月.
概要: This paper presents acquisition of swing movement skills by using only acceleration sensors on real robots. Acquisition of swing movement skills is an interesting theme of controlling real robots. First, we create a hand-coding policy for swing movement and confirm that our robots can control by using only some acceleration sensors. Second, we make our robots learn in such a restricted environment. Finally, we compare results of the hand-coding policy with those of reinforcement learning.

学会大会等

1. 石田　祐介，稲永　俊介，篠原　歩，竹田　正幸:
"漸増的最長共通部分列問題", 日本応用数理学会2005年度年会　講演予稿集, pp. 328–329, 2005年9月.

2. 舞田哲哉, 坂本比呂志:
"算術符号化を利用したXMLデータへの高速な問い合わせ処理の改良"，電子情報通信学会第17回データ工学ワークショップ(DEWS2006), 7B-o4, 2006年3月.

A10: 変移する要素間の関係を条件とする組合せ最適化モデル

宮野 英次 † 廣瀬 英雄 † 朝廣 雄一 ‡

† 九州工業大学情報工学部
〒 820-8502 福岡県飯塚市川津 680-4
{miyano, hirose}@ces.kyutech.ac.jp

‡ 九州産業大学 情報科学部
〒 813-8503 福岡県福岡市東区松香台 2-3-1
asahiro@is.kyusan-u.ac.jp

1 研究目的

本研究では，入力要素の値が時間とともに連続的に変移する環境において，要素間の関係が時々刻々と変化するような様々な問題を扱い，数理最適化モデルとして定式化する統一的な手法の検討と，精度の高い近似解及び高速性能を保証するアルゴリズムの開発を目的とする．

現実世界に現れる多くの情報工学的問題は，離散的な構造を有しており，多くの場合に組合せ計画モデルとして定式化できる．例えば，車両配送計画問題を従来の数理計画モデルに従って定式化する場合には，車両台数，運搬量，配送コスト，締め切り等の制約となる属性パラメータ値を入力要素として捉え，完全かつ固定的に，与えられた要素間の関係ならびに制約条件を数式化する．配送計画作成アルゴリズムは，事前に作成した条件に基づき作業計画を決定することになる．しかし，近年の社会環境の変化は激しく，時間をかけて作成した完全な作業計画が時をおかずに陳腐化してしまうという状況があり，従来の固定的に制約が与えられる計算モデルでは対応できないという問題が生じている．この事態を打開する期待が持てるものとして，オンライン計算モデルが活発に研究されている．オンライン計算モデルでは計算過程の中で必要な情報が徐々に得られ，かつ予測はできないので，随時対応していく形式で処理が進められる．しかし，現実の社会活動に現れる問題を見てみると，問題を解く前に完全な値はわからないまでも，統計的または経験的にある程度の予想を立てることが可能な場合も多い．例えば車両配送計画における車両台数は，故障や追加配備により動的に変化する可能性があるが，制約の変化に随時対応するのではなく，予め故障頻度などの予想を制約に考慮したモデル化を行うことで，将来の変化に対して柔軟な配送計画を作成することが可能になる．

本研究が目標とするのは，以上のような状況に対するモデル化手法とアルゴリズム開発であり，従来の数理計画モデルとオンライン計算モデルの溝を埋めるものと位置づけられる．本研究報告では，移動系における車両配送計画モデル，ディスク・メモリ間のデータ・ブロック転送に対するオフライン計算モデル，データ分類におけるバンプハンティング・モデル，グラフ有向化の頂点出次数最適化モデルに関して，それぞれの定式化，結果概要について述べる．

2 移動系における車両配送計画モデル

固定的に制約が与えられる従来の車両配送計画問題を拡張して，移動系における組合せ最適化問題としてモデル化を行った．これは，ベルトコンベア上を流れる品物をロボット・アーム等で回収する作業を定式化したものである．

2.1 モデル

$B = \{b_1, b_2, \cdots, b_n\}$ をユークリッド xy 平面上の n 個の移動物体の集合とし，b_i の速さを $v(b_i)$ とする．b_i の移動軌跡は折れ線であり，頂点の列 $C_0(b_i) = (x_0(b_i), y_0(b_i))$, $C_1(b_i) = (x_1(b_i), y_1(b_i))$, $\cdots$, $C_{m(b_i)+1}(b_i) = (x_{m(b_i)+1}(b_i), y_{m(b_i)+1}(b_i))$ で表される．すなわち，b_i の軌跡は $m(b_i)$ 回曲がる折れ線とし，$m = \max_{b_i \in B} m(b_i)$ とする．すべての b_i は，時刻 0 に $C_0(b_i)$ を出発し，次の $C_1(b_i)$ に速さ $v(b_i)$ で進む．時刻 $|\overline{C_1(b_i)C_0(b_i)}|/v(b_i)$ に $C_1(b_i)$ に到着後，移

動方向を変えて，$C_2(b_i)$ に進み，以降，同様の移動を $C_{m(b_i)+1}(b_i)$ まで行う．移動系における車両配送計画では，できるだけ多くのこれらの移動物体をロボット・アームで回収することを目的とする．今回考える最適化問題を PDMO (Pickup and Delivery for Moving Objects on Broken Lines) 問題としてモデル化する．

PDMO

入力： 移動物体の集合 $B = \{b_1, b_2, \cdots, b_n\}$ とその移動軌跡，b_i の初期位置 $C_0(b_i)$.

問題： できるだけ多くの移動物体を巡回することができるような速さ $v_R = 1$ で移動可能なロボット・アーム R (もしくは車両) の経路をみつける．ここで，任意の j と k について $b_{i_j} \neq b_{i_k}$ とするとき，$i_1, i_2, \cdots \in \{1, \cdots, n\}$ について，経路は 3 個組の列 (s_1, b_{i_1}, g_1)，(s_2, b_{i_2}, g_2)，$\cdots$，で表され，それぞれの (s_j, b_{i_j}, g_j) は以下の 3 つの条件を満たすものとする：

(i) R は時刻 s_j に原点 O にある．

(ii) (Pickup) R は時刻 s_j に原点 O を出発し，b_{i_j} の軌跡上まで移動し，b_{i_j} を回収することができる．

(iii) (Delivery) R は，時刻 g_j に原点 O に戻ってくることができる．ただし，$g_j \leq s_{j+1}$ でなければならない．

従来の車両配送計画問題は，巡回セールスパーソン問題 (Traveling Sales Person Problem, TSP) を特別な問題として含んでいる．TSP は，最も有名な $\mathcal{NP}$ 困難となる最適化問題の一つであり，さまざまなヒューリスティック法や近似アルゴリズムが考えられている．また，最近では，移動系における TSP 問題である Dynamic k-Collect TSP 問題，Moving-Target TSP 問題，Kinetic TSP 問題などが提案されている．これらの問題は，容量 k のロボット・アーム R と n 個の移動物体 b_j が与えられ，ロボット・アームの速さ v_R と移動物体の速さ $v(b_j)$ の関係が，全ての移動物体に対して $v_R > v(b_j)$ で ある．つまり，どの移動物体よりもロボット・アームが速く移動できるとき，全ての移動物体を最短距離で回収する問題であり，本研究課題でモデル化を行った最大化問題とは異なる．Chalasani らは $k = \infty$ のとき，定数近似アルゴリズムを提案し，さらに $k = 1$ のロボット・アームと移動物体が 1 本の線上を移動する場合は多項式時間で解けることを示ししている (Chalasani et al., Approximation algorithms for robot grasp and delivery, International Workshop on Algorithmic Foundations of Robotics, 1996)．また，Helvig らは $k = \infty$ で，さらに高々$O(\frac{\log n}{\log \log n})$ 個の移動物体が移動しているときは，$(1+\sigma)$-近似アルゴリズムがあることを示している (Helvig et al., Moving target TSP and related problems, ESA'98, 1998)．ここで σ は従来の TSP に対する近似率を表す．Hammar と Nilsson は $k = \infty$ で全ての移動物体が同じ速さで移動するとき，$\mathcal{PTAS}$ であることを示している (Hamma and Nilsson, Approximation results for kinetic variants of TSP, ICALP'99, 1999).

2.2 結果概要

前述のように，v_R よりも移動する速さが遅い移動物体はすべて巡回されることができるため，すべての移動物体はロボット・アーム以上の速さを持つものとする．本年度は上のような PDMO について，以下の結果を得ることができた．

- PDMO 問題は $\mathcal{MAXSNP}$ 困難となり，しかも，すべての i に対して $m(b_i) = 1$ であるような場合についても，$\mathcal{MAXSNP}$ 困難のままである． すなわち，$\mathcal{P} \neq \mathcal{NP}$ を仮定すると，移動物体の軌跡について非常に制限を加えた場合でも，PDMO 問題に対して精度の高い近似アルゴリズムを設計することが困難となる．

- PDMO 問題に対して，$O(mn^2)$ 時間で動作するような 2 近似アルゴリズムを設計することができる．

- すべての i に対して $m(b_i) = 0$ であるならば (すなわち，すべての移動物体が直線上を移動するならば)，ロボット・アームによって巡回する移動物体の総数が最大になる $O(n \log n)$ 時間のアルゴリズムを設計することができる．

3 ブロック転送問題に対するオフライン計算モデル

CPU 性能がバス通信性能を大きく凌ぐようになってきて，ますますディスクとメモリ間のデータ転送による計算遅延が，全体の計算時間のボトルネックとなってきている．このディスク・メモリ間のデータ転送は，ブロックまたはページ単位で行われるため，オンライン計算モデルとして定式化した問題はページング問題として呼ばれる．ページング問題では，できるだけ高い頻度で利用されるデータをメモリに常駐させて，あまり利用されないデータをディスクに戻すことにより全体のパフォーマンス向上を計る．本研究課題では，このブロック単位のデータ転送をオフライン計算モデルとして定式化する．オフライン計算モデルとして定式化した場合には，アクセスするデータ構造のディスク上での配置，すなわち，ブロック単位への効率の良いデータ分割により，全体のデータ転送遅延を小さくすることが目的となる．本年度は，有向非巡回グラフを対象として，ブロック転送問題についての検討を行った．

3.1 モデル

$G = (V, A)$ を有向非巡回グラフ (DAG) とする．もしディスク上にある DAG 構造 G が大き過ぎてすべてのデータをメモリ上に持ってくることができないようなときには，G はそれぞれのサイズが高々B であるような小さなブロックに分割されなければならない．ここで，ブロック集合を $P = \{P_1, P_2, \cdots, P_k\}$ とする．ただし，$i \neq j$ に対して $P_i \cap P_j = \emptyset$, $\bigcup_{i=1}^{k} P_i = V$, $|P_i| \leq B$, $k \geq \lceil |V|/B \rceil$ である．また，すべての i について，$|P_i| \leq B$ であるならば，P をパッキングと呼ぶ．パッキング P の下で，あるブロック $P_i \in P$ について 2 頂点 u および v が P_i に属すとき ($\{u, v\} \in P_i$)，有向辺 (u, v) はパックされると言うことにする．そうでなければ有向辺は外部有向辺と呼ぶことにする．入次数がゼロであるようなあるソースから出次数がゼロであるようなあるシンクまでの経路を q とする．パッキング P が与えられたとき，P の下での q のブロック転送 $bt_P(q)$ とは，経路 q 上の外部有向辺の総数を表し，P の下での有向非巡回グラフ G のブロック転送 $bt_P(G)$ は，$\max_{q \in Q} bt_P(q)$ を表すものとする．ここで Q はすべてのソースからシンクへの経路の集合である．ブロック転送問題 (Minimum Block Transfers with B, MBT(B)) は以下のようにモデル化される：

MBT(B)

入力： 有向非巡回グラフ $G = (V, A)$ と整数 $B \in [1..|V|]$.

問題： 入力 G のブロック転送 $bt_P(G)$ を最小化するパッキング P を求める．

ブロック転送問題に対するオフライン計算モデルは，Gil と Itai により提案され (Giland Itai, Packing trees, ESA'95, 1995)，彼らは，入力グラフを木に限定した場合には多項式時間で外部有向辺の総数を最適にするような動的計画法に基づくアルゴリズムが設計できることを示している．また，ブロック総数も同時に最小化することを考えた場合には，$\mathcal{NP}$ 困難となることも示している．ブロック転送 $bt_P(G)$ を最小化するモデルについては，Diwan ら (Diwan, et al., Clustering techniques for minimizing external path length, VLDB'96, 1996) や，Clark と Munro (Clark and Munro, Efficient suffix trees on secondary storage, SODA'96, 1996) により考えられ，木に対しては多項式時間アルゴリズムを設計できることが示されている．

入力を DAG とした場合についても，Diwan らによって調べられており，MBT(B) に対するヒューリスティック法 (ボトム・アップ・アルゴリズム) が提案されていたが，その精度保証は計算機実験によるものであり，理論的な近似率の解析や計算複雑さに関して未解決な部分が多く残っていた．

3.2 結果概要

本研究課題では，入力例題として有向非巡回グラフを考え，計算複雑さの証明と近似精度保証の理論的解析を行った．本年度の研究成果を以下にまとめる．

– Diwan らによって提案されていたボトム・アップ・アルゴリズムの近似率は，ブロック・サイズ $B = 2$ の場合に 2，$B = 3$ の場合に 3 である．また，それぞれの場合にタイトな例題が存在する．

– MBT(B) は $\mathcal{NP}$ 困難となり，しかも，ブロック・サイズ B が 2 で，入力 DAG の高さが 3 の場合にも $\mathcal{NP}$ 困難のままである．

– $\mathcal{NP}$ 困難性の証明の際に用いた近似ギャップ導入帰着は，$\mathcal{P} \neq \mathcal{NP}$ の仮定の下で，任意の整数 $B \geq 2$ および任意の正数 ε について $\frac{3}{2} - \varepsilon$ 近似アルゴリズムが存在しないことを示している．

– 入力 DAG の高さが高々2 の場合には，線形時間で動作する最適アルゴリズムを設計することができる．

– 上記の線形時間アルゴリズムを手続きとして用いることで，$B = 2$ の場合には，任意の高さの DAG に対して $\frac{3}{2}$ 近似アルゴリズムを設計することができる．すなわち，今回設計することができた $\frac{3}{2}$ 近似アルゴリズムは，近似精度保証の意味で最適なアルゴリズムとなっている．

– $B = 3$ の場合には，入力グラフを階層グラフに限定した場合には，2 近似アルゴリズムを設計することができる．

4 データ分類におけるバンプハンティング・モデル

顧客データベースから一定のルールに従う優良顧客 (あるいは非優良顧客) を抜き出すことを考え，本研究課題では，雑然として分類が一見困難と思われる顧客データベースからできるだけ有用な情報を引き出すようなバンプハンティング・モデルとしての定式化を行った．

4.1 モデル

対象データは 0 および 1 の 2 値のレスポンスを持ち，z 次元の説明変数は連続あるいは属性変数である．これらのデータは混在しており，本研究課題での目標は，2 値データを分離する境界を求めるのではなく，レスポンス 1 となるデータの密度の濃い部分を切り出すことである．すなわち，入力としてデータ密度 d を指定し，切り出した領域のレスポンス 1 が含まれる密度が d 以上のできるだけ広い領域を見つけることが目標となる．このような領域をバンプ領域と呼ぶことにする．d が大きくなるとバンプ領域は減少する特性があり，これを獲得密度-獲得数のトレードオフ曲線と呼び，本曲線を求めることも目標の一つである．

4.2 結果概要

本研究課題では，ある顧客データベースの特徴に近い人工的なデータケースに対して，バンプ領域の切り出しを行う際に決定木を基本手法とし，これに確率的探索法である遺伝的アルゴリズムを組み合わせた方法を用いた．また，確率的手法の収束値の性格から，いくつかの収束値を用いて極値統計を応用して，最適に近い解の精度を保証した上で，獲得密度-獲得数のトレードオフ曲線の近似解を求める方法を提案した．

5 グラフ有向化の頂点出次数最適化モデル

与えられた無向グラフのすべての辺について方向付けを行うことをグラフ有向化 (orientation) と呼び，グラフ理論や組合せ最適化の分野において古くから研究が行われている．例えば，Robbins は，グラフ有向化とグラフ連結度の関係について調べている (Robbins, A theorem on graphs with an application to a problem of traffic control, American Math. Monthly, 1939)．Chvátal と Thomassen は，グラフの直径との関係，および計算複雑さについて研究を行っている (Chvátal and Thomassen, Distance in orientation of graphs, J. Combinatorial Theory, 1978)．本研究課題では，グラフ有向化の際に，出次数 (または入次数) の大きさを目的関数とするような問題のモデル化を行い，計算複雑さ及び近似アルゴリズムに関する検討を行った．

5.1 モデル

頂点集合を V，辺集合を E，辺の重み集合を $w : E \to \mathbb{Z}^+$ とするとき，重みつき無向グラフを $G = (V, E, w)$ とする．ここで，頂点 $u, v \in V$ について，$\{u, v\}$ により辺を表す．グラフ G の有向化 Λ とは，辺 $\{u, v\} \in E$ の向きを決めることである．今年度は，以下のような最大出次数を最小化するグラフ有向化問題 (MMO 問題, Minimum Maximum Outdegree Orientation Problem) としてモデル化を行った．

MMO

入力： 重みつき無向グラフ
$G = (V, E, w)$.

問題： 頂点の最大出次数が最小となるグラフ G の有向化 Λ を求める．

MMO は代表的なスケジューリング問題である終了時刻最小化スケジューリング問題や相互無関係並列計算機のスケジューリング問題とも関連が深い問題である．

5.2 結果概要

本年度の研究成果を以下にまとめる．

- MMO 問題は $\mathcal{NP}$ 困難である．
- 次のような特別な場合には多項式時間で動作する最適なグラフ有向化アルゴリズムを設計することができる．(i) 入力グラフが重み無しグラフの場合．(ii) 入力グラフが木の場合．
- 上記の (i) および (ii) に対する多項式時間アルゴリズムを用いることにより，$\min\{\frac{w_{max}}{w_{min}}, (2-\varepsilon)\}$ の近似率を持つ組合せアルゴリズムを設計することができる．ここで，w_{max} および w_{min} はそれぞれ辺重みの最大値および最小値であり，ε は入力に依存するある正数である．

研究業績一覧

学術論文

1. Yuichi Asahiro, Eiji Miyano, Shinichi Shimoirisa:
"k-Collect Tours for Moving Objects with Release Times and Deadlines", Proceedings of the 9th World Multi-Conference on Systemics, Cybernetics and Informatics, Vol.III, pp.192–197, (2005 年 7 月).
概要: In this paper, we consider a formalization of the following scheduling problem motivated by a variety of practical applications: The input to the problem consists of a robot arm of capacity k (i.e., it can grasp at most k products at a time) and n products, each of which is associated with a release time and a deadline and moves on a predefined path with a fixed constant speed. In each round (tour), the robot arm grasps at most k products by their deadlines and delivers to a specified delivery point. The goal of the problem is to find a collection of tours such that the robot arm of capacity k grasps by their deadlines and delivers as many products as possible. In this paper we show that there is an $O(n\alpha(n)\log n)$ algorithm for the case $k = 1$ if all the products move on given straight lines with faster speeds than the robot arm, where $\alpha(n)$ is the inverse Ackermann function. However, for the similar setting for the paths of the products, we prove that if some of the products' speeds are slower than the robot arm's one, then the problem remains $\mathcal{NP}$-hard.

2. Yuichi Asahiro:
"Simple Greedy Methods for DNA Word Design", Proceedings of the 9th World Multi-Conference on Systemics, Cybernetics and Informatics, Vol.III, pp.186–191, (2005 年 7 月).
概要: For designing a large set of DNA strands, we tested three algorithms based

on traditional greedy heuristics. The constraints to be considered for the set are Hamming Distance (HD) constraint, Reverse Complement (RC) constraint, and GC Content (GC) constraint. The variety of the combinations of these three constraints is the most fundamental target of designing DNA strands. By the algorithms, we found larger sets than previously known ones for some settings of the length n and Hamming Distance d, e.g., $n = 14$ and $d = 3, 10$ with HD, GC, and RC constraints, and $n = 12$ and $d = 5, 6, 7, 8$ with HD and RC constraints. In addition to that, the theoretical complexity of the problem is shown, which does not seem to be explained in the previous studies.

3. Hideo Hirose:
"Optimal boundary finding method for the bumpy regions", Proceedings of the International Federation of Operational Research Societies Triennial 2005 Conference, (2005年7月).
概要: Assuming that the points having response 0 and the points response 1 are very similarly distributed except some regions, we want to find the boundaries for the bumpy regions in which the points with response 1 are much more frequently observed than in the whole support region.

4. Yuichi Asahiro, Eiji Miyano, Shinichi Shimoirisa:
"Pickup and Delivery for Moving Objects on Broken Lines", Proceedings of the 9th Italian Conference on Theoretical Computer Science, Lecture Notes in Computer Science, Vol.3701, pp.36–50, 2005年10月.
概要: We consider the following variant of the Vehicle Routing Problem that we call the *Pickup and Delivery for Moving Objects (PDMO)* problem, motivated by robot navigation: The input to the problem consists of n products, each of which moves on a predefined path with a fixed constant speed, and a robot arm of capacity one. In each round, the robot arm grasps and delivers one product to its original position. The goal of the problem is to find a collection of tours such that the robot arm grasps and delivers as many products as possible. In this paper we prove the following results: (i) If the products move on broken lines with at least one bend, then the PDMO is MAXSNP-hard, and (ii) it can be approximated with ratio two. However, (iii) if we impose the "straight line without bend" restriction on the motion of every product, then the PDMO becomes tractable.

5. Yuichi Asahiro, Eiji Miyano, Hirotaka Ono, Kouhei Zenmyo:
"Graph Orientation Algorithms to Minimize the Maximum Outdegree", Proceedings of the Computing: The Australasian Theory Symposium(CATS), Conferences in Research and Practice in Information Technology, Vol.51, pp.11–20, 2006年1月.
概要: We study the problem of orienting the edges of a weighted graph such that the maximum weighted outdegree of vertices is minimized. This problem, which has applications in the guard arrangement for example, can be shown to be $\mathcal{NP}$-hard generally. In this paper we first give optimal orientation algorithms which run in polynomial time for the following special cases: (i) the input is an unweighted graph, or more generally, a graph with identically weighted edges, and (ii) the input graph is a tree. Then, by using those algorithms as sub-procedures, we provide a simple, combinatorial, $\min\{\frac{w_{max}}{w_{min}}, (2-\varepsilon)\}$-approximation algorithm for the general case, where w_{max} and w_{min} are the maximum and the minimum weights of edges, respectively, and ε is some small positive real number that depends on the input.

6. Hideo Hirose, Takahiro Yukizane, Eiji Miyano:
"The bump hunting method using the genetic algorithm and the extreme-value statistics with application to a messy customer database", Proceedings of the 5th Hawaii International Conference on Statistics, Mathematics and Related Fields, 2006 年 1 月.
概要: In difficult classification problems of the z-dimensional points into two groups giving 0-1 responses due to the messy data structure, we try to find the denser regions for the favorable customers of response 1, instead of finding the boundaries to separate the two groups. Such regions are called the bumps, and finding the boundaries of the bumps is called the bump hunting. The main objective of this paper is to find the largest region of the bumps, specifying the ratio of the number of points of response 1 to the total. Then, we may obtain a trade-off curve between the number of points of response 1 and the specified ratio. The decision tree method with the Gini's index will provide the simple-shaped boundaries for the bumps if the marginal density for response 1 shows rather simple or monotonic shape. Since the computing time searching for the optimal trees will cost much because of the NP-hardness of the problem, some random search methods, e.g., the genetic algorithm adapted to the tree, are useful. Due to the existence of many local maxima unlike the ordinary genetic algorithm search results, the extreme-value statistics will be useful to estimate the global optimum number of captured points; this guarantees the accuracy of the semi-optimal solution with the simple descriptive rules. We show a successful result in applying this method to some artificial messy data case which mimics the real customer database.

7. Yuichi Asahiro, Takashi Horiyama, Kazuhisa Makino, Hirotaka Ono, Toshinori Sakuma, Masafumi Yamashita:
"How to Collect Balls Moving in the Euclidean Plane", Discrete Applied Mathematics, (掲載予定).
概要: 省略.

8. Yuichi Asahiro, Tetsuya Furukawa, Keiichi Ikegami, Eiji Miyano:
"How to Pack Directed Acyclic Graphs into Small Blocks", Proceedings of the 6th International Conference on Algorithms and Complexity, Lecture Notes in Computer Science, (掲載予定).
概要: 省略.

研究会等

1. Yuichi Asahiro, Eiji Miyano, Shinichi Shimoirisa:
"Hardness of Pickup and Delivery for Moving Objects on Broken Lines", 電子情報通信学会技術研究報告, 105 巻・72 号, pp.9–16, 2005 年 5 月.
概要: We consider the following variant of the Vehicle Routing Problem that we call the *Pickup and Delivery for Moving Objects (PDMO)* problem, motivated by robot navigation: The input to the problem consists of n products, each of which moves on a predefined path with a fixed constant speed, and a robot arm of capacity one. In each round, the robot arm grasps and delivers one product to its original position. The goal of the problem is to find a collection of tours such that the robot arm grasps and delivers as many products as possible. In this paper we prove the following results: (i) If the products move on broken lines with at least one bend, then the PDMO is MAXSNP-hard, and (ii) it can be approximated with ratio two. However, (iii) if we impose the "straight line without bend" restriction on every motion of the product,

then the PDMO becomes tractable.

2. Yuichi Asahiro, Eiji Miyano, Hirotaka Ono, Kouhei Zenmyo:
"On the Graph Orientation of Minimizing the Maximum Outdegree", 電子情報通信学会技術研究報告, 105 巻・34 号, pp.53–60, 2005 年 10 月.
概要: We study the problem of orienting the edges of a weighted graph such that the maximum weighted outdegree of vertices is minimized. This problem, which has applications in the guard arrangement for example, can be shown to be $\mathcal{NP}$-hard generally. In this paper we first give optimal orientation algorithms which run in polynomial time for the following special cases: (i) the input is an unweighted graph, or more generally, a graph with identically weighted edges, and (ii) the input graph is a tree. Then, by using those algorithms as sub-procedures, we provide a simple, combinatorial, $\min\{\frac{w_{max}}{w_{min}}, (2-\varepsilon)\}$-approximation algorithm for the general case, where w_{max} and w_{min} are the maximum and the minimum weights of edges, respectively, and ε is some small positive real number that depends on the input.

3. Yuichi Asahiro, Tetsuya Furukawa, Keiichi Ikegami, Eiji Miyano:
"Approximability and Non-approximability of the Minimum Block Transfer Problem", 電子情報通信学会技術研究報告, 105 巻・679 号, pp.17–24, 2006 年 3 月.
概要: The paper deals with the following problem: Given a directed acyclic graph, the objective is to find a mapping of its nodes into blocks of size at most B that minimizes the maximum number of external arcs during traversals of the acyclic structure by following paths from the roots to the leaves. An external arc is defined as an arc connecting two distinct blocks. The problem can be shown to be NP-hard. In this paper we provide a $\frac{3}{2}$ factor approximation algorithm for $B = 2$, and prove that the $\frac{3}{2}$ ratio is optimal in terms of approximation guarantee, while the previous approximation ratio was 2. In the case of $B \geq 3$, we also show that there is no $\frac{3}{2} - \varepsilon$ factor approximation algorithm assuming P $\neq$ NP, where ε is arbitrarily small positive. Furthermore, we give a 2 factor approximation algorithm for $B = 3$ if the input is a layered graph, which improves the known ratio of 3.

学会大会等

1. 朝廣雄一，古川哲也，宮野英次:
"サイズ 2 の最小ブロック転送問題に対する近似アルゴリズム", 夏の LA シンポジウム, pp.23-1 – 10, 2005 年 7 月.

2. 廣瀬英雄:
"分類問題への極値分布の応用", 統計数理研究所研究会，極値理論の工学への応用 (3), pp.54 – 65, 2005 年 9 月.

3. 大井伸哉，行實隆広，廣瀬英雄:
"GA を用いた Bump hunting 法に関する一考察", 電気関係学会九州支部第 58 回連合大会, pp.13-1P-06, 2005 年 9 月.

4. 行實隆広，大井伸哉，廣瀬英雄:
"GA を用いた Bump hunting の特性と最適値の統計的近似計算法", 電気関係学会九州支部第 58 回連合大会, pp.13-1P-07, 2005 年 9 月.

5. 廣瀬英雄，行實隆広，大井伸哉，宮野英次:
"Bump hunting 問題における極値統計の応用", 日本計算機統計学会第 19 回シンポジウム論文集, pp.55–58, 2005 年 10 月.

6. 廣瀬英雄:
"2005 年度 IEEE Reliability Society Japan Chapter Awards (論文賞)", 情報システム学研究科シンポジウム，第 10 回信頼性とシステム安全学, 2006 年 2 月.

B01: 代数的および確率的手法による離散構造の限界の究明

伊東 利哉 † 上野 修一 ‡

† 東京工業大学 学術国際情報センター
〒 152-8550 東京都目黒区大岡山 2-12-1-E2-5
titoh@dac.gsic.titech.ac.jp

‡ 東京工業大学 大学院理工学研究科
〒 152-8550 東京都目黒区大岡山 2-12-1-S3-57
ueno@lab.ss.titech.ac.jp

1 緒言

本年度は，離散構造の限界の解明に関して，

(1) 置換族の構成に関する研究;
(2) 線形符号の距離構造に関する研究;
(3) ネットワーク制御に関する研究;
(4) ネットワークの 3 次元レイアウトに関する研究;
(5) 可逆論理回路に関する研究

を中心に研究を行った．個別の研究内容に関しては，第 2 章以降で詳細に述べるが，各テーマ毎の研究の概略は以下の通りである．

1.1 置換族の構成に関する研究

最小値独立置換族 (とその拡張概念である ε 近似 k 制限最小値独立置換族) は，インターネット上に存在する類似した文書の特定に有用であることが知られている，また，これまでに最小値独立置換族と ε 近似 k 制限最小値独立置換族の構成法及び置換族のサイズに関する (非) 構成的上界・下界が数多く示されているが，未だに ε 近似 k 制限最小値独立置換族のサイズの上界・下界には大きな隔たりがある．そこで本研究では，代数的手法を用いて ε 近似 k 制限最小値独立置換族のサイズに関する良好な下界を導出した．

一方，ε 近似 k 制限ランダム置換族は，乱択アルゴリズムの非乱択化などの応用を持つ理論計算機科学における重要な概念の一つとして知られているが，任意の $k \geq 4$ に対して，多項式時間抽出可能な ε 近似 k 制限ランダム置換族の構成法はこれまでに知られいなかった．そこで本研究では，代表的な共通鍵暗号 DES の基本要素である Feistel 変換を用いて対数領域抽出可能な ε 近似 k 制限ランダム置換族の構成法を導出し，カップリング法を用いてその近似精度の解析を行なった．

1.2 線形符号の距離構造に関する研究

共通鍵暗号の安全性は，差分攻撃及び線形攻撃に対する耐性によって評価されるため，差分攻撃及び線形攻撃に対してある種の一様性が保証されたブール関数の設計が重要となる．そのような一様性を持つ (コンパクトな) ブール関数の設計は，任意の整数 d と $d^{\perp}$ が与えられたとき，以下を満たすような符号 $\mathcal{C}$ の最小符号長 $n = N(d, d^{\perp})$ を求める問題に帰着される: (1) 符号 $\mathcal{C}$ の最小距離は d; (2) 符号 $\mathcal{C}$ の双対符号 $\mathcal{C}^{\perp}$ の最小距離は $d^{\perp}$．そこで本研究では，任意の整数 $d, d^{\perp}$ に対して $N(d, d^{\perp})$ の上界を評価するとともに，代数的手法を用いてその良好な下界を導出した．

1.3 ネットワー制御に関する研究

QoS アルゴリズムの競合比の解析と通信網において先行制約のあるメッセージ集合の最短送信スケジュールを求める問題について考察した．QoS アルゴリズムに関する研究では，各種のパケットをその優先度に応じて効率的に転送制御するための複数キュー QoS アルゴリズムに関して検討した．一般に QoS スイッチに到来するパケットを事前に予測することは不可能であるので，QoS アルゴリズムはオンラインアルゴリズムとして定式化される．そして，キューに格納されているパケットを破棄することが許されないパケット破棄不可能モデルに着目し，複数優先度を持つ複数キュー QoS アルゴリズムの競合比の解析を行ない，良好な上界を示すとともに，これまで未解明であった非自

明な下界を導出した．また，通信網において先行制約のあるメッセージ集合の最短送信スケジュールを求める問題に関しては，それが一般に$\mathcal{NP}$困難であることを明らかにするとともに，近似アルゴリズムの近似比を改善した．

1.4 ネットワークの3次元レイアウトに関する研究

グラフの直交描画，3次元チャネル配線，ネットワークの3次元レイアウト，光結合ネットワーク及びVLSI分解について考察した．グラフの直交描画に関しては，2次元及び3次元直交描画可能であるための十分条件を導出した．3次元チャネル配線に関しては，一般的な3次元チャネル配線のモデルを提案し，与えられた2端子ネットの組を配線するために必要な3次元チャネルの層数の上界と下界を導出した．また，3次元チャネル配線問題は$\mathcal{NP}$困難であることを明らかにした．ネットワークの3次元レイアウトに関しては，N点バタフライネットワークに対して，その3次元レイアウトの最小体積の上界を改善した．光結合ネットワークに関しては，光転置結合システムを実現するために必要なレンズ数の上界を導出した．VLSI分解に関しては，deBruijinネットワークの万能構成ブロックの上界と下界を導出した．

1.5 可逆論理回路に関する研究

出力ベクトルの集合が入力ベクトルの集合の置換であるような論理回路を可逆論理回路と言い，低消費電力設計，デジタル信号処理，ナノ・量子計算などの応用を持つことが知られている．本研究では，可逆論理回路に対する最小完全テスト集合を生成する問題は$\mathcal{NP}$困難であることを示した．

2 置換族の構成に関する研究

2.1 ε近似k制限最小値独立置換族のサイズの下界

任意の整数$a \le b$に対して$[a,b] = \{a,\ldots,b\}$とする．また，任意の整数$n \ge 1$に対してS_nを集合$[0,n-1]$上の置換全体を表すものとする．

定義 2.1: 任意の$0 < \varepsilon < 1$と任意の整数$k \ge 3$に対して，置換族$\mathcal{F} \subseteq S_n$が$\varepsilon$近似$k$制限最小値独立であるとは，以下が成り立つことを言う: 任意の(空でない)集合$X \subseteq [1,n]$(ただし$|X| \le k$)と任意の$x \in X$に対して，

$$\left| \Pr_{\pi\in\mathcal{F}}[\min\{\pi(X)\} = \pi(x)] - \frac{1}{|X|} \right| \le \frac{\varepsilon}{|X|}.$$

ただし，置換πは置換族$\mathcal{F}$上の分布$\mathcal{D}$に従って選択されるものとする．

これまでにε近似k制限最小値独立置換族$\mathcal{F} \subseteq S_n$のサイズに関して，以下のことが知られている:

$$\begin{aligned}
&\text{上界}: \quad |\mathcal{F}| = 2^{4k+o(k)}k^{2\log\log(n/\varepsilon)} \text{ (構成的)};\\
&\text{上界}: \quad |\mathcal{F}| = O\big(\tfrac{k^2}{\varepsilon^2}\log(n/k)\big) \text{ (非構成的)};\\
&\text{下界}: \quad |\mathcal{F}| = \Omega\big(k^2(1-\sqrt{8\varepsilon})\big);\\
&\text{下界}: \quad |\mathcal{F}| = \Omega\Bigg(\min\Bigg\{k^2 2^{k/2}\log(n/k),\\
&\qquad\qquad \tfrac{\log(1/\varepsilon)(\log n - \log\log(1/\varepsilon))}{\varepsilon^{1/3}}\Bigg\}\Bigg).
\end{aligned}$$

任意の整数$k \ge 3$に対して$s = k/3, L = n/s$とする(簡単のためs, Lは整数とする)．ここで集合$[1,n]$をサイズがsの互いに背反なL個の部分集合$X_0, X_1, \ldots, X_{L-1}$に分割する: 各$i \in [0, L-1]$に対して$X_i = \{si+1, si+2, \ldots, (i+1)s\}$．任意の定数$\varepsilon > 0$に対して置換族$\mathcal{F} = \{\pi_1, \pi_2, \ldots, \pi_d\} \subseteq S_n$を$\varepsilon$近似$k$制限最小値独立とする．また$N = L - 1 = n/s - 1$とし，各$h \in [1,s]$に対して，以下のような$N \times d$行列$U_h = (u_{ij}^h)$を定義する．

$$u_{ij}^h = \begin{cases} \dfrac{1}{\sqrt{d}} & \min\{\pi_j(X_0 \cup X_i)\} = \pi_j(h);\\ 0 & \text{その他}. \end{cases}$$

さらに各$h \in [1,s]$に対して，以下のような$N \times N$行列$V_h = (v_{ij}^h)$を定義する．

$$\begin{aligned}
V_h &= (v_{ij}^h) = U_h U_h^T\\
&= \begin{bmatrix}
\frac{\delta_{11}^h}{2s} & \frac{\delta_{12}^h}{3s} & \frac{\delta_{13}^h}{3s} & \cdots & \frac{\delta_{1N}^h}{3s}\\
\frac{\delta_{12}^h}{3s} & \frac{\delta_{22}^h}{2s} & \frac{\delta_{23}^h}{3s} & \cdots & \frac{\delta_{2N}^h}{3s}\\
\frac{\delta_{13}^h}{3s} & \frac{\delta_{23}^h}{3s} & \frac{\delta_{33}^h}{2s} & \cdots & \frac{\delta_{3N}^h}{3s}\\
\vdots & \vdots & \vdots & \ddots & \vdots\\
\frac{\delta_{1N}^h}{3s} & \frac{\delta_{2N}^h}{3s} & \frac{\delta_{3N}^h}{3s} & \cdots & \frac{\delta_{NN}^h}{2s}
\end{bmatrix}.
\end{aligned}$$

仮定より置換族 $\mathcal{F} \subseteq S_n$ は ε 近似 k 制限最小値独立なので，任意の $i,j \in [1,N]$ に対して $1-\varepsilon \leq \delta_{ij}^h \leq 1+\varepsilon$ が成り立つ．従って以下を得る．

補題 2.1: 行列 $V_h = (v_{ij}^h)$ に関して以下が成立:

(i) 任意の $i \in [1,N]$ に対して

$$\frac{1-\varepsilon}{2s} \leq v_{ii}^h \leq \frac{1+\varepsilon}{2s};$$

(ii) 任意の $i,j \in [1,N]$ (ただし $i \neq j$) に対して

$$\frac{1-\varepsilon}{3s} \leq v_{ij}^h \leq \frac{1+\varepsilon}{3s}.$$

行列 U_h の定義より，任意の $h,g \in [1,s]$ (ただし $h \neq g$) に対して $U_h U_g^T = 0$ が成り立つ．ここで $Ns \times d$ 行列 U を $U^T = [U_1^T, U_2^T, \ldots, U_s^T]$ とし，以下のような $Ns \times Ns$ 行列 V を定義する．

$$V = UU^T = \begin{bmatrix} U_1 \\ U_2 \\ \vdots \\ U_s \end{bmatrix} \begin{bmatrix} U_1^T, U_2^T, \ldots, U_s^T \end{bmatrix} = \begin{bmatrix} V_1 & 0 & \cdots & 0 \\ 0 & V_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & V_s \end{bmatrix}.$$

このとき以下の事実に注意する．

$$\begin{aligned} \mathrm{rank}(V) &= \mathrm{rank}(UU^T) \\ &\leq \min\{\mathrm{rank}(U), \mathrm{rank}(U^T)\} \\ &= \mathrm{rank}(U) \leq \min\{d, Ns\} \leq d \end{aligned}$$

これより以下の命題を得る．

補題 2.2: 任意の ε 近似 k 制限最小値独立置換族 $\mathcal{F} \subseteq S_n$ に対して以下が成り立つ．

$$\begin{aligned} |\mathcal{F}| = d &\geq \mathrm{rank}(V) \\ &= \mathrm{rank}(V_1) + \mathrm{rank}(V_2) + \cdots + \mathrm{rank}(V_s). \end{aligned}$$

補題 2.2 より，ε 近似 k 制限最小値独立置換族 $\mathcal{F} \subseteq S_n$ のサイズの下界は，行列 $V_1, V_2, \ldots, V_s$ の階数の下界に還元される．以下の補題は，行列 $V_1, V_2, \ldots, V_s$ の階数を評価する際に重要となる．

補題 2.3: $t \times t$ 行列 $A = (a_{ij})$ が以下の条件を満たすならば，行列 A は正則である．

(C1) 任意の $i,j \in [1,t]$ (ただし $i \neq j$) に対して $a_{ij} = a > 0$;

(C2) $\min\{a_{11}, a_{22}, \ldots, a_{tt}\} > a$.

ここで $K_\ell = (V,E)$ を ℓ 個の節点を持つ完全グラフとし，$\mathcal{C}_m = \{c_1, c_2, \ldots, c_m\}$ を異なる m 色の色集合とする．また，$\chi : E \to \mathcal{C}_m$ を色集合 $\mathcal{C}_m$ による完全グラフ K_ℓ の枝の色塗りとする．任意の整数 $t_1, t_2, \ldots, t_m \geq 3$ に対して，$R(t_1, t_2, \ldots, t_m)$ を以下の条件を満たす最小の整数 ℓ とする:

- 任意の枝の色塗り $\chi : E \to \mathcal{C}_m$ に対して，ある $i \in [1,m]$ が存在し，単一色 c_i のみで塗られたの枝集合を持つ節点数 t_i の完全部分グラフ $K_{t_i} = (V_i, E_i) \subseteq K_\ell$ が存在する．

特に $t_1 = t_2 = \cdots = t_m = t$ であるとき，簡単のため $R_m(t)$ と表記することとする．

補題 2.4: 任意の整数 $m \geq 2, t \geq 1$ に対して，

$$R_m(t) \leq m^{mt-(m-1)}.$$

補題2.3及び補題2.4より，以下の補題が導かれる．

補題 2.5: 任意の定数 $0 < \varepsilon < 1/5$ と任意の整数 $k \geq 3$ に対して置換族 $\mathcal{F} \subseteq S_n$ を ε 近似 k 制限最小値独立とする．また，任意の整数 $m \geq 1$ に対して $|\mathcal{F}| < \frac{k}{2\varepsilon} m$ と仮定すると，各行列 V_h に関して以下が成り立つ．

$$\mathrm{rank}(V_h) \begin{cases} = N & m = 1; \\ \geq \left\lfloor \dfrac{\log(3n/k)}{m \log m} \right\rfloor & m \geq 2. \end{cases}$$

補題 2.5 より，以下の ε 近似 k 制限最小値独立置換族 $\mathcal{F} \subseteq S_n$ のサイズの下界が導出される．

定理 2.1: 任意の定数 $0 < \varepsilon < 1/5$ と任意の整数 $k \geq 3$ に対して，置換族 $\mathcal{F} \subseteq S_n$ が ε 近似 k 制限最小値独立であるとする．このとき，十分大きな整数 n に関して，以下が成り立つ．

$$|\mathcal{F}| = \Omega\left(k \cdot \frac{\log^{1/2-o(1)}(n/k)}{\varepsilon^{1/2+o(1)}} \right).$$

2.2 ε近似k制限ランダム置換族の構成

任意の整数$a \le b$に対して$[a,b] = \{a, a+1, \ldots, b\}$とし，任意の有限集合$A$に対して$S_A$を集合$A$上の置換全体とする．また，任意の整数$n \ge k \ge 1$に対して$[n]_k = n(n-1)\cdots(n-k+1)$とする．

定義 2.2: 任意の定数$0 \le \varepsilon < 1$に対して，置換族$\mathcal{F} \subseteq S_A$が以下の条件を満たすとき，$\varepsilon$近似$k$制限ランダムであると言う: 任意の互いに異なる$k$個の$x_1, x_2, \ldots, x_k \in A$と任意の互いに異なる$k$個の$y_1, y_2, \ldots, y_k \in A$に対して，

$$\left| \Pr_{\pi\in\mathcal{F}} \left[\bigwedge_{i=1}^{k} \pi(x_i) = y_i \right] - \frac{1}{[n]_k} \right| \le \frac{\varepsilon}{[n]_k} = \frac{\varepsilon}{n(n-1)\cdots(n-k+1)}.$$

ただし，置換πは置換族$\mathcal{F}$上の分布$\mathcal{D}$に従って選択されるものとする．

定義 2.3: 任意の集合A, Bと任意の定数$0 \le \varepsilon < 1$に対して，関数族$\mathcal{G} = \{g : A \to B\}$が以下を満たすとき，$\varepsilon$近似$k$制限ランダムであるという言う: 任意の互いに異なるk個の$x_1, x_2, \ldots, x_k \in A$と任意の — 互いに異なるとは限らない — k個の$y_1, y_2, \ldots, y_k \in B$に対して

$$\left| \Pr_{g\in\mathcal{G}} \left[\bigwedge_{i=1}^{k} g(x_i) = y_i \right] - \frac{1}{m^k} \right| \le \frac{\varepsilon}{m^k}.$$

ただし$m = |B|$であり，関数gは関数族$\mathcal{G}$上の分布$\mathcal{D}$に従って選択されるものとする．

加法群G_+に対して，関数$g : G_+ \to G_+$に関するフェイステル変換$h_g : G_+ \times G_+ \to G_+ \times G_+$を以下のように定義する．

定義 2.4: 関数$g : G_+ \to G_+$に対して置換$h_g : G_+ \times G_+ \to G_+ \times G_+$が$g$に関するフェイステル変換であるとは以下のことを言う: 任意の$(\ell, r) \in G_+ \times G_+$に対して$h_g((\ell, r)) = (r, \ell + g(r))$.

ここで任意の素数pと任意の整数$h \ge 1$に対して$G_+ = \mathbf{GF}(p^h)$とすると，関数族$\mathcal{G} = \{g(x) = g_k x^k + g_{k-1}x^{k-1} + \cdots + g_1 x + g_0 : g_i \in \mathbf{GF}(p^h)\}$は$k$制限ランダムとなることが知られている．このとき無作為に選択された関数$g \in \mathcal{G}$に対してG_+^k上の状態遷移行列$\mathbf{P} = (p(x,y))$を以下のように定義する: 任意の$x, y \in G_+^k$に対して$p(x,y) = \Pr[h_g(x) = y]$. 状態空間$\mathcal{X} = G_+^k$上の任意の初期分布をμ_0とし定常分布をπとする．また任意の整数$t \ge 1$に対し$\mu_t = \mathbf{P}\mu_{t-1}$とする．ここで，状態遷移行列$\mathbf{P} = (p(x,y))$に対して

$$\beta = \sum_{y\in\mathcal{X}} \min_{x\in\mathcal{X}} p(x,y)$$

とすると以下の補題が成り立つ．

補題 2.6: 状態遷移行列$\mathbf{P} = (p(x,y))$に対してπをG_+^k上の定常分布とする．このときG_+^k上の任意の初期状態μ_0と任意の整数$t \ge 1$に対して，

$$\|\mu_t - \pi\| \le (1-\beta)^t.$$

ただし$\|\cdot\|$はℓ_1ノルムを表すものとする．

任意の整数kに関するk制限ランダム関数族$\mathcal{G}$に対して独立且つ無作為に選択されたd個の関数$g_1, g_2, \ldots, g_d \in \mathcal{G}$に関するフェイステル変換族$\mathcal{H}_{\mathcal{G}}^d$を以下のように定義する:

$$\mathcal{H}_{\mathcal{G}}^d = \{h_{g_d} \circ \cdots \circ h_{g_2} \circ h_{g_1} : g_1, g_2, \ldots, g_d \in \mathcal{G}\}.$$

このとき$n = p^{2h}$とし，任意の定数$0 < \varepsilon < 1$と任意の整数$k = O(\log n)$に対して

$$d = 3 \cdot \left\lceil \frac{\log[n]_k + \log(1/\varepsilon)}{\log(m/2) - \log\binom{k}{2}} \right\rceil$$

とすると，補題2.6より以下の定理が導出される．

定理 2.2: 任意の素数pと任意の整数$h > 0$に対して$n = p^{2h}$とする．このとき$k = O(\log n)$とすると，以下を満たす対数領域抽出可能なε近似k制限ランダム置換族$\mathcal{F} \subseteq S_{[0,n-1]}$が構成可能:

$$|\mathcal{F}| = \left(\frac{n^{k^2}}{\varepsilon^k}\right)^{3+o(1)}.$$

3 線形符号の距離構造に関する研究

共通鍵暗号の安全性は，差分攻撃及び線形攻撃に対する耐性によって評価されるため，差分攻撃及び線形攻撃に対してある種の一様性が保証されたブール関数の設計が重要となる．そのような一様

性を持つ(コンパクトな)ブール関数の設計は，任意の整数 d と $d^\perp$ が与えられたとき，以下を満たすような符号 $\mathcal{C}$ の最小符号長 $n = N(d, d^\perp)$ を求める問題に帰着される: (1) 符号 $\mathcal{C}$ の最小距離は d; (2) 符号 $\mathcal{C}$ の双対符号 $\mathcal{C}^\perp$ の最小距離は $d^\perp$．そこで本研究では，任意の整数 $d, d^\perp$ に対して，以下のような $N(d, d^\perp)$ の上界を導出した．

定理 3.1: 任意の整数 $n \geq m$ と任意の整数 $d, d^\perp$ が与えられたとき $N(d, d^\perp) \leq n$．ただし n は以下の不等式を満たす最小の整数とする．

$$\frac{2^m - 1}{2^n - 1} \sum_{i=1}^{d-1} \binom{n}{i} + \frac{2^{n-m} - 1}{2^n - 1} \sum_{i=1}^{d^\perp - 1} \binom{n}{i} < 1.$$

ここで，任意の整数 $n \geq d$ に対して

$$\ell(n, d) = \begin{cases} \sum_{i=0}^{(d-1)/2} \binom{n}{i} & d \text{は奇数;} \\ \sum_{i=0}^{d/2-1} \binom{n}{i} + \binom{n-1}{d/2-1} & d \text{は偶数.} \end{cases}$$

このとき，代数的手法を用いることにより，以下のような $N(d, d^\perp)$ の下界を導出した．

定理 3.2: 任意の整数 $d, d^\perp$ 対して

$$N(d, d^\perp) \geq \min\{n : n \geq \lg \ell(n, d) + \lg \ell(n, d^\perp)\}.$$

4 ネットワーク制御に関する研究

4.1 QoS アルゴリズムの競合比の解析

近年のインターネットの爆発的な普及に伴い，ネットワーク機器に過剰な負荷がかかり，また帯域損失・パケット消失・応答遅延などの通信品質の劣化が深刻化している．このような通信品質の劣化を防ぐために Quality of Service (QoS) の概念が注目されている．一般に QoS スイッチは m 個のキューを持ち，各キューは到来するパケットを格納するための B 個のスロットを有する．また各パケットはその優先順位を表す “優先度” が割り当てられている．ネットワーク上の通信量はしばしば変化するため，QoS スイッチは転送パケットの優先度の総和を最大にするように到来するパケットの制御を行う．ここで QoS スイッチは，将来到来するパケットの情報を得ることが不可能であるので QoS アルゴリズムはオンラインアルゴリズムとして定式化され，その効率は競合比によって評価される．QoS アルゴリズム ALG が c-競合的であるとは，全てのパケット列 σ に対して

$$\frac{\text{OPT}(\sigma)}{\text{ALG}(\sigma)} \leq c$$

が成り立つことを言う．ただし $\text{ALG}(\sigma)$ はパケット列 σ に対して QoS アルゴリズム ALG が転送したパケットの優先度の総和を表すものとし，一方 $\text{OPT}(\sigma)$ は，パケット列 σ に対して最適なオフラインアルゴリズム OPT が転送したパケットの優先度の総和を表すものとする．

本研究では，優先度が 1 と $\alpha \geq 1$ に制限された決定性 QoS 問題に関して，その競合比の下界の解析を行い，以下の結果を導出した．

定理 4.1: 任意の QoS アルゴリズム ALG と任意の $\alpha \geq 1$ に対して，パケット列 σ が存在し，

$$\frac{\text{OPT}(\sigma)}{\text{ALG}(\sigma)} \geq \begin{cases} 1 + \frac{1}{\alpha \ln\left(\frac{\alpha}{\alpha-1}\right)} - \Theta\left(\frac{1}{\min\{m,B\}}\right) \\ \qquad\qquad \alpha \geq \alpha^*; \\ \frac{1}{1-e^{-\tau_0}} - \Theta\left(\frac{1}{\min\{m,B\}}\right) \\ \qquad\qquad 1 \leq \alpha < \alpha^*. \end{cases}$$

ただし τ_0 は $e^{-\tau}(1/\alpha + \tau) = 1 - e^{-\tau}$ の根である．

またこの結果より，単一優先度決定性 QoS 問題に関して，その競合比の下界が 1.466 以上となることが容易に導出される．これは単一優先度決定性 QoS 問題の競合比に関する既知の下界 1.366 を改善するものである．

4.2 ネットワークのスケジューリングに関する研究

本研究では，通信網において先行制約のあるメッセージの集合の最短送信スケジュールを求める問題を考察している．特に，この問題が $\mathcal{NP}$ 困難である場合と多項式時間アルゴリズムで解ける場合の境界を明らかにすると共に，$\mathcal{NP}$ 困難な場合に，近似アルゴリズムの近似比の評価を改善している．

5 ネットワークの3次元レイアウトに関する研究

ネットワークのレイアウトに関する研究では，グラフの直交描画，3次元チャネル配線，ネットワー

クの3次元レイアウト，光結合ネットワーク，及びネットワークのVLSI分解について考察している．

5.1 グラフの直交描画に関する研究

グラフの直交描画は2次元及び3次元集積回路の設計などに応用があるために，従来から活発に研究されている．2次元直交描画に関しては以下の事実が知られている:

(i) 最大次数が高々4の平面的グラフは，八面体を除外して，各辺に対するベンド数が高々2で2次元直交描画できる;

(ii) 最大次数が高々3の平面的グラフは，4点完全グラフを除外して，各辺に対するベンド数が高々1で2次元直交描画できる;

(iii) グラフをベンドなしで2次元直交描画できるか否かを判定する問題は$\mathcal{NP}$完全である．

本研究では，2次元直交描画に関して以下のことを明らかにしている:

(1) 最大次数が高々3で三角形を含まない外平面グラフはベンドなしで2次元直交描画できる;

(2) 最大次数が高々4の任意の直並列グラフは各辺に対するベンド数が高々1で2次元直交描画できる．

3次元直交描画に関しては以下の事実が知られている:

(iv) 最大次数が高々6の任意のグラフは各辺に対するベンド数が高々3で3次元直交描画できる;

(v) 最大次数が高々5の任意のグラフは，各辺に対するベンド数が高々2で3次元直交描画できる;

(vi) グラフをベンドなしで3次元直交描画できるか否かを判定する問題は$\mathcal{NP}$完全である．

最大次数が高々6の任意のグラフが各辺に対するベンド数が高々2で3次元直交描画できるか否かを決定することは興味深い未解決問題である．本研究では，3次元直交描画に関して以下のことを明らかにしている:

(3) 最大次数が高々6で三角形を含まない外平面グラフはベンドなしで3次元直交描画できる;

(4) 最大次数が高々6の任意の直並列グラフは各辺に対するベンド数が高々2で3次元直交描画できる．

5.2 3次元チャネル配線に関する研究

3次元チャネル配線は3次元集積回路設計における基本的な問題であり，いくつかの先駆的研究が散見されるが，いずれも本質的には2次元あるいは2.5次元のチャネル配線のモデルであり，本来の3次元チャネル配線のモデルは提案されていない．

本研究では初めて自然で一般的な3次元チャネル配線のモデルを提案すると共に，与えられた2端子ネットの組を配線するために必要な3次元チャネルの層数の上界と下界を明らかにしている．

特に，n個の2端子ネットは$O(\sqrt{n})$層の3次元チャネル内で長さ$O(\sqrt{n})$の配線を用いて配線できることを明らかにすると共に．配線するためには$\Omega(\sqrt{n})$層の3次元チャネルを必要とするようなn個の2端子ネットの組が存在することを示している．

さらに，本研究では，3次元チャネル配線問題は$\mathcal{NP}$困難であることを明らかにしている．一方，2次元チャネル配線問題の計算複雑度は四半世紀以上の間未解決のままである懸案である．

5.3 ネットワークの3次元レイアウトに関する研究

バタフライネットワークは並列計算機の相互結合網やATMスイッチの結線構造としてよく用いられている．N点バタフライネットワークB_Nの3次元レイアウトに関しては，$\mathrm{vol}(B_N)$をB_Nの3次元レイアウトの最小体積としたときに，

$$\mathrm{vol}(B_N) \geq 0.75N^{3/2} + o(N^{3/2})$$

であること，及び

$$\mathrm{vol}(B_N) \leq 723\sqrt{2}N^{3/2} + o(N^{3/2})$$

であることが知られている．

本研究では，B_N の具体的な 3 次元レイアウトを示すことにより，

$$\mathrm{vol}(B_N) \leq 8\sqrt{2}N^{3/2} + o(N^{3/2})$$

であることを証明している．これは既存の上界に対して大幅な改良になっている．

5.4 光結合ネットワークに関する研究

光転置結合システム (OTIS) はネットワークを 3 次元自由空間の光結合によって実現する一つの手法である．deBruijn ネットワークは並列計算機の相互結合網や FFT などの並列計算の基礎構造としてよく用いられている．d 値 D 次元 deBruijn ネットワーク $B(d,D)$ の OTIS 実現に関しては，OTIS 実現に必要なレンズの数が $\Omega(\sqrt{dN})$ であることが知られている．ここで，$N = d^D$ は $B(d,D)$ の点数である．また，D が偶数であるときに，OTIS 実現に必要なレンズの数は $O(d\sqrt{N})$ であることも知られている．

本研究では，任意の正整数 D に対して，OTIS 実現に必要なレンズの数の上界を与えている．すなわち，OTIS 実現に必要なレンズの数は:

(1) $D \equiv 1 \pmod 4$ であるとき，$O(d^{5/2}\sqrt{N})$;

(2) $D \equiv 3 \pmod 4$ であるとき，$O(d^{3/2}\sqrt{N})$;

(3) D が偶数であるとき，$O(d\sqrt{N})$

であることを明らかにしている．これらの上界と下界の間隙を埋めることは今後の課題である．

5.5 ネットワークの VLSI 分解に関する研究

グラフ G の同型で点非共有な部分グラフの族は，G を張るとき，G の VLSI 分解であるという．また，各部分グラフに同型なグラフ H を G の構成ブロックという．G の辺数に対する部分グラフの辺数の総和の比率を H の効率という．グラフ H がグラフの族 $\{G_n\}$ の任意のグラフの構成ブロックであるとき，H は $\{G_n\}$ の万能構成ブロックであるという．2 値 D 次元 deBruijn ネットワーク $B(2,D)$ の族 $\{B(2,D)|D \geq n\}$ の万能構成ブロックの効率は少なくとも $1 - O(1/n)$ であり，多くとも $1 - \Omega(1/n)$ であることが知られている．

本研究では，d 値 D 次元 deBruijn ネットワーク $B(d,D)$ の族 $\{B(d,D)|D \geq n\}$ の万能構成ブロックの効率は少なくとも $1-O(d/n)$ であり，多くとも $1 - \Omega(1/n)$ であることを明らかにしている．これらの上下界の間隙を埋めることは今後の課題である．

6 可逆論理回路に関する研究

出力ベクトルの集合が入力ベクトルの集合の置換であるような論理回路を可逆論理回路という．可逆論理回路は，低消費電力設計，デジタル信号処理，ナノ・量子計算などに応用できることから，最近活発に研究されている．

本研究では，可逆論理回路 C と C の配線の任意の集合 F が与えられたときに，F 上の縮退故障を検出する最小完全テスト集合を生成する問題は $\mathcal{NP}$ 困難であることを明らかにしている．これは，可逆論理回路の故障検出の計算複雑度に関する初めての結果である．

研究業績一覧

著書

1. 上野修一，高橋篤司:
“情報とアルゴリズム（電子情報通信工学シリーズ）”, 森北出版株式会社, 2005 年 4 月.
概要: グラフ理論，アルゴリズム理論，及び計算複雑度の理論の入門書である．

学術論文

1. Toshiya Itoh and Takanobu Nagumo:
“Improved Lower Bounds for Competitive Ratio of Multi-Queue Switches in QoS Networks”, IEICE Trans. Fundamentals, Vol.E88-A, No.5, pp.1155-1165, 2005.
概要: The recent burst growth of the Internet use overloads networking systems and degrades the quality of communications, e.g., bandwidth loss, packet drops, delay of

responses, etc. To overcome such degradation of the communication quality, the notion of Quality of Service (QoS) has received attention in practice. In general, QoS switches have several queues and each queue has several slots to store arriving packets. Since network traffic changes frequently, QoS switches need to control arriving packets to maximize the total priorities of transmitted packets, where the priorities are given by nonnegative values and correspond to the quality of service required for each packet. In this paper, we derive lower bounds for the competitive ratio of deterministic multi-queue nonpreemptive QoS problem of priorities 1 and $\alpha \geq 1$: $1+/\alpha \ln(\frac{\alpha}{\alpha-1})$ if $\alpha \geq \alpha^*$; $1/(1-e^{-\tau_0})$ if $1 \leq \alpha < \alpha^*$, where $\alpha^* \approx 1.657$ and τ_0 is a root of the equality that $e^{-\tau}(1/\alpha+\tau) = 1-e^{-\tau}$. As an immediate result, this shows a lower bound 1.466 for the competitive ratio of deterministic multi-queue nonpreemptive QoS problem of single priority, which slightly improves the best known lower bound 1.366.

2. Kohsuke Ogata, Toshinori Yamada, and Shuichi Ueno:
"A Note on the Implementation of de Bruijn Networks by the Optical Transpose Interconnection System", IEICE Trans. Fundamentals, Vol.E88-A, No.12, pp.3661-3662, 2005.
概要: This note shows an efficient implementation of de Bruijn networks by the Optical Transpose Interconnection System (OTIS) extending previous results by Coudert, Ferreira, and Perennes.

3. Kumiko Nomura, Satoshi Tayu, and Shuichi Ueno:
"On the Orthogonal Drawing of Outerplanar Graphs", IEICE Trans. Fundamentals, Vol.E88-A, No.6, pp.1583-1588, 2005.
概要: In this paper we show that an outerplanar graph G with maximum degree at most 3 has a 2-D orthogonal drawing with no bends if and only if G contains no triangles. We also show that an outerplanar graph G with maximum degree at most 6 has a 3-D orthogonal drawing with no bends if and only if G contains no triangles.

4. Toshinori Yamada, Hiroyuki Kawakita, Tadashi Nishiyama, and Shuichi Ueno:
"On VLSI Decompositions for d-ary de Bruijn Graphs (Extended Abstract)", Proceedings of the IEEE International Symposium on Circuits and Systems, pp.1358-1361, 2005.
概要: A VLSI decomposition of a graph G is a collection of isomorphic vertex-disjoint subgraphs (called building blocks) of G which together span G. The efficiency of a VLSI decomposition is the fraction of the edges of G which are present in the subgraphs. This paper gives a necessary condition and a sufficient condition for a graph to be a building block for d-ary de Bruijn graphs. We also show building blocks for d-ary de Bruijn graphs with asymptotically optimal efficiency. Furthermore, we list the most efficient universal d-ary de Bruijn building blocks we know of.

5. Satoshi Tayu, Patrik Hurtig, Yoshiyasu Horikawa, and Shuichi Ueno:
"On the Three-Dimensional Channel Routing", Proceedings of the IEEE International Symposium on Circuits and Systems, pp.180-183, 2005.
概要: The 3-D channel routing is a fundamental problem on the physical design of 3-D integrated circuits. The 3-D channel is a 3-D grid G and the terminals are vertices of G located in the top and bottom layers. A net is a set of terminals to be connected. The object of the 3-D channel routing problem is to connect the terminals in each net with a tree (wire) in G using as few layers as possible and as short wires as possible in

such a way that wires for distinct nets are disjoint. This paper shows that any set of n 2-terminal nets can be routed in a 3-D channel with $O(n^{1/2})$ layers using wires of length $O(n^{1/2})$. We also show that there exists a set of n 2-terminal nets that requires a 3-D channel with $\Omega(n^{1/2})$ layers to be routed.

6. Koji Goda, Toshinori Yamada, and Shuichi Ueno:
"A Note on the Complexity of Scheduling for Precedence Constrained Messages in Distributed Systems", IEICE Trans. Fundamentals, Vol.E88-A, No.4, pp.1090-1092, 2005.
概要: This note considers a problem of minimum length scheduling for a set of messages subject to precedence constraints for switching and communication networks, and shows some improvements upon previous results on the problem.

研究会等

1. Toshiya Itoh:
"Improved Lower Bounds for Families of ε-Approximate k-Restricted Min-Wise Independent Permutations", Electronic Colloquium on Computational Complexity, TR06-017, 2006.
概要: A family $\mathcal{F}$ of min-wise independent permutations is known to be a useful tool of indexing replicated documents on the Web. For any integer $n > 0$, let S_n be the family of all permutations on $[1, n] = \{1, 2, \ldots, n\}$. For any integer k such that $1 \leq k \leq n$ and any $\varepsilon > 0$, we say that a family $\mathcal{F} \subseteq S_n$ of permutations is ε-approximate k-restricted min-wise independent if for any (nonempty) subset $X \subseteq [1, n]$ such that $|X| \leq k$ and any element $x \in X$, $|\Pr[\min\{\pi(X)\} = \pi(x)] - |X|^{-1}| \leq \varepsilon/|X|$, when π is chosen from $\mathcal{F}$ uniformly at random (where $|A|$ denotes the cardinality of a finite set A). For the size of families $\mathcal{F} \subseteq S_n$ of ε-approximate k-restricted min-wise independent permutations, the following results are known: For any integer k such that $1 \leq k \leq n$ and any real $\varepsilon > 0$, (constructive upper bound) $|\mathcal{F}| = 2^{4k+o(k)} k^{2 \log\log(n/\varepsilon)}$; (nonconstructive upper bound) $|\mathcal{F}| = O\big(\frac{k^2}{\varepsilon^2} \log(n/k)\big)$; (lower bound) $|\mathcal{F}| = \Omega\big(k^2(1 - \sqrt{8\varepsilon})\big)$ and $|\mathcal{F}| = \Omega\big(\min\{k^2 2^{k/2} \log(n/k), \frac{\log(1/\varepsilon)(\log n - \log\log(1/\varepsilon))}{\varepsilon^{1/3}}\}\big)$. In this paper, we first derive an upper bound for the Ramsey number of the edge coloring with $m \geq 2$ colors of a complete graph K_ℓ of ℓ vertices, and by the linear algebra method, we then derive a slightly improved lower bound, i.e., we show that for any family $\mathcal{F} \subseteq S_n$ of ε-approximate k-restricted min-wise independent permutations, $|\mathcal{F}| = \Omega\big(k\sqrt{\frac{1}{\varepsilon} \log(n/k)}\big)$.

2. Toshiya Itoh and Tatsuya Nagatani:
"Improved Lower Bounds for Families of *varepsilon*-Approximate k-Restricted Min-Wise Independent Permutations", IEICE Technical Report, Vol.COMP2006, No.66, pp.23-30, 2006.
概要: A family $\mathcal{F}$ of min-wise independent permutations is known to be a useful tool of indexing replicated documents on the Web. For any integer $n > 0$, let S_n be the family of all permutations on $[1, n] = \{1, 2, \ldots, n\}$. For any integer k such that $1 \leq k \leq n$ and any real $\varepsilon > 0$, we say that a family $\mathcal{F} \subseteq S_n$ of permutations is *ε-approximate k-restricted min-wise independent* if for any (nonempty) subset $X \subseteq [1, n]$ such that $|X| \leq k$ and any element $x \in X$, $|\Pr[\min\{\pi(X)\} = \pi(x)] - |X|^{-1}| \leq \varepsilon/|X|$, when π is chosen from $\mathcal{F}$ uniformly at random (where $|A|$ denotes the cardinality of a finite set A). For the size of families $\mathcal{F} \subseteq S_n$ of ε-approximate k-restricted min-wise independent permutations, the following results are known: For any integer k such that $1 \leq k \leq n$ and any

real $\varepsilon > 0$, (constructive upper bound) $|\mathcal{F}| = 2^{4k+o(k)}k^{2\log\log(n/\varepsilon)}$; (nonconstructive upper bound) $|\mathcal{F}| = O(\frac{k^2}{\varepsilon^2}\log(n/k))$; (lower bound) $|\mathcal{F}| = \Omega(k^2(1-\sqrt{8\varepsilon}))$ and $|\mathcal{F}| = \Omega(\min\{k^2 2^{k/2}\log(n/k), \frac{\log(1/\varepsilon)(\log n - \log\log(1/\varepsilon))}{\varepsilon^{1/3}}\})$. In this paper, we first derive an upper bound for the Ramsey number of the edge coloring with $m \geq 2$ colors of a complete graph K_ℓ of ℓ vertices, and by the linear algebra method, we then derive a slightly improved lower bound, i.e., we show that for any family $\mathcal{F} \subseteq S_n$ of ε-approximate k-restricted min-wise independent permutations, $|\mathcal{F}| = \Omega(k\sqrt{\frac{1}{\varepsilon}\log(n/k)})$.

3. Satoshi Tayu, Kumiko Nomura, and Shuichi Ueno:
"On the Three-Dimensional Orthogonal Drawing of Series-Parallel Graphs", IEICE Technical Report, Vol.105, No.502, pp.7-12, 2006.
概要: It has been known that every 6-graph has a 3-bend 3-D orthogonal drawing, while it has been open whether every 6-graph has a 2-bend 3-D orthogonal drawing. For the interesting open question, it is known that every 5-graph has a 2-bend 3-D orthogonal drawing, and every outerplanar 6-graph without triangles has a 0-bend 3-D orthogonal drawing. We show in this paper that every series-parallel 6-graph has a 2-bend 3-D orthogonal drawing.

4. Satoshi Tayu, Kumiko Nomura, and Shuichi Ueno:
"On the Two-Dimensional Orthogonal Drawing of Series-Parallel Graphs", IEICE Technical Report, Vol.105, No.387, pp.51-56, 2005.
概要: It has been known that every planar 4-graph has a 2-bend 2-D orthogonal drawing with the only exception of octahedron, every planar 3-graph has a 1-bend 2-D orthogonal drawing with the only exception of K_4, and every outerplanar 3-graph with no triangles has a 0-bend 2-D orthogonal drawing. We show in this paper that every series-parallel 4-graph has a 1-bend 2-D orthogonal drawing.

5. Shigeru Ito, Yusuke Ito, Satoshi Tayu, and Shuichi Ueno:
"On the Complexity of Fault Testing for Reversible Circuits", IEICE Technical Report, Vol.105, No.387, pp.13-16, 2005.
概要: This paper shows that it is $\mathcal{NP}$-hard to generate a minimum complete test set for stuck-at faults on a set of wires of a reversible circuit.

6. Toshiya Itoh, Tatsuya Nagatani, and Jun Tarui:
"Explicit Construction for k-Wise Nearly Random Permutations by Iterated Feistel Transform", Proceedings of Randomness and Computation, 2005.
概要: A notion of k-wise random permutations has several applications. From the practical point of view, it often suffices to consider ε-approximate k-wise random permutation families rather than k-wise random permutation families, however, we know little about how to construct families of ε-approximate k-wise random permutations of small size. For any integer $n > 0$, we use S_n to denote the set of all permutations on $\{0, 1, \ldots, n-1\}$. In this paper, we iteratively apply the *Feistel Transform* to construct a family of ε-approximate k-wise random permutations and we show that for any $n = p^{2h}$ with p prime and any $k = O(\log n)$, there exists a family $\mathcal{F} \subseteq S_n$ of ε-approximate k-wise random permutations such that $|\mathcal{F}| = (n^{k^2}/\varepsilon^k)^{3+o(1)}$. This is the first nontrivial construction for families of ε-approximate k-wise random permutations. To capture efficient evaluation of permutation families in the practical point of view, we introduce a notion of "$s(n)$-space

pointwise samplability," and show that the family $\mathcal{F} \subseteq S_n$ of permutations constructed in this paper is $O(\log n)$-space pointwise samplable.

7. Ryutaroh Matsumoto, Kaoru Kurosawa, and Toshiya Itoh:
"Primal-Dual Distance Bounds of Linear Codes with Application to Cryptography", Cryptology ePrint Archive, Report2005/194, 2005.
概要: We propose upper and lower bounds on the minimum code length of linear codes with specified minimum Hamming distance and dual distance. From these bounds we can estimate the minimum input length of Boolean functions with specified cryptographic strength constructed by the design method of Kurosawa et al.

学会大会等

1. Takafumi Yamaguchi, Satoshi Tayu, and Shuichi Ueno:
"On the Complexity of Three-Dimensional Channel Routing", Proceedings of the 68th National Convension of IPSJ, pp.1-193 – 1-194, 2006.

2. Satoshi Tayu, Yoshiyasu Horikawa, and Shuichi Ueno:
"On the Three-Dimensional Layout of Butterfly Networks", Proceedings of the 2005 IEICE Society Conference, A-1-27, p.27, 2005.

3. Shigeru Ito, Yusuke Ito, Satoshi Tayu, and Shuichi Ueno:
"On the Complexity of Fault Testing for Reversible Circuits", Proceedings of the 2005 IEICE Society Conference, A-1-26, p.26, 2005.

B02: 暗号解析手法の計算量理論による改良とそれに基づく暗号方式

田中 圭介 † 渡辺 治 † 戸田 誠之助 ‡ 河内 亮周 †

† 東京工業大学 大学院情報理工学研究科
数理・計算科学専攻
〒 152-8552 東京都目黒区大岡山 2-12-1
{keisuke, watanabe,
kawachi}@is.titech.ac.jp

‡ 日本大学 文理学部 情報システム解析学科
〒 156-8550 東京都世田谷区桜上水 3-25-40
toda@cssa.chs.nihon-u.ac.jp

1 研究の目的と活動の概要

暗号解析手法の計算量理論による改良とそれに基づく暗号方式の提案を行うために，具体的な目標を以下のように三つ定める．これらは独立に存在するわけではなく，おおまかには，目標 3 が，目標 1 および 2 をふまえた最終的な目標となる．また，それぞれの目的における成果は他への研究指針となり互いに密接に関連する．

目的 1：暗号の安全性に関する精密な解析手法の開発

暗号方式に対する攻撃はある種の計算問題であるとみなすことができる．また，暗号方式のモデルはある種の計算モデルであるとみなすことができる．計算量理論は，これまで多種の計算問題に内在する計算構造を明らかにしてきているが，グラフ同型性判定問題や群に関わる様々な計算問題などに象徴される『計算構造が不明な離散的計算問題』もまた数多く存在する．暗号方式に対する攻撃についても，このような計算構造が不明な離散的計算問題であると考えられる．そこで本研究ではまず，このような計算問題に関して，それらに内在するはずの本質的な計算構造を探究する．また，その解析をもとに，それらの計算問題を様々な計算モデル上で計算する際の限界と可能性を明らかにする．この解析手法を応用し，暗号の安全性に関する精密な解析手法を開発する．

目的 2：暗号の効率に関する精密な解析手法の開発

暗号方式は安全であるだけでなく効率的に動作する必要がある．また，通常のコンピュータ上での動作だけではなく，携帯電話や IC カードなどのプロセッサの処理スピードが遅い状況やメモリが少ない状況での動作がしばしば要求される．理論的解析については，定数係数は無視してオーダーで議論するのが主流であり，様々な状況における暗号アルゴリズムの効率の詳細な解析は計算機を用いたシミュレーションを行うなど実験的な手法に頼らざるを得なかった．そこで本研究ではまず，細かな尺度で計算コストを測るための手法として，定数係数までも考慮に入れた計算量理論を開発する．この計算量理論を応用し，暗号の効率に関する精密な解析手法を開発する．

目的 3：目的 1 および 2 に基づく具体的暗号方式の提案

暗号プロトコルのうち最も基本的なものとしては公開鍵暗号がある．そこでまず，この公開鍵暗号に対する具体的方式の提案を行う．設計にあたっては目的 1 および 2 の考察をふまえて行う．すなわち，暗号の安全性および効率に関する精密な解析手法のもとで優れた暗号方式の提案を目的とする．さらには，公開鍵暗号以外の，電子署名，認証など，他の暗号プロトコルに対する具体的方式の提案も行う．

目的 1 に関しては，戸田が，chordal graph を対象としたグラフ自己同型群計算問題に関する研

究を行った．

目的 2 に関しては，渡辺が，NP 完全，あるいは NP 困難な問題の最も代表的なものとして有名な，論理式の充足可能性問題 SAT 問題と総称される問題群に対する，アルゴリズムの改良，あるいは，アルゴリズムの評価方法について研究した．また，河内が，量子状態の識別問題に関して研究を行った．

目的 3 に関しては，田中が，公開鍵暗号に関する様々な考察および提案を行った．また，この目的 3 に関しては，ミニ研究集会を 2 月 16 日にはこだて未来大学において開催し，暗号理論に関する研究成果の発表と，新たな課題探求に向けた討論を行った．

2 暗号の安全性に関する精密な解析手法に関する活動概要

2.1 chordal graph を対象とした自己同型群計算問題

戸田は，chordal graph を対象とした自己同型群計算問題に関する研究を行った．特に，simplicial な要素が小さいサイズをもつ chordal graph を対象とした．任意の chordal グラフは simplicial な要素にユニークに分解できることが知られている．この事実に基づき，与えられた chordal グラフに対してその自己同型群を $O((c! \cdot n)^{O(1)})$ 時間で計算できることを示した．ここで，c は simplicial な要素の最大サイズであり，n はノードの個数である．さらに，chordal グラフの自己同型性は同じ時間で判定できることも示した．多項式時間計算可能性の観点から，我々の結果はクリーク数に対応する以前の結果を真に強めたものとなっている．

3 暗号の効率に関する精密な解析手法に関する活動概要

3.1 充足可能性問題に対するアルゴリズム

渡辺は，NP 完全，あるいは NP 困難な問題の最も代表的なものとして有名な，論理式の充足可能性問題 SAT 問題と総称される問題群に対する，アルゴリズムの改良，あるいは，アルゴリズムの評価方法について研究した．

(1) SAT 問題群（一般の SAT 問題とその変形版）に対する局所探索法に関しては，様々な実験的な研究が行われているが，理論的な解析は少ない．我々は，アルゴリズムの「平均的なよさ」を解析するために，アルゴリズムの「平均的な実行」を追う手法を研究してきたが，その手法を SAT 問題群の局所探索法に応用した．その結果，(i) 局所探索法が成功する場合の理由を準理論的に示すことができた．さらに，(ii) SAT 問題群の中でも，局所探索法に対する相性に差があること，(iii) タブー探索の効果，なども明らかにすることができた．

(2) MAX-SAT 問題の難しさの平均的な解析をする際，問題例の分布に対する確率モデルが必要である．これまで，そのような確率モデルとして妥当なものがなかったが，我々は，MAX-2SAT 問題に対して，まず，テスト例題生成，という観点から問題例生成の手法を提案した．さらに，それを単純化して，MAX-2SAT 問題の問題例に対する自然な確率分布を提案することができた．

(3) 上記の分布のもとでの MAX-2SAT 問題の難しさの解析を目的とし，我々は，その分布に対して比較的よい性能を持ち，線形時間のアルゴリズムを考案した．これは，人工知能の研究で開発された「信念伝播法」という手法にヒントを得て，それを非常に単純化したアルゴリズムである．このアルゴリズムが，上記の分布の元で，MAX-2SAT 問題を高い確率で解くことを証明した．

(4) SAT 問題に対して，最悪時時間計算量の改善を行った．具体的には，まず，3SAT 問題に対し，これまでの変数数 n に対する最悪時計算時間 $O(1.333^n)$ の乱択アルゴリズムに対し，最悪時計算時間が $O(1.330^n)$ のアルゴリズムを設計した．一方，一般の SAT 問題に対しては，決定性アルゴリズムを考え，これまでの最悪時計算時間 $O(^m)$ のアルゴリズム（ただし m は論理式の節数）に対し，$O(1.234^m)$ のアルゴリズムを提案した．

3.2 量子状態の識別問題

河内は，(1) ある特殊な 2 種類の量子状態の識別問題が暗号論的性質を満たすことの理論的証明，

(2) その識別問題に基づいた量子公開鍵暗号系の提案と理論的安全性評価，を行った．

(1) に関して，本研究ではある二つの量子状態の識別問題が (i) 落とし戸を持つ，(ii) 平均時の困難性が最悪時の困難性と等価である，(iii) 最悪時の困難性が少なくともグラフ自己同型性判定問題の最悪時困難性と同等かそれ以上である，という三つの暗号論的性質を満たすことを証明した．例えばこの問題を公開鍵暗号系に利用することを考えた場合，敵対者には暗号文が区別できないが，正しい秘密情報を持つ受信者には暗号文を正しく解読できるという性質が必要となる．性質 (i) はこの機能を提供するものである．また，ある計算困難な問題を暗号に利用した場合，実際にはランダムに問題生成を行うため，その問題の最悪時困難性が保証されているだけでは不十分である．性質 (ii) はこの識別問題の平均時困難性が最悪時困難性によって保証されることを示している．さらにその最悪時困難性は性質 (iii) により保証されている．なお，このグラフ自己同型性判定問題は量子計算機を用いても効率良く解けるかどうか判明しておらず，少なくとも現在のいくつかの量子計算機上のアルゴリズムの設計手法では解けないという否定的な結果もいくつか知られている．

この三つの性質を利用することで (2) の量子公開鍵暗号系を構成することが可能となった．この公開鍵暗号系における暗号の解読は少なくともグラフ自己同型性判定問題を解くことと同等かそれ以上に難しいことが証明可能であるため，現在知られている量子計算機上のアルゴリズムでは解読困難であるといえる．

4 目的 1 および 2 に基づく具体的暗号方式に関する活動概要

田中は具体的暗号方式に関して以下のような様々な考察および提案を行った．

4.1 匿名性をもつ暗号プロトコル

匿名性を持つ暗号プロトコルに関して，以下のような研究を行った．

データに関するプライバシーと鍵に関するプライバシーの関係　公開鍵暗号方式に要求される一般的な安全性は，暗号化されたデータに関するプライバシーを問題としている．データに関するプライバシーの定式化には，一方向性 (OW) や識別不可能性 (IND) などがある．一方向性は，暗号文から平文が復元できないという性質を定式化しており，識別不可能性は，暗号文から平文に関する情報が漏れないという性質を定式化したものである．

一方，Bellare, Boldyreva, Desai, Pointcheval は，新しい安全性の指標として，鍵に関するプライバシーを提案した．これは，暗号化に用いられた鍵に関するプライバシーを問題としている．すなわち，暗号文がどの鍵で暗号化されたかがわからないという性質である．この性質をもつ暗号方式を使うと，攻撃者には暗号文の受信者（最終的に復号する人）が誰だかわからないため，暗号文の受信者に関する匿名性がみたされると見なすことができる．彼らはこの性質を匿名性 (IK, 鍵の識別不可能性) として定式化した．

この安全性指標に関連して，Halevi はシンプルな十分条件 (IKR と呼ぶ) を与え，IND かつ IKR を満たせば IK を満たすことを示した．Hayashi, Tanaka は，Bellare, Boldyreva, Desai, Pointcheval の提案した定義を変形して，強匿名性と呼ばれる匿名性の新しい定義 (sIK と呼ぶ) を提案した．

我々は，以上の結果をふまえて，データに関するプライバシー (IND, OW) と鍵に関するプライバシー (IK, IKR, sIK) の関係を示した．

例えば，IK をみたしても，必ずしも OW をみたすとは限らないが，sIK は OW だけでなく IND もみたすことを示した．さらに，sIK は “IND かつ IKR” であること，IK は “IND かつ IKR” より弱いことも示した．これにより，sIK と “IND かつ IKR” は等価であることがわかった．

適応的選択暗号文攻撃に対する匿名性を得るための一般的な変換　Bellare らによる匿名性の定義は，選択平文攻撃と適応的選択暗号文攻撃の二つの攻撃のもとで定式化されている．この二つの安全性をそれぞれ IK-CPA と IK-CCA と呼ぶ．

我々は，2 つの鍵のもとでの plaintext aware-

ness の概念を提案した．これを PA2 と呼ぶ．公開鍵暗号方式が PA2 の意味で安全であるとは，その方式が IK-CPA をみたし，かつ PA2 のための knowledge extractor が存在するときをいう．PA のための knowledge extractor と，PA2 のための knowledge extractor は相違点がある．

次に，公開鍵暗号方式が PA2 の意味で安全であるならば，IK-CCA の意味でも安全であることを示した．これは，公開鍵暗号方式が PA2 の意味で安全であることを示すことは，IK-CCA の意味で安全であることを示すことと比較して容易であると考えられるため，PA2 は公開鍵暗号方式に関する匿名性の性質として有用なものである．

さらに，匿名性を得るための一般的な変換方式を初めて提案した．具体的には，Fujisaki-Okamoto 変換方式によって，IK-CPA の意味で安全な基本的な暗号方式が，ランダムオラクルモデルにおいて IK-CCA の意味で安全な方式に変換されることを示した．

一般的匿名化可能な公開鍵暗号方式　我々は，一般的匿名化可能な公開鍵暗号方式の概念をはじめて提案した．同じセキュリティーパラメーターでつくられた暗号化データがあり，そのデータは匿名性の性質を満たすとする．ここでは，これらの暗号化データを復号することなしに匿名性をもつ暗号化データに変換したい状況を考える．

この状況を形式化するために，一般的匿名化可能と呼ばれる，公開鍵暗号のための新しい概念を提案した．この一般的匿名化可能な公開鍵暗号方式を用いることにより，暗号文を作成した人だけでなく，暗号化に用いられた秘密鍵を知らなくても暗号化データを匿名化できるようになる．

さらに，ElGamal 暗号方式，Cramer-Shoup 暗号方式，RSA-OAEP 方式を基にした一般的匿名化可能な公開鍵暗号方式を提案し，その安全性を示した．

4.2　特殊な機能をもつ暗号プロトコル

匿名性をもつ暗号プトロコル以外にも特殊な機能をもつ暗号プロトコルを提案した．

1 つめとして，バッチ検証機能付きの Signcryption に関する研究を行った．Signcryption とは，暗号化と署名を同時に 1 つのステップで行う方式であり，暗号化と署名を別々に行うよりも効率がよいという性質を持っている．Signcryption は，鍵生成アルゴリズム，暗号化と署名を同時に行う sincrypt アルゴリズム，復号と検証を同時に行う designcrypt アルゴリズムの 3 つから構成される．我々は，バッチ検証つきの Signcryption のモデルを提案する．このモデルでは，designcrypt アルゴリズムにおいてバッチ検証を行うことができる．バッチ検証を行うと，Signcrypt アルゴリズムにより変換されたメッセージ (signcrypted message) の検証を一括して行うことができるため，検証に必要なコストをおさえることができる．安全性としては，signcrypted message の平文に関する情報が漏れないこと，signcrypted message の偽造ができないこと，署名者と検証者に関する匿名性の 3 つを定式化した．さらに，我々はこのモデルのもとで具体的な方式を提案した．我々の方式は，効率の良いバッチ検証を行うことが可能で，さらに定式化した 3 つの安全性をみたしている．

2 つめとして，リング署名を拡張し，指定検証者リング署名の概念の提案を行った．リング署名において，その検証が誰にでも可能なため生じる「署名の一人歩き問題」があるが，我々の提案する新しいリング署名方式によってこの問題を解決することができる．指定検証者リング署名は，通常のリング署名としても使うことができるだけでなく，リング署名を持っている人なら署名者に限らず誰でも，それを特定の人にしか検証できないものに変換できる機能を持つ．この機能により，指名者が意図する人にのみ署名を検証させることが可能となる．さらに，我々は指定検証者リング署名の具体的な方式も提案した．

3 つめとして，墨塗り署名に関する研究を行った．墨塗り署名とは，墨塗り者と呼ばれる第三者が，署名者から文書とその文書に対する署名を受け取ったとき，文書の一部を墨塗りし，さらにそれに対する署名を生成できる署名方式である．このとき，墨塗りされた部分からは，墨を塗られる前の文書に関する情報は得られない．墨塗り署名は，個人情報のように開示すべきでない情報を除いた部分開示を行う場合などに利用される．我々は，秘密情報を用いた墨塗り署名に注目し，そのモデルと安全性を定式化した．また，そのモデル

のもとで安全な墨塗り署名方式を提案した．この方式は gap co-Diffie-Hellman group の存在を仮定することで安全性が証明されている．さらに，これまでに提案されている多くの方式と我々の方式について比較，整理を行った．

4 つめとして，3 人モデルにおける，効率の良いパスワード認証付き鍵交換プロトコルを提案した．Abdalla，Fouque，Pointcheval は，3 人モデルにおけるパスワード認証付き鍵交換プロトコルの一般的な構成方法を提案した．彼らのプロトコルは自然で有用であるが，安全性を示すには多くの仮定が必要である．具体的には，2 人モデルのパスワード認証付き鍵交換プロトコル，3 人モデルの鍵配布，MAC の存在と，desional Diffie-Hellman problem の困難性を仮定する必要がある．さらに，このプロトコルは多くのラウンド数を必要とする．我々は，一般的な構成方法ではないものの，少ない仮定のもとで安全な 3 人モデルにおけるパスワード認証付き鍵交換プロトコルを提案した．我々のプロトコルは，desional Diffie-Hellman problem の困難性のみを仮定すれば，ランダムオラクルモデルのもとで安全である．さらに，我々のプロトコルは 4 ラウンドで終了するため，非常に効率がよいものとなっている．

4.3 組み合わせ問題を基礎とした暗号方式

組み合わせ問題を基礎とした暗号方式に関して，次のような研究を行った．

まず，ナップザック問題に基づいた量子計算署名に関する研究を行った．これまでに，いくつかのナップザック問題ベースの公開鍵暗号方式が提案されている．しかしながら，ナップザック問題ベースの署名方式はほとんど提案されていない．Shamir の署名方式は線形変換に基づいているが，量子計算機を使うことなくその安全性が破られている．岡本，田中，内山は，量子計算署名の定義を提案した．そして，早稲田，双紙，宮地は，岡本らの定義に基づいたナップザック問題ベースの量子計算署名を提案した．彼らの方式は，符号付きナップザック問題に基づいている．我々は，早稲田，双紙，宮地による方式の詳細な解析を行った．その結果，攻撃者が署名者の秘密鍵を手に入れることができることがわかり，早稲田らの方式は安全ではないことがわかった．さらに我々は，この解析をふまえた上で，ナップザック問題に基づいた量子計算署名を構成することの可能性について議論した．

次に，格子暗号の複数ビット化に関する研究を行った．現在，安全性証明がある格子暗号は 1 ビット暗号しか知られていない．一方，現在までに知られている効率の良い格子暗号は安全性の証明がない. そこで我々は，よく知られている 4 つの 1 ビット格子暗号 (Ajtai-Dwork 暗号，Regev03 暗号，Regev05 暗号，Ajtai 暗号) を対象に，共通の手法を導入し，公開鍵・秘密鍵・暗号文空間のサイズを変えることなく平文空間を複数ビット化した. 具体的には，セキュリティパラメータを n とした際に，平文のビット数を $O(\log n)$ とすることができる. また，複数ビット化した格子暗号も，元の 1 ビット格子暗号と同様に安全性を証明することができる．その際，格子暗号中で使われているガウス分布と安全性の基となる格子問題の解析を行い，平文のビット数・復号エラーの確率と安全性の基となる格子問題の間にトレードオフがあることが分かった．また，我々は “擬似準同型性” という概念を導入した．通常の暗号の準同型性は，2 つの暗号文の和または積が暗号文になるという性質である．一方，擬似準同型性は，2 つの暗号文の和が暗号文にはなるとは限らないが，無視できる確率を除いて正しく復号できるという性質である．複数ビット化した格子暗号は，ガウス分布の再生性により擬似準同型性を持つ．ただし，復号エラーを抑えるために，和の回数はある程度制限される．さらに，先と同様の手法により，その方式の安全性も証明した．

4.4 暗号プロトコルのモデルと方式に関する研究

暗号プロトコルに関するモデルについても以下のような研究を行った．

まず，多対 1 モデルでの公平な署名交換に関する研究を行った．2004 年，Chen，Kudla，Paterson は，concurrent signature の概念を提案した．この署名を用いると，利用する状況はある程度制限されるものの，信用できる第 3 者を仮定したり，多くの通信を必要とすることなく，公平に署名を

交換することができる．彼らのモデルでは 1 対 1 での公平な署名交換を扱っていたが，我々は多対 1 での公平な署名交換を考える．我々は多対 1 モデルにおける concurrent signature のモデルと安全性を定式化するとともに，具体的な方式を提案した．我々の方式は，離散対数問題の困難性を仮定すると，honest-but-curious セッティングかつ random permutation model のもとで安全である．

また，secret handshake と呼ばれる認証プロトコルに関する研究も行った．近年，Balfanz, Durfee, Shankar, Smetters, Staddon, Wong は，プライバシーを考慮した相互認証のひとつである secret handshake のモデルを提案した．secret handshake を用いると，認証を行う 2 人が同じグループのメンバーならば，お互いが同じグループに所属しているということを納得できる．一方で，違うグループに属している場合は，自分が所属しているグループの情報を相手に漏らすことはない．このモデルにおける具体的な方式は，Xu, Young により初めて提案されている．Balfanz らのモデルでは，認証の際に対象とするグループはひとつだけであった．我々は，複数グループにおける secret handshake のモデルと，具体的な方式を提案した．このモデルでは，メンバーがあるグループに加入したり，グループから離脱しても，それ以外のグループの所属情報を変更したり，再構築する必要がない．

5　ミニ研究集会 (暗号理論)

総括班の櫻井の呼びかけをきっかけに，本特定領域研究における暗号理論の研究者：

太田 和夫 (電気通信大学)
國廣 昇 (電気通信大学)
櫻井 幸一 (九州大学)
高木 剛 (はこだて未来大学)
田中 圭介 (東京工業大学)

とそれぞれの研究グループの研究者を中心にミニ研究集会を開催した．はこだて未来大学の高木が会場世話人となり，田中がプログラムのとりまとめをした．

当日の参加者は講演者を含めて約 20 名だった．講演は下記の概要の通りであるが，1, 3 番目の講演は，各自の研究成果に関する内容が中心であり，2, 4, 5 番目の講演は，研究分野のサーベイに関する内容が中心であった．

参加者が少ないこともことも手伝って自由に質問できる雰囲気があった．実際，発表の最中にも質問がでるなど活発な質疑や討論が行われ，それぞれの専門分野に関する理解を深めることができた．ただ，本研究集会は，参加者の都合により，半日で開催することになったが，そのため，発表および質疑応答の時間が十分だとはいえなかった．

研究集会後に開いた懇親会では，通常の学会主催の研究会では得られない貴重な集まりだったという意見が多く，次年度以降も継続してこのような暗号理論の研究集会を開催したいという意見も多かった．

次年度以降も，継続して，このような暗号理論の研究集会を企画し，班を越えた相互の研究討論を通じて，最新の情報交換，共同研究を促進していく計画である．

日時　2006 年 2 月 16 日 (木) 13:00-17:30

場所　はこだて未来大学 小講義室 585 （〒 041-8655 北海道函館市亀田中野町 116 番地 2）

プログラム

1. 13:00-13:30
   Privacy-preserving Text Mining in Distributed Environment
   ○ Chunhua Su, Kouichi Sakurai (九州大学)

2. 13:30-14:00
   Pairing Implementation using Hyperelliptic Curves
   Colm O hEigeartaigh (Dublin City University)

3. 14:15-15:00
   A Survey about Side Channel Attacks on XTR
   ○ Dong-Guk Han, Tsuyoshi Takagi (はこだて未来大学)

4. 15:00-15:45
   オフライン検証性を満たす追跡不可能な量子

現金
國廣 昇 (電気通信大学)

5. 16:00-16:45
離散対数問題系に基づく安全で効率的な署名方式
太田 和夫 (電気通信大学)

6. 16:45-17:30
匿名性をもつ公開鍵暗号
○林 良太郎, 田中 圭介 (東京工業大学)

各発表の概要

1. Privacy-preserving Text Mining in Distributed Environment
○ Chunhua Su, Kouichi Sakurai (九州大学)
概要：プライバシーを考慮したデータマイニングに対する研究のサーベイと今回，テキストデータをとくに扱ったものに関する著者の提案法方式の紹介．キーワードを用いた質疑プロトコルを利用する際に，紛失通信という暗号技術を利用している．

2. Pairing Implementation using Hyperelliptic Curves
Colm O hEigeartaigh (Dublin City University)
概要：ID ベース暗号の実現で注目されている楕円曲線ペアリングを，超楕円曲線の場合に適用した場合のサーベイと著者による最新の実装データを報告した．標数が 2,3 の Duursma-Lee 法を改良した η ペアリングは，現在のところ最も高速にペアリング暗号を実装するアルゴリズムである．1024 ビットのセキュリティを持つ埋込み次数 12 の超特異な超楕円曲線を用いて，Pentium 4 + SSE2 において 1.8ms を達成した．

3. A Survey about Side Channel Attacks on XTR
○ Dong-Guk Han, Tsuyoshi Takagi (はこだて未来大学)
概要：拡大次数 6 の有限体上の離散対数問題を利用した XTR という公開鍵暗号系に対する実装攻撃のサーベイ．発表者 (昨年度は九大で博士課程在籍，今年度は未来大でポスドク) を中心とするここ数年の解読法と防御法に関する研究を紹介した．著者等が提案したユークリッド互助法を応用した防御法は，固定パターン持つ耐 SPA 性クラスの中で最速な方式である．この領域は，未だに「攻撃→防御→攻撃」の繰り返しで研究が進行しているのが現状である．

4. オフライン検証性を満たす追跡不可能な量子現金
國廣 昇 (電気通信大学)
概要：これまでに提案されている量子現金方式は，オフライン検証性または追跡不可能性のどちらか一方を満たす方式であったが，今回はこの 2 つの性質を同時に満足する量子現金の提案を行った．さらに，提案した量子現金を，古典の電子現金の世界だけで見てみた場合の対応付けを考察し，量子現金方式の安全性評価への方向付けを示した．

5. 離散対数問題系に基づく安全で効率的な署名方式
太田 和夫 (電気通信大学)
概要：Schnorr 署名にはじまり，CRYPTO 2005 で発表された最新の Chevallier 署名にいたる離散対数問題系に基づく電子署名の安全性と効率に関するサーベイ．安全性の根拠として，離散対数問題，計算 Deffie-Hellmann 問題，判定 Deffie-Hellmann 問題の困難性を仮定した場合の，署名生成の実現手段，困難な問題を署名偽造に帰着するための帰着効率，計算効率などを比較している．困難な問題の制約を強めると，帰着効率や計算効率が向上していることが，具体例によって確認できた．

6. 匿名性をもつ公開鍵暗号
○林 良太郎, 田中 圭介 (東京工業大学)
概要：暗号文を見ても，それが誰の公開鍵で暗号化されたのかがわからない，という暗号文の受信者の匿名性に関する研究．2001 年ごろ概念が提起・定式化され匿名通信路の実現・電子入札などへの応用をもつ．著者らの開発した技術を含む，4 つの実現テクニックを，RSA 暗号とエルガマル暗号の場合に分けて，比較考察している．今後の課題としては，ランダムオラクルモデルに依存しない標

準モデルの場合の考察・匿名性を満たす ID ベース方式の実現などがある.

研究業績一覧

学術論文

1. R. Hayashi and K. Tanaka:
"Schemes for Encryption with Anonymity and Ring Signature", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Special Section on Cryptography and Information Security, Vol. E89-A, No. 1, 66-73, January, 2006.
概要: In this paper, we present previously unproposed schemes with the anonymity property for encryption and ring signature by applying two techniques. That is, we construct a key-privacy encryption scheme by using N-ary representation, and a ring signature scheme by using the repetition of evaluation of functions. We analyze precisely the properties of these schemes and show their advantage and disadvantage.

2. H. Hiwatari and K. Tanaka:
"A Cramer-Shoup Variant Related to the Quadratic Residuosity Problem", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Special Section on Cryptography and Information Security, Vol. E89-A, No. 1, 203-205, January, 2006.
概要: At Eurocrypt '02, Cramer and Shoup proposed a general paradigm to construct practical public-key encryption schemes secure against the adaptive chosen ciphertext attack as well as several concrete examples. One of these example is the scheme based on the quadratic residuosity (QR) problem. However this scheme is less efficient than the other examples. In this paper, we construct a new variant of the Cramer-Shoup encryption scheme which is related to the QR problem. Our variant is more efficient than the scheme based on the QR problem.

3. O. Watanabe:
"Randomized algorithms for 3-SAT", Theory of Computing Systems, (掲載予定).
概要: SAT 問題に対して，最悪時時間計算量の改善を行った．具体的には，まず，3SAT 問題に対し，これまでの変数数 n に対する最悪時計算時間 $O(1.333^n)$ の乱択アルゴリズムに対し，最悪時計算時間が $O(1.330^n)$ のアルゴリズムを設計した．一方，一般の SAT 問題に対しては，決定性アルゴリズムを考え，これまでの最悪時計算時間 $O(^m)$ のアルゴリズム（ただし m は論理式の節数）に対し，$O(1.234^m)$ のアルゴリズムを提案した.

4. M. Yamamoto:
"Generating instances for MAX2SAT with optimal solutions", Theory of Computing Systems, (掲載予定).
概要: MAX-SAT 問題の難しさの平均的な解析をする際，問題例の分布に対する確率モデルが必要である．これまで，そのような確率モデルとして妥当なものがなかったが，我々は，MAX-2SAT 問題に対して，まず，テスト例題生成，という観点から問題例生成の手法を提案した．さらに，それを単純化して，MAX-2SAT 問題の問題例に対する自然な確率分布を提案することができた.

研究会等

1. A. Kawachi, T. Koshiba, H. Nishimura, T. Yamakami:
"Computational Indistinguishability between Quantum States and Its Applications", Advances in Cryptography – Eurocrypt 2005, Lecture Notes in Computer Science 3494, 268-284, May, 2005.
概要: ある二つの量子状態の識別問題が (i) 落とし戸を持つ，(ii) 平均時の困難性が最悪時の困難性と等価である，(iii) 最悪時の困難性が少なくともグラフ自己同型性判定問題の

最悪時困難性と同等かそれ以上である，という三つの暗号論的性質を満たすことを証明した．さらに，この識別問題をもとにして，量子公開鍵暗号系を提案した．この公開鍵暗号系における暗号の解読は少なくともグラフ自己同型性判定問題を解くことと同等かそれ以上に難しいことが証明可能であるため，現在知られている量子計算機上のアルゴリズムでは解読困難であるといえる．

2. H. Hada and K. Tanaka:
"Security for Authenticated Key Exchange Based on Non-Malleability", International Conference on Information Technology and Applications (ICITA 2005), vol. 2, 508-513, July, 2005.
概要: This paper continues the study of password-based protocols for authenticated key exchange (AKE). In 2000, Bellare, Pointcheval, and Rogaway proposed the formal model on AKE. In this paper, we propose new security notions on AKE, based on the non-malleability of session keys. Then we prove that those security notion are equivalent to that proposed by Bellare, Pointcheval, and Rogaway. Furthermore, we show that there is a protocol secure in the random oracle model, not always secure in the standard model with collision-resistant hash functions.

3. A. Mihara and K. Tanaka:
"Universal Designated-Verifier Signature with Aggregation", International Conference on Information Technology and Applications (ICITA 2005), vol. 2, 514-519, July, 2005.
概要: There is a signature scheme which can aggregate two or more persons' signatures to one, called an aggregate signature. In this paper, we propose a scheme of an aggregate signature which has additional functionality allowing any holder of a signature to designate the signature to any desired designated-verifier. By this functionality, no one other than the designated-verifier can verify the signature, so the signature passed to other persons would not appear where the signer does not intend to send it in the form which anyone can verify.

4. T. Isshiki and K. Tanaka:
"An $(n-t)$-out-of-n Threshold Ring Signature Scheme", Information Security and Privacy – 10th Australasian Conference (ACISP 2005), Lecture Notes in Computer Science 3574, 406-416, July, 2005.
概要: In CRYPTO2002, Bresson, Stern, and Szydlo proposed a threshold ring signature scheme. Their scheme uses the notion of fair partition and is provably secure in the random oracle model. Their scheme is efficient when the number t of signers is small compared with the number n of group members, i.e., $t = O(\log n)$ (we call this scheme BSS scheme). However, it is inefficient when t is $\omega(\log n)$. In this paper, we propose a new threshold ring signature scheme which is efficient when the number of signers is large compared with the number n of group members, i.e., when the number t of non-signers in the group members is small compared with n. This scheme is very efficient when $t = O(\log n)$. This scheme has a kind of dual structure of BSS scheme which is inefficient when the number of signers is large compared with the number of group members. In order to construct our scheme, we modify the trap-door one-way permutations in the ring signature scheme, and use the combinatorial notion of fair partition. This scheme is provably secure in the random oracle model.

5. R. Hayashi and K. Tanaka:
"Universally Anonymizable Public-Key Encryption", Advances in Cryptology – ASIACRYPT 2005, Lecture Notes in Computer Science 3788, 293-312, December, 2005.
概要: We first propose the notion of uni-

versally anonymizable public-key encryption. Suppose that we have the encrypted data made with the same security parameter, and that these data do not satisfy the anonymity property. Consider the situation that we would like to transform these encrypted data to those with the anonymity property without decrypting these encrypted data. In this paper, in order to formalize this situation, we propose a new property for public-key encryption called universal anonymizability. If we use a universally anonymizable public-key encryption scheme, not only the person who made the ciphertexts, but also anyone can anonymize the encrypted data without using the corresponding secret key. We then propose universally anonymizable public-key encryption schemes based on the ElGamal encryption scheme, the Cramer-Shoup encryption scheme, and RSA-OAEP, and prove their security.

6. O. Watanabe:
"Some heuristic analysis of local search algorithms for SAT problems", 3rd International Symposium on Stochastic Algorithms, Foundations and Applications, Lecture Notes in Computer Science 3777, 14-24, October, 2005.
概要: SAT 問題群（一般の SAT 問題とその変形版）に対する局所探索法に関しては，様々な実験的な研究が行われているが，理論的な解析は少ない．我々は，アルゴリズムの「平均的なよさ」を解析するために，アルゴリズムの「平均的な実行」を追う手法を研究してきたが，その手法を SAT 問題群の局所探索法に応用した．その結果，(i) 局所探索法が成功する場合の理由を準理論的に示すことができた．さらに，(ii) SAT 問題群の中でも，局所探索法に対する相性に差があること，(iii) タブー探索の効果，なども明らかにすることができた．

7. M. Yamamoto:
"An improved $\widetilde{\mathcal{O}}(1.234^m)$-time deterministic algorithm for SAT", 16th International Symposium on Algorithms and Computation (ISAAC'05), Lecture Notes in Computer Science 3827, 644-653, December, 2005.
概要: SAT 問題に対して，最悪時時間計算量の改善を行った．具体的には，まず，3SAT 問題に対し，これまでの変数数 n に対する最悪時計算時間 $O(1.333^n)$ の乱択アルゴリズムに対し，最悪時計算時間が $O(1.330^n)$ のアルゴリズムを設計した．一方，一般の SAT 問題に対しては，決定性アルゴリズムを考え，これまでの最悪時計算時間 $O(^m)$ のアルゴリズム（ただし m は論理式の節数）に対し，$O(1.234^m)$ のアルゴリズムを提案した．

8. 林良太郎, 田中圭介:
"Relationships between Data-Privacy and Key-Privacy", 2006 年 暗号と情報セキュリティシンポジウム (SCIS2006), 1A2-1, 2006 年 1 月.
概要: The classical security requirement of public-key encryption schemes is that it provides privacy of the encrypted data. Popular formalizations such as one-wayness (OW) or indistinguishability (IND) are directed at capturing various data-privacy requirements. Bellare, Boldyreva, Desai, and Pointcheval proposed a new security requirement of encryption schemes called "key-privacy" or "anonymity" (IK, which means "indistinguishability of keys."). It asks that an encryption scheme provides privacy of the key under which the encryption was performed. That is, if an encryption scheme provides the key-privacy, then the receiver is anonymous from the point of view of the adversary. Related to this security notion, Halevi provided a simple sufficient condition (which we denote IKR) and he showed IND $\wedge$ IKR implies IK. Hayashi and Tanaka modified the definition by Bellare, Boldyreva, Desai, and

Pointcheval, and proposed a new definition of the anonymity property, which we call the strong anonymity (sIK). In this paper, we show the relationships between data-privacy (IND, OW) and key-privacy (IK, IKR, sIK). For example, we show that wIK does not imply OW, but sIK implies not only OW but IND. We also show that sIK is equivalent to IND $\wedge$ IKR, while IK is weaker than IND $\wedge$ IKR.

9. 林良太郎, 田中圭介:
"Generic Conversion for the Anonymity against the Adaptive Chosen Ciphertext Attack", 2006 年 暗号と情報セキュリティシンポジウム (SCIS2006), 1F3-1, 2006 年 1 月.
概要: Bellare, Boldyreva, Desai, and Pointcheval proposed a new security requirement of encryption schemes called "key-privacy" or "anonymity." It asks that an encryption scheme provides privacy of the key under which the encryption was performed. That is, if an encryption scheme provides the key-privacy, then the receiver is anonymous from the point of view of the adversary. They formalized the property of anonymity, and this can be considered under either the chosen plaintext attack or the adaptive chosen ciphertext attack, yielding two notions of security, IK-CPA and IK-CCA. In this paper, we propose the notion of plaintext awareness in the two-key setting, called PA2. We say that the public-key encryption scheme is secure in the sense of PA2 if the scheme is secure in the sense of IK-CPA and there exists a knowledge extractor for PA2. There are some differences between the definition of knowledge extractor for PA and that for PA2. We also prove that if a public-key encryption scheme is secure in the sense of PA2, then it is also secure in the sense of IK-CCA. Since it looks much easier to prove that a public-key encryption scheme is secure in the sense of PA2 than to prove directly it is secure in the sense of IK-CCA, the notion of PA2 is useful to prove the anonymity property of public-key encryption schemes. We also propose the first generic conversion for the anonymity, that is, we prove that the Fujisaki- Okamoto conversion, where basic public-key encryption scheme is secure in the sense of IK-CPA, is secure in the sense of IK-CCA in the random oracle model.

10. 林良太郎, 田中圭介:
"Universally Anonymizable Public-Key Encryption", 2006 年 暗号と情報セキュリティシンポジウム (SCIS2006), 1F3-2, 2006 年 1 月.
概要: We first propose the notion of universally anonymizable public-key encryption. Suppose that we have the encrypted data made with the same security parameter, and that these data do not satisfy the anonymity property. Consider the situation that we would like to transform these encrypted data to those with the anonymity property without decrypting these encrypted data. In this paper, in order to formalize this situation, we propose a new property for public-key encryption called universal anonymizability. If we use a universally anonymizable public-key encryption scheme, not only the person who made the ciphertexts, but also anyone can anonymize the encrypted data without using the corresponding secret key. We then propose universally anonymizable public-key encryption schemes based on the ElGamal encryption scheme, the Cramer-Shoup encryption scheme, and RSA-OAEP, and prove their security.

11. 金内志津, 田中圭介:
"Signcryption with Batch Verification", 2006 年 暗号と情報セキュリティシンポジウム (SCIS2006), 2A3-4, 2006 年 1 月.
概要: Signcryption is a public-key cryp-

tographic method that performs encryption and signature in a single logical step. It is more efficient than running the sign algorithm and the encryption algorithm separately. In this paper, we propose the signcryption with batch verification. Using batch verification in the de-signcryption algorithm of the signcryption, we improve the efficiency of the verification of the plural signcrypted messages. We also give the proofs of the security property: the chosen ciphertext security against insider attack, the unforgeability against chosen-message attack, and the ciphertext anonymity.

12. 草川恵太，河内亮周，田中圭介:
"Multi-Bit Cryptosystems based on Lattice Problems", 2006 年 暗号と情報セキュリティシンポジウム (SCIS2006), 2A4-4, 2006 年 1 月.
概要: We propose multi-bit versions of several single-bit cryptosystems based on lattice problems, Ajtai and Dwork Cryptosystem [STOC '97] and its error-free version (Goldreich, Goldwasser, and Halevi [CRYPTO '97]), Regev Cryptosystems [STOC 2003] and [STOC 2005], and Ajtai Cryptosystem [STOC 2005]. By analyzing trade-offs between hardness of their underlying lattice problems and probability of decryption errors, it is shown that our cryptosystems encrypt $O(\log n)$-bit plaintexts into ciphertexts of the same length as the original ones with reasonable sacrifices of the hardness of the underlying lattice problems.

13. 八代正俊，田中圭介:
"Analysis of the Waseda-Soshi-Miyaji scheme and on Quantum Computation Signature", 2006 年 暗号と情報セキュリティシンポジウム (SCIS2006), 3C2-1, 2006 年 1 月.
概要: Several knapsack-based public-key encryption schemes were proposed, however the knapsack-based signature schemes are few. Shamir scheme is based on linear transformation. This scheme is broken without the quantum computer. Okamoto, Tanaka and Uchiyama proposed the definition of a quantum computation digital signature scheme. Waseda, Soshi and Miyaji proposed a knapsack-based quantum computation digital signature scheme based on the OTU. Their scheme is based on the signed knapsack problem. In this paper, we analyse the Waseda-Soshi-Miyaji scheme, they claimed that there scheme is secure. In fact, the forger can determine the signer's private key. Therefore we discuss on the possibillity of the construction for quantum computation digital signature scheme based on the knapsak problems.

14. 大山千尋，田中圭介:
"Universal Designated-Verifier Ring Signature", 2006 年 暗号と情報セキュリティシンポジウム (SCIS2006), 3A3-2, 2006 年 1 月.
概要: In this paper, we propose new variant of ring signature called universal designatedverifier ring signature (UDVRS). Like universal designated-verifier signature (UDVS), UDVRS has special functionality that allows any holder of a ring signature, who is not necessarily the signer, to designate the signature to any desired designated-verifier, using the verifier's public key. Only the designated-verifier can verify the signature and be convinced that the signature was signed by one of the ring members: he cannot transfer any conviction to the third party. The purpose of our UDVRS scheme is to allow only a specified entity to verify the ring signature, which keeps the signature from being used beyond the signer's aim.

15. 羽田大樹，田中圭介:
"A Password-Based Authenticated Key Ex-

change Protocol in the Three Party Setting", 2006 年 暗号と情報セキュリティシンポジウム (SCIS2006), 3D3-2, 2006 年 1 月.
概要: In this paper, we continue the study of password-based authenticated key exchange in the three-party setting. Abdalla, Fouque, and Pointcheval contributed the model in the three-party and a generic construction of the protocol. Their protocol is very generic and natural, but assumes twoparty password-based authenticated key exchange, three-party key distribution, message authentication code (MAC), and the decisional Diffie-Hellman problem. Moreover it needs many rounds. We present a specific protocol in their setting which needs only four rounds, and assume the decisional Diffie-Hellman problem in the random oracle model.

16. 樋渡玄良，田中圭介:
"Fair Exchange of Signatures in the Many-to-One Model", 2006 年 暗号と情報セキュリティシンポジウム (SCIS2006), 3A4-4, 2006 年 1 月.
概要: In 2004, Chen, Kudla, and Paterson introduced the concept of concurrent signature. The concurrent signature scheme falls just short of providing a full solution to the problem of fair exchange of signatures, however their schemes require neither a trusted third party nor a high degree of interaction between parties, so this is useful in some situations. They also proposed a protocol only for the one-to-one model. We extend this scheme to the many-to-one model. Consider the situation that a single party A wants to get the all signatures of three parties, B, C, and D, participated in the protocol, while these parties want to get only the signature of the party A. We propose a security model for the concurrent signature scheme applied to the many-to-one model. We also propose a concrete scheme which is secure. By putting an assumption that one party is honest-but-curious, we prove the security in the random permutation model under the discrete logarithm assumption. Our proposed scheme can be applied to the above situation.

17. 鈴木学，一色寿幸，田中圭介:
"Sanitizable Signature with Secret Information", 2006 年 暗号と情報セキュリティシンポジウム (SCIS2006), 4A1-2, 2006 年 1 月.
概要: A sanitizable signature scheme is a signature scheme that allows the sanitizer to sanitize certain portions of the document and to generate the valid signature of the resulting document with no interaction with the signer. There exist many models and schemes for sanitizable signature. In this paper, we precisely formalize the algorithms and the security requirements of sanitizable signature with secret information. We propose a sanitizable signature scheme based on the gap co-Diffie-Hellman groups and prove that our scheme satisfies these security requirements. Furthermore, we discuss various models of sanitizable signature and classify the previously proposed schemes and our scheme.

18. 山下直之，田中圭介:
"Secret Handshake with Multiple Groups", 2006 年 暗号と情報セキュリティシンポジウム (SCIS2006), 4D2-3, 2006 年 1 月.
概要: Recently, a privacy-preserving authentication model called secret handshake was introduced by Balfanz, Durfee, Shankar, Smetters, Staddon, and Wong. It allows two members of a same group to authenticate each other whether they belong to a same group or not secretly, in the sense that each party reveals his affiliation to the other only if the other party is also a group member. Xu and Young constructed the first scheme that achieved this property. Previous works focus on the models which each participant authenticates him-

self as a member of one group. In our study, we present a new secret handshake model. In our model, two users authenticate each other if and only if each one's memberships of the groups are equal. In this paper, we present a definition of this model. We call this model secret handshake with multiple groups and produce a concrete scheme. Furthermore, our scheme can deal with one's change of memberships. Even if a member is added to a new group, or is deleted from the one that he belongs to, there is no need to change his other memberships. Our scheme does not satisfy the unlinkability, but that can be achieved by modifying our scheme.

19. S. Toda:
"Computing Automorphism Groups of Chordal Graphs Whose Simplicial Components Are Of Small Size", IEICE Technical Report, Vol. 105, No.144, COMP2005-24, 37–42, June, 2005.
概要: It is known that any chordal graph can be uniquely decomposed into simplicial components. Based on this fact, it is shown that for a given chordal graph, its automorphism group can be computed in $O((c! \cdot n)^{O(1)})$ time, where c denotes the maximum size of simplicial components and n denotes the number of nodes. It is also shown that isomorphism of those chordal graphs can be decided within the same time bound. From the viewpoint of polynomial-time computability, our result strictly strengthens the previous ones respecting the clique number.

20. M. Yamamoto:
"An improved $\widetilde{\mathcal{O}}(1.234^m)$-time deterministic algorithm for SAT", 電子情報通信学会 コンピュテーション研究会, 信学技報, Vol. 105, No. 499, COMP2005-54, 37–42, December, 2005.
概要: SAT 問題に対して，最悪時時間計算量の改善を行った．具体的には，まず，3SAT 問題に対し，これまでの変数数 n に対する最悪時計算時間 $O(1.333^n)$ の乱択アルゴリズムに対し，最悪時計算時間が $O(1.330^n)$ のアルゴリズムを設計した．一方，一般の SAT 問題に対しては，決定性アルゴリズムを考え，これまでの最悪時計算時間 $O(^m)$ のアルゴリズム（ただし m は論理式の節数）に対し，$O(1.234^m)$ のアルゴリズムを提案した．

21. 渡辺治，山本真基:
"A message passing algorithm for MAX2SAT", 電子情報通信学会全国大会, COMP-NHC 学生シンポジウム, DS-1-6, March, 2006.
概要: MAX-SAT 問題の難しさの平均的な解析をする際，問題例の分布に対する確率モデルが必要である．これまで，そのような確率モデルとして妥当なものがなかったが，我々は，MAX-2SAT 問題に対して，まず，テスト例題生成，という観点から問題例生成の手法を提案した．さらに，それを単純化して，MAX-2SAT 問題の問題例に対する自然な確率分布を提案することができた．さらに，上記の分布のもとでの MAX-2SAT 問題の難しさの解析を目的とし，我々は，その分布に対して比較的よい性能を持ち，線形時間のアルゴリズムを考案した．これは，人工知能の研究で開発された「信念伝播法」という手法にヒントを得て，それを非常に単純化したアルゴリズムである．このアルゴリズムが，上記の分布の元で，MAX-2SAT 問題を高い確率で解くことを証明した．

B03: 量子論理回路の最適化に関する研究

西野 哲朗　垂井 淳　太田 和夫　國廣 昇

電気通信大学 電気通信学部 情報通信工学科
〒 182-8585 東京都調布市調布ケ丘 1-5-1
{nishino,tarui,ota,kunihiro}@ice.uec.ac.jp

1　はじめに

回路計算量理論は，情報理論の創始者として有名な，C. Shannon の 1949 年の論文から始まったと考えられている．一般に，ある関数を計算する回路としては，種々のものが考えられるが，Shannon は，関数 f を計算する最小回路のサイズによって，その関数 f の複雑さを測ることを提案した．

当時の Shannon の動機は，回路を実現するのに必要な素子数を最小化することであったらしい．彼は，すべての n 入力関数の複雑さに関する上界を証明し，さらにほとんどの関数について，この上界が下界とあまり違わないことを**数え上げ論法**を用いて示した．

回路は，計算能力に関して Turing 機械と密接な関係を持っており，回路サイズに関する十分大きな下界は時間計算量に関する下界をただちに与える．回路モデルは，計算モデルのなかでも特に定義が単純なので，組合せ論的解析をより簡単に行なえる．しかし，現在我々は一般の回路サイズに関しては，非常に弱い下界しか示すことができない．

この回路計算量理論は 1980 年代に，**P = NP ? 問題** [9] に対する有望なアプローチとして注目を集めた [8, 11]. P = NP ? 問題に対する 1 つのアプローチは，計算モデルの能力に制限を加え，可能なアルゴリズムのクラスを制限して議論を行うことであった．実際，このアプローチにより，いくつかの興味深い結果が証明された．しかし，これらの結果に基づいて，より一般的な計算モデルに対する強い下界を導くことはできていない．

一方, Razborov と Rudich は論文 [16] のなかで，**Natural Proof** という概念を導入し，以下のことを示した．非一様ブール計算量についてすでに知られている証明手法を用いた，非単調回路モデルに対する下界の証明はすべて，natural であるか，または natural に表現できる．さらに彼らは，ある妥当な仮定のもとで, 一般回路に対する超多項式下界を証明する natural proof は存在しないことを示した．つまり, P = NP ? 問題の解決に向けては, 新たな証明法を開発しなければならないという状況証拠が示されたのだ．

そこで, 本年度の研究では, 回路計算量の下界を導出するための natural ではない証明手法として, Nielsen によって提案された, 量子論理回路サイズの下界を求めるための幾何学的手法 [13] に着目し研究を進めた．本報告では, 筆者らによる量子論理回路の深さ最小化に関する結果 [12] と, この Nielsen の結果を組み合わせることで得られた新たな知見について報告する．

2　Natural Proof

1994 年カナダのモントリオールで開催された，The 26th ACM Symposium on Theory of Computing (STOC'94) において，A. A. Razborov と S. Rudich による "Natural Proofs" という論文 [16] が発表された．本節では，その内容の概略を紹介する．

多くの人々が，P = NP ? 問題を解くことは非常に難しそうだと感じている．そのことを数学的に示すことはできないであろうか？そのためのひとつの方法は，現在知られている証明手法が，P = NP ? 問題を解決するのには弱過ぎることを示すことである．この方針に従った最初の結果を示したのは，Baker, Gill と Solovay [2] であった．彼らは，相対化可能な証明手法では，P = NP ? 問題は解決できないことを示した．相対化可能な証明手法には，対角線論法やシミュレーションと

いった当時知られていた主要な証明方法が含まれていたため，研究者は路線変更を余儀なくされた．

そこで多くの研究者が回路計算量の研究を始めた．そして，1980 年代に入ると，前節で述べたように，非常に多くの相対化不可能な証明手法が発見され，それらの手法を用いて強い下界が示された．これらの手法では組み合わせ論が巧妙に用いられている．

Razborov と Rudich は [16] のなかで，**Natural Proof** という概念を導入し，以下のことを示した．非一様ブール計算量についてすでに知られている証明手法を用いた，非単調回路モデルに対する下界の証明はすべて natural であるか，または natural に表現できる．さらに彼らは，暗号を破ることの難しさ（f の値は容易に計算できるが，f^{-1} の値の計算が非常に難しいような，一方向性関数 f の存在）を仮定すれば，一般回路に対する超多項式下界を証明する natural proof は存在しないことを示した．

ある特定の関数 $\{g_n\}$ が多項式サイズの回路を持たないという証明は，通常，以下のように展開される．

(1) ブール関数についてのある性質 C_n を提示する．

(2) 任意の $f_n \in C_n$ に対し，f_n を計算する回路のサイズが n に関する超多項式である（すなわち $\{f_n\} \notin P/poly$ である）ことを証明する．言い換えれば，性質 C_n を持つすべてのブール関数は計算することが難しいことを示す．以下では，このような性質 C_n を useful と呼ぶことにする．

(3) 最後に，g_n が性質 C_n を持つことを示し，これにより，$\{g_n\} \notin P/poly$ が導かれる．もし，関数 $\{g_n\}$ が NP に属していれば，以上は P $\neq$ NP の証明になっている．

ここで，$P/poly$ とは，入力の長さごとに一意に定まる，アドバイス列と呼ばれる記号列（ただし，入力サイズに関する多項式長とする）が与えられれば，多項式サイズの回路で認識できるような言語のクラスである．言語 L が $P/poly$ に属する必要十分条件は，$f_n^{-1}(1) = L \cap \{0,1\}^n$ により定義される関数 f_n が，n に関する多項式サイズの回路で計算できることであることが知られている．

以上のことを形式的に述べるために，いくつかの概念を導入する．ブール関数の**組み合わせ論的性質**とは，ブール関数の集合 $\{C_n \subseteq F_n \mid n \in \omega\}$ のことをいう．組み合わせ論的性質 C_n が**自然**（natural）であるとは，それが，次の条件 1, 2 を満たす部分集合 C_n^* を含むときをいう．また，組み合わせ論的性質 C_n は，条件 3 を満たすとき，$P/poly$ に対して **useful** であるという．

1. (Constructivity) 述語 $f_n \in C_n^*$ が P に属する．すなわち，C_n^* は f_n の真理値表の長さ（2^n）に関する多項式時間で計算可能である．
2. (Largeness) $|C_n^*| \geq 2^{-O(n)} \cdot |F_n|$
3. (Usefulness) 任意の関数の列 $f_1, f_2, \ldots, f_n, \ldots$（ただし $f_n \in C_n$）の回路サイズは，超多項式，すなわち $\{f_n\} \notin P/poly$ である．

ある関数が多項式サイズ回路を持たないという証明は，それが，$P/poly$ に対して useful で，かつ自然な組み合わせ論的性質 C_n の定義を明確に含んでいるとき，$P/poly$ **に対して自然** (natural against $P/poly$) であるという．

上で述べた形の証明が，$P/poly$ に対して natural になるためには，証明で使われる性質 C_n それ自身が natural でなければならない．すなわち，C_n は上の条件 1, 2 を満足する部分集合 C_n^* を含まなければならない．条件 2 は，n 変数ブール関数の全体 F_n のうちの，少なくとも（2^n に関する）多項式分の 1 の個数の関数について，C_n^* が真であることを述べている．また，条件 1 は，$f_n \in C_n^*$ の真偽が，Turing 機械によって関数 f_n の真理表の長さ（すなわち 2^n）に関する多項式時間で決定できることを要求している．

制限された非単調回路モデルに対する下界の証明で，現在までに知られているものはすべて，上で述べたように行われていることがわかる．実際，Razborov と Rudich は，Furst, Saxe と Sipser による $PARITY \notin AC_0$ の証明などがすべて natural である（あるいは natural proof に書き直すことができる）ことを示した．

一方，単調回路モデルに対する下界の証明においては，constructive な組み合わせ論的性質は用

いられているが，largeness 条件に対する形式的なアナロジーは存在しない.（特に，random 単調関数の useful な定義は明かではない.）しかし，単調回路計算量の指数下界を示す際に Razborov が用いた近似法は，一般回路に適用してもほとんど効果を発揮しないことが，Razborov 自身によってすでに示されている [15].

Razborov と Rudich は，Natural Proof が，下界の証明においてある意味の限界を持っていることを示した．その基本的アイディアは以下の通りである．まず，SAT $\notin P/Poly$ の natural proof が存在したとすると，その proof に対応したある種のアルゴリズムが存在する．その proof は SAT と pseudo-random function を区別しなければならないから，その proof に対応したアルゴリズムもそれらを区別できなければならない．したがって，そのアルゴリズムは pseudo-random generator を破るのに用いることができる．

以上のことを，もう少し形式的に述べてみよう．pseudo-random generator $G_n : \{0,1\}^n \to \{0,1\}^{2n}$ の hardness $H(G_n)$ とは，以下の条件を満足する S の最小値である．

サイズ S 以下の回路 C のなかに，次の関係式を満たすものが存在する：

$$| \mathbf{Pr}[C(G_n(\mathbf{x})) = 1] - \mathbf{Pr}[C(\mathbf{y}) = 1] | \geq \frac{1}{S}$$

ただし，通常のように，$\mathbf{x}$ は $\{0,1\}^n$ からランダムに選ばれ，また，$\mathbf{y}$ は $\{0,1\}^{2n}$ からランダムに選ばれるものとする．

上の定義の意味を考えてみる．$H(G_n)$ の定義から，サイズが $S < H(G_n)$ であるすべての回路 C に対し，次の関係式が成り立つ：

$$| \mathbf{Pr}[C(G_n(\mathbf{x})) = 1] - \mathbf{Pr}[C(\mathbf{y}) = 1] | < \frac{1}{S}$$

この関係式の右辺は，n が限りなく大きくなるとき 0 に限りなく近づく．したがって，この関係式は,（漸近的には）サイズ S の回路 C には G_n が生成した pseudo-random 列 $\mathbf{y}$ と，真に random な列 $\mathbf{x}$ との区別がつかなくなることを示している．つまり，$\mathbf{y}$ の pseudo random 性の判定は，サイズ $S < H(G_n)$ の回路には，難し過ぎて行えないことを示している．Razborov と Rudich は以下の定理を示した.

定理 2.1 (Razborov & Rudich) *$P/poly$ に対して $P/poly$-natural な下界の証明が存在したとする．このとき，すべての多項式時間計算可能な $G_n : \{0,1\}^k \to \{0,1\}^{2k}$ に対し，以下が成り立つ.*

$$H(G_k) \leq 2^{k^{o(1)}}$$

言い換えれば，もし 2^{n^ε}-hard 関数が存在すれば，$P/poly$ に対する $P/poly$-natural な証明は存在しない. ■

P = NP ? 問題の解決には，従来の証明手法はおそらく適用できず，また，この問題を解くことは暗号を解くのと同じくらい難しいであろうということは，従来から多くの研究者が抱いてきた直観ではないだろうか？Razborov と Rudich の結果は，まさにそれらのことを数学的に正確に述べている．STOC'94 での講演のなかで，Rudich は次のように述べた.「Baker, Gill と Solovay の仕事によって，ある種の手法は P $\neq$ NP を証明するには弱過ぎることがわかった．そして我々の今回の結果によって，それ以後開発された手法が P $\neq$ NP を証明するには強過ぎることがわかった．今後，我々が進むべき道は，それらの中間に位置する強さの証明手法を開発することである.」

そのような natural ではない中間的強さの証明手法を, どのようにして発見するのかについては, 未だ明確な指針が得られているわけではないが, 筆者は, 量子論理回路サイズの下界を証明するための幾何学的アプローチが有望ではないかと考えている．そこで, 以下では, その幾何学的アプローチについて紹介していくことにする.

3 量子論理回路

1985 年に，英国人物理学者 David Deutsch は，**量子 Turing 機械**（quantum Turing machine, 以下 QTM と略す）という量子力学的動作原理に基づく新たな計算モデルを提案した [4, 6, 14]．この QTM に基づくコンピュータが，**量子コンピュータ**と呼ばれている.

通常のコンピュータのメモリの一区画には，0 または 1 が保持できるが，QTM のメモリの一区画には，0 と 1 の任意の重ね合わせ状態が保持できる．ここで，重ね合わせ状態とは，0 に対応す

る状態ベクトル $|0\rangle$ と 1 に対応する状態ベクトル $|1\rangle$ を，それぞれ，

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

とするとき，$\alpha|0\rangle + \beta|1\rangle$ の形で表されるベクトルの和のことをいう．ただし，α と β は，条件式 $|\alpha|^2 + |\beta|^2 = 1$ を満たす任意の複素数であり，振幅と呼ばれる．この重ね合わせ状態を観測すると，0（または 1）が確率 $|\alpha|^2$（$|\beta|^2$）で読めるものと仮定する．

QTM のテープの一区画が保持できる情報量を **1 量子ビット**（quantum bit, qubit）という．QTM の動作は，量子ビットに対するユニタリ変換と呼ばれる線形変換の適用という形で表現できる．一方，QTM 上で実行されるアルゴリズムを量子アルゴリズムと呼ぶ．そこで以下では，量子アルゴリズムを量子ビットに適用されるユニタリ変換の系列として記述することにする．

1994 年に，AT & T の Peter Shor は，整数の因数分解を小さな誤り確率で高速に行う量子アルゴリズムの設計に成功し，世界的な注目を集めた．というのは，現在広く用いられている RSA などの公開鍵暗号が，因数分解問題の難しさを前提として設計されているからである．この Shor の結果に影響されて，量子コンピュータの物理的実現に関する研究が現在盛んに行われている．

通常の組み合わせ論理回路のアナロジーとして，Deutsch によって導入されたのが，量子論理回路である．一般に電気回路は，多数の**論理ゲート**から構成されている．通常のコンピュータを実現するのに用いられている論理ゲートとしては，AND, OR, NOT ゲートなどがある．例えば，AND と NOT，または OR と NOT の 2 種類のゲートを用いれば，任意の Turing 機械の計算を模倣する回路を構成することができる．

一方，量子計算は量子ビットに適用されるユニタリ変換の系列で表現される．Deutsch [7] や Yao [17] らの研究によって，QTM の動作は**量子回路**で模倣できることがわかっている．最近，量子回路を実現するための量子論理ゲートについて盛んに研究が行われているが，現在までに，例えば以下のような量子論理ゲートが考案されている．なお，量子論理ゲートの各入出力は，1 つの量子ビットに対応している．

制御 NOT ゲート ... このゲートは 2 入力 2 出力である．最も単純な場合について説明すると，制御 NOT ゲートにおいては，入力の第一ビット x_1 の値が 0 ならば，入力の第 2 ビット x_2 の値がそのまま出力の第 2 ビット y_2 の値となるが，x_1 の値が 1 ならば，x_2 の値が反転された値が y_2 の値となる．すなわち，$x_1 = 1$ のときには，x_2 の否定が y_2 に代入される．なお，いずれの場合においても，$y_1 = x_1$ である．制御 NOT ゲートは，以下のような 4 次の正方行列で表現される，2 量子ビットに対するユニタリ変換を実行する．

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

ここで，この行列の各行各列は，それぞれ順に，$|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ という状態に対応している．例えば，上の行列の第 3 行は $|10\rangle$ という状態に対応し，第 4 列は $|11\rangle$ という状態に対応するが，その第 3 行第 4 列成分が 1 であることは，以下のことを表している．制御 NOT ゲートへの入力が $x_1 = 1, x_2 = 0$ である場合には，その出力は $y_1 = 1, y_2 = 1$ となる．

ユニタリ変換ゲート ... このゲートは 1 入力 1 出力であり，入力に対して指定されたユニタリ変換 U を行う．ただし，このユニタリ変換 U は，行列式が 1 であるような，2 行 2 列のユニタリ行列で表現されるものである．ユニタリ変換ゲートの具体例としては，以下に示す Hadamard ゲート H を参照されたい．

通常の組み合わせ論理回路 [8] の量子アナロジーとして，Deutsch によって導入されたのが，**量子回路**である [7]．これは，フィードバックを持たない古典的回路の量子版である．量子回路を定義するために，ある基本ゲートの集合が **基底**として選ばれるが，ここでの各基本ゲートは，$2^k \times 2^k$ ユニタリ行列によって規定される k-入力 k-出力素子である．

以下では $h = 2^k$ とし，$\mathbf{C}^h$ で h-組の複素数をから構成されるベクトル空間を表す．$u, v \in \mathbf{C}^h$ に対し，**内積**を $< u, v >= \sum_{1 \le i \le h} u_i^* v_i$ により

定義し，ベクトル u の**長さ**を $(< u, u >)^{1/2}$ で定義する．また，$< u, v >= 0$ が成り立つとき，u と v は**直交する**という．ただひとつの成分のみが 1 で，その他のすべての成分が 0 であるような自然な単位ベクトルは，全部で h 個存在するが，それらは $\{0,1\}^k$ 内の要素と同一視できる．$2^k \times 2^k$ ユニタリ行列 U は，ベクトル $u \in \mathbf{C}^h$ を別のベクトル $u' \in \mathbf{C}^h$ に次のような方法で変換する：入力 $u = \sum_{x\in\{0,1\}^k} c_x x$ に対し，出力は $u' = \sum_{x\in\{0,1\}^k} c_x U_{x,y} y$ によって与えられる．ただし，x と y は $\mathbf{C}^h$ 内の単位ベクトルである．定義より，ユニタリ行列は，互いに直交する単位ベクトルの集合を，互いに直交する単位ベクトルの別の集合に変換することに注意せよ．

量子回路は，通常のブール回路と同様に，基本ゲートを適当な遅延時間を伴ってワイヤで結合することにより構成される．量子回路は，何本かの入力ワイヤと出力ワイヤを持つ．何本かの入力ワイヤには，繰り返しを許して変数の集合 $x_1, x_2, \cdots, x_n$ が対応し，残りの入力ワイヤには定数 0 と 1 が対応する．一方，出力ワイヤの何本かを，特定の時刻に測定される出力変数 $y_1, y_2, \cdots, y_m$ に対応させる．すべての m-入力 m-出力量子ゲートの集合を B_m で表す．

Deutsch は，$n \geq 3$ の場合に，n 個のブール変数により定義される $\mathbf{C}^{2^n}$ のすべてのユニタリ変換は，B_3 を基底とする量子回路によって計算できることを示した [7]．回路からフィードバック・ループを無くすには，最初，定数 0 または 1 に設定されており，出力時にはその同じ定数値に戻されているような，補助ワイヤを追加すればよいことが知られている．

通常のブール回路においては，AND, OR, NOT の 3 種類のゲートがあれば（実際は AND と NOT，または OR と NOT の 2 種類で十分），任意のブール関数を計算する回路を構成することができる．このような性質があるため，ゲートの集合 { AND, OR, NOT } は**万能基底**と呼ばれる．量子回路に対しては，次のような万能基底が知られている [5].

無限基底 ...　制御 NOT ゲートと，すべての 1 量子ビットユニタリ変換ゲートから成るゲートの**無限集合** G_U は万能基底である．任意の k 量子ビット ユニタリ作用素を，G_U に属する $O(4^k k)$ 個のゲートを用いて正確に模倣できることが知られている [5]．したがって，G_U から，局所的ユニタリ変換ゲートから成る別の万能基底（3 量子ビット ゲート全体の集合など）に切り替えても，対応する回路サイズは定数倍にしか増加しない．

有限基底 ...　任意の 2 量子ビット ゲートは，Hadamard ゲート

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

と，2 量子ビット ゲートである制御 V ゲート，ただし，

$$V = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

を，合計で $O(\log^c(1/\varepsilon))$ (c : 定数) 個用いて，与えられた近似率 ε 以内で近似できることが知られている．したがって，これら 2 つのゲートを含む集合は，任意のゲートを近似できるという意味において万能基底である．

入力が $x_1, x_2, \ldots, x_n$, 出力が $y_1, y_2, \ldots, y_m$ である量子回路 K は, 各入力 $x \in \{0,1\}^n$ に対し, $\{0,1\}^m$ 上の確率分布 p_x を対応させる．n 入力量子回路 K が QTM M を (n,t)-**模倣する**とは, K によって生成される確率分布 p_x の族が, 入力 x に対する t ステップの M の様相の確率分布と等しいときをいう．ただし, M の様相とは, テープセル $-t$ から t までに含まれるテープ記号のリストと, 状態およびヘッド位置を 2 進列として符号化したものとする．

定理 3.1 (Yao) *M を QTM とし, n, t を正整数とする．このとき, M を (n,t)-模倣するような, サイズ $poly(n,t)$ の量子回路 K が存在する．*

定理 3.2 (Yao) *$L \in P$ ならば, L_n を受理する量子回路の最小サイズは $O(n^k)$ である．ただし, L_n は L に属する長さ n の記号列の集合とする．* ■

L_n に対する量子回路サイズの超多項式下界が得られれば，この定理 3.2 からただちに，$L \notin P$ が導かれる．このことは，量子回路計算量からの P = NP ? 問題に対する新たなアプローチの可能性を示唆している．

4 量子論理回路の深さ最小化

n 変数論理関数 $f:\{0,1\}^n \to \{0,1\}$ の値は, 演算の可逆性のために直接的には量子回路上では計算できない. しかし,

$$U_{f\text{-C-NOT}}|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle \qquad (2.15)$$

で定義される ***f*-C-NOT 回路**(f-Controlled-NOT 回路) で実質的に計算することができる. [10]

定義 1 (量子論理回路) 本稿では, これ以降, この $U_{f\text{-}C\text{-}NOT}$ を計算する回路 *(f-C-NOT 回路)* のことを**量子論理回路**と呼ぶことにする.

この作用素の入力は,

$$|x\rangle = |x_1\rangle|x_2\rangle|x_3\rangle\cdots|x_n\rangle \qquad (2.16)$$

の形で n 量子ビットで構成される制御レジスタ x で保持される. そして出力は 1 量子ビットから成るレジスタ y を通して与えられる.

式 (2.15) における f-C-NOT 回路は, 最小項に対応するユニタリ変換である**最小項ゲート**で簡単に構成されうる. どの最小項ゲート M_y^x も

$$M_y^x \equiv \left(\prod N_{x_i}\right) T_y^x \left(\prod N_{x_i}\right) \qquad (2.17)$$

のように NOT ゲートで挟まれた 1 つの $(n+1)$ ビット Toffoli ゲートによって実現されうる. ここで N_{x_i} と T_y^x は, それぞれ, 制御レジスタの第 i 量子ビットの状態だけを反転する NOT ゲートと, n 個の制御ビット x と 1 個のターゲットビット y を持つ $(n+1)$ ビット Toffoli ゲートを表す. その積 ($\prod$) は, 0 を持つような x のすべてのビットに関するものである. どの最小項ゲートも, 入力の 1 つの状態だけに対して動作する. また, 最小項ゲートの積の順序は, 可換である.

そして, f-C-NOT 回路は,

$$U_{f\text{-C-NOT}} = \prod M_y^x \qquad (2.18)$$

のように, その最小項ゲートすべての積で得られる. ここで, この積は, $f(x)=1$ を満たす x に関するものである. 筆者らは, 以下の定理を示した。

定理 4.1 (Nakui et al.) 最小項ゲートの乗算は, 対応する論理表現においては, その最小項の排他的論理和 *(EXOR)* で表すことができる.

証明 最小項ゲートの定義, あるいは, Toffoli ゲートの定義から容易に示すことができる.

Toffoli ゲート T_y^x は, 次のように定義される.

$$\begin{aligned}&\forall x_1,\ldots,x_n,y \in \{0,1\},\\ &T_y^x|x_1,\ldots,x_n,y\rangle\\ &\equiv \begin{cases}|x_1,\ldots,x_n\rangle \otimes N|y\rangle, & \text{if} \quad x_1\wedge\cdots\wedge x_n = 1\\ |x_1,\ldots,x_n,y\rangle, & \text{if} \quad x_1\wedge\cdots\wedge x_n = 0\end{cases}\end{aligned} \qquad (2.19)$$

ここで, $a\wedge b$ は a,b の論理積を表し, $N=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$ である. これは, また,

$$\begin{aligned}&\forall x_1,\ldots,x_n,y \in \{0,1\},\\ &T_y^x|x_1,\cdots,x_n\rangle|y\rangle\\ &= |x_1,\ldots,x_n\rangle|y \oplus (x_1\wedge\cdots\wedge x_n)\rangle\end{aligned} \qquad (2.20)$$

と書くことができる. すなわち, これは, 作用前のターゲットビットの状態 y に論理積 $x_1\wedge\cdots\wedge x_n$ が EXOR で足しこまれることを意味する.

最小項ゲートの定義から, 最小項ゲートは, Toffoli ゲートにおける N が有効になる制御ビットの状態を (NOT ゲートを用いて) 最小項表現に一致するように変えただけである. したがって, 最小項ゲートを作用させるということは, 作用前のターゲットビットの状態にその最小項が EXOR で足し込まれることを意味する. ■

定義 2 (積項ゲート) 各変数に対して高々*1* つのリテラル *($x,\bar{x}$)* を論理積で結合した式を**積項**と呼ぶことにする. *Toffoli* ゲートを *NOT* ゲートで挟み, この積項に対応する状態で制御されるようにしたゲートを**積項ゲート**と呼ぶことにする.

また, この積項ゲートについても次のことがいえる.

定理 4.2 (Nakui et al.) 積項ゲートの乗算は, 対応する論理表現においては, その積項の排他的論理和 *(EXOR)* で表すことができる. ■

文献 [10] では, f-C-NOT 回路の簡単化のルールが 3 つ述べられている:

ルール 1 $m \le n$ に対して, 2 つの $(m+1)$ ビット積項ゲートの制御ビットの論理表現が, 1 つ

のビットの状態を除いて同じで, かつ, それらの 2 つのゲートが連続してあるならば, それらは, 1 つの m ビット積項ゲートによって置き換えられうる.

ルール 2 2 つの $(m+1)$ ビットの積項ゲートが連続してあり, かつ, それらの制御ビットの論理表現が 2 つのビットの状態を除いて同じならば, 1 つの m ビット積項ゲートと 2 つの C-NOT ゲートによって置き換えられうる.

ルール 3 f-C-NOT 回路に積項ゲートの偶数回のべき乗をかけても不変である.

定義 3 (ESOP) 任意の積項を排他的論理和で結合した *AND-EXOR* 論理式を ***ESOP(Exclucive-or Sum Of Product)*** と呼ぶ. また, 論理関数 f を *ESOP* で表現したときに積項数が最小になる *ESOP* を論理関数 f の **最小 *ESOP*** と呼ぶ.

以上のことから, 次の量子論理回路の深さ最小化定理が導かれる.

定理 4.3 (Nakui et al.) 論理関数 f の最小 *ESOP* は, *f-C-NOT* 回路に対する深さ最小の量子回路を与える.

証明 これまでに示した定理 4.1, 4.2, および, 積項ゲートの定義より, f-C-NOT 回路を構成する積項ゲートの数は, 論理関数 f の ESOP の積項数と一致し, ESOP から直接的に f-C-NOT 回路が構成できることがわかる.

また, 積項ゲートは, NOT ゲートで挟まれた Toffoli ゲートであるのでこれは, 高々深さ 3, すなわち, 定数オーダ深さ O(1) で構成されることになる.

したがって, f-C-NOT 回路全体の深さを浅くするためには, それの構成要素である積項ゲートの数を少なくすればよいことになる.

最小 ESOP は積項数が最小になるものであるから最小 ESOP が深さ最小の f-C-NOT 回路を与えることになる.

また, 逆に深さ最小の f-C-NOT 回路が与えられた場合, そこから, 最小 ESOP を求めることは, 容易である. ■

5 量子回路計算量の下界導出に向けて

Nielsen は, 最近の論文 [13] において, 量子計算論において特徴的な幾何学的性質を利用して, 量子論理回路のサイズの下界を求める方法論を提案し, 以下の定理を示した. なお, Nieisen が示したこの証明法は, natural proof の範疇には入らないものである.

定理 5.1 (Nielsen) G を $SU(2^n)$ 上の万能量子基底とし, F を $SU(2^n)$ 上のある条件を満たす計量とするとき, $SU(2^n)$ に属する任意の U に対して, 以下が成り立つ.

$$d_F(I,U) \leq m_G(U)$$

ただし, $d_F(I,U)$ は, F を計量とする可微分多様体上における n 量子ビット恒等変換 I と U との距離, $m_G(U)$ は, ユニタリ変換 U を実現する G を基底とする量子回路の最小サイズとする. ■

この定理と, 前節で示した定理 4.3 から, 以下の定理が導かれた.

定理 5.2 G を $SU(2^n)$ 上の万能量子基底とし, F を $SU(2^n)$ 上のある条件を満たす計量とするとき, 任意の $n-1$ 変数ブール関数に対応するユニタリ変換 U に対して, 以下が成り立つ.

$$d_F(I,U) \leq m_G(U) \leq n \cdot l_G(U) \leq n \cdot ESOP(U)$$

ただし, $l_G(U)$ は, ユニタリ変換 U を実現する G を基底とする量子回路で, 前述の条件を満たすものの最小深さとし, $ESOP(U)$ は, U に対応する $n-1$ 変数ブール関数の最小 *ESOP* の積項数とする. ■

このような結果を足がかりとして, 今後, 具体的なブール関数に対する量子回路計算量の下界を示して行くためには, 以下のような問題が, まず最初に解決されなければならない.

1. 特定のブール関数に対応する U について, $d_F(I,U)$ の強い下界を求めること. Nielsen の結果は, 一般のユニタリ変換 U に関するものなので, 通常の計算量理論で議論されて

いるようなブール関数や, 特定の NP 完全問題に対応する U についての議論を展開し, $d_F(I,U)$ に対する強い下界を導き出して行く必要がある. 当然, Nielsen の論文では, 変換 U の一様性も成立していないが, 計算量理論を展開するためには, 変換 U の一様性についても考慮しなければならない.

2. 補助量子ビットが, 量子回路計算量に及ぼす影響を明らかにすること. Nielsen の論文では, 補助量子ビットの存在は仮定しない枠組みで, 結果が導かれている. しかし, 具体的な計算を行う通常の量子論理回路の設計においては, 補助量子ビットは頻繁に用いられるので, 補助量子ビットの存在が, 量子回路計算量の下界の導出にどのような影響を与えるのかを明らかにして行く必要がある. ちなみに, 前節で示した筆者らの結果においては, 補助量子ビットを用いない量子論理回路を取り扱っている.

以上のような問題を解決して行くことで, 量子論理回路を用いた回路計算量の下界導出に関する研究を推進していく計画である.

参考文献

[1] K. Amano, and A. Maruoka, "Potential of the approximation method", In *Proceedings of the 37th Annual Symposium on Foundations of Computer Science*, pp.431-440, 1996.

[2] T. P. Baker, J. Gill, and R. Solovay, "Relativizations of the P = NP question", *SIAM Journal on Computing*, Vol. 4, pp.431-442 (1975).

[3] R. Beals, T. Nishino and K. Tanaka : "On the Complexity of Negation-limited Boolean Networks", *SIAM Journal on Computing*, Vol. 27, pp. 1334-1347 (1998).

[4] E. Bernstein and U. V. Vazirani, "Quantum Complexity Theory", *SIAM Journal on Computing*, Vol.26, No.5, pp.1411-1473, 1997. (An earlier version appeared in *Proc. 25th Annual ACM Symposium on Theory of Computing*, pp.11-20, 1993.)

[5] R. Cleve, "An Introduction to Quantum Complexity Theory", preprint quant-ph/9906111, 1999.

[6] D. Deutsch, "Quantum Theory,the Church-Turing Principle and the Universal Quantum Computer", *Proc. R. Soc. Lond.*, Vol. A 400, pp.97-117 (1985).

[7] D. Deutsch, "Quantum Computational Networks", *Proc. R. Soc. Lond.*, Vol. A 425, pp.73-90 (1989).

[8] P. E. Dunne, *The Complexity of Boolean Networks*, Academic Press (1988).

[9] M.R.Garey and D.S.Johnson: "COMPUTERS AND INTRACTABILITY A Guide to the Theory of NP-Completeness", Freeman, San Fransisco, 1979.

[10] Jae-Seung Lee, Yongwook Chung, Jaehyun Kim, and Soonchil Lee: "A Practical Method of Constructing Quantum Combinational Logic Circuits", Department of Physics, Korea Advanced Institute of Science and Technology, 1999. LANL quant-ph/9911053

[11] J. van Leeuwen (Ed.), *Handbook of Theoretical Computer Science, Vol. A, Algorithms and Complexity*, The MIT Press / Elsevier (1990) (邦訳：「コンピュータ基礎理論ハンドブック I」, 丸善, 第 14 章「有限関数の複雑さ」, by R. B. Boppana and M. Sipser, 西野哲朗訳).

[12] Yukihide Nakui, Tetsuro Nishino and Seiya Okubo: On the Minimization of the Depth of Certain Quantum Circuits, International Symposium on Energy, Informatics and Cybernetics (EIC 2005), July 10-13, Orlando, Florida, USA (2005).

[13] M. A. Nielsen, “A geometric approach to quantum circuit lower bounds”, quant-ph/0502070, Feb. 2005.

[14] 西野哲朗 :「量子コンピュータ入門」, 東京電機大学出版局, 1997.

[15] A. A. Razborov, “On the Method of Approximations”, In *Proceedings of the 21st ACM Symposium on Theory of Computing*, pp.167-176, 1989.

[16] A. A. Razborov, and S. Rudich, “Natural Proofs”, In *Proceedings of the 26th ACM Symposium on Theory of Computing*, pp.204-213, 1994.

[17] A. Yao, “Quantum Circuit Complexity”, *Proc. 34th Annual IEEE Symposium on Foundations of Computer Science*, pp.352-361, 1993.

研究業績一覧

著書

1. 太田和夫，國廣昇:
“ほんとうに安全？現代の暗号（岩波科学ライブラリー）”, 岩波書店, 2005.
概要: 今日のネット社会は暗号なしには成立しない。したがって、情報セキュリティの研究において暗号が大変重要となる。特に、公開鍵暗号と呼ばれる暗号は、見知らぬ人との通信を可能にしてくれる大変便利なものである。公開鍵暗号の多くは、素因数分解などの数学的問題の難しさを安全性の根拠としている。素因数分解は、一見簡単そうに見えるが、実は現在のコンピュータにとっては非常に難しい問題である。この素因数分解を高速に行う研究には、量子コンピュータも登場する。本書では、そのような暗号技術に関する最先端の話題を、易しく紹介して行く。まず、開発のエピソードをまじえながら、現在主流といなっている公開鍵暗号について解説する。素因数分解などの簡単な数学を用いて、暗号のしくみを実感する知的刺激に満ちた入門書である。さらに暗号解読の最新の研究も紹介しながら、暗号はどこまで安全か？量子コンピュータが実現したら暗号はどうなるのか？などの問題についても解説する。

学術論文

1. Yasuhiro Takahashi and Noboru Kunihiro : “A quantum circuit for Shor’s factoring algorithm using 2n+2 qubits”, Quantum Information and Computation, Vol.6 No.2, pp. 184–192, 2006.
概要: We construct a quantum circuit for Shor’s factoring algorithm that uses $2n + 2$ qubits, where n is the length of the number to be factored. The depth and size of the circuit are $O(n^3)$ and $O(n^3 \log n)$, respectively. The number of qubits used in the circuit is less than that in any other quantum circuit ever constructed for Shor’s factoring algorithm. Moreover, the size of the circuit is about half the size of Beauregard’s quantum circuit for Shor’s factoring algorithm, which uses $2n + 3$ qubits.

2. Yasuhiro Takahashi and Noboru Kunihiro : “A Linear-Size Quantum Circuit For Addition With No Ancillary Qubits”, Quantum Information and Computation, Vol.5 No.6, pp. 440–448, 2005.
概要: We construct a quantum circuit for addition of two n-bit binary numbers that uses no ancillary qubits. The circuit is based on the ripple-carry approach. The depth and size of the circuit are $O(n)$. This is an affirmative answer to the question of Kutin as to whether a linear-depth quantum circuit for addition can be constructed without ancillary qubits using the ripple-carry approach. We also construct quantum circuits for addition modulo 2^n, subtraction, and comparison that use no ancillary qubits by modifying the circuit for addition.

3. 大久保誠也, 西野哲朗, 太田和夫, 國廣昇:
“物理的実現可能性に優れた NMR 量子探索アルゴリズム”, 情報処理学会論文誌, Vol.46 No.06, pp. 1416–1425, 2005.
概要: 本論では，測定誤差が $\varepsilon < 1$ である NMR（Nuclear Magnetic Resonance）量子計算機（NMRQC と略記）上で動作する，新しい量子探索アルゴリズムを提案する．具体的には，解が複数個存在する探索問題に対する，新しい NMR 量子探索アルゴリズムを提案する．探索問題の解空間のサイズを N とするとき，このアルゴリズムは， $\varepsilon N + \min\{n, \log \varepsilon\}$ 回のオラクル呼び出しを行うことにより，成功確率 1 で解を発見する．通常の量子計算機上で成功確率 1 で解探索を行うためには，N 回のオラクル呼び出しが必要であることが知られているので，提案アルゴリズムの方がより高速に動作する．そして，量子オラクルを作り替えることができるような問題に対しては，提案アルゴリズムの実行において必要となる量子ビット数を節約できることを示す．さらに，提案アルゴリズムは，量子重ね合わせ状態を維持しなければならない時間が短いので，物理的実現可能性が非常に高い．

4. 大久保誠也, 西野哲朗, 太田和夫, 國廣昇:
“Bulk 量子計算モデル上における Grover のアルゴリズムの繰り返し回数について”, 情報処理学会論文誌:数理モデル化と応用, Vol.46, No.SIG 17, pp. 10–19, 2005.
概要: 本論文では，NMR 量子計算機をモデル化した，Bulk 量子計算モデル上で動作する，Grover のアルゴリズムの繰り返し回数について考察する．最初に，Bulk 量子計算モデル上で Grover のアルゴリズムを用いて論理式の充足可能性判定問題 (SAT) を解くのに必要となる繰り返し回数について議論する．次に，解がただ一つのみ存在する探索問題に対する量子アルゴリズムを提案する．また，この探索アルゴリズムの秘密鍵探索問題に対する応用についても述べる．さらに，解が複数存在する探索問題に対する量子アルゴリズムも提案する．以上の考察から，本論で提案する Bulk 量子計算モデルは，通常の量子計算モデルよりも Grover のアルゴリズムを高速に実行できる場合があることがわかる．

研究会等

1. J. Tarui:
“On the Minimum Number of Completely 3-Scrambling Permutations”, DMTCS-EuroComb05: DMTCS-Proceedigns of EuroComb05: European Conference on Combinatorics, Graph Theory and Applications (Berlin, Germanay, Sep05–09, 2005), pp. 351–356, 2005.
概要: A family $\mathcal{P} = \{\pi_1, \ldots, \pi_q\}$ of permutations of $[n] = \{1, \ldots, n\}$ is *completely k-scrambling* [Spencer, 1972; F̈uredi, 1996] if for any distinct k points $x_1, \ldots, x_k \in [n]$, permutations π_i's in $\mathcal{P}$ produce all $k!$ possible orders on $\pi_i(x_1), \ldots, \pi_i(x_k)$. Let $N^*(n, k)$ be the minimum size of such a family. This paper focuses on the case $k = 3$. By a simple explicit construction, we show the following upper bound, which we express together with the lower bound due to F̈uredi for comparison.

$$\frac{2}{\log_2 e} \log_2 n \le N^*(n, 3) \le$$

$$2 \log_2 n + (1 + o(1)) \log_2 \log_2 n.$$

We also prove the existence of $\lim_{n\to\infty} N^*(n, 3)/\log_2 n = c_3$. Determining the value c_3 and proving the existence of $\lim_{n\to\infty} N^*(n, k)/\log_2 n = c_k$ for $k \ge 4$ remain open.

2. K. Amano and J. Tarui:
“Monotone Boolean Functions with s Zeros Farthest from Threshold Functions”, DMTCS-EuroComb05: DMTCS-Proceedigns of EuroComb05: European Conference on Combinatorics, Graph Theory and Applications (Berlin, Germanay, Sep05–09, 2005), pp. 11–16, 2005.
概要: Let T_t denote the t-threshold function on the n-cube: $T_t(x) = 1$ if $|\{i : x_i =$

$1\}| \geq t$, and 0 otherwise. Define the distance between Boolean functions g and h, $d(g,h)$, to be the number of points on which g and h disagree. We consider the following extremal problem: Over a monotone Boolean function g on the n-cube with s zeros, what is the maximum of $d(g,T_t)$? We show that the following monotone function p_s maximizes the distance: For $x \in \{0,1\}^n$, $p_s(x) = 0$ if and only if $N(x) < s$, where $N(x)$ is the integer whose n-bit binary representation is x. Our result generalizes the previous work for the case $t = \lceil n/2 \rceil$ and $s = 2^{n-1}$ by Blum, Burch, and Langford [BBL98-FOCS98], who considered the problem to analyze the behavior of a learning algorithm for monotone Boolean functions, and the previous work for the same t and s by Amano and Maruoka [AM02-ALT02].

3. N. Kanayama, M. Kida, N. Kunihiro, T. Nishino, K, Ohta and S. Okubo:
"Quantum Algorithms for Solving Exact Shortest Vector Problem", ERATO Workshop on Quantum Information Science 2005, pp. 179–180, 2005.
概要: In this paper, we propose a method for solving the shortest vector problem (SVP) by combing classical and quantum computations. Our method is composed of two steps. First, a searching space of the shortest vector is determined by classical computation. Next, the shortest vector in the fixed searching space is obtained by quantum computation. The complexity of quantum part depends on the size of searching space. Hence, as the searching space is smaller, we can find the shortest vector faster. We propose a method for choosing smaller searching space. First, we introduce a theorem characterizing a searching space of the shortest vector. By this theorem, we determine the appropriate searching space from the tentative shortest vector. Hence, we must obtain the relatively short vector before searching the true shortest vector. In this paper, we give a such vector by LLL-lattice basis reduction. Finally, we evaluate the efficiency of our LLL based Algorithm.

4. Y. Takahashi and N. Kunihiro:
"A Linear-size Quantum Circuit for Addition with no ancillary qubits", ERATO Workshop on Quantum Information Science 2005, pp. 113–114, 2005.
概要: We construct a quantum circuit for addition of two n-bit binary numbers that uses no ancillary qubits. The circuit is based on the ripple-carry approach. The depth and size of the circuit are $O(n)$. This is an affirmative answer to the question of Kutin as to whether a linear-depth quantum circuit for addition can be constructed without ancillary qubits using the ripple-carry approach. We also construct quantum circuits for addition modulo 2^n, subtraction, and comparison that use no ancillary qubits by modifying the circuit for addition.

B04: 回路計算量の下限の研究とその応用

築地 立家 † 陳 致中 ‡ 松浦 昭洋 §

† 東京電機大学 理工学部 情報科学科
〒 350-0394 埼玉県比企郡鳩山町石坂
tsukiji@j.dendai.ac.jp

‡ 東京電機大学 理工学部 数理科学科
〒 350-0394 埼玉県比企郡鳩山町石坂
chen@r.dendai.ac.jp

§ 東京電機大学 理工学部 情報システム工学科
〒 350-0394 埼玉県比企郡鳩山町石坂
matsu@k.dendai.ac.jp

1 はじめに

本研究の目的は、「回路計算量の下限研究における未解決問題の解決」と「下限研究の応用」にわけられる。前者は長期研究による革新的な結果が期待できる一方、後者は比較的短期で着実な成果をあげることが期待される。以下に、各々の要点を述べる。

「回路計算量の下限研究における未解決問題の解決」

回路計算量の下限研究はＮＰ完全性仮説に迫る伝統的な手法である。最近ラズボロフらは、下限証明に関する既存の手法がＮＰ完全性仮説を証明「できない」ことを示した。新しい下限証明手法を開発することは理論計算機科学の最重要課題とみなされている（Workshop on Challenges for Theoretical Computer Science 2000）。そこで本研究は定数次数予想と呼ばれる次の数学予想の解決を目指す。「論理積関数は、『任意の定数 T および異なる素数 P,Q について、上段は次数無制限の P 周期素子、中段は次数無制限の Q 周期素子、下段は次数 T の素子からなる 3 段回路』に関して指数下限をもつであろう。」この予想は 1990 年に Barrington により提起され、下限証明技術の発達を促してきたが、T=1 の場合の 1 次数予想を除いて未解決である。本研究は 2 次数予想の解決を目指し、定数次数予想の解決、そして ACC 回路の下限証明へと進む。これらはいずれもＮＰ完全性仮説にとり最重要の未解決問題であり、その解決により下限証明のための新しい代数的手法が創出されると考えられる。

「下限研究の応用」

築地立家は以下の研究を行う。

- 陳致中と共同して遺伝的系統図を再構築するための近似アルゴリズムの計算量解析を行う。
- 西野哲郎 (B04 班) と共同して最短格子ベクトル問題を解く量子アルゴリズムの計算量解析を行う。
- 相田慎 (C07 班) と共同して NP 探索問題の平均時間計算量解析を行う。

陳致中は以下の研究を行う。

- 築地立家と共同して遺伝的系統図を再構築するための近似アルゴリズムの計算量解析を行う。
- グラフとそのアルゴリズムの研究を行う.

松浦昭洋は以下の研究を行う。

- 論理式の充足解の数え上げに関する組合せ的性質の解明、アルゴリズムの解析を行う。
- 三次元空間における幾何学的形態の運動アルゴリズムの解析を行う。

2 2 次数予想の解決

t 次数関数とは，t 次の $\mathbb{Z}_2$ 整数係数多項式 $P(x_1,\ldots,x_n)$ について $(-1)^{P(x_1,\ldots,x_n)}$ とかけるような関数のことである．ここでは，論理関数を有限体上で計算する際の計算複雑さを考えたい．そこで，t 次数関数の定義域はブール球 $(x_1,\ldots,x_n)\in\{0,1\}^n$ とし，値域は任意に固定された，有限ガ

ロア体 $\mathbb{F} \subseteq \{0,1\}$ とする．ただし，体 $\mathbb{F}$ の標数は奇数とする．このとき，t 次数予想とは，AND 関数を t 次数関数の $\mathbb{F}$ 上線形結合で書くときに，$2^{\Omega(n)}$ 個以上の非零成分を要するであろう，という予想である．この予想は，Barrington，Straubing，Thérien が 1990 年に書いた共著論文において提出された．彼らは，1 次数予想を解決している．本研究において，長年の未解決問題であった，2 次数予想が解決された（投稿準備中）．

さて，1 次数予想は，AND 関数を $\mathbb{F}$ 上でフーリエ変換した際のフーリエ係数の中で，非零成分はいくつあるか，という問題である．AND 関数のフーリエ基底 $(-1)^{\sum_{i\in S} x_i}$ 成分は，$(-1)^{n+|S|} \in \{-1,1\}$ であり，全て非零なので，1 次数予想は成立する．さらに，Barrington らは，フーリエ基底として $\omega^{\sum_{i\in S} x_i}$（$\omega$ は体の任意の元）を許したとしても，1 次数予想が成立することを示した．

計算量の下限を見積もる技術は，計算機構の幾何的構造，あるいは組合せ的構造に対して，ある程度有効である．例えば，有限段論理回路（AC^0 と呼ばれる）の指数下界が知られている．また，AND,OR,NOT 素子に加えて，周期 p の計算を行う MOD_p 素子（p は固定された素数）を許す回路についての指数下界も知られている．この場合の下限証明は，位数 p の体上のフーリエ係数を計算する問題に帰着して行われている (Razborov (1987), Smolensky (1987))．しかし，異なる素数の周期をもつ代数構造上で計算素子数を数える技術は，未だに未発達である．例えば，上段が MOD_3 素子，中段が MOD_2 素子，下段が MOD_4 素子からなる，3 段 MOD 回路を考える．いかなる NP 問題についても，この回路サイズの下限証明は（非線形下限ですら）得られていなかった．本研究において，GF(3) 上の 2 次数予想が解決されたので，AND 関数のこの回路に関する指数サイズ下限が得られたことになる．

3 唯一最短格子ベクトル問題を解く量子アルゴリズム

本研究において，唯一最短格子ベクトル問題を解く量子アルゴリズムを設計し，それが多項式時間内で動作することを解析する．1994 年に，P. Shor は，素因数分解を多項式時間でとくような量子アルゴリズムを提案した．これにより，RSA 暗号系は，量子コンピュータが実現した場合，破られてしまう危険性が高いことが判明した．その後，唯一最短格子ベクトル問題をはじめとして，暗号解読の決め手となる問題を解くような量子アルゴリズムの研究がすすめられたが，いまだに成功していない．本研究において，この問題を解く量子アルゴリズムが確立されれば，非可換群における隠れ部分群発見問題などの重要未解決問題の解決に関しても，重要な知見が得られることになる．

4 相関データグラフから遺伝系統図を構築する問題の計算量

遺伝系統図に関して，次数が Δ の最適な k 次の根を構築する問題とは，与えられたグラフ $G = (V, E)$（相関データグラフ）から次のような（遺伝系統図をあらわす）木 T を構築する問題である．

(1) T の内部頂点の次数は 3 以上 Δ 以下である．

(2) T の外部頂点（すなわち葉）は V の要素とぴったり対応している．

(3) 不一致数，すなわち $|E \oplus \{\{u,v\} : u,v$ は T の葉で，$d_T(u,v) \le k\}|$ は，与えられた数を超えない．ここで $d_T(u,v)$ は木 T における u と v の間の距離をあらわす．

本研究において，この問題が，任意の定数 $\Delta, k \ge 3$ について NP 完全であることを証明した．

5 論理式の充足解数え上げ問題に対するアルゴリズムの設計

CNF 論理式の充足解の総数を数え上げる問題は #P 完全であり，充足解の総数を数え上げるために整除公式（Inclusion-Exclusion Formula）を用いると，論理式の項数を m とすると公式中に計算項が $2m$ 個存在するため，計算時間は最悪指数時間要する．2003 年に Amano らによって発表された論文”Inclusion-Exclusion for k-CNF Formulas”（Inform. Process. Lett., Vol. 87 (2), pp. 111-117, 2003）において，論理式を各項に含まれる変数（リテラル）の数が k 個以下である論理式に限った場合，多項式個の計算項の値が充足解の総数を定めるという性質が証明されていたが，そこ

での証明は背理法によるもので，それらの計算項から実際に充足解の総数を求めるアルゴリズムは知られていなかった．本研究では，整除公式において与えられる下位の多項式個の計算項から，漸次，構成的にその他の計算項を求めていくことができることを示し，多項式個の項から充足解の総数を求めるアルゴリズムを示した [7].

研究業績一覧

学術論文

1. Hosam M. Mahmoud, Tatsuie Tsukiji:
"Limit laws for terminal nodes in random circuits with restricted fan-out: a family of graphs generalizing binary search trees. ", Acta Informatika, 41(2-3), 99-110, 2004.
概要: We introduce a family of graphs $C(n, i, s, a)$ that generalizes the binary search tree. The graphs represent logic circuits with fan-in i, restricted fan-out s, and arising by n progressive additions of random gates to a starting circuit of a isolated nodes. We show via martingales that a suitably normalized version of the number of terminal nodes in binary circuits converges in distribution to a normal random variate.

2. Zhi-Zhong Chen, Tatsuie Tsukiji:
"Computing Bounded-Degree Phylogenetic Roots of Disconnected Graphs", Journal of Algrithms, （掲載予定）.
概要: The Phylogenetic kth Root Problem (PRk) is the problem of finding a (phylogenetic) tree T from a given graph $G = (V, E)$ such that (1) T has no degree-2 internal nodes, (2) the external nodes (i.e. leaves) of T are exactly the elements of V , and (3) $(u, v) \in E$ if and only if the distance between u and v in tree T is at most k, where k is some fixed threshold k. Such a tree T, if exists, is called a phylogenetic kth root of graph G. The computational complexity of PRk is open, except for $k \leq 4$. Recently, Chen et al. investigated PRk under a natural restriction that the maximum degree of the phylogenetic root is bounded from above by a constant. They presented a linear-time algorithm that determines if a given connected G has such a phylogenetic kth root, and if so, demonstrates one. In this paper, we supplement their work by presenting a linear-time algorithm for disconnected graphs.

3. Tatsuie Tsukiji, Zhi-Zhong Chen:
"Computing Phylogenetic Roots with Bounded Degrees and Errors Is Hard", Theoretical Computer Science, （掲載予定）.
概要: The Degree-Δ Closest Phylogenetic kth Root Problem (ΔCPRk) is the problem of finding a (phylogenetic) tree T from a given graph $G = (V, E)$ such that (1) the degree of each internal node of T is at least 3 and at most Δ, (2) the external nodes (*i.e.* leaves) of T are exactly the elements of V, and (3) the number of disagreements, $|E \oplus \{\{u, v\} : u, v$ are leaves of T and $d_T(u, v) \leq k\}|$ does not exceed a given number, where $d_T(u, v)$ denotes the distance between u and v in tree T. We show that this problem is NP-hard for all fixed constants $\Delta, k \geq 3$. Our major technical contribution is the determination of all phylogenetic roots that approximate the almost largest cliques. Specifically, let $s_\Delta(k)$ be the size of the largest clique having a kth phylogenetic root with maximum degree Δ. We determine all the phylogenic kth roots with maximum degree Δ that approximate the $(s_\Delta(k) - 1)$-clique within error 2, where we allow the internal nodes of phylogeny to have degree 2.

4. Zhi-Zhong Chen, Yong Gao, Guohui Lin, Robert Niewiadomski, Yang Wang, Junfeng Wu:
"A space-efficient algorithm for sequence

alignment with inversions and reversals", Theoretical Computer Science, 325(3), 361-372, 2004.

概要: A dynamic programming algorithm to find an optimal alignment for a pair of DNA sequences has been described by Sch ¨oniger and Waterman. The alignments use not only substitutions, insertions, and deletions of single nucleotides, but also inversions, which are the reversed complements, of substrings of the sequences.With the restriction that the inversions are pairwise non-intersecting, their proposed algorithm runs in $O(n^2m^2)$ time and consumes $O(n^2m^2)$ space, where n and m are the lengths of the input sequences respectively. We develop a space efficient algorithm to compute such an optimal alignment which consumes only $O(nm)$ space within the same amount of time. Our algorithm enables the computation for a pair of DNA sequences of length up to $10,000$ to be carried out on an ordinary desktop computer. Simulation study is conducted to verify some biological facts about gene shuffling across species.

5. Zhi-Zhong Chen, Xin He:
"Disk Embeddings of Planar Graphs.", Algorithmica, 38(4), 539-576, 2004.

概要: Given a planar graph $G = (V, E)$ and a rooted forest $\mathcal{F} = (V_{\mathcal{F}}, A_{\mathcal{F}})$ with leaf set V, we wish to decide whether G has a plane embedding G satisfying the following condition: There are $|V_{\mathcal{F}}| - |V|$ pairwise non-crossing Jordan curves in the plane one-to-one corresponding to the nonleaf vertices of $\mathcal{F}$ such that for every nonleaf vertex f of $\mathcal{F}$, the interior of the curve Jf corresponding to f contains all the leaf descendants of f in F but contains no other leaves of $\mathcal{F}$. This problem arises from theoretical studies in geographic database systems. It is unknown whether this problem can be solved in polynomial time. This paper presents an almost linear-time algorithm for a nontrivial special case where the set of leaf descendants of each nonleaf vertex f in $\mathcal{F}$ induces a connected subgraph of G.

6. Zhi-Zhong Chen:
"New Bounds on the Number of Edges in a k-Map Graph", COCOON 2004, Lecture Notes in Computer Science, 3106, 319-328, 2004.

概要: It is known that for every integer $k \geq 4$, each k-map graph with n vertices has at most $kn - 2k$ edges. Previously, it was open whether this bound is tight or not. We show that this bound is tight for $k = 4$. We also laboriously show that this bound is not tight for large enough k; more precisely, we show that for every $0 < \epsilon < \frac{3}{328}$ and for every integer $k \geq \frac{140}{41e}$, each k-map graph with n vertices has at most $(\frac{325}{328}+\epsilon)kn-2k$ edges. This result implies the first polynomial (indeed linear) time algorithm for coloring a given k-map graph with less than $2k$ colors for large enough k. We further show that for every positive multiple k of 6, there are infinitely many integers n such that some k-map graph with n vertices has at least $(\frac{11}{12}k + \frac{1}{3})n$ edges.

7. Akihiro Matsuura:
"A Note on Approximating Inclusion-Exclusion for k-CNF Formulas", IEICE Trans. on Information and Systems, E88-D(1), 100-102, 2005.

概要: The number of satisfying assignments of k-CNF formulas is computed using the inclusion-exclusion formula for sets of clauses. Recently, it was shown that the information on the sets of clauses of size $\log k + 2$ already uniquely determines the number of satisfying assignments of k-CNF formulas. The proof was, however, only existential and no explicit procedure was presented. In this paper, it is shown that such a procedure exists.

B05: ブール理論に基づく離散システムの構造解析と計算限界の研究

牧野 和久

東京大学 大学院 情報理工学系研究科
〒 113-8656 東京都文京区本郷 7-3-1
makino@mist.i.u-tokyo.ac.jp

摘要: 本文では，平成 17 年度の B05 班の研究活動に関係する成果を報告する．特に, 連結度要求に基づくネットワークデザイン問題としての施設配置問題に対する計算量，近似可能性などについて重点を置き説明する．

キーワード: 計算効率，近似可能性，アルゴリズム，施設配置問題，連結度

1 はじめに

社会システムや産業活動などに関連して現れる生産計画，環境計画，スケジューリング，最適投資などを始めとする重要な問題の多くは，離散構造を有するシステムの問題として捉えることができる．この離散構造を有するシステムの問題が答易に解けるか否かは, その対象となるシステムの構造に強く依存する. 比較的容易に解ける最適化問題の組合せ的, 代数的, あるいは, ブール関数的構造については, 例えばマトロイド構造や劣モジュラ構造というような離散的な構造が深く関係することが知られているが, それだけでは説明のつかない問題も数多い. また，最適化問題以外の問題，例えば，列挙問題などが，効率的に解けるために離散構造を解析することは極めて重要である．本研究班では，比較的容易に解ける問題の構造的性質をさらに詳細に吟味し, その構造を明らかにし, 効率的なアルゴリズムを設計するための統一的な指針を与えること，および，計算量理論を用いて計算量下界の提示などの計算限界を明らかにすることを試みる．

本研究班では，以上のような目的意識を持って, 主に理論的な研究に重点をおいて活動を続けて来た．以下の節では，本年度の成果である連結度に基づく施設配置問題に関する成果 [8, 9] について報告する．

2 連結度要求に基づく施設配置問題

連結度要求に基づく施設配置問題とは，与えられたネットワークにおいて，フロー（連結度）に基づく制約条件の下で最小コストを与えるソース集合（配置）を求める問題である．この問題は，例えば，マルチメディアネットワーク中にサービス要求量を指定した複数のクライアントが与えられたとき，その要求を満足しながら最小コストで（ミラー）サーバを配置するという問題をモデル化したものであり，信頼度を考慮に入れた施設配置問題として，ソース配置問題とも呼ばれ，近年盛んに研究されている（例えば，[1, 2, 4, 5, 6, 7, 10, 11] など）．また，ネットワーク理論で有名な連結度増大問題とも深く関連している．

ソース配置問題における制約条件としては，枝連結度，および，点連結度に基づくものがある．枝連結度要求はリンク故障に対する信頼度，点連結度要求は点故障に対する信頼度に対応しており，点連結度要求に対しては，ソース故障の存否に関して 2 種類の要求が考察されている [6, 7].

これまでの研究成果： ソース配置問題に対するアルゴリズム論的研究は，無向，あるいは，有向

ネットワーク中で，コスト関数と要求関数がそれぞれ，一様，あるいは，一般の場合に分けて行われている．表 1, 2, 3 にこれまで得られている最良の結果を示す．ただし，n, m はそれぞれネットワーク中の点数，枝数を示す．表から分かるよう

表 2.1: ソース配置問題に対する既存の結果（枝連結度）

		コスト：一様	コスト：一般
要求：一様	無向	$O(n(m+n\log n))$	$O(n(m+n\log n))$
	有向	$O(n^3 m\log(n^2/m))$	強 NP 困難
要求：一般	無向	$O(nM(n,m))$	**弱 NP 困難**
	有向	強 NP 困難	強 NP 困難

$M(n,m)$: ネットワーク (n 点, m 枝) 中の最大フローの計算時間

表 2.2: ソース配置問題に対する結果（点連結度・ソース故障なし）

	コスト：一様	コスト：一般
要求：一様	強 NP 困難	強 NP 困難
要求：一般	強 NP 困難	強 NP 困難

表 2.3: ソース配置問題に対する結果（点連結度・ソース故障あり）

		コスト：一様	コスト：一般
要求：一様	無向	$O(\min\{k,\sqrt{n}\}kn^2)$	$O(\min\{k,\sqrt{n}\}kn^2)$
(k:要求量)	有向	$O(\min\{k,\sqrt{n}\}mn)$	$O(\min\{k,\sqrt{n}\}mn)$
要求：一般		強 NP 困難	強 NP 困難

に，一ヶ所（太字）を除き，全て多項式時間で（効率的に）解けるか，あるいは，強 NP 困難であるかが知られている．

しかしながら，NP 困難な場合に対する近似精度保証付きの近似アルゴリズムは，未だ開発されておらず，ネットワークが特別な構造（例えば，木構造）をもつときに効率的に解けるかどうかも分かっていない．また，ソース配置問題では，コスト関数として建設費用のみを扱っているが，建設費用に加え，供給量にも依存するコスト関数の考察が求められていた．

本研究班の成果： 本研究では，以下の成果を得る．

1. まず，未解決問題として残されていた，無向ネットワーク中の枝連結度に基づくソース配置問題の強 NP 困難性を示す．さらに近似困難性も示す．

2. ソース配置問題を劣モジュラ被覆問題として定式化することにより，すべての NP 困難な場合に適用可能な精度保証付きの近似アルゴリズムを開発する．このアルゴリズムは，枝連結度要求に対して最適な近似精度を与える．

3. 木構造ネットワークにおけるソース配置問題は，枝連結度要求のときは擬多項式時間で解け，（２種類の）点連結度要求のときは多項式時間で解けることを示す．ここで，擬多項式時間の改善は，[1] の弱 NP 困難性より，不可能である．

4. 供給量に関して凹なコスト関数も扱えるようソース配置問題を拡張し，これに対して 2. と同様の結果を得る．

5. 無向ネットワーク中の一様な枝連結度要求を持つ拡張されたソース配置問題を，ラミナー被覆問題として定式化することにより，$O(nm+n^2(q+\log n))$ 時間アルゴリズムを開発する．ただし，q は供給に対するコストを求めるために要する時間であり，コスト関数がオラクルで与えられるとき，上記のアルゴリズムは最適である．

   また，コスト関数が建設費と線形な運営費の和として記述できる場合はさらに高速に $O(n(m+n\log n))$ 時間で解け，より一般的なコスト関数に対しては計算困難であることを示す．

また，本論文で開発した 2., 4. の劣モジュラ被覆問題，5. のラミナー被覆問題に対するアルゴリズムはソース配置問題以外の多くの離散最適化問題へ適用可能である．

以下の節の構成： 第 2．1 節では，ソース配置問題とその拡張についての定義を与える．第 2．2，2．3 節ではそれぞれ，ソース配置問題とその拡張に関する結果を示す．頁数制限のため，定理の証明，アルゴリズムなど多くを省略する．

2.1 ソース配置問題とその拡張

点集合 V と枝集合 A をもつグラフ G に容量関数 $u : A \to \mathbb{R}_+$ を付与したネットワーク $\mathcal{N} = (G = (V, A), u)$ を考える．ただし，$\mathbb{R}_+$ は非負実数の集合である．このネットワーク $\mathcal{N}$，要求関数 $d^-, d^+ : V \to \mathbb{R}_+$，コスト関数 $c : V \to \mathbb{R}_+$ が与えられたとき，ソース配置問題は以下のように記述できる．

$$
\begin{aligned}
\text{(SLP)}\quad \text{Min.}\ & \textstyle\sum_{v\in S} c(v) \\
\text{s.t.}\ & \psi^-(S, v) \geq d^-(v), \\
& \psi^+(v, S) \geq d^+(v)\ \ (v \in V), \\
& S \subseteq V.
\end{aligned}
$$

ただし，$\psi^-(X, Y)$，$\psi^+(X, Y)$ は点集合 X から Y への連結度を表す．また，$\psi^-(S, \{v\})$，$\psi^+(\{v\}, S)$ をそれぞれ簡潔に $\psi^-(S, v)$，$\psi^+(v, S)$ と書く．本論文では，$\psi^{\pm}$ として，次の 3 種類の連結度を考察する．

(i) $\psi^-(S, v) = \lambda(S, v)$, $\psi^+(v, S) = \lambda(v, S)$,

(ii) $\psi^-(S, v) = \kappa(S, v)$, $\psi^+(v, S) = \kappa(v, S)$,

(iii) $\psi^-(S, v) = \hat{\kappa}^-(S, v)$, $\psi^+(v, S) = \hat{\kappa}^+(v, S)$,

ただし，$\lambda(X, Y)$ は点集合 X から Y への最大フロー値で，$X \cap Y \neq \emptyset$ のとき $\lambda(X, Y) = +\infty$ とする．また，$\kappa(X, Y)$ は X から Y への端点以外の点を共有しない最大パス数で，$X \cap Y \neq \emptyset$，または，$v \in X, w \in Y$ である枝 $(v, w) \in A$ が存在するとき，$\kappa(X, Y) = +\infty$ とする．$\hat{\kappa}^-(S, v)$，および，$\hat{\kappa}^+(v, S)$ は，それぞれ点集合 S から点 v，および，v から S への v 以外の点を共有しない最大パス数を表し，$X \cap Y \neq \emptyset$ のとき $\hat{\kappa}^-(S, v) = \hat{\kappa}^+(v, S) = +\infty$ とする．(i) は枝連結度，(ii) はソース故障を許さない点連結度，(iii) はソース故障を許す点連結度を表す．

問題の拡張： 上記のソース配置問題では，コスト関数として施設の建設費用 (v における建設費用 $c(v)$) のみを扱っている．しかしながら，現実的なコスト関数として，建設費用に加え，供給量にも依存するものを考察することが求められている．従って，本論文では以下のように供給量を考慮したソース配置問題を考察する．ここでは，頁数制限のため，枝連結度 λ に対する拡張についてのみ述べる．

ネットワーク $\mathcal{N}$ 中のフロー $\varphi : A \to \mathbb{R}_+$ が以下の条件を満たすとき，供給 $x : V \to \mathbb{R}_+$ に対して実行可能であると呼ぶ．

$$-x(v) \leq \partial\varphi(v) \leq x(v) \quad (v \in V) \tag{1}$$

$$0 \leq \varphi(a) \leq u(a) \quad (a \in A) \tag{2}$$

ただし，$\partial\varphi(v)$ はフロー φ の点 v における境界を示し，

$$\partial\varphi(v) = \sum_{(v,w)\in A} \varphi(v, w) - \sum_{(w,v)\in A} \varphi(w, v)$$

と定義される．$\lambda^-(x; v)$ と $\lambda^+(x; v)$ をそれぞれ供給 x における点 v への最大流入量 $(-\partial\varphi(v)+x(v))$ と v からの最大流出量 $(\partial\varphi(v)+x(v))$ とする．枝連結度要求を持つ拡張されたソース配置問題は，ネットワーク $\mathcal{N} = (G = (V, A), u)$，要求関数 $d^-, d^+ : V \to \mathbb{R}_+$，各点 $v \in V$ におけるコストを表す単調な凹関数 $c_v : \mathbb{R}_+ \to \mathbb{R}_+$ が与えられたとき，以下のように記述できる．

$$
\begin{aligned}
\text{Min.}\ & \textstyle\sum_{v\in V} c_v(x(v)) \\
\text{s.t.}\ & \lambda^-(x; v) \geq d^-(v), \\
& \lambda^+(x; v) \geq d^+(v)\ \ (v \in V), \\
& x(v) \geq 0\ \ (v \in V).
\end{aligned}
$$

ここで，c_v の単調凹性は，ネットワーク設計問題などでよく扱われる自然な仮定である．

2.2 ソース配置問題に対する成果

ソース配置問題に対して以下の結果を得る．

無向・枝連結度要求をもつ場合の計算困難性： 無向ネットワーク中の枝連結度要求（すなわち，ψ $(= \psi^- = \psi^+) = \lambda$, $d = d^+ (= d^-)$) を持つソース配置問題に対して，以下の定理が成立する．

定理 1 無向ネットワーク中の枝連結度要求を持つソース配置問題は強 NP 困難である．

これは，[1] で提示されていた未解決問題を解くものである．この定理は，NP 困難問題として有名な集合被覆問題 [3] をソース配置問題に帰着させることによって示される．

さらに，我々は，集合被覆問題の近似困難性，および，帰着のギャップ保存性より以下の定理を得る．

定理 2 *NP*⊈*DTIME*($N^{\log\log N}$) ならば，ある定数 $c>0$ が存在して，どんな連結度要求を持つソース配置問題に対しても多項式時間 $c\ln\sum_{v\in V} d(v)$-近似アルゴリズムは存在しない．

ここで，NP⊈DTIME($N^{\log\log N}$) とは，N を入力長としたとき，任意の NP 完全問題が $O(N^{\log\log N})$ 時間の決定性アルゴリズムを持たないことを意味し，多くの計算量理論の研究者によって信じられている．また，α-近似アルゴリズム A とは，近似比（すなわち，(A の出力する解のコスト値)/(最適値)）が必ず α 以内である解を出力するアルゴリズムのことをいう．

木構造ネットワーク中のソース配置問題： また，与えられたネットワーク $\mathcal{N}$ が木構造であるとき，以下の肯定的な定理が成立する．

定理 3 木構造ネットワーク $\mathcal{N}$ におけるソース配置問題は，容量関数と要求関数が整数のとき，擬多項式時間で解ける．

定理 4 木構造ネットワーク $\mathcal{N}$ 中の点連結度要求 $\kappa, \hat{\kappa}$ をもつソース配置問題はともに多項式時間で解ける．

[1] の弱 NP 困難性の結果から，定理 3 の擬多項式時間は計算限界である．また，定理 4 は，点連結度要求を持つソース配置問題に対する初めての効率的に計算可能な部分クラスを示している．

2.3 拡張されたソース配置問題に対する成果

拡張されたソース配置問題に対しては，以下の肯定的な結果を得る．

近似アルゴリズム： 拡張されたソース配置問題を劣モジュラ被覆問題として定式化する．

V を有限集合，単調な劣モジュラ関数 $f:\mathbb{R}_+^V\to\mathbb{R}_+$，実数 M，各 $v\in V$ におけるコストを表す単調な凹関数 $c_v:\mathbb{R}_+\to\mathbb{R}_+$ が与えられたとき，劣モジュラ被覆問題は以下のように記述できる．

$$\begin{array}{ll}\text{Min.} & \sum_{v\in V} c_v(x(v)) \\ \text{s.t.} & f(x)\geq M,\ \ x(v)\geq 0\ \ (v\in V).\end{array}$$

ただし，関数 $f:\mathbb{R}^V\to\mathbb{R}$ が劣モジュラであるとは，任意の $x,y\in\mathbb{R}^V$ に対して，$f(x)+f(y)\geq f(x\wedge y)+f(x\vee y)$ が成り立つことをいう．ここで，$(x\wedge y)(v)=\min\{x(v),y(v)\}$, $(x\vee y)(v)=\max\{x(v),y(v)\}$ である．この劣モジュラ被覆問題は，劣モジュラ集合被覆問題の拡張である．拡張されたソース配置問題は，例えば，枝連結度要求の場合，

$$\begin{aligned} f(x) &= \sum_{v\in V}(\min\{\lambda^-(x;v),d^-(v)\} \\ &\qquad +\min\{\lambda^+(x;v),d^+(v)\}) \\ M &= \sum_{v\in V}(d^-(v)+d^+(v)) \end{aligned}$$

とすることで，劣モジュラ被覆問題として定式化できる．

本研究では，この劣モジュラ被覆問題に対して，貪欲アルゴリズムを開発する．詳細は省略するが，このアルゴリズムを拡張されたソース配置問題に適用すると，任意の $x\in\mathbb{R}_+^V$ と $v\in V$ に対して，$g(\alpha)=f(x+\alpha\chi_v)-f(x)$ (ただし，χ_v は v に対する特性ベクトル) が高々$2n+1$ 区分からなる区分線形関数となり，また，その折れ点は最大フロー問題を高々$2n$ 回解くことにより計算可能であることなどを用いて，以下の結果を得る．

定理 5 （拡張された）ソース配置問題は，容量，および，要求関数が整数である場合，多項式時間で $(1+\ln\sum_{v\in V}(d^-(v)+d^+(v)))$-近似可能である．

定理 2 より，この貪欲アルゴリズムは枝連結度要求に対して，（オーダーの意味で）最適である．

無向・一様な枝連結度要求をもつ拡張ソース配置問題： 無向ネットワークにおいて一様な枝連結度要求（すなわち，$d(v)=k$ $(v\in V)$）をもつ拡

張されたソース配置問題をラミナー被覆問題として定式化する．

有限集合 V 上のラミナー族 $\mathcal{F} \subseteq 2^V$，コストを表す単調な凹関数 $F : \mathbb{R}_+^V \to \mathbb{R}_+$，要求関数 $d : \mathcal{F} \to \mathbb{R}_+$ が与えられたとき，ラミナー被覆問題は以下のように記述できる．

$$\begin{aligned} &\text{Min.} \quad F(x) \\ &\text{s.t.} \quad \textstyle\sum_{v \in X} x(v) \geq d(X) \ (X \in \mathcal{F}), \\ &\qquad x(v) \geq 0 \ (v \in V). \end{aligned}$$

ここで，ラミナー族 $\mathcal{F}$ とは，任意の $X, Y \in \mathcal{F}$ に対して，$X \cap Y$, $X - Y$, $Y - X$ のいずれか一つは空集合となる集合族である．

ラミナー族は様々な組織の階層構造を表現できるため，この問題は多くの応用をもつ．また，最大フロー・最小カットの定理などを用いることにより，無向ネットワーク中の枝連結度増大問題やこの拡張されたソース配置問題もラミナー被覆問題として定式化可能なことが分かる．

本論文では，この問題に対して以下の結果を得る．

定理 6 ラミナー被覆問題は，

1. F が分離可能な単調凹関数で記述できるならば，$O(n^2q)$ 時間で解ける．さらに，F がオラクルで与えられるときは，$\Omega(n^2q)$ 時間必要である．
2. F が固定費つき線形関数（すなわち，施設建設費と線形運営コストの和）の和で記述できるならば，$O(n \log^2 n)$ 時間で解ける．
3. F が一般の凹関数ならば，NP 困難であり，さらに F がオラクルで与えられるときは $\Omega(2^{\frac{n}{2}}q)$ 時間必要である．

ただし，q は各 $x \in \mathbb{R}_+$ に対して $F(x)$ を求めるために要する時間である．*1.* の結果は，F がオラクルで与えられるとき，最適なアルゴリズム開発に成功したことを意味する．

この系として，以下の結果を得る．

系 1 無向ネットワーク中の一様な枝連結度要求を持つ拡張されたソース配置問題は，

1. $O(nm + n^2(q + \log n))$ 時間で解ける．
2. 各コスト関数 c_v が固定費つき線形関数として記述できる場合は，$O(n(m + n \log n))$ 時間で解ける．
3. より一般的なコスト関数（すなわち，F が一般の凹関数）のとき，計算困難である．

参考文献

[1] K. Arata, S. Iwata, K. Makino and S. Fujishige, Locating sources to meet flow demands in undirected networks, *Journal of Algorithms*, 42 (2002) 54-68.

[2] M. Bárász, J. Becker, and A. Frank: An algorithm for source location in directed graphs, *Operations Research Letters*, **33** (2005), 221–230.

[3] M. R. Garey and D. S. Johnson, *Computers and Intractability*, Freeman, New York, 1979.

[4] J. van den Heuvel and M. Johnson: Transversals of subtree hypergraphs and the source location problem in digraphs, *CDAM Research Report*, LSE-CDAM-2004-10, London School of Economics.

[5] H. Ito and M. Yokoyama, Edge connectivity between nodes and node-subsets, *Networks*, 31 (1998) 157-164.

[6] H. Ito, M. Ito, Y. Itatsu, K. Nakai, H. Uehara, and M. Yokoyama: Source location problems cosidering vertex-connectivity and edge-connectivity simultaneously. *Networks*, 40 (2002) 63-70.

[7] H. Nagamochi, T. Ishii and H. Ito, Minimum cost source location problem with vertex-connectivity requirements in digraphs, *Information Processing Letters*, 80 (2001) 287–294.

[8] M. Sakashita, K. Makino, and S. Fujishige: Minimizing a monotone concave function with laminar covering constraints, *ISAAC2005*, LNCS **3827** (2005), 71–81.

[9] M. Sakashita, K. Makino, and S. Fujishige: Minimum cost source location problems with flow requirements, *LATIN2006* LNCS **3887** (2006), 769–781.

[10] H. Tamura, M. Sengoku, S. Shinoda and T. Abe, Some covering problems in location theory on flow networks, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E75-A (1992) 678-683.

[11] 田村, 菅原, 仙石, 篠田, 無向フローネットワークにおける総合被覆問題について, 電子情報通信学会論文誌, J81-A (1998) 863-869.

研究業績一覧

学術論文

1. M. Sakashita, K. Makino, S. Fujishige: "Minimizing a Monotone Concave Function with Laminar Covering Constraints", ISAAC 2005, Lecture Notes in Computer Science, 3827, 71-81, 2005.
   概要: Let V be a finite set with $|V| = n$. A family $\mathcal{F} \subseteq 2^V$ is called *laminar* if for arbitrary two sets $X, Y \in \mathcal{F}$, $X \cap Y \neq \emptyset$ implies $X \subseteq Y$ or $X \supseteq Y$. Given a laminar family $\mathcal{F}$, a demand function $d : \mathcal{F} \to \mathbf{R}_+$, and a monotone concave cost function $F : \mathbf{R}_+^V \to \mathbf{R}_+$, we consider the problem of finding a minimum-cost $x \in \mathbf{R}_+^V$ such that $x(X) \geq d(X)$ for all $X \in \mathcal{F}$. Here we do not assume that the cost function F is differentiable or even continuous. We show that the problem can be solved in $\mathcal{O}(n^2 q)$ time if F can be decomposed into monotone concave functions by the partition of V that is induced by the laminar family $\mathcal{F}$, where q is the time required for the computation of $F(x)$ for any $x \in \mathbf{R}_+^V$. We also prove that if F is given by an oracle, then it takes $\Omega(n^2 q)$ time to solve the problem, which implies that our $\mathcal{O}(n^2 q)$ time algorithm is optimal in this case. Furthermore, we propose an $\mathcal{O}(n \log^2 n)$ algorithm if F is the sum of linear cost functions with fixed setup costs. These also make improvements in complexity results for source location and edge-connectivity augmentation problems in undirected networks. Finally, we show that in general our problem requires $\Omega(2^{\frac{n}{2}} q)$ time when F is given implicitly by an oracle, and that it is NP-hard if F is given explicitly.

2. M. Sakashita, K. Makino, S. Fujishige: "Minimum Cost Source Location Problems with Flow Requirements", LATIN 2006, Lecture Notes in Computer Science, 3887, 769-780, 2006.
   概要: In this paper, we consider source location problems and their generalizations with three connectivity requirements λ, κ and $\hat{\kappa}$. We show that the source location problem with edge-connectivity requirement λ in undirected networks is strongly NP-hard, and that no source location problems with three connectivity requirements in undirected/directed networks are approximable within a ratio of $\mathcal{O}(\ln D)$, unless NP has an $\mathcal{O}(N^{\log \log N})$-time deterministic algorithm. Here D denotes the sum of given demands. We also devise $(1 + \ln D)$-approximation algorithms for all the extended source location problems if we have the integral capacity and demand functions. Furthermore, we study the extended source location problems when a given graph is a tree. Our algorithms for all the extended source location problems run in pseudo-polynomial time and the ones for the source location problem with vertex-connectivity requirements κ and $\hat{\kappa}$ run in polynomial time, where pseudo-polynomiality for the source location problem with the arc-connectivity requirement λ is best possible unless P=NP, since it is known to be weakly NP-hard, even if a given graph is a tree.

3. K. Makino, U. Uno:
"Minimum Edge Ranking Spanning Trees of Split Graphs", Discrete Applied Mathematics, (掲載予定).
概要: Given a graph G, the minimum edge ranking spanning tree problem (MERST) is to find a spanning tree of G whose edge ranking is minimum. However, this problem is known to be NP-hard for general graphs. In this paper, we show that the problem MERST has a polynomial time algorithm for split graphs, which have useful applications in practice. The result is also significant in the sense that this is a first non-trivial graph class for which the problem MERST is found to be polynomially solvable. We also show that the problem MERST for threshold graphs can be solved in linear time, where threshold graphs are known to be split.

4. Y. Asahiro, T. Horiyama, K. Makino, H. Ono, T. Sakuma, M. Yamashita:
"How to Collect Balls Moving in the Euclidean Plane", Discrete Applied Mathematics, (掲載予定).
概要: In this paper, we study how to collect n balls moving with constant velocities in the Euclidean plane by k robots moving on straight track-lines through the origin. Since all the balls might not be caught by robots, differently from Moving-Target TSP, we consider the following 3 problems in various situations: (i) deciding if k robots can collect all n balls, (ii) maximizing the number of the balls collected by k robots, and (iii) minimizing the number of the robots to collect all n balls. The situations considered here contain the cases in which track-lines are given (or not), and track-lines are identical (or not). For all problems and situations, we provide polynomial time algorithms or proofs of intractability, which clarify the tractability-intractability frontier in the ball collecting problems in the Euclidean plane.

研究会等

1. 坂下 麻里子, 牧野 和久, 藤重 悟:
"Approximation Algorithms for Source Location Problems with Flow Requirements", 電子情報通信学会コンピュテーション研究会, COMP2005-25, 43-50, 2005 年 6 月.
概要: In this paper, we consider source location problems with three kinds of connectivity requirements, where the problem with arc-connectivity requirement λ is, for example, to find a minimum-cost set $S \subseteq V$ in a given graph $G = (V, A)$ with a capacity function $u : A \to \mathbb{R}_+$ such that for each vertex $v \in V$, the arc-connectivity $\lambda^-(S, v)$ from S to v (resp., $\lambda^+(S, v)$ from v to S) at least a given demand $d^-(v)$ (resp., $d^+(v)$). We show that the source location problem with edge-connectivity requirement in undirected networks is strongly NP-hard, which solves an open problem posed by Arata *et al.* [1], and that it is not approximable within a ratio of $\emptyset(\ln \sum_{v \in V} d(v))$, unless NP has an $\emptyset(N^{\log \log N})$-time deterministic algorithm. We also study the source location problems when a given graph is a tree. We devise a pseudo-polynomial time algorithm for the source location problem with arc-connectivity requirement, and a polynomial time algorithm for the source location problems with two kinds of vertex-connectivity requirements, where pseudo-polynomiality for the arc-connectivity requirement is best possible unless P=NP, since it is known to be weakly NP-hard, even if a given graph is a tree. We further study the extensions of the source location problems to take supply value of each source into account, where the extended problems has monotone concave cost functions c_v $(v \in V)$ which model the ones depending not only on the fixed setup cost,

but also on the supply value. We devise $(1+\ln\sum_{v\in V}(d^-(v)+d^+(v)))$-approximation algorithms for the extended source location problems if we have the integral capacity and demand functions. This shows that our approximation algorithm for the problem with arc-connectivity requirement is optimal.

2. 坂下 麻里子, 牧野 和久, 藤重 悟:
“ソース配置問題とその拡張”, 日本オペレーションズ・リサーチ学会アルゴリズム研究部会, 2005 年 5 月.
概要: フロー要求に基づく施設配置問題であるソース配置問題とその拡張にたいして主に計算量論的観点から考察する．解くに近似の可能性について議論する．

B06: 暗号システムに対する実装攻撃の適用と限界に関する計算的研究

酒井 康行 † 高木 剛 ‡ 田端 利宏 § 櫻井 幸一 ¶

† 三菱電機株式会社 情報技術総合研究所
〒 247-8501 神奈川県鎌倉市大船 5-1-1
Sakai.Yasuyuki@aj.MitsubishiElectric.co.jp

‡ 公立はこだて未来大学 システム情報科学部
〒 041-8655 函館市亀田中野町 116-2
takagi@fun.ac.jp

§ 岡山大学 大学院自然科学研究科
〒 700-8530 岡山市津島中 3-1-1
tabata@it.okayama-u.ac.jp

¶ 九州大学 大学院システム情報科学研究院
〒 812-8581 福岡県福岡市東区箱崎 6-10-1
sakurai@csce.kyushu-u.ac.jp

1 はじめに

楕円曲線暗号は，IEEE，ANSI，ISO，CRYPTREC など様々な機関において推奨暗号アルゴリズムとして採用され，現在様々な情報セキュリティシステムで実用化が進んでいる．一方，暗号が実装されたデバイスから得ることができるサイドチャネル情報を利用して秘密情報得る解析法，すなわちサイドチャネル解析が，特にスマートカードなどの携帯機器で現実的脅威となっている．楕円曲線暗号は，RSA 暗号と比べて鍵長を小さくできることから，携帯機器上でより利点を発揮する．したがって，楕円曲線暗号をサイドチャネル解析に対して安全に実装することは重要な課題である．

楕円曲線暗号では楕円点倍算 $Q \leftarrow kP$ (k は整数，P と Q は楕円曲線上の点) と呼ばれる計算を行う．楕円点倍算は，楕円曲線暗号において計算時間が支配的な演算であり，様々な計算法が研究されている．また，署名生成や復号においては，整数 k は秘密情報であるため，サイドチャネル情報から k を導き出すことが楕円曲線暗号に対するサイドチャネル解析の目的となる．

楕円点倍算に対するサイドチャネル解析の方法および対策法はすでに数多く提案されている．単純電力解析 (SPA) に対しては，Double-and-Add always 法など，暗号処理手順を秘密鍵に依存させずに一定にする対策法があり [2, 11]，差分電力解析 (DPA) に対しては，べき指数のランダム化や入力点のランダム化 (ランダム化射影座標)[2] などの対策法がある．

DPA 対策として何らかの方法でランダム化を取り入れることは一般的である．しかし，ランダム化にも関わらず，暗号演算中の中間変数が乱数の影響を受けないある不変な性質を持つことがあり，この不変な性質を利用してサイドチャネル解析が可能となることが Goubin により指摘された [5]．例えば，点の座標値が 0 ならば，ランダム化しても 0 であり続ける．このような特殊な性質を持つ点を利用して行う電力解析を改良電力解析 (Refined Power Analysis, RPA) と呼ぶ [5]．また，RPA の拡張であるゼロ値解析 (Zero-Value Register Attack, ZRA) と呼ばれる手法も開発された [1]．

さらに，値が 0 ということの他，点の座標値のハミング重みに関する相関を不変な性質として扱う解析法も提案されている [3]．National Institute of Standards and Technology (NIST)，ANSI，Standards for Efficient Cryptography Group (SECG)，などが推奨する楕円曲線では，素体 $\mathbb{F}_p$ 上楕円曲線の定義体標数 p として一般化メルセンヌ素数を用いるなど，高速演算可能なドメインパラメータが選ばれている．[3] では，このような定義体標数を持つ楕円曲線において射影座標系 $(x, y) \leftarrow (X/Z, Y/Z)$ 表現を用いた場合，アファイン座標に変換した時に点 $(2^\lambda, y)$，λ は小さい非負整数，という形になる点 (X, Y, Z) は，X 座標値と Z 座標値とのハミング距離が近くなることが示された．

本稿では，このような，楕円点倍算中に現れる不変な性質を持つ中間変数の存在についてさらに考察する．素体 $\mathbb{F}_p$ 上 NIST 推奨楕円曲線を，Jacobian 座標系 $(x, y) \leftarrow (X/Z^2, Y/Z^3)$，Double-and-Add always 法，ランダム化射影座標法，を用いて実装する場合を検討する．この場合，楕円点倍算の途中で $(2^\lambda, y)$，$(2^\lambda + 1, y)$，$(x, 2^\lambda)$ という形の点になるような点を楕円点倍算への入力として与えると，点 2 倍算においてハミング重みに強い相関を持つ中間変数の組が出現することを示す．

2 推奨楕円曲線

楕円曲線ドメインパラメータは，楕円離散対数問題が困難になるように選ばなければならない．しかし，実際の情報セキュリティシステムへ楕円曲線暗号を適用する際は，安全であるだけでなく，高い速度性能が得られるようなドメインパラメータを選択することも重要な要件となる．素体 $\mathbb{F}_p$ 上楕円曲線においては，定義体標数 p として特別な型，例えば一般化 Mersenne 素数を選ぶと p による剰余算を高速に行うことができる [12]．NIST が推奨する 5 つの素体 $\mathbb{F}_p$ 上楕円曲線は，一般化 Mersenne 素数と呼ばれる次の 5 つの素数を定義体標数としている [4]．

曲線 P-192: $p_{192} = 2^{192} - 2^{64} - 1$
曲線 P-224: $p_{224} = 2^{224} - 2^{96} + 1$
曲線 P-256: $p_{256} = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$
曲線 P-384: $p_{384} = 2^{384} - 2^{128} - 2^{96} + 2^{32} - 1$
曲線 P-521: $p_{521} = 2^{521} - 1$

例えば p_{192} による剰余算は，$2^{192} \equiv 2^{64} + 1 \bmod p_{192}$ であることを利用すると，Algorithm 1 のように除算無しで高速に行える．

さらに，例えば $2 \times a \bmod p_{192}$ を計算する場合は，Algorithm 1 において $c_3 = 1$ (シフトによるキャリーがあった場合)，$c_4 = 0$，$c_5 = 0$ となるので，a の最下位ビット (0 番目のビット) と 64 番目のビットにそれぞれ 1 を加算するだけの簡単な処理となる．

Algorithm 1 Fast reduction modulo $p_{192} = 2^{192} - 2^{64} - 1$

`Input` an integer $c = (c_5, c_4, c_3, c_2, c_1, c_0)$, where each c_i is a 64-bit word, and $0 \le c < p_{192}^2$.
`Output` $c \bmod p_{192}$.

1. `Define 192-bit integers:`
   $s_0 = (c_2,\ c_1,\ c_0)$
   $s_1 = (\ 0,\ c_3,\ c_3)$
   $s_2 = (c_4,\ c_4,\ 0\ )$
   $s_3 = (c_5,\ c_5,\ c_5)$
2. `return` $s_0 + s_1 + s_2 + s_3 \bmod p_{192}$

3 楕円点倍算に対する電力解析

ディジタル署名生成や，復号，鍵共有などで実行される楕円点倍算は，ユーザプライベート鍵などの秘密情報を用いる．したがって，楕円点倍算はサイドチャネル解析の対象となり，電力解析に関しても様々な解析法や対策法が提案されている．

単純電力解析 (SPA): SPA は，演算手順が秘密べき指数の値に依存している時可能となる．例えば，Algorithm 2 に示す左バイナリ法は，秘密べき指数 k のビットが 1 の時のみ点加算を実行する．したがって，点加算と点 2 倍算のシーケンスが電力解析により識別できれば，k を導出可能となる．

SPA 対策には，Algorithm 3 に示した Double-and-Add always 法や Montgomery ladder など，加算鎖を秘密べき指数に依存させずに一定にする方法がある [2, 10, 11]，

差分電力解析 (DPA): DPA では，解析者は複数の入力に対して消費電力を測定し，秘密情報の推測を行う．秘密情報の推測値が正しいかどうかを，測定した消費電力を用いて判定する [8]．DPA が可能となるためには，暗号演算中のある中間値が，暗号演算への既知の入力と，秘密情報 (の一部) に依存して決まる必要がある．したがって，DPA 対策としては，乱数を用いて何らかのランダム化を行い，暗号演算中の中間値が，既知の入力と秘密情報 (の一部) とから一意に決まらないようにす

ることが一般的である．楕円点倍算の DPA 対策には，入力点のランダム化 (ランダム化射影座標) やべき指数のランダム化などがある [2].

ランダム化射影座標法は，射影座標系 $(x, y) \leftarrow (X/Z, Y/Z)$ において，$\theta \in \mathbb{F}_p^\times$ に対して点 $(X : Y : Z)$ と点 $(\theta X : \theta Y : \theta Z)$ が等価であることを利用する．まずランダムに $\theta \in \mathbb{F}_p^\times$ を生成し，入力点 (x, y) を射影座標表現 $(\theta x, \theta y, \theta)$ に変換してから楕円点倍算を実行する．楕円点倍算処理中の中間値は，入力点と秘密情報とだけからでは決まらない乱数の影響を受けているため，DPA 対策となる．

改良電力解析 (RPA)，ゼロ値解析 (ZRA): DPA 対策としてランダム化射影座標を用いた場合でも，使用された乱数に影響されない不変な性質を持つ中間変数が存在し得ることが指摘された [5]．例えば，ある座標値が 0 であった場合，ランダム化しても 0 であり続ける．RPA[5] とその拡張である ZRA[1] は，不変な中間変数の性質として，点の座標値が 0 であることや，点 2 倍算や点加算中の中間値が 0 であることを利用する．これら不変な性質を持つ中間変数が存在し，電力解析などにより解析者がその中間変数の出現を認識できると，秘密べき指数の導出が可能となる．解析法の詳細は次章で述べる．

RPA や ZRA に対する対策には，ランダム化初期点を用いる方法がある [7, 9].

Algorithm 2 Left-to-right binary method

Input a point P, an integer k, where $k = (k_{t-1}k_{t-2}\cdots k_0)_2$
Output kP

1. $R \leftarrow \mathcal{O}$
2. for i from $t-1$ down to 0
3. $\quad R \leftarrow 2R$
4. $\quad$ If $k_i = 1$ then
5. $\quad\quad R \leftarrow R + P$
6. $\quad$ end if
7. end for
8. return R

Algorithm 3 Double-and-Add always method

Input a point P, an integer k, where $k = (k_{t-1}k_{t-2}\cdots k_0)_2$
Output kP

1. $R[0] = \mathcal{O}$
2. for i from $t-1$ down to 0
3. $\quad R[0] \leftarrow 2R[0]$
4. $\quad R[1] \leftarrow R[0] + P$
5. $\quad R[0] \leftarrow R[k_i]$
6. end for
7. return $R[0]$

4 特殊な性質を持つ中間変数を利用した電力解析法

本章では，楕円点倍算において，入力点のランダム化に対して不変な性質を持つ中間変数を利用した電力解析法を述べる．$p > 3$ を素数とし，$a, b \in \mathbb{F}_p$，$4a^3 + 27b^2 \neq 0$ とする．次に示す素体 $\mathbb{F}_p$ 上楕円曲線 E を対象とする．

$$E : y^2 = x^3 + ax + b \tag{2.21}$$

素体 $\mathbb{F}_p$ 上楕円曲線として NIST が推奨する曲線，Jacobian 座標，を用いた場合において，ランダム化に依存しない特殊な性質を持つ中間が存在することを示す.

4.1 解析法の一般的枠組み

楕円点倍算中に現れるある特殊な性質を持つ点 P_0 の出現を認識できると仮定する．この認識は，例えば電力解析などによってランダムな点と識別することにより行う．特殊な性質を持つ点を認識することを利用した解析法が Goubin によって提案され [5]，その後いくつかの拡張が行われてい

る [1, 3]．これら，特殊な性質を持つ点を利用した解析法の一般的枠組みを以下に記述する．

楕円点倍算 Algorithm 3 への入力を P, $k = (k_{t-1}k_{t-2}\dots k_0)_2$ とする．$K_j = \sum_{i=t-1-j}^{t-1} k_i 2^{i-(t-1-j)}$ とすると，j 番目のループ終了時には，次の点 K_jP が計算されているはずである．

$$K_jP = \sum_{i=t-1-j}^{t-1} k_i 2^{i-(t-1-j)} P$$

したがって，n をベースポイントの位数とすると，点 $(K_j^{-1} \bmod n)P_0$ を入力点とすれば，j 番目のループ終了時に点 P_0 が現れる．

よって，k の上位ビット $K_{j-1} = (k_{t-1}\dots k_{t-j})$ が既知であると仮定すると，次のビット k_{t-1-j} は次のようにして推測することができる．

- $k_{t-1-j} = 0$ つまり $K_j = 2K_{j-1}$ と仮定する．点 $(K_j^{-1} \bmod n)P_0$ を入力点として与えた時，もし点 P_0 が認識できれば，$k_{t-1-j} = 0$ という仮定は正しいと判断する．
- もし認識できなければ，$k_{t-1-j} = 1$ つまり $K_j = 2K_{j-1} + 1$ と判断する．

以上の操作を k の上位ビットから繰り返せば，秘密べき指数 k の全ビットを推測することができる．

4.2 ハミング重みに関する相関

素体 $\mathbb{F}_p$ 上の NIST 推奨楕円曲線において，Dupuy らはアファイン座標系で表現した場合に，

$$P_0 = (2^\lambda, y),\ \lambda \text{は小さい非負整数}$$

となる点を，特殊な点 P_0 として考察した [3] [1]．

射影座標系 $(x, y) \leftarrow (X/Z, Y/Z)$ を用いると，ランダムな $\theta \in \mathbb{F}_p^\times$ に対して，λ が小さな非負整数の場合，$X = 2^\lambda\theta$ と $Z = \theta$ とのハミング距離は小さくなる可能性が高い．ハミング距離が小さくなるのは，NIST 推奨の素体 $\mathbb{F}_p$ 上楕円曲線が (SECG など他の機関の推奨楕円曲線も)，定義体標数 p として *sparse* な素数を用いていることが大きく影響している．

[1] 文献 [3] では，標数 2 拡大体 $\mathbb{F}_{2^m}$ 上楕円曲線についても議論されている．$\mathbb{F}_{2^m}$ 上の場合は，特殊な点として，点 $P_0 = (x^\lambda, y)$ が考察されている．

例えば $\lambda = 1$ の場合，第 2 章で述べたように，$2\theta \bmod p_{192}$ の計算は，θ を 1 ビット左シフトした時にキャリーが生じた場合に限り，θ の 0 番目のビットと 64 番目のビットに 1 を加算することにより行われる．よって，$X = 2\theta$ と $Z = \theta$ のハミング距離は小さいと期待できる．ハミング距離の詳細な評価は文献 [3] を参照のこと．

本稿における以下の議論では，上記 P_0 は認識可能な特殊な性質を持つと仮定する．楕円点倍算の途中で P_0 が現れるような入力点を与えると，4.1 節で述べた手法により秘密べき指数を導出することができる．

4.3 解析対象の実装

本稿で解析対象とするデバイスの実装は，次の特徴を持つと仮定する．

- 素体 $\mathbb{F}_p$ 上 NIST 推奨楕円曲線を用いる．すなわち，定義体標数 p は sparse な素数である．
- 楕円点倍算中，点は Jacobian 座標 $(x, y) \leftarrow (X/Z^2, Y/Z^3)$ で表現する．
- 入力点はランダム化する．すなわち入力点 (x, y) は，ランダムに生成された $\theta \in \mathbb{F}_p^\times$ を用いて，$(\theta^2 x, \theta^3 y, \theta)$ と変換する．
- 加算鎖のランダム化等，計算手順のランダム化は行わない．
- 楕円点倍算には Double-and-Add always 法 (Algorithm 3) を用いる．
- 楕円点 2 倍算は，Algorithm 4 に示す計算手順で実行する．

IEEE 1363-2000 に記述されている素体 $\mathbb{F}_p$ 上楕円曲線 Jacobian 座標系における点 2 倍算アルゴリズムを Algorithm 4 に示す [6]．ただし，入力点が無限遠点 $\mathcal{O}$ だった場合などに必要な例外処理は記述を省略した．また，一般の a に対するアルゴリズムを記述したが，NIST 推奨楕円曲線は全て $a = -3$ である．

Algorithm 4 Point doubling in terms of Jacobian coordinates

Input $P_1(X_1, Y_1, Z_1) \in E(\mathbb{F}_p)$

Output $P_2(X_2, Y_2, Z_2) = 2P_1$

1. $T_1 \leftarrow X_1$
2. $T_2 \leftarrow Y_1$
3. $T_3 \leftarrow Z_1$
4. if $a = -3$ then
5. $\quad T_4 \leftarrow T_3^2$
6. $\quad T_5 \leftarrow T_1 - T_4$
7. $\quad T_4 \leftarrow T_1 + T_4$
8. $\quad T_5 \leftarrow T_4 \times T_5$
9. $\quad T_4 \leftarrow 3 \times T_5$
10. else
11. $\quad T_4 \leftarrow a$
12. $\quad T_5 \leftarrow T_3^2$
13. $\quad T_5 \leftarrow T_5^2$
14. $\quad T_5 \leftarrow T_4 \times T_5$
15. $\quad T_4 \leftarrow T_1^2$
16. $\quad T_4 \leftarrow 3 \times T_4$
17. $\quad T_4 \leftarrow T_4 + T_5$
18. end if
19. $T_3 \leftarrow T_2 \times T_3$
20. $T_3 \leftarrow 2 \times T_3$
21. $T_2 \leftarrow T_2^2$
22. $T_5 \leftarrow T_1 \times T_2$
23. $T_5 \leftarrow 4 \times T_5$
24. $T_1 \leftarrow T_4^2$
25. $T_1 \leftarrow T_1 - 2 \times T_5$
26. $T_2 \leftarrow T_2^2$
27. $T_2 \leftarrow 8 \times T_2$
28. $T_5 \leftarrow T_5 - T_1$
29. $T_5 \leftarrow T_4 \times T_5$
30. $T_2 \leftarrow T_5 - T_2$
31. $X_2 \leftarrow T_1$
32. $Y_2 \leftarrow T_2$
33. $Z_2 \leftarrow T_3$
34. return (X_2, Y_2, Z_2)

4.4 Jacobian 座標系点 2 倍算における特殊な中間変数

本節では，前節で述べた実装に対し，点のランダム化にも関わらず点 2 倍算中に現れる特殊な性質を持つ中間変数について考察する．前述のように，このような中間変数が存在すれば，電力解析が可能となる．

特殊な性質を持つ点として次がすでに考察されている [1, 5] [2].

特殊点 1: 点の座標値が 0 の点，および点 2 倍算中の中間変数が 0 となる点.

点 P_0 が上記特殊点 1 である必要十分条件は，次の条件 C1∼C5 のいずれか 1 つを満たすことである [1].

C1. $x = 0$ または $2P_0$ の x 座標が 0
C2. $y = 0$ または $2P_0$ の y 座標が 0
C3. P_0 の位数が 3
C4. $3x^2 + a = 0$
C5. $5x^4 + 2ax^2 - 4bx + a^2 = 0$

また，[3] においては，NIST 推奨曲線の定義体標数 p が sparse であることに着目し，特殊な性質を持つ点として次が考察された.

特殊点 2: 射影座標表現において X 座標と Z 座標とのハミング距離が小さくなるような点 $P_0 = (x, y)$.

我々は，点 2 倍算 (Algorithm 4) 中の中間変数に着目し，上記概念を次のように拡張する.

特殊点 3: 点 2 倍算 (Algorithm 4) の演算中，中間変数 T_i のうち，ハミング距離が小さい T_i の組が存在するような点 $P_0 = (x, y)$.

[2] [1] では，点 2 倍算だけでなく，点加算中の中間変数についても検討されている.

定義より，特殊点 2 は特殊点 3 に含まれる．特殊点 3 が電力解析などによりランダムな点と識別できると仮定すれば，電力解析が可能となる．次に，Algorithm 4 中に上記特殊点 3 が存在することを示す．

特殊点 $P_0 = (x, y)$ は，楕円点倍算中，ランダムな $Z \in \mathbb{F}_p^\times$ に対して $P_0 = (Z^2x, Z^3y, Z)$ と表現されているものとする．Algorithm 4 では，x 座標に関して次の計算を行っている．

X1. $T_1 = Z^2x$ (step 1)

X2. $T_4 = Z^2$ (step 5)

X3. $T_5 = Z^2(x-1)$ (step 6)

X4. $T_4 = Z^2(x+1)$ (step 7)

$x = 2^\lambda$，λ は小さい非負整数，とすれば標数 p が sparse なため，式 X1 と X2 における T_1 と T_4 のハミング距離は小さくなる確率が高い．また，$x = 2^\lambda + 1$，λ は小さい非負整数，とすれば $x - 1 = 2^\lambda$，$x + 1 = 2^{\lambda+1}$ であるから，式 X3 と X4 における T_5 と T_4 のハミング距離は小さくなる確率が高い．(詳細な確率評価は今後の課題である．)

次に，y 座標に関しては次の計算を行っている．

Y1. $T_3 = Z^4y$ (step 19)

Y2. $T_3 = Z^42y$ (step 20)

よって，$y = 2^\lambda$，λ は小さい非負整数，とすれば式 Y1 と Y2 における T_3 と T_3 のハミング距離は小さくなる確率が高い．

以上より，特殊点 3 として次の 3 種類が存在することがわかる．

1. $P_0 = (2^\lambda, y)$
2. $P_0 = (2^\lambda + 1, y)$
3. $P_0 = (x, 2^\lambda)$

Algorithm 4 の step 21 以降は，全ての中間値 T_i は，X 座標値と Y 座標値との積に依存する値，または，X 座標値または Y 座標値の奇数倍となるため，ハミング距離が小さい T_i の組は現れない．

なお，$a \neq -3$ の場合は次の計算が行われる．

X′1. $T_5 = Z^4$ (step 13)

X′2. $T_4 = Z^4x^2$ (step 15)

よって，$x = 2^\lambda$，λ は小さい非負整数，とすれば式 X′1 と X′2 における T_5 と T_4 のハミング距離は小さくなる確率が高い．

素体 $\mathbb{F}_p$ 上楕円曲線 (式 (2.21)) においては，点 $(2^\lambda, y)$ は $2^3\lambda + a2^\lambda + b$ が平方剰余の時，点 $(2^\lambda + 1, y)$ は $(2^\lambda + 1)^3 + a(2^\lambda + 1) + b$ が平方剰余の時に存在する．5 つの素体 $\mathbb{F}_p$ 上 NIST 推奨楕円曲線においては，いずれの曲線も小さい非負整数 λ に対して解を持つ．λ が最小な $(2^\lambda, y)$ と $(2^\lambda + 1, y)$ を付録 5 に示す．

5 まとめ

本稿では，楕円点倍算の DPA 対策であるランダム化射影座標を用いた実装に対する電力解析を考察した．素体 $\mathbb{F}_p$ 上 NIST 推奨楕円曲線による楕円点倍算を，Jacobian 座標系による点の表現とランダム化射影座標とを用いて実装した場合，点 $(2^\lambda, y)$，点 $(2^\lambda + 1, y)$，点 $(x, 2^\lambda + 1)$ λ は小さい非負整数，はランダム化の影響を受けない特殊な性質を持つこと，すなわち，ハミング距離が小さくなる中間変数が現れることを示した．この中間変数を利用して，選択入力解析によって秘密べき指数を導出可能となる．

ハミング距離に関する詳細な評価，および標数 2 拡大体 $\mathbb{F}_{2^m}$ 上楕円曲線に対する中間変数の評価は今後の課題である．

本稿で述べた解析法の対策としては，べき指数のランダム化などの暗号処理手順のランダム化や，ランダム化初期点法 [7, 9] などが考えられる．

参考文献

[1] T. Akishita and T. Takagi, “Zero-value resister attack on elliptic curve cryptosystems,” IEICE, Trans. Fundamentals, vol. E88-A, No.1, pp.132–139, 2005.

[2] J.-S. Coron, “Resistance against differential power analysis for elliptic curve cryptosystems,” Cryptographic Hardware and Embedded Systems – CHES ’99, LNCS 1717, pp.292–302, Springer-Verlag, 1999.

[3] W. Dupuy and S.K. Jacques, “Resistance of randomized projective coordinates against power analysis,” Cryptographic Hardware and Embedded Systems – CHES 2005, LNCS 3659, pp.1–14 Springer-Verlag, 2005.

[4] “Digital signature standard (DSS),” FIPS PUB 186-2, U.S. National Institute of Standards and Technology, 2000.

[5] L. Goubin, “A refined power-analysis attack on elliptic curve cryptosystems,” Public Key Cryptography – PKC 2003, LNCS 2567, pp.199–211, Springer-Verlag, 2003.

[6] IEEE 1363-2000, “Standard Specifications for Public Key Cryptography,” 2000.

[7] 伊藤，伊豆，武仲，“ランダム化初期点を用いた電力解析対策法について (その 3),” SCIS 2005.

[8] P.C. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” Advances in Cryptology – CRYPTO’99, LNCS 1666, pp.388–397, Springer-Verlag, 1999.

[9] M. Mamiya, A. Miyaji, and H. Morimoto, “Efficient countermeasure against RPA, DPA, and SPA,” Cryptographic Hardware and Embedded Systems – CHES 2004, LNCS 3156, pp.343–356, Springer-Verlag, 2005.

[10] P. Montgomery, ”Speeding the Pollard and elliptic curves methods of factorization,” Math. Comp, vol. 44, 1985.

[11] K. Okeya and T. Takagi, “SCA-resistant and fast elliptic scalar multiplication based on wNAF,” IEICE, Trans. Fundamentals, vol. E87-A, No.1, pp.75–84, 2004.

[12] J.A. Solinas, “Generalized Mersenne numbers,” Technical Report CORR 99-39, University of Waterloo, 1999.

付録：素体 $\mathbb{F}_p$ 上の NIST 推奨楕円曲線上の点 $(2^\lambda, y)$ および $(2^\lambda + 1, y)$

素体 $\mathbb{F}_p$ 上 NIST 推奨楕円曲線上に存在する点 $(2^\lambda, y)$ および $(2^\lambda + 1, y)$ のうち，非負整数 λ が最小である点を以下に示す.

P-192:

$x = 2$

y = 2df5fa08 ab474e8f 8f2ad5ca ca826434
7d1fb300 43214687

$x = 3$

y = 64fc66b7 c0f932d5 564fa514 b3ba7858
c8ee083f 8c728022

P-224:

$x = 8$

y = 2f2754f8 eca72d77 84910c31 1e78caf3
88d07390 3d01dba6 956fb093

$x = 3$

y = 8353d963 9842aa15 eb1000b1 52101a17
b687aeb5 0eb37705 4b913fbb

P-256:

$x = 8$

y = b706288a ca290db0 d624d1d2 3f37f6a6
27249b16 d631ff69 2242d085 636041b3

$x = 5$

y = 459243b9 aa581806 fe913bce 99817ade
11ca503c 64d9a3c5 33415c08 3248fbcc

P-384:

$x = 2$

y = 8cdeadbb d04911a3 c1931e26 df3fa643
9dca9c7e b286fbd4 6fc319f0 e2bb7802
32baf578 25fc0c19 12ada2fe fe84024c

$x = 3$

y = 6660041b 1c798462 0e8d7fd7 ccdb50cc
3ba816da 14d41a4d 8affaba8 488867f0
ca5a24f8 d42dd7e4 4b530a27 dc5b58da

P-521:

$x = 2$

y = d9 254fdf80 0496acb3 3790b103
c5ee9fac 12832fe5 46c63222 5b0f7fce
3da4574b 1a879b62 3d722fa8 fc34d5fc
2a8731aa d691a9a8 bb8b554c 95a051d6
aa505acf

$x = 1$

y = 10 e59be93c 4f269c02 69c79e2a
fd65d6ae aa9b701e acc194fb 3ee03df4
7849bf55 0ec636eb ee0ddd4a 16f1cd94
06605af3 8f584567 770e3f27 2d688c83
2e843564

研究業績一覧

学術論文

1. Yasuyuki Sakai, Kouichi Sakurai:
" Simple Power Analysis on Fast Modular Reduction with Generalized Mersenne Prime for Elliptic Curve Cryptosystems," ", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences,, E89A, No. 1, pp.231–237, Jan.2006.
概要: We discuss side channel leakage from modular reduction for NIST recommended domain parameters. FIPS 186-2 has 5 recommended prime fields. These primes have a special form which is refered to as generalized Mersenne prime. These special form primes facilitate especially efficient implementation. A typical implementation of efficient modular reduction with such primes includes conditional reduction. A conditional reduction in modular reduction can constitute an information channel on the secret exponent. Several researchers have produced unified code for elliptic point addition and doubling in order to avoid a simple power analysis (SPA). However, Walter showed that SPA still be possible if Montgomery multiplication with conditional reduction is implemented within the unified code. In this paper we show SPA on the modular reduction with NIST recommended primes, combining with the unified code for elliptic point operations. As Walter stated, our results also indicate that even if the unified codes are implemented for elliptic point operations, underlying field operations should be implemented in constant time. The unified approach in itself can not be a countermeasure for side channel attacks.

2. Katja Schmidt-Samoa, Olivier Semay, and Tsuyoshi Takagi:

"Analysis of Fractional Window Recoding Methods and Their Application to Elliptic Curve Cryptosystems", IEEE TRANSACTIONS ON COMPUTERS,, VOL. 55, NO. 1,, JANUARY 2006.

概要: Elliptic curve cryptosystems (ECC) are suitable for memory-constraint devices like smart cards due to their small key-size. A standard way of computing elliptic curve scalar multiplication, the most frequent operation in ECC, is window methods, which enhance the efficiency of the binary method at the expense of some precomputation. The most established window methods are sliding window on NAF (NAF+SW), wNAF, and wMOF, where NAF and MOF are acronyms for nonadjacent form and mutually opposite form, respectively. A common drawback of these schemes is that only a small portion of the numbers are possible sizes for precomputation tables. Therefore, in practice, it is often necessary to waste memory because there is no table fitting exactly the available storage. In the case of wNAF, there exists a variant that allows arbitrary table sizes, the so-called fractional wNAF (Frac-wNAF). In this paper, we give a comprehensive proof using Markov theory for the estimation of the average nonzero density of the Frac-wNAF representation. Then, we propose the fractional wMOF (Frac-wMOF), which is a left-to-right analogue of Frac-wNAF. We prove that Frac-wMOF inherits the outstanding properties of Frac-wNAF. However, because of its left-to-right nature, Frac-wMOF is preferable as it reduces the memory consumption of the scalar multiplication. Finally, we show that the properties of all discussed previous schemes can be achieved as special instances of the Frac-wMOF method. To demonstrate the practicability of Frac-wMOF, we develop an on-the-fly algorithm for computing elliptic curve scalar multiplication with a flexibly chosen amount of memory.

研究会等

1. Tatsuya Toyofuku and Toshihiro Tabata and Kouichi Sakurai:
   " Program Obfuscation Scheme Using Random Numbers to Complicate Control Flow", The First International Workshop on Security in Ubiquitous Computing Systems (SECUBIQ 2005) in EUC Workshops 2005, Springer LNCS, pp.916-925, 2005 Dec..
   概要: For the security technology that has been achieved with software in the computer system and the protection of the intellectual property right of software, software protection technology is necessary. One of those techniques is called obfuscation, which converts program to make analysis difficult while preserving its function. In this paper, we examine the applicability of our program obfuscation scheme to complicate control flow and study the tolerance against program analysis.

2. Yasuyuki Sakai, Kouichi Sakurai,:
   ""Simple Power Analysis on Fast Modular Reduction with NIST Recommended Elliptic Curves,"", ICICS 2005, Springer LNCS, pp.169-180, 2005.
   概要: We discuss side c hannel leakage from modular reduction for NIST recommended domain parameters. FIPS 186-2 has 5 recommended prime fields. These primes have a special form which is referred to as generalized Mersenne prime. These special form primes facilitate especially efficient implementation. A typical implementation of efficient modular reduction with such primes includes extra reduction. The extra reduction in modular reduction can constitute an information channel on the secret

exponent. Several researchers have produced unified code for elliptic point addition and doubling in order to avoid a simple power analysis (SPA). However,Walter showed that SPA still be possible if Montgomery multiplication with extra reduction is implemented within the unified code. In this paper we show SPA on the modular reduction with NIST recommended primes, combining with the unified code for elliptic point operations. As Walter stated, our results also indicate that even if the unified codes are implemented for elliptic point operations, underlying field operations should be implemented in constant time. The unified approach in itself cannot be a countermeasure for side channel attacks.

学会大会等

1. 酒井 康行:
“”ランダム化射影座標を用いた楕円曲線暗号実装に対する電力解析,””, 2006 年暗号と情報セキュリティシンポジウム (SCIS 2006),, Jan. 2006. 楕円曲線暗号実装に対する電力解析について考察する．差分電力解析対策の 1 つに，入力点のランダム化 (ランダム化射影座標) があるが，適切な入力点を与えると，ランダム化にも関わらず，楕円点倍算の途中でランダム化の影響を受けないある種の特徴を持つ中間変数が現れることがある．このような中間変数が存在すると，電力解析可能となる場合があることが知られている．本稿では，このような中間変数の存在について考察する．素体 $\mathbb{F}_p$ 上の NIST 推奨楕円曲線を，Jacobian 座標系，単純電力解析対策法である Double-and-Add always 法，差分電力解析対策法であるランダム化射影座標法，とを組み合わせて実装した場合，楕円点倍算中の点 2 倍算中に，ハミング重みに強い相関を持つ中間変数がいくつか存在することを示す．

C01: グラフ描画アルゴリズムとそのWeb情報検索への応用

西関 隆夫 † 周 暁 † 三浦 一之 ‡ 浅野 泰仁 †

† 東北大学 大学院 情報学研究科
〒 980-8579 仙台市青葉区荒巻字青葉 6-6-05
{nishi,zhou}@ecei.tohoku.ac.jp,
asano@nishizeki.ecei.tohoku.ac.jp

‡ 福島大学 共生システム理工学類
〒〒 960-1296 福島市金谷川 1 番地
miura@sss.fukushima-u.ac.jp

1 はじめに

本研究課題の本年度の研究成果概要は以下の通りである.

(1) グラフの隣接する点・辺が異なる色になるように，それぞれの点・辺に予め与えた色候補リストの中から選んだ色で塗り分けるリスト全彩色問題について研究し，直並列グラフがリスト全彩色を持つための色候補リストのサイズの下限を与えた.

(2) 平面的グラフの折れ曲がりなし直交描画問題について，グラフが 3 連結立方グラフの細分であれば，折れ曲がりなし直交描画を線形時間で求めることのできるアルゴリズムを提案した.

(3) 平面グラフの格子凸描画において，別個に研究されてきた標準分解，リアライザ，シュナイダーラベリング，順序つき全域木がすべて同等であることを証明した.

(4) 電力供給問題のモデル化であり，一般には強 NP 困難問題として知られる，需要・供給付きグラフの分割問題について研究し，分割数を最少・最多にする問題および与えられた数の分割を求める問題に対して，グラフが木 (または部分 k-木) であるときに厳密解を求める多項式時間 (または擬似多項式時間) アルゴリズムを提案した.

(5) 不正コピーを防ぐ目的で作成された電子透かしに対して，複数の犯罪者が結託して電子透かしの一部を発見・改ざんするという結託攻撃が問題になっている．本研究では，結託攻撃に対する電子透かしの安全性を評価する手法を提案し，犯罪者を特定できる条件を示すことに成功した.

(6) 購入した計算機を用いてウェブ文書データを解析し，サイトのデータを抽出し，このデータからサイトを点とするサイト間グラフを構築した．さらに，サイト間グラフの特徴を利用して，著名な情報検索手法である max-flow based method の品質を大幅に改善する手法を確立し，実験によってその性能を検証した.

(7) 選挙区分割に応用できる問題である，グラフの均一分割問題を研究した．均一分割問題は，各点に重みの付いたグラフが与えられ，それをいくつかの連結成分に分解し，各成分に属する点の重みの合計が与えられた範囲に収まっているようにする問題である．本研究では，直並列グラフに対し，均一分割問題を擬多項式時間で解くアルゴリズムを与えた．さらに，このアルゴリズムが部分 k-木に拡張できることを示した.

以下，各節において，順に (1)–(7) の各成果について述べる.

2 リスト全彩色

点集合 V, 辺集合 E からなるグラフを $G = (V, E)$ と書く．また, $V = V(G)$, $E = E(G)$ とも書くことがある．多重辺やループを含まないグラフを **単純グラフ** という．グラフ $G = (V, E)$ の **全彩色** とは, 隣接する任意の 2 点, 端点を共有する任意の 2 辺, 任意の点とそれに接続する任意の辺が異なる色になるように, G のすべての点と辺に彩色することである．したがって全彩色は

$V \cup E$ から色集合 C への写像 $f : V \cup E \to C$ である．グラフ G における点 v の次数を $d(v, G)$ と書く．また G の最大次数を $\Delta(G)$ と書く．グラフ G を全彩色するのに必要な最少色数を $\chi_t(G)$ とすると，明らかに $\chi_t(G) \geq \Delta(G) + 1$ である．写像 $L : E \cup V \to 2^C$ を G のリストという．L に対するグラフ G の **リスト全彩色** $f : V \cup E \to C$ とは，各要素 $x \in V \cup E$ に対して $f(x) \in L(x)$ なる G の全彩色である．このような G のリスト全彩色を G の L-**全彩色** ともいう．リスト全彩色は全彩色の一般化である．リスト全彩色問題とは，グラフ G がリスト全彩色をもつかどうかを判定する問題である．図 2.1 はグラフ G とリスト L が与えられたときのリスト全彩色の例である．

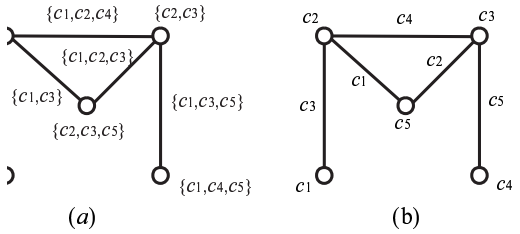


図 2.1: (a) グラフ G とリスト L　(b) リスト全彩色の例

直並列グラフとは 4 点からなる完全グラフ K_4 の細分を部分グラフとしてもたないグラフである．本研究では，直並列グラフにおいてさえ，リスト全彩色問題が NP 完全であることを証明した．また，直並列グラフがリスト全彩色をもつ十分条件を与えた．すなわち，直並列グラフ G の各点 u に $|L(u)| \geq \min\{5, \Delta(G) + 1\}$，各辺 $e = vw$ に $|L(e)| \geq \max\{5, d(v) + 1, d(w) + 1\}$ を満たすリストが与えられたとき，グラフ G にはリスト全彩色が存在するという定理を証明した．ここで $\Delta(G)$ はグラフ G の最大次数であり，$d(v)$,$d(w)$ は点 v, w の次数である．この定理から，$\Delta(G) \geq 4$ の直並列グラフ G は $\Delta(G) + 1$ 色で全彩色できることも証明できた．最後に，直並列グラフ G に十分条件を満足するリストが与えられたとき，G のリスト全彩色を求める線形時間アルゴリズムを構築した．以下はそのアルゴリズムの概要である．

Algorithm List Total Color(G, L)

1. グラフ G において図 2.2 に示されている部分構造 (a)–(e) を探す;
2. Step 1 で見つけた部分構造により適切に部分グラフ G' と H をつくる;
3. 帰納的に部分グラフ G' のリスト全彩色 φ' を求める;
4. 部分グラフ H のリスト全彩色 φ_H を求める;
5. φ' と φ_H をグラフ G のリスト全彩色 φ に拡張する．

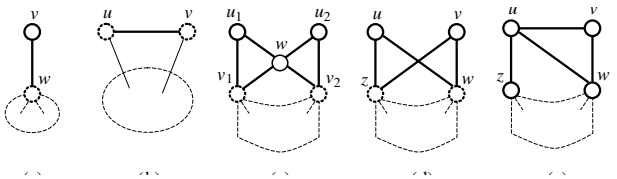


図 2.2: 直並列グラフの部分構造.

3 直並列グラフの折れ曲がりなし直交描画

グラフ G が (始点 v_{in} と終点 v_{out} をもつ) **直並列グラフ**であるとは，$G = (V, E)$ が 1 本の辺によってつながっている点のペア 1 つからなる (Fig. 2.3(a) 参照) か，あるいは 2 つの直並列グラフ $G_i = (V_i, E_i), i = 1, 2$ (始点はそれぞれ $v_{in,i}$, 終点はそれぞれ $v_{out,i}$) を $V = V_1 \cup V_2, E = E_1 \cup E_2$ かつ下の (1), (2) どちらかを満たすようにつなげたものになっている

(1) $v_{in} = v_{in,1}$, $v_{out,1} = v_{in,2}$, v_{out2}, $= v_{out}$ (Fig. 2.3(b) 参照),

(2) $v_{in} = v_{in,1} = v_{in,2}$, $v_{out} = v_{out,1} = v_{out,2}$ (Fig. 2.3(c 参照).

かどちらかである．Fig. 2.3(d) のグラフは，直並列グラフの一例である．

直並列グラフは平面的グラフでもある．**平面的グラフ**とは，平面に辺を交わることなく描画可能なグラフであり，その描画は通常何通りもある．平面グラフとは，平面的グラフの点と辺で囲ま

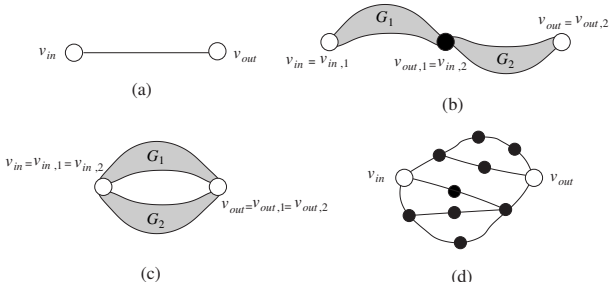


図 2.3: (a) もっとも単純な直並列グラフ, (b) 直列結合, (c) 並列結合 (d) 直並列グラフ.

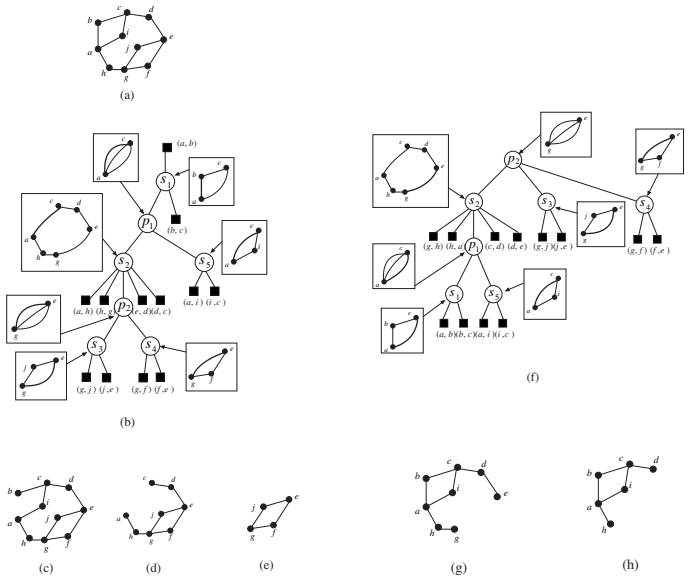


図 2.4: (a) 最大次数 3 の 2 連結グラフ G, (b) G の SPQ-tree $\mathcal{T}$, (c) S-node s_1 に関連づけられたグラフ, (d) s_2 に関連づけられたグラフ, (e) P-node p_2 に関連づけられたグラフ, (f) $\mathcal{T}$ の根を p_2 に置き換えたもの, (g) s_1 に関連づけられたグラフ, (h) その核グラフ.

れる面の位置関係をひとつに定めたものである. したがって，平面的グラフより可能な描画は少ない．平面的グラフの折れ曲がりなし直交描画とは辺を水平線分ないし垂直線分で描いた描画である. Rahman, 西関らは以前，最大次数 3 以下の平面グラフが折れ曲がりなし直交描画をもつための必要十分条件と，その描画を求めるための線形時間アルゴリズムを与えた．しかし，最大次数 3 以下の平面的グラフに関しては，Di Battista らの計算量 $O(n^5 \log n)$ (n はグラフの点数) で折れ曲がりなし直交描画をもつかどうか判定できるという結果しか知られていない.

今回，われわれは最大次数 3 以下の直並列グラフが折れ曲がりなし直交描画をもつかどうか線形時間で判定できるアルゴリズムを与えた.

基本的なアイディアとしては，直並列グラフを Di Battista と Tamassia らによって提案された SPQR 木 (ここではその特殊な場合の SPQ 木) に分解し，その木の葉の方から根に向かって描画を与えてゆく．すなわち，部分的な描画を組み合わせて全体の描画を構築していくことになる．図 2.4 は，SPQ 木の例を示している．各ノードは元のグラフの部分グラフ (厳密には少し異なる) に対応する直並列グラフである.

ここで，各ノードに対応する直並列グラフの描画を考える際に，始点と終点の位置によって，図 2.5 に示される 3 種類のパターンを与える．この 3 パターンのうち，L-shape drawing が可能ならばそうするが，そうでないときには side-on drawing, diagonal drawing の順で優先して描画をしていく．こうすることで，部分の描画と，それを組み合わせて得られる，より大きな部分の描画のパターンを限定することができ，最終的に全体の描画が得られれば与えられた直並列グラフが折れ曲がりなし直交描画可能かどうか判定できるということを示した.

4 平面グラフの格子凸描画

外面を三角形とする格子凸描画とは，図 2.6 のようなものである.

2 連結平面グラフが外面を三角形とする格子凸描画をもつための条件としては，Chrobak, Kant によって提案された標準分解，Di Battista, Tamassia, Vismara によって提案されたリアライザ，Schnyder によって提案されたシュナイダーラベリング，Chiang, Lin, Lu によって提案された順序つき全域木がある．しかし，これらの概念は独立して研究されたもので，一部が等価であることは知られていたものの，すべてが等価であるかどうかは知られていなかった．われわれは本研究において，上記のすべての概念が等価，すなわち与えられたグラフが上記のいずれかをもてば上記

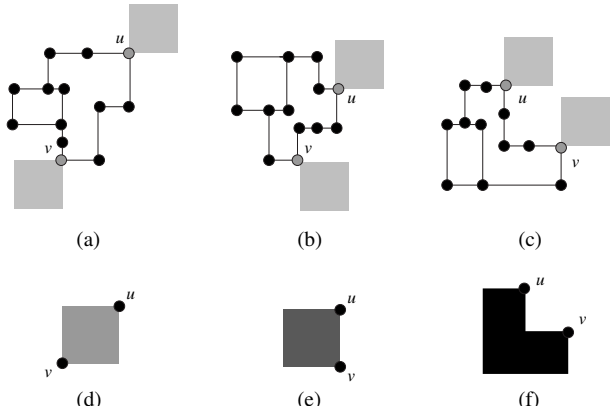


図 2.5: u と v が始点･終点になっているような直並列グラフの描画パターン: (a) diagonal drawing, (b) side-on drawing, (c) L-shape drawing, (d)-(f) それぞれの簡単化したイメージ.

のすべてをもつことを示した.

以下に，参考として，標準分解がどのようなものか記す.

4.1 標準分解

任意の 3 連結平面グラフは標準分解をもつ. **標準分解**とは，グラフの点集合の分割 $\Pi = (V_1, V_2, \cdots, V_h)$ で，以下の性質を満たすものである．なお，グラフの点集合 $V = \{u_1, u_2, \cdots, u_n\}$ のうち 3 点 u_1, u_2, u_n が時計回りに外周上に配置されるものとする．$V_1 \bigcup V_2 \bigcup \cdots \bigcup V_k$ によって誘導される部分グラフを G_k とし，$V_{k+1} \bigcup V_{k+2} \bigcup \cdots \bigcup V_h$ によって誘導される部分グラフを $\overline{G_k}$ とする.

(cd1) V_1 は 外辺 (u_1, u_2) を含んでいる内面の境界上のすべての点からなり，かつ $V_h = \{u_n\}$ である.

(cd2) $1 \leq k \leq h$ の各 k について，G_k は内部 3 連結である.

(cd3) $2 \leq k \leq h$ の各 k について，V_k のすべての点は G_k の外点である．さらに，

(a) もし $|V_k| = 1$ ならば，その唯一の点 w は G_{k-1} 上に 2 つ以上の隣接点をもち，$k < h$ のときは $\overline{G_k}$ 上に 1 つ以上の隣接点をもつ.

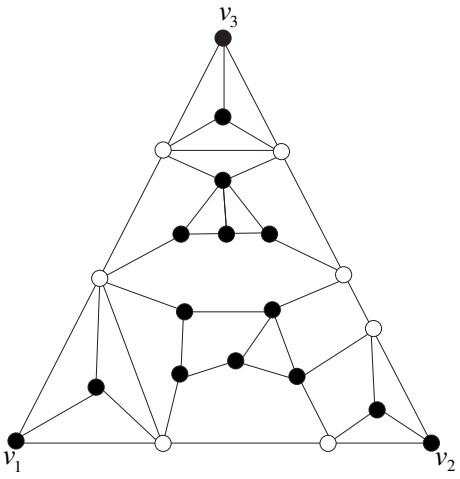


図 2.6: 平面グラフの外面を三角形とする格子凸描画

(b) もし $|V_k| \geq 2$ ならば，V_k の点は G_k の描画上で連続して現れる．さらにその最初の点と最後の点は，G_{k-1} 上の点ひとつずつと隣接する．他の点は G_{k-1} に隣接点をもたない．また，各点は $\overline{G_k}$ 上に 1 つ以上の隣接点をもつ.

図 2.6 で与えられるグラフの標準分解の例を図 2.7 に示す.

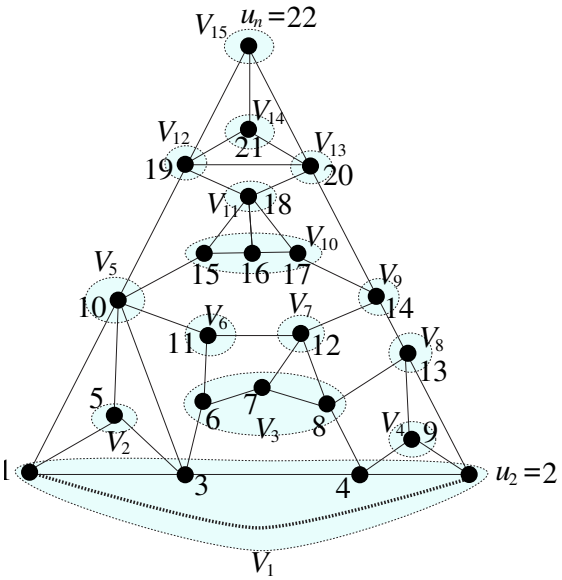


図 2.7: 図. 2.6 のグラフの標準分解 $\Pi = (V_1, V_2, \cdots, V_{15})$.

5　需要点と供給点があるグラフの分割問題

本研究では，需要点と供給点があるグラフの分割問題を扱う．グラフ G の各点は供給点または需要点であるとする．各供給点には供給量と呼ばれる正の実数が割当てられており，各需要点には需要量と呼ばれる正の実数が割当てられている．各需要点は高々1 個の供給点からしか供給を受けることができないとする．したがって，G から何本かの辺を取り除いて G をいくつかの連結成分に分割し，各連結成分には供給点がちょうど 1 個だけあるようにしたい．むろん，その供給量はその連結成分にある需要点の需要量の合計以上でなければならない．与えられたグラフ G に対し，このような分割があるかどうか判定する問題を**分割問題**と呼ぶ．即ち，分割問題は全ての需要点に供給できるような分割が存在するかどうか判定する問題である．例えば，図 2.8(a) のグラフは全ての需要点に供給できるような分割を持つ．ここで，各供給点は四角で描かれ，各需要点は丸で描かれ，供給量と需要量はそれぞれ点の中に書かれ，辺は直線分で描かれ，削除された辺は点線で描かれている．また，各連結成分は点線で囲まれている．

もしグラフ G に全ての需要点に供給できる分割が存在しない場合は，G から何本か辺を取り除いて G をいくつかの連結成分に分割し，各連結成分には供給点がないか，あるいはちょうど 1 個だけあるようにしたい．ただし，供給点のある各連結成分に対してはその供給量はその連結成分にある需要点の需要量の合計以上であるようにし，しかも供給点のある全ての連結成分に含まれる需要点の需要量の合計を最大にしたい．このような最大化問題を**最大分割問題**と呼ぶ．即ち，最大分割問題は供給を受けることができる需要点の需要量の合計を最大化する分割を見つける問題である．図 2.8(b) は，与えられた木に対する最大分割問題の解の一例を示している．この分割において，供給を受けている需要点の需要量の合計は，(2+4+3)+(5+6)+3+(4+6+7) = 40 であり，これがこの木に対しては最大である．

分割問題や最大分割問題は，電力系統の配電融通問題などに応用される．グラフの各供給点は発電所や変電所に対応し，グラフの各需要点は電力の負荷区間に対応する．また，グラフの各辺はスイッチング操作ができる送電線に対応する．したがって，分割問題や最大分割問題は，ある区間で停電が起こった際，スイッチングを再構成して停電を解消する，もしくは停電をできるだけ少なくすることに応用できる．

現在までに非常に多種多様なグラフの分割問題が知られているが，需要点と供給点があるグラフの分割問題は，その重要な応用にもかかわらず現在まで考えられておらず，本研究が世界で初めて定式化した．分割問題は直並列グラフに対して NP 完全であり，したがって直並列グラフに対してさえ多項式時間で解けそうにない．また，分割問題は一般のグラフに対しては強 NP 完全であることが知られており，一般のグラフに対しては擬多項式時間でさえ解けそうにない．一方で，最大分割問題は，木に対してさえ NP 困難であり，一般のグラフに対しては強 NP 困難である．

本研究では，木と呼ばれるグラフのクラスを扱う．木は単純なグラフのクラスの 1 つであるが，ほとんどの電力網は木構造をしているため，応用上最も重要なグラフのクラスである．本研究では，木に対し 3 つのアルゴリズムを与える．1 つ目は，木に対する分割問題を線形時間で解くアルゴリズムである．2 つ目は，全ての需要量と供給量が整数である木に対し，最大分割問題の最適解を擬多項式時間で求めるアルゴリズムである．3 つ目は，全ての需要量と供給量が整数とは限らない木に対し，任意の精度の近似解を多項式時間で求める完全近似スキーム（FPTAS）である．

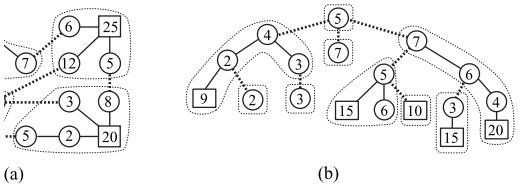


図 2.8: (a) グラフの分割の例，(b) 最大分割問題の解の一例．

6　結託攻撃に耐性のある電子透かし

デジタルデータはコピーが容易であるため，著作権侵害が問題になってきている．この問題に対

処する手法の 1 つが，電子透かしである．電子透かしはデータの内部に埋め込まれるが，電子透かしが埋め込まれたデータを通常の手段で使用しても，電子透かしが埋め込まれていないデータと同様に扱える．例えば，電子透かしが埋め込まれた画像や動画は，表示または再生しても，電子透かしが埋め込まれていないものと見分けがつかないようになっている．電子透かしとして埋め込む情報は，著作者 ID またはユーザー ID が用いられるのが一般的である．前者の場合，データの制作者が，自分がそのデータを作成したことを証明するために使用される．後者は，そのデータの配布者が，そのデータを配布されたユーザーを識別するために用いられる．

ユーザーを識別するために用いられる電子透かしは，結託攻撃を受けることがある．すなわち，複数のユーザーが結託して，彼らが受け取ったデータを照合し，電子透かしが埋め込まれた部分を一部なりとも特定して，その部分を書き換えた後にデータを複製することである．こうすることによって，誰がデータを複製したのか特定することが難しくなるからである．

本研究では，電子透かしの結託攻撃に対する安全性を計る指標として，結託するユーザーの人数の上限を c としたときに，“$(c, p/q)-$ 安全性” を提案する．$(c, p/q)-$ 安全である電子透かしは，結託攻撃によって改ざんされたデータを調べることで，q 人のユーザーの集合のうち，少なくともその中の p 人のユーザーが結託攻撃に参加しているという保証がある集合を必ず発見することができる．また，c を固定したときに，どのような電子透かしを用いても p/q の値をこれ以上大きくできないという上限) を **安全度**と呼び，$s(c)$ で表す．安全度 $s(c)$ の上界と下界に関する既存の結果は少なく，$s(1) = 1/1$, $s(2) = 2/3$, $s(3) = 3/7$ であることは知られているが，$c \geq 4$ のときに関しては，図 2.9 のグラフで三角の点でプロットしてある上界と，四角の点でプロットしてある下界の結果しか得られておらず，上界と下界の差がかけ離れていた．

本研究では，まず安全度 $s(c)$ を達成する電子透かしの特徴付けを行う．さらに，ブロックデザインの性質を利用して，$s(c)$ の上界に関する結果，すなわち $s(c) \leq c/(c^2 - c + 1)$ を示した．図 2.10

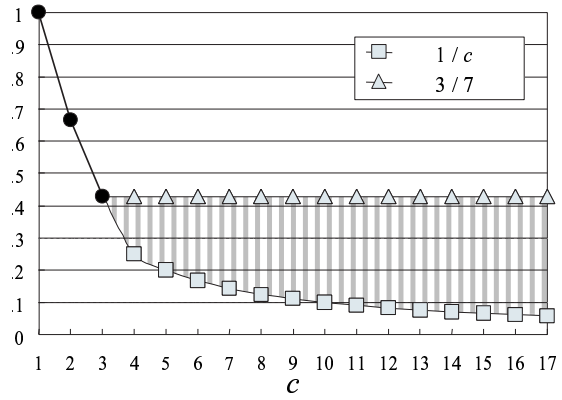


図 2.9: $s(c)$ の上界と下界に関する結果

で表されているように，この上界は既知の下界ときわめて近く，既知の上界と下界のギャップを埋められたことが分かる．また，このことから，c を大きくしていけば，$s(c)$ は $1/c$ に収束していくということがわかる．この事実は，どのような電子透かしを用いても，データの配布者側が改ざんされたデータを調べたとき，c 人のうち 1 人しか犯人である保証がないようなユーザー集合しか発見できないということを示している．

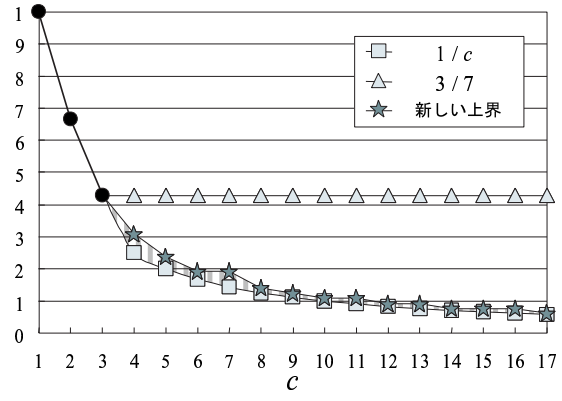


図 2.10: $s(c)$ の新しい上界

7 Web 情報発見手法への応用

近年，急速に発展しているウェブ (World Wide Web) は, 情報を得る手段として日常に欠かせないものとなっている．ウェブから必要な情報を発見する手段としては, Google, Yahoo!, Goo, Infoseek などの検索エンジンが代表的なものである． こ

れらの検索エンジンは, ユーザーが入力したキーワードを含んでいるページを見つける．すなわち, 検索エンジンはテキストを用いた情報発見手法と考えられる．

これに対して，ウェブのハイパーリンク構造を利用した情報発見手法の研究も進められている．このリンクを用いた手法は, テキストを用いた手法のように同綴異義語やダミーキーワードなどの言語的問題に惑わされないという長所がある．リンクを情報発見に用いるための基本的な考えは, あるページ u からリンクされている ページ v は, u の作者にとって価値のある情報を含んでいる可能性が高いという仮定であり, これらの研究のほとんどは，以下のような枠組みに基づいている．(1) ウェブ中のページ群の URL とリンクのデータを収集する．(2) このデータからウェブグラフを作成する．(3) ウェブグラフ中の特徴的な部分グラフ構造を互いに関連しているページまたはサイトの集合である**コミュニティ**として抽出する．なお, 点集合 V がウェブページの集合を表し, 辺集合 E が V 中のページ間のリンクを表す有向グラフ $G = (V, E)$ を, **ウェブグラフ**と呼ぶ.

リンク構造を用いてコミュニティを求める手法の研究としてよく知られたものに，Kleinberg の提案した HITS，Kumar らの trawling, Flake らによる max-flow based method などがある．とくに, max-flow based method はユーザーが与えたページ群 (以下では**シードページ群**と呼ぶ) に関連するコミュニティを求めることができる手法である．

一方, 近年浅野らがリンク構造を用いてコミュニティを求める手法のための, サイトを用いた新しい枠組みを提案し, trawling などを用いてこの枠組みの有効性を示した．この枠組みは, 次のようになっている．(1) ウェブ中のページ群の URL とリンクのデータを収集する．(2) このデータから**フィルタ**手法を用いて**ディレクトリベースドサイト**を抽出する．(3) ディレクトリベースドサイトを点とし, ディレクトリベースドサイト間のリンクを辺とする**サイト間グラフ**を作成する．(4) サイト間グラフ中の特徴的な部分グラフ構造を**コミュニティ**として抽出する．

すなわち, 従来の枠組みではページを単位として用いていたのに対して, この枠組みではサイト (正確にはその近似的なモデルであるディレクトリベースドサイト) を単位として用いているといえる．これは, あるサイト A から他のサイト B へのリンクが, そのサイト A の作者にとって価値のある情報への参照を表している可能性が高いのに対して, サイト内のリンクはサイト内のページを見やすく整理するというナビゲーション目的で作られていることが多いため, リンクを用いた情報発見には両者を区別して用いることが重要と考えられるからである．

もっとも, サイトという言葉は日常的に用いられているが，それ自体曖昧な概念であり，唯一の定義もない．たとえ, いくつかの研究で用いられている「ひとりの個人，ひとつの企業，ひとつの集団がつくるページの集合をそれぞれサイトとする」という定義を用いたとしても, ウェブのページには作者の情報は一般的には含まれていないので，サイトを計算することは困難であると考えられてきた.

これに対して，近年，浅野らによって，ある時点での URL とリンクのデータ (スナップショットと呼ぶ) からこの**ディレクトリベースドサイト**というモデルと**フィルタ**という手法を用いて，サイトを近似的ではあるが実用的には十分な精度で識別する方法が発表された．さらに, これらの研究では, trawling と彼らの提案した極大クリーク法を用いて, サイトを用いた枠組みがコミュニティ発見に役立つこと, とくに個人サイトを含むコミュニティを多く見つけることに大きな効果があることを示している．だが, リンクを用いた有力なコミュニティ発見法である max-flow based method に関しては, この枠組みがどのような効果を持つかはわかっていない.

本研究では，このサイト識別の方法と豊田，喜連川らによって収集・作成された 2003 年度 2 月の `.jp` ドメインを主体とした日本語ページからなるスナップショットを用いて，実際にサイトのデータとサイト間グラフのデータを構築し，max-flow based method をサイト間グラフとウェブグラフ両方の上で実行し，双方の性能を評価した．また, ウェブグラフ上で max-flow based method を実行する際に精度 (コミュニティ内の実際に関連しているページの割合) を落とす 4 つの問題を指摘し, サイトを用いることによって解決する方法を示し

た．さらに，その解決法がどのような効果があるかを詳しく解析した．結果として，本研究で提案した解決法を加えた改良 max-flow based method をサイト間グラフ上で実行することで，オリジナルの max-flow based method よりも遙かに大きなサイズのコミュニティが得られ，しかもその精度も大幅に向上することがわかった．この結果は，サイトを用いることが Web 情報発見手法に大きく役立つことを示している．

さらに，サイト間グラフのリンク，サイト内のリンクを描画してコミュニティとリンクの関係をわかりやすく図示するためのツール (図 2.11 参照) を上述のグラフ描画アルゴリズムを応用して開発した．

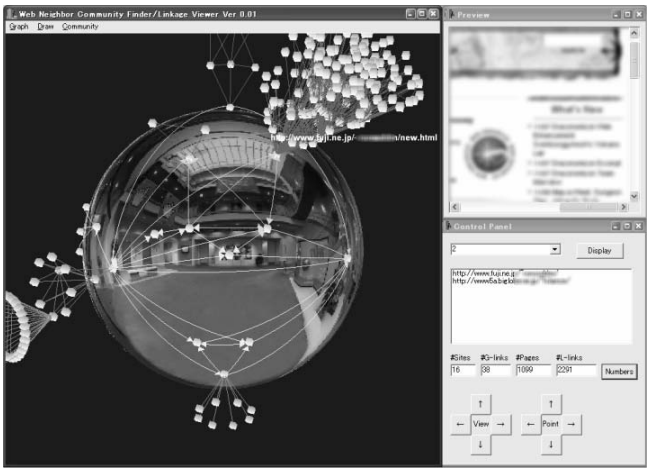


図 2.11: リンク描画ツール．

8 グラフの均一分割問題

点に整数重みの付いたグラフの均一分割問題も扱った．グラフ G の各点 v には非負整数の重み $\omega(v)$ が割当てられているとする．また，**連結成分の重みの合計の下界と上界**と呼ばれる非負整数をそれぞれ l と u とする．本論文では，G から何本かの辺を取り除いて G をいくつかの連結成分に分割し，各連結成分に含まれる点重みの合計がほぼ均一になるようにグラフを分割したい．すなわち，与えられた連結成分の下界 l と上界 u に対し，各連結成分に含まれる点重みの合計が l 以上 u 以下になるようにグラフを分割したい．このような均一分割を G の (l,u)-**分割**と呼ぶ．本論文では，与えられたグラフ G の (l,u)-分割を見つける以下の 3 つの問題を扱う．まず**最少分割問題**とは，最少の連結成分数を持つ G の (l,u)-分割を見つける問題である．**最大分割問題**は，同様に定義される．最後に p-**分割問題**とは，与えられた整数 p に対し，ちょうど p 個の連結成分を持つ G の (l,u)-分割を見つける問題である．例えば，図 2.12 は同じグラフ G に対する 2 つの $(10,20)$-分割の例である．ここで，各点は丸で描かれ，点重みは丸の中に描かれ，辺は直線分で描かれ，削除された辺は点線で描かれている．図 2.12(a) の $(10,20)$-分割には 4 つの連結成分があり，これが最少分割問題の解の一つになる．また，図 2.12(b) の $(10,20)$-分割には 6 つの連結成分があり，これが最大分割問題の解の一つになる．これら 3 つの分割問題は，選挙区割問題に応用される．即ち，グラフの各点 v を都市に，点 v の重み $\omega(v)$ を人口に対応させ，グラフの各辺を都市間の隣接関係に対応させる．選挙区割では，各選挙区は飛び地がなく，かつ各選挙区の人口がほぼ均一になるように，地域をいくつかの選挙区に分割したい．したがって，ある適切な l と u に対し，(l,u)-分割を見つけてやればよい．3 つの分割問題は直並列グラフに対して NP 困難であり，したがって直並列グラフに対してさえ多項式時間で解けそうにない．また，直並列グラフに対する最少分割問題および最大分割問題は，任意の定数 $c>0$ に対し，多項式時間の c 倍近似アルゴリズムを持ちそうにない．さらに，3 つの分割問題は一般のグラフに対しては強 NP 困難であり，一般のグラフに対しては擬多項式時間でさえ解けそうにない．本研究では，直並列グラフに対し，3 つの分割問題を擬多項式時間で解くアルゴリズムを与えた．まず，直並列グラフの最少分割問題および最大分割問題が $O(u^4n)$ 時間で解けることを示した．したがって，u が定数であるとき，アルゴリズムの計算時間は線形である．次に，直並列グラフの p-分割問題が $O(p^2u^4n)$ 時間で解けることを示した．さらに，これら直並列グラフに対するアルゴリズムが，部分 k-木に拡張できることを示した．

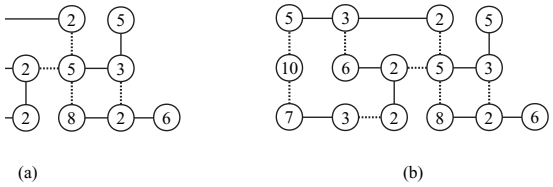


図 2.12: (a) 最少分割問題の解の一例，(b) 最大分割問題の解の一例.

研究業績一覧

学術論文

1. X. Zhou, Y. Matsuo and T. Nishizeki:
"List total colorings of series-parallel graphs", Journal of Discrete Algorithms, 3 巻 1 号, 47–60, 2005 年 3 月.
概要: A total coloring of a graph G is a coloring of all elements of G, i.e., vertices and edges, in such a way that no two adjacent or incident elements receive the same color. Let $L(x)$ be a set of colors assigned to each element x of G. Then a list total coloring of G is a total coloring such that each element x receives a color contained in $L(x)$. The list total coloring problem asks whether G has a list total coloring. In this paper, we first show that the list total coloring problem is NP-complete even for series-parallel graphs. We then give a sufficient condition for a series-parallel graph to have a list total coloring, that is, we prove a theorem that any series-parallel graph G has a list total coloring if $|L(v)| \geq \min\{5, \Delta + 1\}$ for each vertex v and $|L(e)| \geq \max\{5, d(v) + 1, d(w) + 1\}$ for each edge $e = vw$, where Δ is the maximum degree of G and $d(v)$ and $d(w)$ are the degrees of the ends v and w of e, respectively. The theorem implies that any series-parallel graph G has a total coloring with $\Delta + 1$ colors if $\Delta \geq 4$. We finally present a linear-time algorithm to find a list total coloring of a given series-parallel graph G if G satisfies the sufficient condition.

2. Md. S. Rahman, N. Egi and T. Nishizeki:
"No-bend orthogonal drawings of subdivisions of planar triconnected cubic graphs", IEICE Trans. INF. SYST., E88-D No.1, 23–30, 2005 年 1 月.
概要: A plane graph is a planar graph with a fixed embedding. In a no-bend orthogonal drawing of a plane graph, each vertex is drawn as a point and each edge is drawn as a single horizontal or vertical line segment. A planar graph is said to have a no-bend orthogonal drawing if at least one of its plane embeddings has a no-bend orthogonal drawing. In this paper we consider a class of planar graphs, called subdivisions of planar triconnected cubic graphs, and give a linear-time algorithm to examine whether such a planar graph G has a no-bend orthogonal drawing and to find one if G has.

3. K. Miura, M. Azuma and T. Nishizeki:
"Canonical decomposition, realizer, Schnyder labeling and orderly spanning trees of plane graphs", International Journal of Foundations of Computer Science, 16 巻 1 号, 117–141, 2005 年.
概要: A canonical decomposition, a realizer, a Schnyder labeling and an orderly spanning tree of a plane graph play an important role in straight-line grid drawings, convex grid drawings, floor-plannings, graph encoding, etc. It is known that the triconnectivity is a sufficient condition for their existence, but no necessary and sufficient condition has been known. In this paper, we present a necessary and sufficient condition for their existence, and show that a canonical decomposition, a realizer, a Schnyder labeling, an orderly spanning tree, and an outer triangular convex grid drawing are notions equivalent with each other. We also show that they can be found in linear time whenever a plane graph satisfies the condition.

4. T. Ito, X. Zhou and T. Nishizeki:
"Partitioning trees of supply and demand", International Journal of Foundations of Computer Science, 16巻4号, 803–827, 2005年.
概要: Assume that a tree T has a number n_s of "supply vertices" and all the other vertices are "demand vertices." Each supply vertex is assigned a positive number called a supply, while each demand vertex is assigned a positive number called a demand. One wishes to partition T into exactly n_s subtrees by deleting edges from T so that each subtree contains exactly one supply vertex whose supply is no less than the sum of demands of all demand vertices in the subtree. The "partition problem" is a decision problem to ask whether T has such a partition. The "maximum partition problem" is an optimization version of the partition problem. In this paper, we give three algorithms for the problems. The first is a linear-time algorithm for the partition problem. The second is a pseudo-polynomial-time algorithm for the maximum partition problem. The third is a fully polynomial-time approximation scheme (FPTAS) for the maximum partition problem.

5. K. Banno, S. Orihara, T. Mizuki and T. Nishizeki:
"Security index for digital fingerprinting", IEICE Trans. Fundamentals, E89-A No.1, 169–177, 2006年1月.
概要: Digital watermarking used for fingerprinting may receive a collusion attack; two or more users collude, compare their data, find a part of embedded watermarks, and make an unauthorized copy by masking their identities. In this paper, assuming that at most c users collude, we give a characterization of the fingerprinting codes that have the best security index in a sense of "$(c, p/q)$-secureness" proposed by Orihara et al. The characterization is expressed in terms of intersecting families of sets. Using a block design, we also show that a distributor of data can only find asymptotically a set of c users including at least one cluprit, no matter how good fingerprinting code is used.

6. T. Ito, X. Zhou and T. Nishizeki:
"Partitioning a graph of bounded tree-width to connected subgraphs of almost uniform size", Journal of Discrete Algorithms, 4巻, 142–154, 2006年.
概要: Assume that each vertex of a graph G is assigned a nonnegative integer weight and that l and u are nonnegative integers. One wishes to partition G into connected components by deleting edges from G so that the total weight of each component is at least l and at most u. Such an "almost uniform" partition is called an (l, u)-partition. We deal with three problems to find an (l, u)-partition of a given graph; the minimum partition problem is to find an (l, u)-partition with the minimum number of components; the maximum partition problem is defined analogously; and the p-partition problem is to find an (l, u)-partition with a fixed number p of components. All these problems are NP-complete or NP-hard, respectively, even for series-parallel graphs. In this paper we show that both the minimum partition problem and the maximum partition problem can be solved in time $O(u^4 n)$ and the p-partition problem can be solved in time $O(p^2 u^4 n)$ for any series-parallel graph with n vertices. The algorithms can be extended for partial k-trees, that is, graphs with bounded tree-width.

研究会等

1. K. Miura and T. Nishizeki:
"Rectangle-of-influence drawings of four-connected plane graphs (extended ab-

stract)", Proc. of APVIS 2005, 71–76, 2005 年.
概要:

2. T. Ito, X. Zhou and T. Nishizeki:
"Partitioning graphs of supply and demand", Proc. of ISCAS 2005, 160–163, 2005 年.
概要:

3. Takehiro Ito, Xiao Zhou and Takao Nishizeki:
"Algorithm for partitioning graphs of bounded tree-width of supply and demand", Proc. of the 4th Japanese-Hungarian Symposium on Discrete Mathematics and its Applications (JH 2005), 114–121, 2005 年.
概要:

4. T. Ito, A. Kato, X. Zhou and T. Nishizeki:
"Algorithms for finding distance-edge-colorings of graphs", Proc. of COCOON 2005, LNCS 3595, 798–807, 2005 年.
概要:

5. K. Banno, S. Orihara, T. Mizuki and T. Nishizeki:
"Best security index for digital fingerprinting (Extended abstract)", Proc. of IH 2005, LNCS 3727, 398–412, 2005 年.
概要:

6. Y. Asano, T. Nishizeki and M. Toyoda:
"Mining Communities on the Web Using a Max-Flow and a Site-Oriented Framework", Proceedings of the 6th International Conference on Web Information Systems Engineering, LNCS 3806, 1–14, 2005 年 11 月.
概要: There are several methods for mining communities on the Web using hyperlinks. One of the well-known ones is a max-flow based method proposed by Flake *et al.* The method adopts a page-oriented framework, that is, it uses a page on the Web as a unit of information, like other methods including HITS and trawling. Recently, Asano *et al.* built a site-oriented framework which uses a site as a unit of information, and they experimentally showed that trawling on the site-oriented framework often outputs significantly better communities than trawling on the page-oriented framework. However, it has not been known whether the site-oriented framework is effective in mining communities through the max-flow based method. In this paper, we first point out several problems of the max-flow based method, mainly owing to the page-oriented framework, and then propose solutions to the problems by utilizing several advantages of the site-oriented framework. Computational experiments reveal that our max-flow based method on the site-oriented framework is significantly effective in mining communities, related to the topics of given pages, in comparison with the original max-flow based method on the page-oriented framework.

7. X. Zhou and T. Nishizeki:
"Orthogonal drawings of series-parallel graphs with minimum bends", Proc. of ISAAC 2005, LNCS 3827, 166–175, 2005 年 12 月.
概要:

学会大会等

1. 浅野泰仁:
"A Site-oriented Framework for Mining Communities", 特定領域研究「新世代の計算限界」研究集会「複雑ネットワーク，ウェブグラフ」, 2005 年 9 月.

C02: 連続と離散の統合によるロバストアルゴリズム構築

杉原 厚吉　室田 一雄　今井 浩　松井 知己　岩田 覚　大石 泰章　西田 徹志

東京大学 大学院 情報理工学系研究科
〒 113-8656 東京都文京区本郷 7-3-1
sugihara@mist.i.u-tokyo.ac.jp

1　はじめに

本研究の目的は，今まで連続計算の分野と離散計算の分野に分かれてそれぞれ独立になされてきたアルゴリズム研究の知見を融合し，両者の手法の長所を補完し合うことによって，諸計算のロバスト性を確保するための計算原理を開拓することである．この目的に沿って，離散計算，代数計算，幾何計算，組合せ計算，量子計算，最適化計算，制御計算において，連続と離散の知見を融合したロバストアルゴリズムを追求してきた．その主な成果をまとめる．

2　細分割曲面の拡張

三角形メッシュという離散表現となめらかな曲面という連続表現をつなぐ細分割操作は，ロバストな曲面の設計・加工のための基本技術であるが，従来のものは頂点に対する操作であつた．これに対して本研究では，面に対する操作と辺に対する操作に基づいた二つの新しい細分割の方法を構成した．

第一の新手法である面に対する細分割操作は，3 次元空間における頂点と面の双対性を利用して構成できる [8]．すなわち，もとの世界での従来の細分割理論を双対世界へ移すことによって面に基づいた細分割理論を作った．ただし，この双対性の利用は自明ではない．なぜなら，点と双対な関係にあるのは，無限に広がった平面であって，ポリゴンメッシュに必要な有界多角形ではないからである．したがって，双対をとったとき形状が有界であることを保証しなければならない．本研究では，そのための必要十分条件を明らかにした．すなわち，双対形状が有界であるためには，もとの形状が星状形で，双対をとるときの原点がその核の中に含まれることが必要十分である．この結果は，双対操作が万能ではなく，限られた形状にしか適用できないことを示すものでもあるが，これが形状表現の大きな障害になるわけではない．なぜなら，理論の枠組は，双対性を通して従来の理論を移したが，具体的形状の表現には，必ずしも双対操作を施す必要はなく，はじめから双対空間で作ればよいからである．

第二の新手法は，辺に対する細分割操作である [7]．辺を含む直線の全体は，ブリュッカー座標を用いることによって，6 次元空間の中の 5 次元部分集合として特徴づけることができる．本研究では，その中で，辺の細分割操作によって閉じた代数系としての 4 次元部分空間を特徴づけることができた．

3　円ボロノイ図のロバスト構成法

円に対するユークリッド距離ボロノイ図は, 領域の境界線が曲線となるため，点ボロノイ図と比べて安定に構成することは格段に難しい．本年度は，この円ボロノイ図の構成算法とその応用について，多面的に研究した．

まず第一に，円のボロノイ図を，円の中心点のボロノイ図から出発して接続関係を変更していくことによって構成するアルゴリズムを構成した [9]．すなわち，まず円の中心点に対する点ボロノイ図を作る．次に，それらの中心点を，半径をもった円に置き換えながら，それに対応するボロノイ領域の境界を修正していく．この修正は，双対図形の世界では，四角形の対角線をもう一つの対角線に置き換える純粋に組合せ位相的操作であるため，数値誤差による破綻の心配のない手続きとして構成できた．

これとは別に，厳密計算法の考え方を直接適用して円ボロノイ図を構成する算法についても検討を加えた [25]．3 個の円のボロノイ図から出発して，円を一つずつ添加しながら，対応するボロノイ図を更新する逐次添加法において，位相構造を誤らないために必要な計算精度を調べた．その結果，三つの円が共通外接円と共通内接円を一つずつ持つ位置関係にあるとき，対応するボロノイ点が，新しく添加された円の領域に入るか否かを，入力データの 8 倍精度で判定する方法を構成できた．

一方，3 個の円が二つの共通外接円をもつ場合に対しては，スツルム列を用いた判定法は構成できたが，必要な精度が膨大で，そのままでは実用にならないこともわかった．したがって，この場合に対する厳密計算法のアルゴリズムは未解決のまま残されている．

ディジタル位相優先法による円ボロノイ図構成算法についてもアルゴリズムを作った．すなわち，まず与えられた円のボロノイ図の近似図形をディジタル画像の形で構成し，次に，そのディジタル画像近似から位相構造を抽出し，最後に，この位相構造を使って位相優先法を実行するというアルゴリズムである．

この方法では，ディジタル画像による近似は，位相構造が整合のとれた形で得られる範囲でできるだけ粗い解像度を用いるのがよい．そのための解像度の限界を，与えられた円の最小半径と，異なる円の最小距離によって特徴づけることができた．またこの方法で作ったソフトウェアの有効性を，円のパッキング問題へ適用することによって確認できた [24]．

さらにこの考え方を 3 次元へ拡張して，球のボロノイ図の構成算法も作ることができた．球ボロノイ図は，領域の境界が頂点をもたないことがあるなど，2 次元にはない難しさをもつが，3 次元ディジタル画像近似を利用することによって安定に計算できる見通しを立てることができた [12]．

さらに，円ボロノイ図の頂点位置を求める方法について，アポロニウスの第 10 問題と関連させて基礎的性質を調べた [10]．その結果，各種の円の配置に対するボロノイ頂点の統一的な計算法を構成することができた．

4 ジャンプシステム上の M 凸関数

4.1 概要

M 凸関数 [16] は，効率良く解ける非線形離散最適化問題の枠組を与えている．本研究では M 凸関数の概念を定パリティジャンプシステム上の関数に一般化し，その最小化のための最急降下型アルゴリズムを提案した (詳細は [17], [18] 参照)．これによって，Apollonio と Sebő [1] によって考察されたグラフの最小二乗因子問題に対する一般的枠組が与えられたことになる．

4.2 定義と基本的性質

V を有限集合とする．ベクトル $s \in \mathbf{Z}^V$ は，ある $u \in V$ に対し $s = \pm\chi_u$（単位ベクトル）で，$\|x-y\|_1 = \|x+s-y\|_1 + 1$ を満たすとき (x,y)-増分と呼ばれる．その全体を $\mathrm{Inc}(x,y)$ と書く．

定義 4.1 (M 凸関数) $J \subseteq \mathbf{Z}^V$ を定パリティジャンプシステムとする．関数 $f : J \to \mathbf{R}$ が M 凸であるとは，f が次の交換公理を満たすことを言う．

(M-EXC[J]) $\forall x, y \in \mathrm{dom} f$, $\forall s \in \mathrm{Inc}(x,y)$,
$\exists t \in \mathrm{Inc}(x+s,y)$ $s.t.$ $x+s+t \in J$, $y-s-t \in J$,
$f(x)+f(y) \geq f(x+s+t)+f(y-s-t)$.

定理 4.2 (最適性条件) $f : J \to \mathbf{R}$ を定パリティジャンプシステム J 上の M 凸関数とし，$x \in J$ とする．このとき，$f(x) \leq f(y)$ $(\forall y \in J)$ $\Longleftrightarrow$ $f(x) \leq f(y)$ $(\forall y \in J$ $s.t.$ $\|x-y\|_1 \leq 2)$.

4.3 最急降下法

定理 4.2 より次のアルゴリズムは自然である．

S0 ベクトル $x \in J$ を見出す．

S1 $f(x+s+t)$ を最小にする $s,t \in \{\pm\chi_u \mid u \in V\}$ $(s+t \neq 0)$ を見出す．

S2 $f(x) \leq f(x+s+t)$ となったら停止．このとき x が f の最小化元である．

S3 $x := x+s+t$ として S1 へ行く．

定理 4.3 f が唯一の最小化元 x^* を持つとする．このとき最急降下法の反復回数は $\|x^\circ - x^*\|_1/2$ で与えられる．ただし x° はステップ *S0* で見出された初期ベクトルを表す．

最小化元が複数ある一般の場合にも，最急降下法のステップ S1 において適当なタイブレークルールを設計すると，最急降下法の反復回数を $\max\{\|x-y\|_1 \mid x,y \in J\}/2$ で抑えられる．

4.4 諸演算

マトロイドやジャンプシステムに対しては，ミンコフスキー和やグラフによる変換などの演算が定義できる．さらに，これらの演算は付値マトロイドや M 凸関数などの離散関数にも定義されることが知られている．論文 [11] では，ジャンプシステム上の関数に対してもこれらの演算が一般化できることを示した．

5 量子情報での連続と離散の融合

量子情報処理においては，量子状態を用いて情報を表現・操作・伝送することによって情報処理を実現する．ここで重要なことは，これまでの情報処理が古典力学系に依存して展開されていたのに対して，量子状態を用いた場合の情報処理ではどのような新しいことができるかを解明することである．本年度の研究では，古典力学系の状態では表現できない量子的相関について精緻に解析を行い，それを情報処理方式へと発展させることに重点を置いた．具体的には，量子力学において真の量子性を示すための Bell 不等式の理論を現代の組合せ的凸多面体論と対話証明の枠組みを適用することによって研究を進め，次のような 2 つの論文について掲載・採択に至った．

(1) Avis, Imai, Ito, Sasaki の 4 名の共著で初期の成果をまとめたものを Journal of Physics A: Mathematical and General に投稿し掲載まで至ることができた．この論文では，上述の分離可能状態の相関表全体が凸多面体が 3 部グラフのカット凸多面体であることを指摘し，組合せ的凸多面体論で詳細に調べられているカット凸多面体の結果をこの Bell 不等式の場合に適用することを試みた．具体的には，従来研究で完全グラフのカット凸多面体のファセットは完全グラフの場合で 9 点くらいまで調べ上げられていることに鑑み，それらファセットを完全 3 部グラフのファセットに変換する汎用的手法として 3 角消去を提案した．

3 角消去のうちの「3 角」は，カット凸多面体の理論が距離埋め込みとも直結していて，いわゆる距離の 3 角不等式に対応する不等式がカット凸多面体のファセットを定めることから来ている．3 角消去の「消去」は凸多面体論での一般的技法である Fourier-Motzkin 消去に由来している．3 角消去は Fourier-Motzkin 消去を一方の不等式を 3 角不等式にして適用したものであるが，Fourier-Motzkin 消去が単にファセットを表現する不等式を足し合わせただけではファセットを導出する不等式に必ずしもならないのに対し，3 角消去では土台の完全グラフにはない点を絡ませた 3 角不等式を用いることで，導出された不等式が必ずファセットを定義することが保証できるようになっている．

この論文ではさらに 3 角消去により膨大な数の Bell 不等式が系統的に獲得できることを具体的に示し，またカット凸多面体の超幾何不等式クラス等に対応する無限個からなる Bell 不等式のクラスが構成できることを示した．またこの問題の背景にある対称性に関して，違う過程を経て得られる 3 角不等式同士が異なるものになっていることを示すことも行っている．

(2) Avis, Imai, Ito は量子性に関してさらに研究を推し進めることにより，Bell inequalities stronger than the Clauser-Horne-Shimony-Holt inequality for three-level isotropic States という論文を Physical Review A に投稿，採択されるまでに至った．量子情報で有名な Werner 状態等の量子特有の対称性を満たす量子状態について，これまでは CHSH 不等式より強力なものが知られていなかったが，この論文ではそのような Bell 不等式が存在するかという未解決問題に対して肯定的な解決を与えることに成功した．具体的には，本研究の過程で得られた Bell 不等式を系統的に調べ，測定数が相対的に少ない 89 個の不等式に着目し，その上で精緻な数値計算を行うことによって，3 準位系の isotropic 状態という対称性をもつ量子状態に対して，5 つの Bell 不等式が CHSH 不

等式より強力であることを示した．すなわち，その 5 つの Bell 不等式それぞれに対して isotropic 状態なある量子状態が存在し，それに対してうまく測定して相関表を得るとその Bell 不等式が破れるが，CHSH 不等式に対してはどのような測定をしても決して CHSH 不等式は破れないという状態が存在し得るということである．本研究で調査できたものはまだまだ限られているが，その中で本質的に CHSH 不等式よりも強力なものが 5 つも発見できたということは，傾向としてどのような Bell 不等式についてもそれが最強である量子状態が存在する可能性を提示されていると思われる．

一方で，大きな未解決問題としては上記肯定的結果は 3 準位系では得られたものの，2 準位系に限った場合においては，同じ対象とした 89 個の Bell 不等式についてかなり詳細に数値計算したもののそのような結果については得ることができていないことが上げられる．

また，従来量子計算では 2 準位系量子状態を 1 量子ビットと呼び，ほぼこれに限ってアルゴリズムや情報量の理論を展開しているが，このように多準位系を基礎としてそのテンソル積空間を考えることが 2 準位系とそのテンソル積空間でのみ発想する場合と違った様相を示すことに繋がることを示したことで，従来のアプローチ法に対する反省を促す知見を与えるものになっているかもしれない．

6　多重彩色問題とチャネル割当問題

6.1　概要

本研究では，グラフ彩色問題の拡張である多重彩色問題とチャネル割当問題に対する近似解法の枠組みを提案する．本研究で扱う 2 つの問題は，携帯電話ネットワーク等の周波数割当問題という工学的背景を持っており，1970 年代より研究されているものである．しかしながら，近年の携帯電話に代表される情報機器の劇的とも言える発達により，問題の重要性は以前とは比べものにならないほど増している．更に実務において周波数割当問題を解く場面は，地球規模のネットワークの設計や，災害時の緊急無線網の設営等，様々な状況が新たに出現している．このような時代の要請から，状況毎に異なる要求に答える，様々な性能を持つアルゴリズムを導く枠組みを構築する必要がある．本研究で提案する枠組みを種々のグラフクラスに適用することにより，理論的な近似精度及び必要計算量等を得ることができる．本研究で提案する解法に共通する特徴として，パーフェクトグラフと呼ばれる数学的に美しい構造を持つグラフクラスの特徴を積極的に用いている事が挙げられる．

携帯電話ネットワーク等における周波数割当問題に出現するグラフは，パーフェクトグラフではなく，その解法を直接適用する事は困難であるが，２次元平面の点，特に格子点を頂点として持つという特殊性を持つ場合が多い．これに対し本研究では，格子点上に定義されるグラフをパーフェクトグラフに分解し，分割統治法の変種を適用するという解法の枠組みを提案している．この枠組みは，三角格子あるいは四角格子上に定義される様々なグラフクラス等に適用可能であり，またその際の近似比率の算定方法も与えている．

6.2　格子状グラフの多重彩色問題

論文 [13, 14] では，三角格子及び四角格子上に定義されるグラフに対する多重彩色問題に対する近似解法の枠組みを提案している．提案する解法のアイデアの根幹を成すのは，格子状グラフのパーフェクトグラフへの分解手法である．本研究では，三角格子状のグラフがパーフェクトグラフとなる必要十分条件を導き，この構造を積極的に利用して多重彩色問題を解く近似解法の枠組みを提案している．上記の必要十分条件は本研究で初めて得られたものであり，離散数学における結果としても興味深いものとなっている．

6.3　チャネル割当問題

論文 [15] では，広いグラフクラスへ適用可能な，チャネル割当問題の近似解法の枠組みを提案している．提案する解法の枠組みは，パーフェクトグラフ，単位円グラフを等のグラフクラスへ適用可能である．また一般のグラフに適用した場合の近似精度についても考察を行なっている．解法は，グラフの最大クリーク問題の解を利用してグラフ

を分割し，分割して得られた個々のグラフに対し近似彩色法で得られた解を元にチャネルの割り当てを行なうものである．例えばパーフェクトグラフにおいては，(最大) クリーク数と (最小) 彩色数が一致することから，良い近似精度を持つ解法が構築できる．

7　線形計画問題の符号可解性

社会現象を線形方程式系で記述する際には，選好順序や係数の正負などの情報は容易に知ることができるのに対し，係数の数値化が困難である場合が多い．定性的な情報のみが与えられた状況下で線形モデルを解析するには，係数行列が要素の絶対値によらず正則（符号正則）かどうかを知る必要が生じる．この符号正則性を判定する問題の計算複雑度は長い間未解決であったが，1999 年に Robertson, Seymour, Thomas [23] によって多項式時間解法が与えられた．

このような定性的行列理論の最新の成果を最適化手法に応用することを目指して，昨年度は，対称行列の Sylvester 符号指数を各要素の符号情報から計算する手法を研究した．その研究成果は，本年度に，第 11 回整数計画法・組合せ最適化国際会議 (IPCO XI) で発表した．本年度は，最適化の分野で中心的な役割を果たしている線形計画法に注目し，入力の符号情報のみから最適解の符号情報が得られる条件を与え，その条件の下で，実際に最適基底解の符号を決定する効率的なアルゴリズムを開発した．

線形計画問題

$$\begin{array}{ll} \text{maximize} & cx \\ \text{subject to} & Ax = b \\ & x \geq 0 \end{array}$$

を $\mathrm{LP(A, b, c)}$ と書くことにする．同じ符号パタンの任意の $\tilde{A}$, $\tilde{b}$, $\tilde{c}$ に対して，$\mathrm{LP(\tilde{A}, \tilde{b}, \tilde{c})}$ の最適解の符号パタンの集合が常に一致するとき，$\mathrm{LP(A, b, c)}$ は符号可解であるという．一般に，与えられた線形計画問題が符号可解でないことを判定するのは NP 完全である．

そこで，線形計画問題が符号可解であるための十分条件を与えるために，完全符号正則の概念を導入する．まず，正方行列において，行列式の展開式の中に非零項が存在するとき，この正方行列を項別正則という．さらに，$m \times n$ 行列の全ての項別正則な m 次小行列が符号正則であるとき，この行列は完全符号正則であるという．与えられた行列が完全符号正則かどうかの判定は，符号正則性判定のアルゴリズムを用いて，多項式時間で可能である．線形計画問題 $\mathrm{LP(A, b, c)}$ は，

$$A_{\mathrm{p}} = \begin{pmatrix} A & b \end{pmatrix}, \qquad A_{\mathrm{d}} = \begin{pmatrix} c \\ A \end{pmatrix}$$

が共に完全符号正則であるときに，完全符号正則であるという．完全符号正則線形計画問題に対して，最適基底解の符号パタンを効率的に見出すアルゴリズムを開発した．このアルゴリズムの計算量は，入力の非零要素数を ℓ としたときに $O(m\ell)$ である．

8　ロバスト半正定値計画問題の領域分割型解法

8.1　概要

ロバスト半正定値計画問題は，ロバスト制御やゲインスケジュールド制御の多くの問題がそれに帰着されるという制御において重要な問題であり，多項式最適化を特殊な場合として含むため最適化においても重要である．本研究では，ロバスト半正定値計画問題を解く領域分割型の解法を提案し [3]，それが既存の解法にはない良い性質を持つことを示した [22].

8.2　領域分割型解法

ロバスト半正定値計画問題は次のように記述される：

$$P: \quad \begin{array}{ll} \text{minimize} & c^{\mathrm{T}} x \\ \text{subject to} & F(x, \theta) \succeq O \quad (\forall \theta \in \Theta). \end{array}$$

ただし，c は与えられた非零の実ベクトルであり，実ベクトル x は設計変数，θ は不確かなパラメータで，その定義域である Θ は p 次元の（凸とは限らない）有界多面体であるとする．また $F(x, \theta)$

は対称行列値の関数で，x についてアフィン，θ について多項式であるものとし，$F(x,\theta) \succeq O$ は左辺の行列が半正定値であることを表すものとする．

この問題は重要ではあるが，効率的に解くのが困難であり，実際，NP 困難であることが証明されている．そのためこの問題を直接解くのではなく，問題の制約をより強くてより扱いやすい制約で置き換えた近似問題を構成して解く方法が開発されてきた．特に最近提案された KYP 補題に基づく方法や，二乗和多項式に基づく方法は，近似精度をいくらでも高くできるという漸近的厳密性を持つために注目されている．

本研究では，新しい漸近的に厳密な解法として，以下のような領域分割型の解法を提案した [3]．まず，適当な行列 $G(x)$ と $M(\theta)$ を使って $F(x,\theta) = (1/2)M(\theta)^{\mathrm{T}} G(x) M(\theta)$ と表し，さらに $[M(\theta)\ H(\theta)]$ が正則行列となり，$M(\theta)^{\mathrm{T}} H(\theta)$ が恒等的に零となり，かつ θ についてアフィンであるような行列 $H(\theta)$ を構成できることに注目する．このとき，多面体 Θ を凸多面体の集合 $\{\Theta^{[j]}\}_{j=1}^{J}$ に分割し，個々の凸多面体の頂点の集合を $\mathrm{ver}\,\Theta^{[j]}$ で表すことにすると，問題

$$
\begin{aligned}
&P(\{\Theta^{[j]}\}):\\
&\quad \text{minimize} \quad c^{\mathrm{T}} x\\
&\quad \text{subject to} \quad G(x) + H(\theta) W^{\mathrm{T}} + W H(\theta)^{\mathrm{T}} \succeq O\\
&\qquad\qquad\qquad (\forall \theta \in \mathrm{ver}\,\Theta^{[j]},\ \ \forall j = 1, 2, \ldots, J)
\end{aligned}
$$

はもとの問題 P の近似問題であり，しかも分割 $\{\Theta^{[j]}\}$ を細かくすることで，いくらでも近似精度を上げることができる．

8.3 性質

領域分割型解法の近似誤差は，もとの問題と近似問題の最小値の差である $|\min P(\{\Theta^{[j]}\}) - \min P|$ で表される．また，部分領域 $\Theta^{[j]}$ の半径を $\mathrm{rad}\,\Theta^{[j]}$ で表すとき，分割 $\{\Theta^{[j]}\}$ の細かさは最大半径 $\overline{\mathrm{rad}}\,\{\Theta^{[j]}\} := \max_j \mathrm{rad}\,\Theta^{[j]}$ で表される．近似誤差は，最大半径を小さくすると零に収束することが定性的にわかっていたが，さらに定量的に次の性質を持つことを示せた [22].

定理． 正数 C_1, C_2 が存在して，$\overline{\mathrm{rad}}\,\{\Theta^{[j]}\} \leq C_1$ ならば

$$|\min P(\{\Theta^{[j]}\}) - \min P| \leq C_2 \overline{\mathrm{rad}}\,\{\Theta^{[j]}\}.$$

□

既存の KYP 補題や二乗和多項式に基づく解法では，このような定量的結果は得られていない．

この結果により，最大半径を小さくするとき，近似誤差は最大半径の高々1 次のオーダーで零に収束することがわかる．また，係数 C_1, C_2 を計算することも可能である．さらに上の結果を改良することで，少ない計算量で近似誤差を小さくするような効率的な分割を得ることも可能である．

9 流れの中での最短路探索のための新粒子法

流れの中の最短到達時間問題とは，流れを伴う領域に始点の集合と終点の集合が与えられとき，ボートが始点の集合から終点の集合まで動くのにかかる最短時間を求める問題のことである．我々はその最短時間をボート航行距離と呼ぶ．この問題を最適制御に帰着すると，最善の操縦方法は，ボートを常に等距離曲線の法線方向へ進めるということがわかる．もちろん，解析解を得ることは難しいので，数値計算に頼ることになるが，その典型的な方法は，マーカー粒子法と呼ばれる類のものである．等距離曲線をマーカーと呼ぶ粒子で近似し，ある時間幅で各粒子の次の位置を計算し，再び等距離曲線を構築する．これを繰り返しながら計算を進めて行く方法である．このとき，各粒子の法線方向は，近傍の粒子を使って決定される．

しかしながら，我々の問題の難しさは，初期条件として滑らかな曲線を与えたとしても，等距離曲線は滑らかさを失うことにある．それは，ある場所では，最短時間を達成する経路が複数存在することに起因する．このとき，等距離曲線を用いて法線を決める方法，すなわち近傍に依存する方法では，破綻を起こしてしまう．

今回，我々は，近傍に依存することなく法線方向を決定し，この破綻を回避する安定な数値計算法を考案した [21]．以下その方法を説明する．

$E(t)$ を時刻 t での等距離曲線とし，図 2.1 のように, $E(t)$ は $s \in S \subset \mathbf{R}$ により滑らかにパラメー

タ化されているとする．ただし，$t = 0$ のとき弧長になるように取る．F は正の定数，$f(x, y) = (g(x, y), h(x, y))^{\mathrm{T}}$ を滑らかな流れベクトルとする．このとき，$p(s, t) = (x(s, t), y(s, t))^{\mathrm{T}} \in E(t)$ を，固定した s に対して，

$$E(t) = \{p(s, t) \in \mathbf{R}^2 \mid s \in S\}, \quad |p_s(s, t)| \neq 0,$$
$$p_t(s, t) = Fn(s, t) + f(p(s, t))$$

を満たす，すなわち，最短時間を達成する経路を動く粒子の位置とする．ただし，$p_s(s, t)$ は s による微分を表し，$p(s, t)$ で $E(t)$ に接するベクトルである．そして，$p_t(s, t)$ は t による微分を表し，$n(p)$ は $p \in E(t)$ での $E(t)$ の単位法線ベクトルを表す．また，ベクトル τ を

$$\tau(s, t) \equiv a(s, t)p_s(s, t), \quad a(s, t) = 1/|p_s(s, t)|$$

と定義する．これは点 p での単位接ベクトルで，n に直交し，図 2.1 のように，$n(s, t)$ を反時計回りに 90 度回転させたものである．

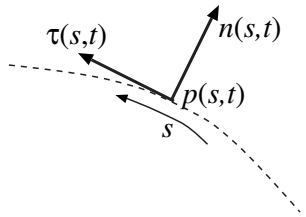


図 2.1: 位置 p での接ベクトルと法線ベクトルの関係

法線ベクトル $n(s, t)$ が t に対してどのように変化するかを導出する．以下では，それぞれの変数は省略する．

p_t の s による微分は，

$$p_{ts} = Fn_s + f_s = F\kappa p_s + (\nabla^{\mathrm{T}} f)p_s$$

となる．ただし，κ は p での曲率を表し，

$$\nabla^{\mathrm{T}} f = \begin{pmatrix} g_x & g_y \\ h_x & h_y \end{pmatrix}.$$

また，a が，固定した s に対して，初期値問題

$$a_t + \{F\kappa + ((\nabla^{\mathrm{T}} f)\tau) \cdot \tau\}a = 0, \quad a(s, 0) = 1$$

の解であることに注意すると，τ の t による微分は，

$$\tau_t = ap_{st} + a_t p_s = (I - \tau\tau^{\mathrm{T}})(\nabla^{\mathrm{T}} f)\tau$$

となる．ゆえに，n は τ を時計回りに 90 度回転させたものであったので，

$$n_t = \left(I - nn^{\mathrm{T}}\right)(\nabla^{\mathrm{T}} f)^{\mathrm{T}} n$$

を得る．この微分方程式から得られる法線ベクトルは、長さ 1 を保存し続けることを注意しておく．

以上より，近傍に依存しない新たな方程式系

$$p_t(s, t) = Fn(s, t) + f(p(s, t)),$$
$$n_t(s, t) = \left(I - n(s, t)n^{\mathrm{T}}(s, t)\right)(\nabla^{\mathrm{T}} f)^{\mathrm{T}} n(s, t)$$

を構成することができる．つまり，それぞれの粒子を独立に計算することができるのである．

また，この問題に対する有限要素法的な解法も開発しているが，それについては，体系化の作業を行なうことができた [19, 20].

今後は，高次元および曲面への拡張を行なって行きたい．

参考文献

[1] N. Apollonio and A. Sebő: Minsquare Factors and Maxfix Covers of Graphs, in: D. Bienstock and G. Nemhauser, eds., *IPCO*, Lecture Notes in Computer Science, 3064, Springer-Verlag, 2004, pp. 388–400.

[2] D. Avis, H. Imai, T. Ito and Y. Sasaki: Two-Party Bell Inequalities Derived from Combinatorics via Triangular Elimination. *Journal of Physics A: Mathematical and General*, Vol. 38 (2005), pp. 10971–10987.

[3] 江本・大石: 有理式で表される不確かさを持つ制御系の解析・設計法. 計測自動制御学会論文集，Vol. 41, No. 4 (2005), pp. 314–321.

[4] M. Hayashi, H. Imai, K. Matsumoto, M. B. Ruskai and T. Shimono: Qubit Channels which Require Four Inputs to Achieve Capacity: Implications for Additivity Conjectures. *Quantum Information and Computation*, Vol. 5 (2005), pp. 13–31.

[5] T. Ito, H. Imai and D. Avis: Bell Inequalities Stronger than the Clauser-Horne-Shimony-Holt Inequality for Three-Level Isotropic States. *Physical Review A*, 2006, to appear.

[6] N. Kakimura and S. Iwata: Computing the Inertia from Sign Patterns. *Proceedings of the Eleventh International Conference on Integer Programming and Combinatorial Optimization*, LNCS **3509**, Springer-Verlag, 2005, pp. 236–248.

[7] H. Kawaharada and K. Sugihara: Line Subdivision. *Mathematics of Surfaces* XI, Lecture Notes in Computer Science 3604 (Proceedings of the 11th IMA International Conference), July 2005, pp. 240–254.

[8] H. Kawaharada and K. Sugihara: Dual Subdivision—A New Class of Subdivision Scheme Using Projective Duality. *14th International Conference in Central Europe on Computer Graphics, Visualization and Computer Vision 2005*, Plzen, Czech Republic, 2006.

[9] D. Kim, D.-S. Kim and K. Sugihara: Euclidean Voronoi Diagram for Circles in a Circle. *International Journal of Computational Geometry and Applications*, Vol. 15, No. 2 (2005), pp. 209–228.

[10] D. Kim, D.-S. Kim and K. Sugihara: Apollonius Tenth Problem via Radius Adjustment and Möbius Transformation. *Computer-Aided Design*, Vol. 38 (2006), pp. 14–21.

[11] Y. Kobayashi, K. Murota and K. Tanaka: Operations on M-convex functions on jump systems. METR 2006-13, Department of Mathematical Informatics, University of Tokyo, February 2006.

[12] S. Matuura and K. Sugihara: Robust Construction of Sphere Voronoi Diagrams Using Digital Topology. *Proceedings of the 2nd International Symposium on Voronoi Diagrams in Science and Engineering*, Seoul, Korea, October 10–13, 2005, pp. 125–133.

[13] Y. Miyamoto and T. Matsui: Multicoloring Unit Disk Graphs on Triangular Lattice Points. *Proceedings of the Sixteenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 2005, pp. 895–896.

[14] Y. Miyamoto and T. Matsui: Perfectness and Imperfectness of the kth Power of Lattice Graphs. *Lecture Notes in Computer Science*, Springer, **3521** (2005), pp. 233–242.

[15] Y. Miyamoto and T. Matsui: Approximation Algorithms for Minimum Span Channel Assignment Problems. METR 2005-28, September 2005.

[16] K. Murota: *Discrete Convex Analysis*. SIAM, Philadelphia, 2003.

[17] K. Murota: M-convex Functions on Jump Systems: A General Framework for Mminsquare Graph Factor Problem. *SIAM Journal on Discrete Mathematics*, Vol. 20 (2006), pp. 213–226.

[18] K. Murota and K. Tanaka: A Steepest Descent Algorithm for M-convex Functions on Jump Systems. *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, to appear.

[19] T. Nishida and K. Sugihara: Boat-Sail Voronoi Diagram and Its Computation Based on a Cone-Approximation Scheme. *Japan Journal of Industrial and Applied Mathematics*, Vol. 22, No. 3 (2005), pp. 367–383.

[20] T. Nishida and K. Sugihara: Boat-Sail Voronoi Diagram on a Curved Surface. *Japan Journal of Industrial and Applied Mathematics*, Vol. 22, No. 2 (2005), pp. 267–278.

[21] T. Nishida, K. Sugihara and M. Kimura: Stable Marker-Particle Method for the Voronoi Diagram in a Flow Field, *Journal of Computational and Applied Mathematics*, accepted.

[22] Y. Oishi: A Region-dividing Approach to Robust Semidefinite Programming and Its Error Bound. *Technical Report* METR2006-10, Department of Mathematical Informatics, The University of Tokyo, Tokyo, Japan, February 2006.

[23] N. Robertson, P. D. Seymour and R. Thomas: Permanents, Pfaffian orientations, and even directed circuits. *Annals of Mathematics*, Vol. 150 (1999), pp. 929–975.

[24] K. Sugihara and S. Matuura: Fast and Robust Disk Packing Based on Digital Topology. *2nd Meeting of Euro Special Interest Group on Cutting and Packing*, Southampton, UK, April 14–16, 2005.

[25] Y. Tanaka and K. Sugihara: Exact Computation of a Circle Voronoi Diagram. *Proceedings of the 2nd International Symposium on Voronoi Diagrams in Science and Engineering*, Seoul, Korea, October 10–13, 2005, pp. 173–183.

[26] T. Yamasaki, H. Kobayashi and H. Imai: Quantum versus Deterministic Counter Automata. *Theoretical Computer Science*, Vol. 334, Issues 1-3 (2005), pp.275–297.

研究業績一覧

著書

1. 青本和彦，上野健爾，加藤和也，神保道夫，砂田利一，高橋陽一郎，深谷賢治，俣野博，室田一雄:
“数学入門辞典”, 岩波書店, 2005 年 9 月.
概要: 高校から大学で学ぶ数学用語を中心に解説した．数学を学ぶために必要な概念の解説のみならず，数学の歴史や社会的な背景にも配慮して解説をつけた．とくに、小学校から高等学校で扱われる数学に関しては，その歴史的背景に触れ、あわせて現代数学における位置づけも理解できるように書いた．

2. 土谷隆，室田一雄:
“応用数学ハンドブック 第 7 章「最適化」”, 丸善, 2005 年.
概要: 連続変数に関する最適化手法について，基本的に重要なものに最近の話題を加えて，理論を中心に記述した．

学術論文

1. Tetsushi Nishida and Kokichi Sugihara:
“Boat-Sail Voronoi Diagram and Its Computation Based on a Cone-Approximation Scheme”, Japan Journal of Industrial and Applied Mathematics, Vol. 22, No. 3, 367-383, 2005.
概要: A new concept called a boat-sail distance is introduced on the surface of water with flow, and it is used to define a generalized Voronoi diagram, in such a way that the water surface is partitioned into regions belonging to the nearest harbors with respect to this distance. The problem of computing this Voronoi diagram is reduced to a boundary value problem of a partial differential equation, and a numerical method for solving this problem is constructed. The method is a modification of a so-called fast marching method originally proposed for the eikonal equation. Computational experiments show the efficiency and the stableness of the proposed method.

2. Tetsushi Nishida and Kokichi Sugihara:
“Boat-Sail Voronoi Diagram on a Curved Surface”, Japan Journal of Industrial and Applied Mathematics, Vol. 22, No. 2, 267-278, 2005.
概要: We propose a new generalized Voronoi diagram, called a “boat-sail

Voronoi diagram on a curved surface". This is an extension of the boat-sail Voronoi diagram. The boat-sail Voronoi diagram is the partition of a two-dimensional flow field according to the shortest arrival time of a boat. On the other hand, our new Voronoi diagram subdivides the curbed surface with flow into the regions. In this paper, we derive a partial differential equation to solve the boat-sail Voronoi diagram on a curved surface and show some numerical examples.

3. Takeshi Kanda and Kokichi Sugihara:
"Two-dimensional Range Search Based on the Voronoi Diagram", International Journal of Computational Geometry and Applications, Vol. 15, No. 2, 151-166, 2005.
概要: This paper studies the two-dimensional range search problem, and constructs a simple and efficient algorithm based on the Voronoi diagram. In this problem, a set of points and a query range are given, and we want to enumerate all the points which are inside the query range as quickly as possible. In most of the previous researches on this problem, the shape of the query range is restricted to particular ones such as circles, rectangles and triangles, and the improvement on the worst-case performance has been pursued. On the other hand, the algorithm proposed in this paper is designed for a general shape of the query range in the two-dimensional space, and is intended to accomplish a good average-case performance. This performance is actually observed by numerical experiments. In these experiments, we compare the execution time of the proposed algorithm with those of other representative algorithms such as those based on the bucketing technique and the k-d tree. We can observe that our algorithm shows the better performance in almost all the cases.

4. Donguk Kim, Deok-Soo Kim and Kokichi Sugihara:
"Euclidean Voronoi Diagram for Circles in a Circle", International Journal of Computational Geometry and Applications, Vol. 15, No. 2, 209-228, 2005.
概要: Presented in this paper is an algorithm to compute a Euclidean Voronoi diagram for circles contained in a large circle. The radii of circles are not necessarily equal and no circle inside the large circle wholly contains another circle. The proposed algorithm uses the ordinary point Voronoi diagram for the centers of inner circles as a seed. Then, we apply a series of edge-flip operations to the seed topology to obtain the correct topology for the desired one. Lastly, the equations of edges are represented in a rational quadratic Bézier curve form.

5. Kohei Murotani and Kokichi Sugihara:
"New Spectral Decomposition Method for Three-dimensional Shape Models and Its Applications", Journal of Computing and Information Science in Engineering, Vol. 55, 277-282, 2005.
概要: This paper presents a generalization of a data analysis technique called a singular spectrum analysis (SSA). The original SSA is a tool for analyzing one-dimensional data such as time series, whereas the generalization presented in this paper is suitable for multi-dimensional data such as 3D polygonal meshes. The basic idea is to generalize the autocorrelation matrix so as to represent mutual relations of multi-dimensional data flexibly. Two applications of the proposed generalization are also shown briefly.

6. Donguk Kim, Deok-Soo Kim and Kokichi Sugihara:
"Apollonius Tenth Problem via Radius Adjustment and Möbius Transformation", Computer-Aided Design, Vol. 38, 14-21,

2006.
概要: The Apollonius Tenth Problem, as defined by Apollonius of Perga circa 200 B.C., has been useful for various applications in addition to its theoretical interest. Even though particular cases have been handled previously, a general framework for the problem has never been reported. Presented in this paper is a theory to handle the Apollonius Tenth Problem by characterizing the spatial relationship among given circles and the desired Apollonius circles. Hence, the given three circles in this paper do not make any assumption regarding on the sizes of circles and intersection/inclusion relationship among them. The observations made provide an easy-to-code algorithm to compute any desired Apollonius circle which is computationally efficient and robust.

7. Kazuo Murota and Akiyoshi Shioura:
"Substitutes and Complements in Network Flows Viewed as Discrete Convexity", Discrete Optimization, Vol. 2, 256-268, 2005.
概要: We study combinatorial properties of the optimal value function of the network flow problem. It is shown by Gale-Politof (1981) that the optimal value function has submodularity and supermodularity w.r.t. problem parameters such as weights and capacities. In this paper we shed a new light on this result from the viewpoint of discrete convex analysis to point out that the submodularity and supermodularity are naturally implied by discrete convexity, called M-convexity and L-convexity, of the optimal value function.

8. Satoru Iwata, Satoko Moriguchi and Kazuo Murota:
"A Capacity Scaling Algorithm for M-Convex Submodular Flow", Mathematical Programming, Vol. 103, 181-202, 2005.
概要: This paper presents a faster algorithm for the M-convex submodular flow problem, which is a generalization of the minimum-cost flow problem with an M-convex cost function for the flow-boundary, where an M-convex function is a nonlinear nonseparable discrete convex function on integer points. The algorithm extends the capacity scaling approach for the submodular flow problem by Fleischer, Iwata and McCormick (2002) with the aid of a novel technique of changing the potential by solving maximum submodular flow problems.

9. Satoru Fujishige and Satoru Iwata:
"Bisubmodular function minimization", SIAM Journal on Discrete Mathematics, Vol. 19, 1065-1073, 2006.
概要: This paper presents the first combinatorial polynomial algorithm for minimizing bisubmodular functions, extending the scaling algorithm for submodular function minimization due to Iwata, Fleischer, and Fujishige. Since the rank functions of delta-matroids are bisubmodular, the scaling algorithm naturally leads to the first combinatorial polynomial algorithm for testing membership in delta-matroid polyheda.

10. Satoru Iwata, S. Thomas McCormick and Maiko Shigeno:
"A Strongly Polynomial Cut Caneling Algorithm for Minimum Cost Submodular Flow", SIAM Journal on Discrete Mathematics, Vol. 19, 304-320, 2005.
概要: This paper presents a new strongly polynomial cut canceling algorithm for minimum cost submodular flow. The algorithm is a generalization of our similar cut canceling algorithm for ordinary min-cost flow. The algorithm scales a relaxed optimality parameter and creates a seconf, inner relaxation that is a kind of submodular max flow problem. The outer relaxation uses a novel technique for relaxing the submodular con-

straints that allows our previous proof techiniques to work. The algorithm uses the min cuts from the max flow subproblem as the relaxed most positive cuts it chooses to cancel. We show that this algorithm needs to cancel only $O(n^3)$ cuts per scaling phase, where n is the number of nodes. Furthermore, we show how to slightly modify this algorithm to get a strongly polynomial running time. Finally, we briefly show how to extend this algorithm to the separable convex cost case and that the same technique can be used to construct a polynomial time maximum mean cut canceling algorithm for submodular flow.

11. Isao Saiki, Kiyohiro Ikeda and Kazuo Murota:
"Flower Patterns Appearing on a Honeycomb Structure and Their Bifurcation Mechanism", International Journal of Bifurcation and Chaos, Vol. 15, No. 2, 497-515, 2005.
概要: Illuminative deformation patterns of a honeycomb structure are presented. A representative volume element of a honeycomb structure consisting of hexagonal cells is modeled to be a system with a group symmetry. The bifurcation mechanism and an exhaustive list of possible bifurcated patterns are obtained by group-theoretic bifurcation theory. A flower mode of the honeycomb is shown to have the same symmetry as the so-called anti-hexagon in the Rayleigh-Benard convection. A numerical bifurcation analysis is conducted on an elastic in-plane honeycomb structure consisting of 2 by 2 cells to produce beautiful wallpapers of bifurcating deformation patterns and, in turn, to highlight the achievement of the paper. New deformation patterns of a honeycomb structure have been found and classified in a systematic manner. Knowledge of the symmetries of the bifurcating solutions has turned out to be vital in the successful numerical tracing of the bifurcated paths. This paper paves the way for the introduction of the results hitherto obtained for flow patterns in fluid dynamics into the study of patterns on materials.

12. Satoko Moriguchi and Kazuo Murota:
"Discrete Hessian Matrix for L-convex Functions", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E88-A, No. 5, 1104-1108, 2005.
概要: L-convex functions are nonlinear discrete functions on integer points that are computationally tractable in optimization. In this paper, a discrete Hessian matrix and a local quadratic expansion are defined for L-convex functions. We characterize L-convex functions in terms of the discrete Hessian matrix and the local quadratic expansion

13. Hiroshi Hirai, Kazuo Murota and Masaki Rikitoku:
"SVM Kernel by Electric Network", Pacific Journal of Optimization, Vol. 1, No. 3, 509-526, 2005.
概要: We propose a new classifier, named electric network classifiers, for semi-supervised learning on graphs. Our classifier is based on nonlinear electric network theory and classifies data set with respect to the sign of electric potential. Close relationships to C-SVM and graph kernel methods are revealed. Unlike other graph kernel methods, our classifier does not require heavy kernel computations but obtain the potential directly using efficient network flow algorithms. Furthermore, with flexibility of its formulation, our classifier can incorporate various edge characteristics; influence of edge direction, unsymmetric dependence and so on. Therefore, our classifier has the potential to tackle large complex real world problems. Experimental re-

sults show that the performance is fairly good compared with the diffusion kernel and other standard methods.

14. Takuya Iimura, Kazuo Murota and Akihisa Tamura:
"Discrete Fixed Point Theorem Reconsidered", Journal of Mathematical Economics, Vol. 41, No. 8, 1030-1036, 2005.
概要: The aim of this note is to indicate an example that demonstrates the incorrectness of Iimura's discrete fixed point theorem [J. Mathematical Economics, 39 (2003) 725] and to present a corrected statement using the concept of integrally convex sets.

15. Kazuo Murota and Kenichiro Tanaka:
"A Steepest Descent Algorithm for M-convex Functions on Jump Systems", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E89-A, No. 5, 2005.
概要: The concept of M-convex functions has recently been generalized for functions defined on constant-parity jump systems. The b-matching problem and its generalization provide canonical examples of M-convex functions on jump systems. In this paper, we propose a steepest descent algorithm for minimizing an M-convex function on a constant-parity jump system.

16. James F. Geelen and Satoru Iwata:
"Matroid Matching via Mixed Skew-Symmetric Matrices", Combinatorica, Vol. 25, 187-215, 2005.
概要: Tutte associates a V by V skew-symmetric matrix T, having indeterminate entries, with a graph $G = (V, E)$. This matrix, called the Tutte matrix, has rank exactly twice the size of a maximum matching of G. Thus, to find the size of a maximum matching it suffices to compute the rank of T. We consider the more general problem of computing the rank of $T + K$ where K is a real V by V skew-symmetric matrix. This modest generalization of the matching problem contains the linear matroid matching problem and, more generally, the linear delta-matroid parity problem. We present a tight upper bound on the rank of $T + K$ by decomposing $T + K$ into a sum of matrices whose ranks are easy to compute.

17. Taiji Suzuki, Satoshi Aoki and Kazuo Murota:
"Use of Primal-Dual Technique in the Network Algorithm for Two-Way Contingency Tables", Japan Journal of Industrial and Applied Mathematics, Vol. 22, No. 1, 133-145, 2005.
概要: An algorithm for the longest-path subproblem in the network algorithm of Mehta and Patel for Fisher's exact test in two-way contingency tables is proposed. Use of the primal-dual technique for convex-cost flows and the maximum likelihood estimate makes the algorithm more efficient in time and space than existing algorithms.

18. Hiroko Satoh, Hiroyuki Kochino, Takeaki Uno, Shungo Koichi, Satoru Iwata and Tadashi Nakata:
"Effective Consideration of Ring Structures in CAST/CNMR for Highly Accurate CNMR Chemical Shift Prediction", Tetrahedron, Vol. 61, 7431-7437, 2005.
概要: A new function that effectively takes into account ring structural environments achieves extensive highly accurate prediction of C NMR chemical shift in the CAST/CNMR system. The approach adapts a fast and flexible ring perception algorithm and a new CAST coding method for the ring information. C NMR chemical shift prediction is performed for complicated polycyclic natural products and their synthetic intermediates as demonstration, which shows the reliability of the function in extending the scope of the practically ac-

curate C NMR prediction for wide range of organic compounds.

19. Masahito Hayashi, Hiroshi Imai, Keiji Matsumoto, Mary Beth Ruskai and Toshiyuki Shimono:
"Qubit channels which require four inputs to achieve capacity: Implications for additivity conjectures", Quantum Information & Computation, Vol. 5, No. 1, 13-31, 2005.
概要: An example is given of a qubit quantum channel which requires four inputs to maximize the Holevo capacity. The example is one of a family of channels which are related to 3-state channels. The capacity of the product channel is studied and numerical evidence presented which strongly suggests additivity. The numerical evidence also supports a conjecture about the concavity of output entropy as a function of entanglement parameters. However, an example is presented which shows that for some channels this conjecture does not hold for all input states. A numerical algorithm for finding the capacity and optimal inputs is presented and its relation to a relative entropy optimization discussed.

20. David Avis, Hiroshi Imai, Tsuyoshi Ito and Yuuya Sasaki:
"Two-Party Bell Inequalities Derived from Combinatorics via Triangular Elimination", Journal of Physics A: Mathematical and General, Vol. 38, No. 50, 10971-10987, 2005.
概要: Relatively few families of Bell inequalities have previously been identified. Some examples are the trivial, CHSH, I_{mm22}, and CGLMP inequalities. This paper presents a large number of new families of tight Bell inequalities for the case of many observables. For example, 44,368,793 inequivalent tight Bell inequalities other than CHSH are obtained for the case of 2 parties each with 10 2-valued observables. This is accomplished by first establishing a relationship between the Bell inequalities and the facets of the cut polytope, a well studied object in polyhedral combinatorics. We then prove a theorem allowing us to derive new facets of cut polytopes from facets of smaller polytopes by a process derived from Fourier-Motzkin elimination, which we call triangular elimination. These new facets in turn give new tight Bell inequalities. We give additional results for projections, liftings, and the complexity of membership testing for the associated Bell polytope.

21. Tomohiro Yamasaki, Hirotada Kobayashi and Hiroshi Imai:
"Quantum versus deterministic counter automata", Theoretical Computer Science, Vol. 334, 275-297, 2005.
概要: This paper focuses on quantum analogues of various models of counter automata, and almost completely proves the relation between the classes of languages recognizable by bounded error quantum ones and classical deterministic ones in every model of counter automata. It is proved that (i) there are languages that can be recognized by two-way quantum one-counter automata with bounded error, but cannot be recognized by two-way deterministic one-counter automata, (ii) under some reasonable restriction, every language that can be recognized by two-way deterministic one-counter automata can also be recognized by two-way reversible one-counter automata (and hence by bounded error two-way quantum one-counter automata), and (iii) for any fixed k, quantum ones and deterministic ones are incomparable in one-way k-counter automata.

22. Tsuyoshi Ito, Hiroshi Imai and David Avis:
"Bell Inequalities stronger than the Clauser-Horne-Shimony-Holt Inequality for Three-Level Isotropic States", Physical Review A, (to appear), 2006.

概要: We establish a relation between the two-party Bell inequalities for two-valued measurements and a high-dimensional convex polytope called the cut polytope in polyhedral combinatorics. Using this relation, we propose a method, triangular elimination, to derive tight Bell inequalities from facets of the cut polytope. This method gives two hundred million inequivalent tight Bell inequalities from currently known results on the cut polytope. In addition, this method gives general formulas which represent families of infinitely many Bell inequalities. These results can be used to examine general properties of Bell inequalities.

23. Ryuhei Miyashiro and Tomomi Matsui:
"A Polynomial Time Algorithm to Find an Equitable Home-away Assignment", Operations Research Letters, Vol. 33, No. 3, 235-241, 2005.
概要: We propose a polynomial time algorithm to find an equitable home-away assignment for a given timetable of a round-robin tournament. Our results give an answer to a problem raised by Elf, Jünger and Rinaldi (Operations Research Letters 31 (2003) 343–349), which concerns the computational complexity of the break minimization problem in sports timetabling.

24. 谷口隆晴, 杉原厚吉:
"空間多次元 Navier-Stokes 方程式に対する無反射境界条件", ながれ, Vol. 24, No. 1, 81-91, 2005.
概要: 空力学の諸問題を扱った数値シミュレーションにおいては，広大な現実の空間に比べ計算機の中で扱うことのできる領域は高々有限であるため，計算対象となる空間の打ち切りが必要となる．このとき，打ち切られた断面という人工的な境界が生じてしまうが，そのような人工的な境界上で特別な取り扱いをしなければ，現実的な解を得ることはできない．そこで，無反射境界条件，すなわち，人工的な境界上で反射が起こらないようにするための境界条件の設定が重要となる．無反射境界条件は既にいくつか提案されているが，特に Poinsot-Lele の境界条件は現在広く利用されている手法のひとつである．しかし，Poinsot-Lele の手法の基礎となった Thompson の境界条件においては，波が境界に対して垂直に入射する，という仮定がおかれており，この点の改善が望まれていた．本論文ではこの要望に答える．すなわち，数値計算時のデータを利用することによって，流れの向きに対する仮定をおかない Euler 方程式に対する無反射境界条件を提案し，その Navier-Stokes 方程式への拡張法について述べる．

25. 江本健斗，大石泰章:
"有理式で表される不確かさを持つ制御系の解析・設計法"，計測自動制御学会論文集, Vol. 41, No. 4, 314-321, 2005.
概要: This paper provides a new point of view to the method of Masubuchi and Shimemura, which is useful for analysis and synthesis of uncertain control systems, and presents an improvement and an extension of the method. In particular, this paper shows some properties of a transformation used in this method and reformulates the transformation as a decomposition of a rational matrix function. Combination of this decomposition and a technique of matrix dilation clarifies how conservative the above method is and shows how this conservatism is attenuated. Furthermore, the proposed method is extended to a general parameter-dependent linear matrix inequality.

26. 笠井大幹，大石泰章:
"確率的時変システムの安定化可能性と安定化法"，計測自動制御学会論文集，Vol. 41, No. 2, 118-125, 2005.
概要: Stabilizability and stabilization are considered on a first order system whose dynamics stochastically changes subject to a Markov chain. Although a necessary and

sufficient condition is known for the stabilizability, it is not convenient in the sense that it can be checked only through minimization of a non-convex function. In this paper, a more convenient sufficient condition is presented, which is based on conditional variance. It is also shown that a control law simpler than the known one stabilizing the system when the presented condition is satisfied. These results are considered to be useful for better understanding of stabilizability and stabilization of such systems.

27. Takaharu Yaguchi and Kokichi Sugihara: "A New Characteristic Nonreflecting Boundary Condition for the Multidimensional Navier-Stokes Equations", AIAA Paper, 2005-2868, 2005.
概要: A characteristic nonreflecting boundary condition for the Navier-Stokes equations is described. Because the computational resources are finite, one needs to truncate the computational domain when he/she simulates a physical problem. This truncation gives rise to non-physical artificial boundaries and one cannot obtain proper solutions without appropriate boundary conditions on such boundaries. Practically nonreflecting boundary conditions, which are boundary conditions that prevent the generation of reflections, are of great importance. One of the most popular methods for the Navier-Stokes equations right now is the PionsotLele boundary condition. Their boundary condition is based on Thompson 's boundary condition for the Euler equations, which is, however, theoretically one-dimensional, and hence is valid only when the flow is perpendicular to the boundary. Here we propose a boundary condition for the Euler equations which does not have the assumption for the direction of the flow. We also discuss its extension to the Navier-Stokes equations. Our basic idea is to estimate the direction of the flow from numerical data. Assuming that there are only simple waves, we derived a form of the ordinary differential system of the characteristic curves for the multi-dimensional Euler equations. By using this form we can apply flux vector splitting and calculate the velocity of each wave packet numerically.

28. Kohei Murotani and Kokichi Sugihara: "New Spectral Decomposition for 3D Polygonal Meshes and Its Application to watermarking", 13th International Conference in Central Europe on Computer Graphics, Visualization and Computer Vision 2005, 2005.
概要: This paper present a generalization of a data analysis technique called a singular spectrum analysis (SSA). The original SSA is a tool for analyzing one-dimensional data such as time series, whereas our generalization is suitable for multi-dimensional data such as 3D polygonal meshes. One of applications of the proposed generalization are also shown. The application of the generalized SSA is a new robust watermarking method that adds a watermark to a 3D polygonal mesh. Watermarks embedded by our method are resistant to similarity transformations and random noises. Our method has the advantage in that it requires smaller calculation cost than other methods with nearly equal performance.

29. Hiroshi Kawaharada and Kokichi Sugihara: "Line Subdivision", Mathematics of Surfaces XI, Lecture Notes in Computer Science (Proceedings of 11th IMA International Conference), No. 3604, 240-254, 2005.
概要: This paper proposes a new subdivision scheme based on line geometry. We name the scheme "line subdivision". Line subdivision scheme acts on the line space, and generates two-dimensional manifolds contained in the Klein quadric. The two-

dimensional manifolds are the Klein images of line congruences in P^3. So, this new subdivision scheme generates line congruences at the limit. Here, we define the line subdivision surface as an envelope surface which is made by the line congruence. Then, this paper derives basic properties of the surface. Moreover, we show that line subdivision contains ordinary subdivision and dual subdivision.

30. Hiroshi Kawaharada and Kokichi Sugihara: "Dual Subdivision", 14th International Conference in Central Europe on Computer Graphics, Visualization and Computer Vision 2006, Vol. E-53, 2006.
概要: This paper proposes a new class of subdivision schemes. Previous subdivision processes are described by the movement and generation of vertices, and the faces are specified indirectly as polygons defined by those vertices. In the proposed scheme, on the other hand, the subdivision process is described by the generation of faces, and the vertices are specified indirectly as the intersections of these faces. In this sense, this paper gives a framework for a wide class of new subdivision methods. In short, the new subdivision is a dual framework of an ordinary subdivision based on the principle of duality in projective geometry. So, the new subdivision scheme inherits various properties of the ordinary subdivision schemes. In this paper, we define the dual subdivision and derive its basic properties.

31. Satoru Iwata and Ryo Shimizu: "Combinatorial Analysis of Generic Matrix Pencils", Proceedings of the 11th International IPCO Conference, 335-348, 2005.
概要: This paper investigates the Kronecker canonical form of matrix pencils under the genericity assumption that the set of nonzero entries is algebraically independent. We provide a combinatorial characterization of the sums of the row/column indices supported by efficient bipartite matching algorithms. We also give a simple alternative proof for a theorem of Poljak on the generic ranks of matrix powers.

32. Naonori Kakimura and Satoru Iwata: "Computing the Innertia from Sign Pattern", Proceedings of the 11th International IPCO Conference, 236-248, 2005.
概要: A symmetric matrices A is said to be sign-nonsingular if every symmetric matrix with the same sign pattern as A is nonsingular. Hall, Li and Wang showed that the inertia of a sign-nonsingular symmetric matrix is determined uniquely by its sign pattern. The purpose of this paper is to present an efficient algorithm for computing the inertia of such matrices. The algorithm runs in $O(nm)$ time for a symmmetric of order n with m nonzero entries. The correctness of the algorithm provides an alternative proof of the result by Hall et al. In addition, for a symmetric matrix in general, it is shown to be NP-complete to decide whether the inertia of the matrix is not determined by the sign pattern.

33. Kimikazu Kato, Mayumi Oto, Hiroshi Imai and Keiko Imai: "Voronoi Diagrams for 1-qubit Pure Quantum States", The 2nd International Symposium on Voronoi Diagrams in Science and Engineering (VD2005), 293-299, 2005.
概要: 1-qubit quantum states form a space called the three-dimensional Bloch ball, and the Voronoi diagrams with respect to the quantum divergence have been considered. These diagrams basically treat mixed quantum states corresponding to points in the interior of the Bloch ball. Due to the existence of logarithm in the quantum divergence, the diagrams are not defined on pure quantum states corresponding to points on the two-dimensional sphere. This paper

first defines the Voronoi diagrams for pure quantum states on the Bloch sphere by the Fubini-Study distance and the Bures distance. We also introduce other Voronoi diagrams on the sphere obtained by taking a limit of Voronoi diagrams for mixed quantum states by the quantum divergences in the Bloch ball. These diagrams are shown to be equivalent to the ordinary Voronoi diagram on the sphere.

34. Shuji Kijima and Tomomi Matsui:
"Approximate/Perfect Aamplers for Closed Jackson Networks", The 2005 Winter Simulation Conference, 862-868, 2005.
概要: In this paper, we propose two samplers for the product-form solution of basic queueing networks, closed Jackson networks with multiple servers. Our approach is sampling via Markov chain, but it is NOT a simulation of behavior of customers in queueing networks. We propose two of new ergodic Markov chains both of which have a unique stationary distribution that is the product form solution of closed Jackson networks. One of them is for approximate sampling, and we show it mixes *rapidly*. To our knowledge, this is the first approximate polynomial-time sampler for closed Jackson networks with multiple servers. The other is for perfect sampling based on monotone CFTP (coupling from the past) algorithm proposed by Propp and Wilson, and we show the *monotonicity* of the chain.

35. Masashi Kiyomi, Takeaki Uno and Tomomi Matsui:
"Efficient Algorithms for the Electric Power Transaction Problem", Internet and Network Economics: First International Workshop (Lecture Notes in Computer Science), No. 3828, 602-611, 2005.
概要: We present two efficient algorithms for solving the electric power transaction problem. The electric power transaction problem appears when maximizing the social benefit on electric power transactions among some private companies. The problem is a special case of the minimum cost flow problem defined on a network with many leaves, where each leaf corresponds to a (private) company who wants to sell or buy electric power. Our first algorithm is based on the minimum mean cycle canceling algorithm and the second algorithm uses a linear time median finding algorithm. The first algorithm finds an optimal solution in $\mathrm{O}(n \log n\ k^5 \log(kC))$ time where n is the number of leaves, k is the number of non-leaf vertices and C is the highest electric power price per unit that companies may offer. The time complexity of the second algorithm is bounded by $\mathrm{O}((n+k^3)2^k k!)$ time, which is linear in n. In many practical instances, k is small and n is very large, hence these algorithms solve the problem more efficiently than the ordinary network flow algorithms.

36. Shuji Kijima and Tomomi Matsui:
"Rapidly Mixing Chain and Perfect Sampler for Logarithmic Separable Concave Distributions on Simplex", Proceedings of the 2005 International Conference on the Analysis of Algorithms, 369-380, 2005.
概要: In this paper, we are concerned with random sampling of an n dimensional integral point on an $(n-1)$ dimensional simplex according to a multivariate discrete distribution. We employ sampling via Markov chain and propose two "hit-and-run" chains, one is for approximate sampling and the other is for perfect sampling. We introduce an idea of *alternating inequalities* and show that a *logarithmic separable concave* function satisfies the alternating inequalities. If a probability function satisfies alternating inequalities, then our chain for approximate sampling mixes in $\mathrm{O}(n^2 \ln(K\varepsilon^{-1}))$, namely

$(1/2)n(n-1)\ln(K\varepsilon^{-1})$, where K is the side length of the simplex and ε $(0 < \varepsilon < 1)$ is an error rate. On the same condition, we design another chain and a perfect sampler based on monotone CFTP (Coupling from the Past). We discuss a condition that the expected number of total transitions of the chain in the perfect sampler is bounded by $\mathrm{O}(n^3 \ln(Kn))$.

37. Ayami Suzuka, Ryuhei Miyashiro, Akiko Yoshise, Tomomi Matsui:
"Semidefinite Programming Based Approaches to Home-away Assignment Problems in Sports Scheduling", The First International Conference on Algorithmic Applications in Management (Lecture Notes in Computer Science), No. 3521, 95-103, 2005.
概要: For a given schedule of a round-robin tournament and a matrix of distances between homes of teams, an optimal home-away assignment problem is to find a home-away assignment that minimizes the total traveling distance. We propose a technique to transform the problem to MIN RES CUT. We apply Goemans and Williamson's 0.878-approximation algorithm for MAX RES CUT, which is based on a positive semidefinite programming relaxation, to the obtained MIN RES CUT instances. Computational experiments show that our approach quickly generates solutions of good approximation ratios.

38. Yuichiro Miyamoto and Tomomi Matsui:
"Perfectness and Imperfectness of the kth Power of Lattice Graphs", The First International Conference on Algorithmic Applications in Management (Lecture Notes in Computer Science), No. 3521, 233-242, 2005.
概要: Given a pair of non-negative integers m and n, $S(m,n)$ denotes a square lattice graph with a vertex set $\{0,1,2,\ldots,m-1\}\times\{0,1,2,\ldots,n-1\}$, where a pair of two vertices is adjacent if and only if the distance is equal to 1. A triangular lattice graph $T(m,n)$ has a vertex set $\{(x\boldsymbol{e}_1+y\boldsymbol{e}_2) \mid x\in\{0,1,2,\ldots,m-1\},\ y\in\{0,1,2,\ldots,n-1\}\}$ where $\boldsymbol{e}_1=(1,0)$, $\boldsymbol{e}_2=(1/2,\sqrt{3}/2)$, and an edge set consists of a pair of vertices with unit distance. Let $S^k(m,n)$ and $T^k(m,n)$ be the kth power of the graph $S(m,n)$ and $T(m,n)$, respectively. Given an undirected graph $G=(V,E)$ and a non-negative vertex weight function $w: V\to \mathrm{Z}_+$, a multicoloring of G is an assignment of colors to V such that each vertex $v\in V$ admits $w(v)$ colors and every adjacent pair of two vertices does not share a common color. In this paper, we show necessary and sufficient conditions that $[\forall m, S^k(m,n)$ is perfect] and/or $[\forall m,\ T^k(m,n)$ is perfect], respectively. These conditions imply polynomial time approximation algorithms for multicoloring $(S^k(m,n),w)$ and $(T^k(m,n),w)$.

研究会等

1. Shiro Matuura and Kokichi Sugihara:
"Robust Construction of Sphere Voronoi Diagrams Using Digital Topology", Proceedings of the 2nd International Symposium on Voronoi Diagrams in Science and Engineering, 125-133, 2005年10月.
概要: This paper proposes the use of digital topology for constructing the sphere Voronoi diagram in a robust manner. This is a new version of the topology-oriented method. While the previous version requires a general description of the topological invariants, the proposed version uses topological structures that are automatically extracted from the digital approximation of geometric objects. So the implementation is simple and the resulting software runs fast, although the output is an approximation of the true Voronoi diagram.

2. Hiroshi Hirai, Kazuo Murota and Masaki Rikitoku:
"Electric Network Kernel for Support Vector Machines", International Symposium on the Art of Statistical Metaware, 2005年3月.
概要: We propose a new classifier, named electric network classifiers, for semi-supervised learning on graphs. Our classifier is based on nonlinear electric network theory and classifies data set with respect to the sign of electric potential. Close relationships to C-SVM and graph kernel methods are revealed. Unlike other graph kernel methods, our classifier does not require heavy kernel computations and obtain the potential directly using efficient network flow algorithms. Furthermore, with flexibility of its formulation, our classifier can incorporate various edge characteristics; influence of edge direction, unsymmetric dependence and so on. Therefore, our classifier has the potential to tackle large complex real world problems. Experimental results show that the performance is fairly good compared with the diffusion kernel and other standard methods.

3. 森口聡子，室田一雄:
"L 凸関数に対する離散ヘッセ行列", 日本応用数理学会，平成１７年研究部会連合発表会, 2005 年 3 月.
概要: L-convex functions are nonlinear discrete functions on integer points that are computationally tractable in optimization. In this paper, a discrete Hessian matrix and a local quadratic expansion are defined for L-convex functions. We characterize L-convex functions in terms of the discrete Hessian matrix and the local quadratic expansion.

4. 齊藤廣大，室田一雄:
"ロバスト混合整数計画に対する Benders 分解法", 日本オペレーションズ・リサーチ学会 2005 年度春季研究発表会, 236-237, 2005 年 3 月.
概要: We consider mixed integer programming (MIP) problems with ellipsoidal uncertainty in problem data. Robust solutions to such problems are formulated as solutions of second-order cone programming problems with integer constraints, which we solve by an adaptation of the Benders decomposition technique towards MIP with conic constraints. Numerical computation against robust 0-1 knapsack problems and generalized assignment problems indicates that robustness can be achieved without substantial deterioration in optimal values.

5. 森口聡子，室田一雄:
"L 凸関数に対する離散ヘッセ行列", 日本オペレーションズ・リサーチ学会 2005 年度春季研究発表会, 238-239, 2005 年 3 月.
概要: L-convex functions are nonlinear discrete functions on integer points that are computationally tractable in optimization. In this paper, a discrete Hessian matrix and a local quadratic expansion are defined for L-convex functions. We characterize L-convex functions in terms of the discrete Hessian matrix and the local quadratic expansion.

6. Hiroshi Hirai, Kazuo Murota and Masaki Rikitoku:
"Electric Network Kernel for Support Vector Machines", 日本オペレーションズ・リサーチ学会 2005 年度春季研究発表会, 240-241, 2005 年 3 月.
概要: We propose a new classifier, named electric network classifiers, for semi-supervised learning on graphs. Our classifier is based on nonlinear electric network theory and classifies data set with respect to the sign of electric potential. Close relationships to C-SVM and graph kernel methods are revealed. Unlike other graph

kernel methods, our classifier does not require heavy kernel computations and obtain the potential directly using efficient network flow algorithms. Furthermore, with flexibility of its formulation, our classifier can incorporate various edge characteristics; influence of edge direction, unsymmetric dependence and so on. Therefore, our classifier has the potential to tackle large complex real world problems. Experimental results show that the performance is fairly good compared with the diffusion kernel and other standard methods.

7. 田中健一郎，室田一雄:
“ジャンプシステム上の M 凸関数の最小化”, 日本応用数理学会 2005 年度年会, 2005 年 9 月.
概要: The concept of M-convex functions has recently been generalized for functions defined on constant-parity jump systems. The b-matching problem and its generalization provide canonical examples of M-convex functions on jump systems. In this paper, we propose a steepest descent algorithm for minimizing an M-convex function on a constant-parity jump system.

8. 原辰次，森口聡子，室田一雄，高松吉郎:
“連続・離散ハイブリッド凸関数”, 日本応用数理学会 2005 年度年会, 2005 年 9 月.
概要: 近年，ハイブリッドシステムのモデル予測制御などにおいて，混合整数 2 次計画問題を短時間で解くアルゴリズムの構築が求められている．一方で，最適化の分野では離散凸解析という枠組みが確立しつつある．本論文では，まず解きやすいクラスとしてハイブリッド凸関数の概念を提案する．具体的には，L 凸関数の概念をもとにハイブリッド L 凸関数を定義し，これに基づいて混合整数計画問題のサブクラスにあたるハイブリッド凸計画問題を定式化する．最後にハイブリッド L 凸関数に対する最適性規準を導出する．

C03: ネットワーク上での社会的効用と個人的効用の対立問題に対するアルゴリズム的研究

浅野 孝夫 † 渡邉 敏正 ‡ 今井 桂子 †

† 中央大学 理工学部 情報工学科
〒 112-8551 文京区春日 1-13-27
{asano,imai}@ise.chuo-u.ac.jp

‡ 広島大学 大学院 工学研究科
〒 739-8527 東広島市鏡山 1-4-1
watanabe@infonets.hiroshima-u.ac.jp

1 はじめに

計算理論・アルゴリズム理論の代表的問題の一つである集合カバー問題は、社会学・経済学にも関係して、サービスの提供と利用という形で説明できる問題である。一般に、サービスを提供する事業者は負担したコストをこのサービスの受益者から回収することになるが、その際どのように受益者にコストを負担してもらうかということになる。サービスを開業した複数の事業者からサービスが受けられる状況のときには、利用者は負担が軽くなる事業者からのサービスを希望するようになる。こうして利用者が利己的に行動をするようになると、開業した事業者は、開業のコストを回収できなくなり、このシステムは破綻に向かって進んでいくことになってしまう。これに対して、どの利用者も、他の利用者の負担金をそのままにしておいて、勝手に自分の負担金を減らすとサービスが受けられなくなってしまうとき、このときの状態はゲーム理論の専門用語で Nash 均衡にあると呼ばれる。Nash 均衡を求めるための計算困難性や近似困難性の上界・下界の研究が活発に実行されていて、現在、情報科学の世界的な権威の国際会議では、この分野の研究がホットなトピックスとして注目を浴びている。

上記のような研究動向を踏まえて、本研究は、集合カバー問題、施設配置問題 (集合カバー問題と類似する問題であるが、各受益者はサービスを提供する施設の開設コストを負担するだけでなくサービスを受け取るための接続コストも支払うという問題)、インターネットの回線利用問題、通信網 (道路網) の混雑による遅延対策問題、などの NP-困難な組合せ最適化問題に対して、利己的な利用者と全体の管理者との間の対立問題をアルゴリズムの観点から研究し、計算困難性・近似困難性のより良い下界と上界を得ることを目的としている。

ネットワーク上での全体からの社会的効用の最適化と利己的な各利用者の納得できる個人的効用の達成という対立問題は、問題の下界を証明する際にもしばしば生じる問題で、情報科学の分野ではなじみの問題である。さらに、実際の現場で生じる全体と個との対立の観点からの問題は、NP-困難な組合せ最適化問題であり、整数計画問題として定式化できるものが多い。このような問題に対しては、近似アルゴリズムの理論が強力な道具である。以上を踏まえて、以下の研究を実行した。

1. インターネットや道路網などで社会的効用の最適化と利己的な各利用者の納得できる個人的効用の達成という対立問題の生じる実際の具体例とこれまでの研究を調査した。

2. ゲーム理論や社会学、経済学で扱われている全体と個の対立問題の Nash 均衡に基づく理論的研究を調査した。

3. 集合カバー問題、施設配置問題などの NP-困難な組合せ最適化問題に対して開発された近似アルゴリズムの設計と解析の技法が、本研究に有効であることが既に知られている。そこで、1,2 の調査においては、高性能近似アルゴリズムの分野で最先端の研究をしている内外の研究者と情報およびアイデアを交換した。

4. 1,2,3 の研究調査で得られた問題および集合カバー問題、施設配置問題、インターネットの回線利用問題、通信網 (道路網) の混雑による遅延対策問題などの、NP-困難な組合せ問題に対して、利己的な利用者と全体の管理者との間の対立問題

を近似アルゴリズム、グラフ理論、計算幾何学の観点から研究した。また、近似アルゴリズムの設計と解析の技法の有効性を検討中である。

以上の研究を通して得られた成果は、研究業績一覧に載せているが、その中の１つを以降の節で詳しく述べる。

2 サービスを考慮した施設配置問題に対する近似アルゴリズムの実験評価

2.1 序論

施設配置問題は1960年代前半からオペレーションズ・リサーチ (OR) の分野で中心的な問題として幅広く研究されている問題であり, 工場, 倉庫, 学校, 病院などの設立地計画をモデル化した問題といえる. 応用問題としては, データやキャッシュなどのコンテンツ配置問題, ネットワークの安全性 (耐故障性) を考慮した様々なネットワーク設計問題が挙げられる. そのため, 近年のインターネット普及に伴い, ウェブのプロキシサーバーの設置計画などにも応用されており, より現実的な環境に対応させた様々な関連問題も広く研究されている.

本稿では, 施設配置問題の 1 つである**サービスを考慮した施設配置問題** (Facility Location Problem with Service Installation costs) についての研究を述べる [4] . この問題の応用として, 倉庫と小売店間の在庫管理やインターネット問題が挙げられる. 目的は, この問題に対して Shmoys et al. によって発表された 6 近似アルゴリズム [4] よりさらに性能の良いアルゴリズムを開発する事である. 具体的には, **容量制約なし施設配置問題** (Uncapacitated Facility Location Problem) に帰着させることによって得られる手法と, 容量制約なし施設配置問題において現在もっとも近似比率の良い 1.52 近似 [2] , 1.61 近似アルゴリズム [1] の考え方に基づく手法を提案する.

2.2 問題定義

最も有名な施設配置問題は容量制約なし施設配置問題と呼ばれるものである. これは, 入力として n_f 個の開設候補施設の集合 F と n_c 人の利用者集合 C が与えられる. 施設 i には施設を開設するための非負の開設コスト f_i が与えられ, 施設 i と利用者 j との間には非負の接続コスト c_{ij} が与えられる. なお, 接続コストは三角不等式を満たすものとする. この入力において, いくつかの施設を開設し, すべての利用者を適切な施設に接続することを考える.

これに対して, サービスを考慮した施設配置問題では, 入力として n_s 個のサービス集合 S が加えられ, 各利用者にはそれぞれが必要とするサービス $g(j)$ が決められている. また, 各施設 i にサービス l をインストールするためのサービスインストールコスト f_i^l が与えられる. このとき本問題の目的は, 総コスト (開設コストとサービスインストールコストと接続コストの合計) を最小とすることである. すなわち, いくつかの施設を開設し, 開設した施設に対してインストールするサービスを決定し, すべての利用者を必要としているサービスがインストールされている施設に接続させることである.

この問題は, 容量制約なし施設配置問題と同様, 以下のように整数計画問題として定式化することができる.

$$
\begin{aligned}
\min \quad & \sum_{i\in F} f_i y_i + \sum_{i\in F}\sum_{l\in S} f_i^l y_i^l + \sum_{i\in F}\sum_{j\in C} c_{ij} x_{ij} \\
\text{s.t.} \quad & \sum_{i\in F} x_{ij} = 1 \quad (j \in C), \\
& x_{ij} \le y_i^{g(j)} \quad (i \in F, j \in C), \\
& x_{ij} \le y_i \quad (i \in F, j \in C), \\
& x_{ij}, y_i, y_i^l \in \{0,1\} \quad (i \in F, j \in C, l \in S).
\end{aligned}
$$

2.3 Shmoys et al. の手法

ここでは, Shmoys, Swamy and Levi が提案した, 6 近似アルゴリズム [4] について述べる. このアルゴリズムは**施設の優先順位** $\mathcal{O}$ と呼ばれる仮定の下で, 6 近似を達成するアルゴリズムである. まず, 施設の優先順位について述べることにする.

施設の優先順位 $\mathcal{O}$

施設 i と i' を比べたとき, すべてのサービス

$l \in S$ に対して,

$$f_i^l \leq f_{i'}^l$$

が成り立つならば, 施設の優先順位は $i \leq i'$ である.

次にアルゴリズムの概観を説明する. 6 近似アルゴリズムはフェイズ 1 とフェイズ 2 から構成される. フェイズ 1 では実行可能な双対問題の解と一時的に開設する (仮開設) 施設集合, 一時的にインストールする (仮インストール) 集合を求める. フェイズ 2 ではフェイズ 1 の仮開設施設, 仮インストール集合から正式に開設, インストールするものを決定し, すべての利用者を必要とするサービスがインストールされている施設に接続する.

アルゴリズム

フェイズ 1

各利用者 j に施設 i への費用 α_j を設ける. 費用 α_j は, 施設 i に接続するための費用, $g(j)$ をインストールするための費用 θ_{ij}, 施設 i を開設させるための費用 β_{ij} からなるものとする.

すべての利用者を未凍結の状態にする. 3 つの条件 (1. 利用者を接続, 2. $g(j)$ をインストール, 3. 施設を開設) が成立したら凍結する. 未凍結の利用者の費用 α_j をすべての割合で増加させながら以下の (a), (b), (c) を繰り返す. すべての利用者が凍結したら終了とする. なお, (a), (b), (c) の条件が同時に成立する場合は, 任意の順番で行なう.

(a) **if** (i, j に対して, $\alpha_j \geq c_{ij}$) **then**
利用者 j を施設 i へ仮接続する.
- **if** ($y_i^{g(j)} = 0$) **then**
θ_{ij} を増やし始める.
- **if** ($y_i^{g(j)} = 1$ かつ $y_i = 0$) **then**
β_{ij} を増やし始める.
- **if** ($y_i^{g(j)} = 1$ かつ $y_i = 1$) **then**
利用者 j を凍結する.

(b) **if** (i, l に対して, $\sum_{j \in G_l} \theta_{ij} = f_i^l$) **then**
施設 i にサービス l を仮インストールする.
- **if** ($y_i = 0$) **then**
β_{ij} を増やし始める.
- **if** ($y_i = 1$) **then**
利用者 j を凍結する.

(c) **if** (i に対して, $\sum_j \beta_{ij} = f_i$)**then**
施設 i を仮開設し, 3 つ条件が揃っている利用者 j を凍結する.

$\alpha_j, \theta_{ij}, \beta_{ij}$ は未凍結な利用者にのみ発生し, 凍結した利用者は各操作に参加しない.

フェイズ 2

フェイズ 2 では正式に開設する施設, インストールするサービス, 利用者の接続を決定する. ここで, F は仮開設した施設の集合を表し, $F_l \subseteq F$ はサービス l が仮インストールされた仮開設施設集合を表す. 施設 $i \in F$ に対して, 仮開設した時刻を t_i とする. また施設 $i \in F_l$ に対して, 施設 i にサービス l がインストールされた時刻を t_{il} とする.

開設施設の決定

仮開設施設集合 F から正式に開設施設集合を決定する. もし利用者 j において, β_{ij} と $\beta_{i'j}$ の両方が**活性** ($\beta_{ij}, \beta_{i'j} > 0$) であるとき, 施設 $i, i' \in F$ は**従属施設**と呼ばれる. このとき, 施設の優先順位 $\mathcal{O}$ をもとに, 仮開設した施設を考え, 極大独立集合 $F' \subset F$ を選ぶ. 集合 F' を開設施設集合とする.

サービスインストールの決定

サービス l と集合 F_l を考える. もし利用者 $j \in G_l$ において, θ_{ij} と $\theta_{i'j}$ の両方が活性 ($\theta_{ij}, \theta_{i'j} > 0$) であるとき, 施設 $i, i' \in F_l$ は**サービス-l-従属**と呼ばれる. このとき, 特定の順序によって集合 F_l から極大独立集合 F_l' を選ぶ. ここでいう特定の順序とは,

(1) 開設施設集合 $F_l \cap F'$ から t_{il} の早い順に考える.
(2) 開設されていない施設 $F_l - F'$ から t_i の早い順に考える.

である. 具体的には, まず特定の順序 (1) に該当される施設を調べていき, すべての施設にサービス l をインストールする (極大独立集合 F_l' に加える). その後, 特定の順序 (2) に該当する施設を調べていき, 施設の優先順位 $\mathcal{O}$ をもとに, 施設 i と施設 i' が従属施設であるような施設 i' を見つけ, この施設 i' にサービス l をインストー

ルする．この施設 i' は施設 i の隣接施設であり，$\mathbf{nbr}(i)$ と表す．ここで注意すべきことは，$\mathbf{nbr}(i)$ はサービス l ではなく施設 i でのみ決定されるという点である．

接続

すべての利用者 j を，必要としているサービス $g(j)$ がインストールされているもっとも近い開設施設 i に接続する．

2.4 提案手法

この手法は容量制約なし施設配置問題に帰着させることによって解を得るものである．ポイントは与えられた入力に対して 1 つのサービスに絞って考えると，容量制約なし施設配置問題と等価となる点である (図 1 参照)．本稿では現在もっとも近似率の良い 1.52 近似アルゴリズムを用いている．具体的な手順を以下に示す．

1. 与えられた入力に対して，サービス l を必要としている利用者にのみ注目し，新たに開設コストを $f_i + f_i^l$ とする．これにより，サービスの数 n_s だけ容量制約なし施設配置問題の入力を構築する．

2. 上記の入力に対して，容量制約なし施設配置問題に対するアルゴリズムを適用する．

3. 得られた n_s 個の解を足し合わせ，本問題の解とする．

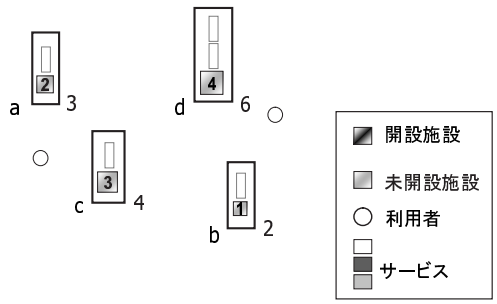


図 2.1: 帰着の様子

2.5 1.61 近似に基づく提案手法

1.61 近似に基づく提案手法は Jain, Mahdian and Saberi の手法 [1] を本問題に拡張したものである．

アルゴリズムの流れとしては，Shmoys et al. の手法のフェイズ 1 と類似しているが，利用者が凍結したら，凍結する要因となった施設以外の施設への貢献を無効にし，未接続の状態に戻す点が異なる．この操作によってアルゴリズムの終了時には，利用者は凍結する要因となった施設にのみ接続している．さらに，1.61 近似に基づく提案手法の特徴として重要な点は，凍結した利用者に対しても総コストが減少するならば接続を変更することである．

アルゴリズムの詳細を述べる前に，1.61 近似に基づく提案手法で用いられる，利用者 j による施設 i への貢献 β_{ij} を定義する．

貢献 β_{ij} の定義

- **if** (利用者 j が未凍結) **then**
  $\beta_{ij} = \max\{\alpha_j - c_{ij} - \theta_{ij}, 0\}$ とする．

- **if** (利用者 j が凍結) **then**
  $\beta_{ij} = \max\{c_{i'j} - c_{ij}, 0\}$ とする．

なお，接続を変更することで，施設 i' にインストールされているサービスが必要なくなったらアンインストールする．また，接続している利用者がいなくなったら，施設 i' は未開設に戻すことにする．

アルゴリズム

各利用者 j に施設 i への費用 α_j を設ける．費用 α_j は，施設 i に接続するための費用，$g(j)$ をインストールするための費用 θ_{ij}，施設 i を開設させるための費用 β_{ij} からなるものとする．以下詳しい手順を述べる．

すべての利用者を未凍結の状態する．3 つの条件 (1. 利用者を接続，2. $g(j)$ をインストール，3. 施設を開設) が成立したら凍結する．未凍結の利用者の費用 α_j をすべての割合で増加させながら以下の (a), (b), (c) を繰り返す．すべての利用者

が凍結したら終了とする.

(a) **if** (i, j に対して, $\alpha_j \geq c_{ij}$) **then**
利用者 j を施設 i に接続する.
- **if** ($y_i^{g(j)} = 0$) **then**
θ_{ij} を増やし始める.
- **if** ($y_i^{g(j)} = 1$ かつ $y_i = 0$) **then**
β_{ij} を増やし始める.
- **if** ($y_i^{g(j)} = 1$ かつ $y_i = 1$) **then**
利用者 j を凍結する.

(b) **if** (i, l に対して, $\sum_j \theta_{ij} = f_i^l$) **then**
施設 i にサービス l をインストールする.
- **if** ($y_i = 0$) **then**
β_{ij} を増やし始める.
- **if** ($y_i = 1$) **then**
利用者 j を凍結する.

(c) **if** (i に対して, $\sum_j \beta_{ij} = f_i$)**then**
施設 i を開設し, 3 つ条件が揃っている利用者 j を凍結する.
- **if** (j が既に i' に接続 かつ $c_{ij} < c_{i'j}$) **then**
利用者 j の接続を i' から i に変更し, 必要なければ施設 i' にインストールされているサービス $g(j)$ をアンインストールする.

2.6 1.52 近似に基づく提案手法

1.52 近似に基づく提案手法は Mahdian, Ye and Zhang の手法 [2] を本問題に拡張したものである. このアルゴリズムにおいて, 総コストが減少する値として $gain$ を用いる.

$gain(i,l)$ の定義
未開設施設 i を開設し, さらにその施設にサービス l をインストールして, 利用者を必要とするサービスがインストールされている最も近い開設施設に接続する. このとき, 接続コストが c から c' になるとすると,

$$gain(i,l) = c - c' - f_i - f_i^l$$

と定義する.

(初期解) スケーリングパラメータを $\delta = 1.504$ とする. このとき, 開設コストを一様に δ 倍した問題に対して, 1.61 近似に基づく提案手法を適用する.
(貪欲改善) 開設コストをもとに戻した問題に対して, 総コストが減少する ($gain(i,l) > 0$ である) かぎり以下を繰り返す.

- **if** (ある未開設施設 i, ある未インストールサービス l の $\frac{gain(i,l)}{f_i}$ が正かつ最大) **then**
施設 i を開設し, サービス l をインストールして, 利用者は必要とするサービスがインストールされている最も近い開設施設に接続を変更する.

2.7 計算機実験 1

実験の方法

今回の実験では,

A. Shmoys et al. が提案する 6 近似アルゴリズム
B. 容量制約なし施設配置問題に帰着させる提案手法 (以下, 提案手法と呼ぶ)
C. 1.61 近似に基づく提案手法 (以下, 1.61 近似ベースとも呼ぶ)
D. 1.52 近似に基づく提案手法 (以下, 1.52 近似ベースとも呼ぶ)

の 4 手法を Visual C++を用いて実装し, 実際的性能評価を行なう. 最適解としては, IP を線形計画ソフト NUOPT で解くことで得られる整数解を用いることにする. 実験で使用した計算機を表 2.1 に示す. 入力には次の入力データを用いこの入力データの一部を変化することで様々な実験を行なう.

標準入力データ 1

(1) 施設は, 整数格子点の座標 (0, 0) から (500, 500) の間でランダムに 100 個ずつ発生
(2) 利用者は, 整数格子点の座標 (0, 0) から (500, 500) の間でランダムに 100 個ずつ発生
(3) サービスは 50 種類ずつ発生させ, 利用者が

表 2.1: 実験環境

CPU	Intel Pentium4 2.8 GHz
メモリ	512 MB RDRAM
OS	Microsoft windows XP
コンパイラ	Visual C++ 6.0

必要とするサービスはランダムに決定

(4) 開設コストは, 1 から 1000 の間のランダムな正整数

(5) サービスインストールコストは, 1 から 300 の間のランダムな正整数

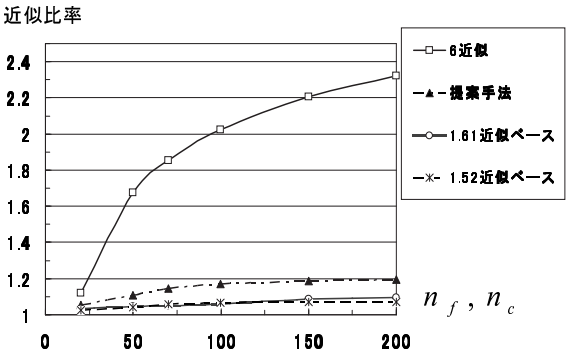
(6) 施設と利用者の接続コストは, 施設と利用者のユークリッド距離

図と表の説明

図は, 実験を 20 回行ったときの平均の近似比率, 以下では特に明記しないかぎり簡略化して近似比率と呼ぶ, を表すもので, 縦軸にはこの近似比率を用いている.

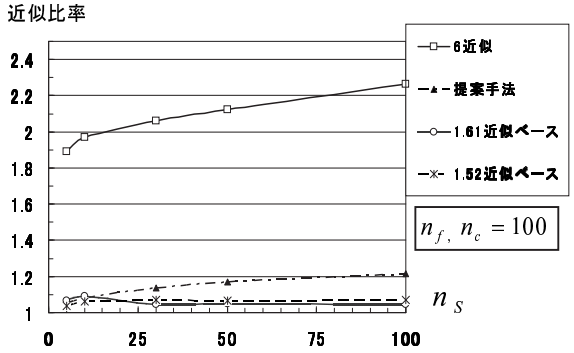
実験 1 施設数 n_f, 利用者数 n_c を変化させた場合

標準入力データの施設数 n_f, 利用者数 n_c をそれぞれ同じ割合で増加した場合の計算機実験を行う. ここでは, 線形計画ソフト NUOPT で IP を解くことのできる $n_f = n_c = 200$ までの計算機実験を行う.



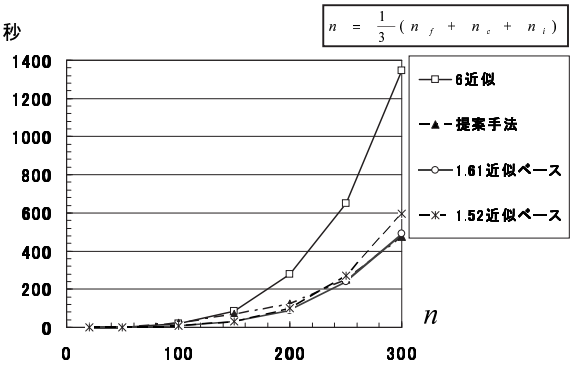
実験 2 サービス数 n_s を変化させた場合

標準入力データのサービス数 n_s を増加した場合の計算機実験を行う.



実験 3 計算時間 $(n = \frac{1}{3}(n_f + n_c + n_s))$

入力のサイズを n とし, 表 2.1 に示した計算機を使用したときの計算時間を算出する.



計算機実験 1 のまとめ

実験 1 より, 提案する 3 つの手法は, Shmoys らによって提案された 6 近似アルゴリズムより, かなり良い値を出力することがわかる. 特に 1.61 近似, 1.52 近似に基づく提案手法はもっとも良い値を出力している. これは 6 近似アルゴリズムは開設する施設数が極端に少なく, 逆に提案手法は開設する施設数が多いので, 余分なコストがかかってしまっているためと考えられる.

実験 2 より, サービス数 n_s が少ない場合, 提案手法, 1.61 近似, 1.52 近似に基づく手法の間に差がないことがわかる. これは, 提案手法はサービスの数だけ 1.52 近似アルゴリズムを再帰的に実行するので, サービスの数が少なければ, それらを足し合わせた時に生じる誤差が少なくなるためと考えられる.

実験 3 より, 提案する 3 つの手法は計算時間においても短縮できていることがわかる. したがって, 提案する 3 つの手法は近似比率と計算時間の両面で有効な手法であるといえる.

2.8 容量制約つきサービスを考慮した施設配置問題 (ソフト容量版)

サービスを考慮した施設配置問題では, 施設にインストールできるサービスの容量は設けていない. そこで, “容量制約つき” の場合に発展させた, 容量制約つきービスを考慮した施設配置問題 (ソフト容量版) を提唱し, この問題に対する解法を提案する.

問題定義

この問題は, サービスを考慮した施設配置問題の入力において, 各施設 i に整数 u_i が付随していて, 基本的に施設 i は u_i 個のサービスしかインストールできないというものである. ソフト容量版では, 各施設が (コピーして) 何回でも開設可能である.

問題の目的は, 容量制約を守りつつ, 総コスト (開設コストとサービスインストールコストと接続コストの合計) を最小とすることである. すなわち, いくつかの施設を複数回開設し, 開設した施設に対して容量制約を守りつつインストールするサービスを決定し, すべての利用者を必要としているサービスがインストールされている施設に接続させることである. この問題も, 以下のように整数計画問題 (IP) として定式化することができる.

$$
\begin{aligned}
\min \quad & \sum_{i\in F} f_i y_i + \sum_{i\in F}\sum_{l\in S} f_i^l y_i^l + \sum_{i\in F}\sum_{j\in C} c_{ij} x_{ij} \\
\text{s.t.} \quad & \sum_{i\in F} x_{ij} = 1 \quad (j \in C), \\
& x_{ij} \le y_i^{g(j)} \quad (i \in F, j \in C), \\
& x_{ij} \le y_i \quad (i \in F, j \in C), \\
& \sum_{l\in S} y_i^l \le u_i y_i \quad (i \in F), \qquad (2.22) \\
& x_{ij},\ y_i^l \in \{0,1\} \quad (i \in F, j \in C, l \in S), \\
& y_i \text{は非負の整数} \quad (i \in F).
\end{aligned}
$$

サービスを考慮した施設配置問題との違いは, 制約式 (1) が追加されたことである. この制約式は, 施設 i が k 個のサービスをインストールするとき, 施設を $\lceil k/u_i \rceil$ 回開設しなければならないことを表している.

提案手法 1

ここでは, 容量制約つきサービスを考慮した施設配置問題に対する解法を提案する. この提案手法 1 は Mahdian, Ye and Zhang [2] によって提案された 2.89 近似アルゴリズムの考え方も基にしている. 具体的には, サービスを考慮した施設配置問題に帰着させ, サービスを考慮した施設配置問題に対するアルゴリズムを適用するというものである.

---

1. 施設 i を開設するための開設コストを $(1-\lambda)f_i$, 施設 i にサービス l をインストールするためのサービスインストールコストを $f_i^l + \lambda_i \cdot \frac{f_i}{u_i}$ とするサービスを考慮した施設配置問題の入力を構築する.
2. 1 で作られた入力において, スケーリングパラメータを γ_c/γ_f とする. このとき, 開設コストを一様に γ_c/γ_f 倍する.
3. 上記の入力に対して, サービスを考慮した施設配置問題に対するアルゴリズムを適用する.
4. 結果を, 各施設 $i \in F$ に対して $\lceil \sum_{l\in S} y_i^l/u_i \rceil$ 回施設を開設した容量制約つきービスを考慮した施設配置問題の解として出力する.

提案手法 2

この節では, Mahdian, Ye and Zhang [3] によって提案された 2 近似アルゴリズムの考え方に基づく提案手法 2 を述べる.

---

1. 施設 i を開設するための開設コストを

$$
f_i(k) = \begin{cases} 0 & (k=0) \\ (1+\frac{k-1}{u_i})f_i & (k \ge 1) \end{cases}
$$

とし, サービスを考慮した施設配置問題の入力を構築する. ここでいう k とは施設にインストールするサービス数を指す.

2. 上記の入力に対して, サービスを考慮した施設配置問題に対するアルゴリズムを適用する.

3. 結果を, 各施設 $i \in F$ に対して $\lceil \sum_{l \in S} y_i^l / u_i \rceil$ 回施設を開設した容量制約つきービスを考慮した施設配置問題の解として出力する.

2.9 計算機実験 2

実験の方法

今回の実験では,

A. 1.61 近似に基づく手法を適用した提案手法 1

B. 1.61 近似に基づく手法を適用した提案手法 2

の 2 手法を Visual C++を用いて実装し, 実際的性能評価を行なう. 最適解としては, IP を線形計画ソフト NUOPT で解くことで得られる整数解を用いることにする. 入力には次の入力データを用い, この入力データの一部を変化することで様々な実験を行なう.

標準入力データ 2

(1) 施設は, 整数格子点の座標 (0, 0) から (500, 500) の間でランダムに 100 個ずつ発生

(2) 利用者は, 整数格子点の座標 (0, 0) から (500, 500) の間でランダムに 100 個ずつ発生

(3) サービスは 50 種類ずつ発生させ, 利用者が必要とするサービスはランダムに決定

(4) 開設コストは, 1 から 1000 の間のランダムな正整数

(5) 施設の容量は, 1 から 10 の間のランダムな正整数

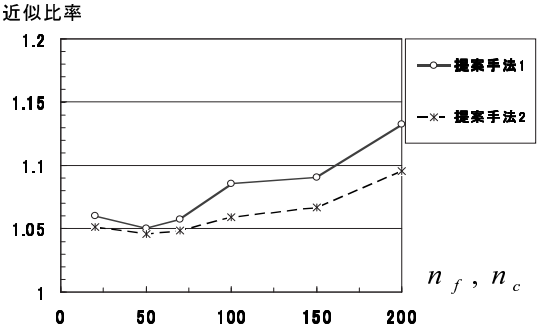
(6) サービスインストールコストは, 1 から 300 の間のランダムな正整数

(7) 施設と利用者の接続コストは, 施設と利用者のユークリッド距離

図と表の説明

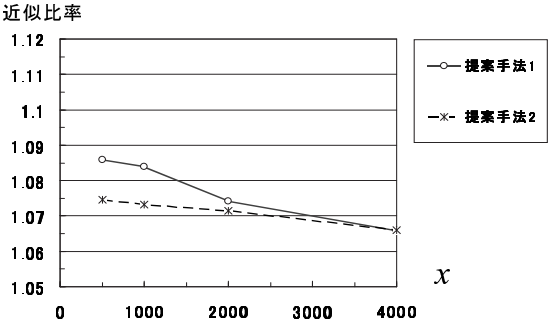
図は, 実験を 20 回行ったときの平均の近似比率, 以下では特に明記しないかぎり簡略化して近似比率と呼ぶ, を表すもので, 縦軸にはこの近似比率を用いている.

実験 1 施設数 n_f, 利用者数 n_c を変化させた場合



実験 2 接続コストを変化させた場合

座標範囲 (x, x) を広くすることで接続コストが増加した場合を考える.

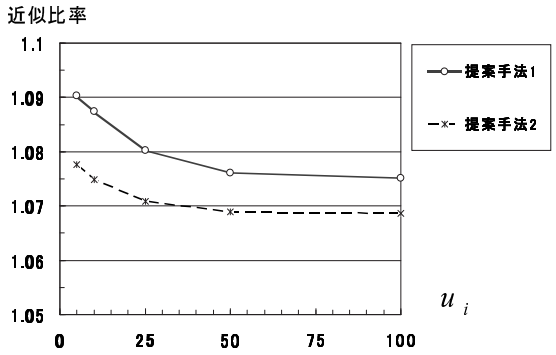


実験 3 施設の容量 u_i を変化させた場合

施設の容量 u_i を一定とし, 標準入力データの施設の容量 u_i を増加した場合の計算機実験を行う.

計算機実験 2 のまとめ

実験 1 より, 提案手法 1 と提案手法 2 が共に良い近似比率を得ているといえる. これより, 容量制約つきサービスを考慮した施設配置問題に対する解法として, サービスを考慮した施設配置問題に帰着させる手法は有効であるといえる. また提



案手法 2 の方が良い近似比率を得ている要因としては, 容量制約つきサービスを考慮した施設配置問題の場合においても, 2 近似アルゴリズムの考え方が優れているためと考えられる.

実験 2 より, 接続コストを増加させていくと, 提案手法 1 と提案手法 2 が共に近似比率が良くなっていることがわかる. これは提案手法 1 と提案手法 2 が共に, 1.61 近似に基づく提案手法に帰着させる際に, 開設コストの影響を受けやすいためと考えられる. つまり, 接続コストを増加することで開設コストの影響が少なくなり, 1.61 近似に基づく提案手法の本来の性能が発揮されるため, 近似比率がよくなっているといえる.

実験 3 より, 容量の制約を厳しくした場合, 提案手法 1 と提案手法 2 が共に近似比率が悪くなっていることがわかる. そして容量の制約を緩めていくにつれて, 1.61 近似アルゴリズムの本来の性能が発揮され, 近似比率が良くなっている.

2.10 結論

本論文では, Shmoys, Swamy and Levi が提唱したサービスを考慮した施設配置問題を扱った. この問題に対して, 3 つの手法を提案し, Shmoys et al. によって提案された 6 近似アルゴリズムと実験的性能を比較, 検討することによって, 提案手法が近似比率と計算時間の両面で高い性能を持つことを示すことができた. さらに, この問題をより現実に近い “容量制約つき” の場合に発展させ, 容量制約つきサービスを考慮した施設配置問題に対する手法も提案した. 計算機実験により, サービスを考慮した施設配置問題に帰着させるこの手法は有効であることを示すことができた.

今後の課題としては, これらの提案手法に対して理論的な近似保証を与えることが挙げられる. また, 計算機実験において結果が悪くなるような入力データを発見し, 実験を行うことも挙げられる.

参考文献

[1] K. Jain, M. Mahdian and A. Saberi: A new greedy approach for facility location problems. *ACM Symposium on Theory of Computing*, 2002, pp. 731–740.

[2] M. Mahdian, Y. Ye and J. Zhang: Improved approximation algorithms for metric facility location problems. *APPROX*, http://www.mit.edu/~mahdian/pub.html, 2002.

[3] M. Mahdian, Y. Ye and J. Zhang: A 2-Approximation Algorithm for the Soft-Capacitated Facility Location Problem. http://www.mit.edu/~mahdian/pub.html, *APPROX*, 2003.

[4] D. B. Shmoys, C. Swamy and R. Levi: Facility Location with Service Installation Costs. *Proceedings of the Fifteenth Annual ACM-SIAM Symposium on Disctrete Algorithms*, 2004, pp. 1081–1090.

研究業績一覧

著書

1. 浅野孝夫，平田富夫，小野孝男，浅野泰仁: “組合せ最適化：理論とアルゴリズム（B. Korte and J. Vygen: Combinatorial Optimization: Theory and Algorithm, Springer, 3rd edition, 2006の日本語訳）”, シュプリンガー・フェアラーク東京, 2005年11月.
概要: 組合せ最適化の全般を簡潔にまとめた本で最新の成果まで含む内容である。全部で22章からなり、その詳細は以下の通りである。第1章 はじめに、第2章 グラフ、第3章 線形計画法、第4章 線形計画アルゴリズム、第5章 整数計画法、第6章 全点木と有向木、第7章 最短パス、第8章 ネットワークフロー、第9章 最小費用フロー、第10章 最大マッチング、第11章 重み付きマッチング、第12章 b-マッチングと T-ジョイン、第13章 マトロイド、 第14章 マトロイドの一般化、第15章 NP-完全性、第16章 近似アルゴリズム、第17章 ナップサック問題、第18章 ビンパッキング問題、第19章 多品種フローと辺素パス、第20章ネットワーク設計問題、第21章 巡回セールスマン問題、第22章 施設配置問題。

学術論文

1. Takao Asano:
“An Improved Analysis of Goemans and Williamson’s LP-relaxation for MAX SAT”, Theoretical Computer Science, 2006, to appear .
概要: For MAX SAT, which is a well-known NP-hard problem, many approximation algorithms have been proposed. Two types of best approximation algorithms for MAX SAT were proposed by Asano and Williamson: one with best *proven* performance guarantee 0.7846 and the other with performance guarantee 0.8331 if the performance guarantee of the Zwick’s algorithm for MAX SAT is as conjectured. Both algorithms are based on their sharpened analysis of Goemans and Williamson’s LP-relaxation for MAX SAT. In this paper, we present an improved analysis which is simpler than the previous analysis. Furthermore, algorithms based on this analysis will play a role as a better building block in designing an improved approximation algorithm for MAX SAT. Actually we show an example that algorithms based on this analysis lead to approximation algorithms with performance guarantee 0.7877 and conjectured performance guarantee 0.8353 which are slightly better than the best known corresponding performance guarantees 0.7846 and 0.8331 respectively.

2. Koichi Nihei, Takao Asano:
“Congestion Minimization Confluent Flow Problem: Experimental Evaluation of Algorithms”, Proc. 4th Japanese-Hungarian Symposium on Discrete Mathematics and Its Applications, 16–24, June 2005.
概要: A flow is called confluent if, at every node, all the flow leaves along a single edge. The congestion minimization confluent flow problem is stated as follows: given a directed graph, sinks and nonnegative demands on nodes, find a minimum congestion confluent flow that routes all the demands to sinks. For this problem, a $(1+\ln k)$-approximation algorithm was proposed by Chen et al. in 2004, where k is the number of sinks. In this paper, we evaluate its experimental performance and show that a greedy post-processing works well.

3. M. Tamura, S. Taoka, T. Watanabe:
“Improving Performance Ratios by Repeatedly Executing Approximation Algorithms for Several Graph Connectivity Related Problems”, Proc. 4th Japanese-Hungarian Symposium on Discrete Mathematics and Its Applications, 385–397, June 2005.
概要: 与えられた辺重み付きグラフの最小

重み強連結グラフを求める問題と最小重みk辺連結グラフを求める問題を考える．いずれの問題もネットワーク構成に関わる基礎的な問題であり、NP-困難であることが知られている。本稿では，これらの問題に対する$(2-2/|V|)$-近似アルゴリズムを提案する．また，与えられたグラフの辺連結度を1だけ増加させる最小重みの付加辺集合を求める問題を考え，この問題に対する$(2-2/|L|)$-近似アルゴリズムを提案する．ここで，Lは与えられたグラフから構成される木の葉集合である．

4. S. Toriumi, H. Endo, K. Imai:
"Label Size Maximization for Rectangular Node Labels", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E89-A, No.4, 2006, to appear.
概要: GISにおける地図利用の際，人間が見て分かりやすい地図を表示することは重要な課題となっている．数値地図の普及によって，コンピュータを用いて自動的に地図を作成することが多くなり，注記も自動で配置する必要に迫られてきた．地図に注記を配置する，ラベル配置問題には，ラベルの大きさを与え，なるべく多くのラベルを配置するという，ラベル数最大化問題と，全てを配置できるようなラベルの最大の大きさを求める，ラベルサイズ最大化問題の2つの最適化問題が存在する．本論文ではラベルサイズ最大化問題の解法を提案している．

5. Y. Yokosuka, K. Imai:
"Guaranteed-Quality Anisotropic Mesh Generation for Domains with Curves", Proc. 22nd European Workshop on Computational Geometry, March 27-29, 2006, Delphi, Greece.
概要: メッシュ生成は実用の分野において多くの応用があり，その基礎を計算幾何学に置くものである．曲面における三角形メッシュには，正三角形に近い三角形を出力する等方性メッシュと，指定された方向に引き伸ばされた非等方性メッシュの2種類がある．境界が曲線で与えられているようなパラメトリック曲面に，どちらを生成しても三角形の形状を保証する手法を提案している．

研究会等

1. 中塩 英良，浅野孝夫:
"サービスを考慮した施設配置問題に対する近似アルゴリズムの実験評価", 情報処理学会アルゴリズム研究会報告, AL105-2, pp.9–16, 2006.
概要: 施設配置問題の1つとして, 2004年にShmoys, Swamy and Leviが提唱したサービスを考慮した施設配置問題がある．本論文ではこの問題に対して, 容量制約なし施設配置問題に帰着させることによって得られる手法, 容量制約なし施設配置問題において現在もっとも近似率の良い1.52近似に基づく手法と, 1.61近似基づく手法を提案する．そして, Shmoys et al.によって提案された6近似アルゴリズムの実験的性能評価を行い, 提案手法が高い性能を持つことを示す.

C04: 実践的な列挙アルゴリズムの理論構築

宇野 毅明 † 中野 眞一 ‡ 松井 泰子 § 岡本 吉央 ¶

† 国立情報学研究所情報学基礎研究系
〒 101-8430 東京都千代田区一ツ橋
uno@nii.jp

‡ 群馬大学工学部情報工学科
〒 376-8515 群馬県桐生市
nakano@cs.gunma-u.ac.jp

§ 東海大学理学部情報数理学科
〒 259-1292 平塚市北金目 1117
yasuko@ss.u-tokai.ac.jp

¶ 豊橋技術科学大学工学部情報工学系
〒 441-8580 愛知県豊橋市
okamotoy@ics.tut.ac.jp

2005 年度は，列挙アルゴリズムの研究にとって発展の年であった．最適化，人工知能，データベースなどの情報学分野を中心に列挙を用いたモデル化が行われ，物理・化学をはじめとする他の科学領域，および産業分野でも，それらのモデルを用いた研究が進められている．特に機械学習やデータマイニングといった，数理的な対象を分析し，知識を発見する分野において，列挙アルゴリズムが広く使われ，また研究されてきている．応用分野においても，web データ，テキストデータ，実験データ，金融時系列データ，顧客データ，販売データ，事故・故障記録データ，ゲノム配列など，機械的に収集された巨大なデータがますます増加し，そこから有用な情報を探し出すためには，列挙のような網羅的なアプローチを高速に行うことが肝要となっている．このため，ここ 1-2 年で列挙を用いたモデル化とその解法は活発に研究されてきたが，複雑な構造の列挙は容易でないため，簡単な構造，あるいはその列挙手法に工夫を加えて構築したモデル・解法の研究が多くなっている．

また，巨大データの取り扱いのため，列挙アルゴリズムの高速化に対しては，以前よりも要求が高まってきている．高速な列挙アルゴリズムの開発のみに焦点をあてた研究も増えてきており，特に著名な問題においては，多くの研究が行われている．しかし，これらの研究はそれほど系統立てて行われているわけではなく，いくつもの技術が乱立している．この問題点を解決しようと，データマイニング分野において，データベース中に頻出する集合を列挙する問題に対するプログラムのコンテストが 2003 年度，2004 年度と 2 回にわたって行われてきた．このコンテストには多くのアルゴリズムとその実装が投稿され，応用分野から取り出したデータセットに対して，計算効率の検証が行われた．結果，多くの技術が 1 箇所に集積され，参照されることとなり，頻出パターン列挙に関する応用研究の大きな助けとなっている．また，このコンテスト以降，頻出する集合の列挙アルゴリズムの開発研究は多少減少したようだが，これは技術の整理によって，無駄な開発が行われなくなったと見るべきであろう．本研究課題からも，このコンテストにプログラムの投稿を行った．このプログラムは，審査の結果，最優秀賞を収めることができた．これは，理論的なアルゴリズム研究に対して，実践的な技術を付加し，応用上有用なアルゴリズムの設計理論を構築しようとする，本研究課題の方向性が世界的な舞台でも認められ，その有効性が実証されたと言えるであろう．

このような研究背景を鑑み，今年度はデータマイニングなど応用分野での活用を意識した，列挙アルゴリズムの研究を行った．特に，アルゴリズムの単純性や，応用上重要と思われるモデルに対する問題やアルゴリズムの拡張には重点を置いた．以下でその成果を簡単にまとめる．

色付き木とは，各頂点に色集合の中から選ばれた色が 1 つ塗られているような木のことをいう．色をラベルだと考えれば，ラベル付きの木と考えてもよい．通常，アルゴリズム理論やグラフアルゴリズムの研究では，ラベルは無視されることが多いが，現実のデータでは，各ノードに情報が付加され，ラベル付きの木となっていることが多い．例としては，環構造を含まない化合物のデータや，XML のデータなどがある．このようなデータベースを解析する際に，列挙的なアプローチがしばし

ばとられる．例えば特徴的な，あるいは頻出する木構造を列挙して知識発見のベースとしたり，分類，あるいはクラスタリングのため，仮説となる木構造を列挙したりするものである．これらの列挙的なアプローチは，ラベル付き木の効率的な列挙手法を必要とする．しかし，列挙自体はそれほど単純な問題ではなく，直接的な手法では重複を回避するためにメモリを大量に使用することになり，また，1 つの解を複数回探索することによる計算時間の増大も問題となる．

今回の研究では，このラベル付きの木を効率良く列挙する列挙手法の開発を行った．このアルゴリズムは，すべての色付き木の上に木構造型の探索ルートを暗に構築し，それを深さ優先探索することにより列挙を行う．そのため，重複の回避が容易である．また，探索ルート上での色付き木の隣接構造が数学的に良い構造を持っているため，一回の移動を定数時間で行うことができる．このため，色付き木を１つあたり定数時間で列挙することができる．

この探索ルート上では，根から葉のほうへと進むにつれ，色付き木の大きさが１つずつ増えるようになっている．そのため，知識発見や仮説の列挙などで重要な,「ある種の単調な性質を満たす木のみを見つける」という作業にも適している．実際，このアルゴリズムを用いることで，データマイニングの分野で未解決であった，データベースの中で頻出するラベル付き木を列挙する問題に対する多項式時間アルゴリズムを与えることができる．

上記の色付き木列挙アルゴリズムは効率が良く，計算量の観点からも最適となっている．しかし，データマイニングなどの応用分野を考えた場合，必ずしもこのアルゴリズムを用いることが最良の選択とはなりえない．なぜなら，いくつもの色付き木が同じような意味合いを持つのであれば，それらはひとまとまりとして考えられ，まとまりの中からいくつもの解が出力されるるべきではないからである．このようなまとまりを考慮したモデルを用いることで，解が大量に生成され，次の操作に多大な影響を与えるような事態を回避することができる．

まとまりを考慮したモデルとして，近年飽和パターンが注目されている．データベースに頻出するパターンを列挙する問題を考える．ここで，いくつかのパターンがデータベース上のまったく同じ位置に現れるとしよう．このとき，これらのパターンの持つ情報はある意味で同じだと考えられる．そのため，このなかから代表を１つ選び，代表となっているパターンのみを列挙することで，ある意味で冗長なパターンを意味の損失なく抽出することができる．ある種の問題では，パターンが出現している位置の集合に関してある種の演算を施すと，その位置に出現するパターンの中で極大なものが得られる．これを飽和パターンと呼ぶ．頻出アイテム集合列挙における飽和パターンの列挙は著名な問題であり，本研究課題においても，前年度いくつかの研究を行って効率の良いアルゴリズムを得ている．

今回の研究では，この飽和パターンの概念をラベル付きの木構造に拡張した．通常のラベル付き木では，飽和パターンが上手に定義できないため，今回は任意の頂点は，同じラベルを持つ子供を持たない，という仮定をおいた．このような性質を満たす木は rank tree と呼ばれ，論理などの分野で研究されている．rank tree に対しては，パターンの出現位置の共通部分をとることで飽和パターンを定義することができ，数学的にも安定したモデルとなっている．この飽和 rank tree を列挙する問題は直接的には効率よく解けないが，昨年度開発した prefix 保存飽和拡張と呼ばれる，飽和パターンを列挙するための一般的な手法を用いることで，効率よく列挙できる．今回開発したアルゴリズムは，飽和 rank tree を１つあたり $O(n^2)$ 時間で列挙することができる．ここで n は入力したデータベースの大きさである．このような多項式時間アルゴリズムが存在することはアルゴリズム理論の側面からすると非常に興味深いことである．

この他にも，本年度の研究ではいくつかの基礎的な構造に対する列挙アルゴリズムの研究を行っている．いわゆるコンピュータサイエンスや人工知能などの分野では，基礎的な列挙問題に対するツール的なアルゴリズムの欠落があり，これが研究を阻害するひとつの要因となっていると思われる．この欠落を埋めるべく，いくつかの基礎的な構造に対して構造が単純であり，かつ効率のよいアルゴリズムを開発した．

１つ目は，集合の分割を列挙する問題である．

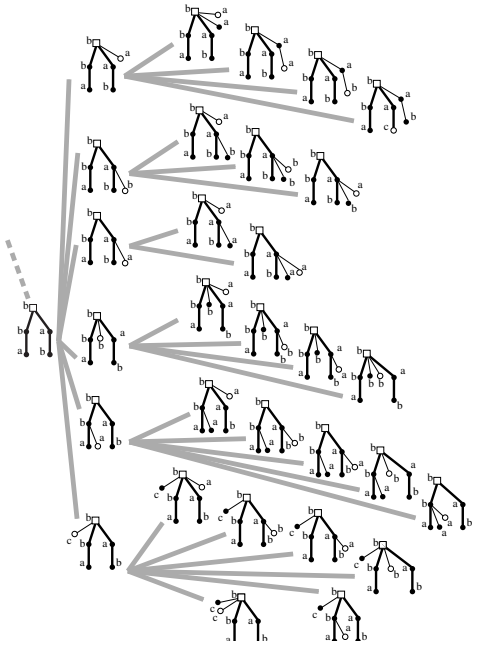


図 2.1: 色付き木の集合上に定義された探索ルート (一部)

集合 $\{1, 2, \cdots, n\}$ が与えられたとき，これを k 個の集合へ分割する分割のしかたを列挙する問題を考える．単純な問題ではあるが，ごく単純な総当り的な手法では効率よく列挙できない．すでに既存のアルゴリズムが存在し，1 つの分割あたり”平均”定数時間で生成できるのだが，今回の研究では，より効率的な探索ルートを構築することで，各分割を，分割 1 つあたり真に定数時間で生成できるようにした．ここでいう真の定数時間とは，任意の出力から次の出力までの時間が定数時間で抑えられるというものである．このような探索ルートの構築がシンプルな定義から行えるということは，計算理論や組合せ数学の見地から興味深い．

2 つ目は，正の整数 n の整数分割を列挙するアルゴリズムである．整数分割とは，n をいくつかの数 $a_1, ..., a_k$ に，$a_1 + \cdots + a_k = n$ となるように分割するものである．この問題は, 組合せ論において基本的な問題の 1 つであり, 長い間, 広く研究されてきた．これまで, 整数分割を 1 つ当たり平均定数時間で列挙する方法しか知られていなかったが，今年度の研究において，整数分割を 1 つあたり真に定数の時間で列挙するアルゴリズムを開発した．これもやはり，整数分割の集合上に効率よい木型の探索ルートを構築できたところが大きな貢献である．

ここまでで報告した列挙アルゴリズムは，パターン列挙型のアルゴリズムである．つまり，ある性質を満たすような構造をすべて列挙するという問題である．それに対して部分構造列挙という問題は，ある与えられた構造の中に含まれる部分構造で，与えられた性質を満たすものを列挙する問題である．簡単のため，構造をグラフだと考えれば，グラフを入力し，その中にある，与えられた 2 点を結ぶパスを列挙する問題，などがこれにあたる．今年度の研究でも，このような部分構造列挙アルゴリズムに関する研究も行った．

まず 1 つ目は部分コーダルグラフの列挙である．コーダルグラフとは，長さ 4 以上のサイクルが必ずショートカット，つまりサイクルの枝ではないが，サイクルの頂点を結んでいるような枝, を持つようなグラフのことをいう．別の見方をすると，すべてのサイクルが三角形に分割されていることになり，三角化グラフともよばれる．このような性質から，統計などの分野ではコーダルグラフが大きな役割を担っている．つまり，グラフがコーダルであるという条件は，統計的な尺度から見てある種のアドバンテージがあるのである．このような観点から，グラフに含まれるすべての部分コーダルグラフを列挙するという問題が考え

られている．コーダルグラフ自身まだそれほどポピュラーな存在ではないため，応用例は少ないが，基礎的かつ重要な問題であることは間違いない．この問題に対して，今年度の研究で，コーダル部分グラフ１つあたり定数時間で列挙を行うアルゴリズムを開発した．また，単純な手法で列挙を行うと，子問題が NP-困難な問題を含むことなり，効率の良い列挙手法を用いることが肝要であることも証明した．

またコーダルグラフを入力として，そのコーダルグラフに含まれる独立集合の数，最大独立集合の数，大きさ k の独立集合の数を計算する線形時間アルゴリズムも開発した．また，入力したコーダルグラフに含まれる，すべての独立集合，すべての最大独立集合，すべての大きさ k の独立集合，すべての極大独立集合を列挙するアルゴリズムも開発した．それぞれ，計算時間は１つあたり定数時間である．また，計算量の観点から，極大独立集合の数を計算する問題は# P-完全 と呼ばれる困難な計算量クラスに属することも証明した．

２つ目の問題は，与えられた 2 部グラフの辺彩色を列挙する問題である．グラフの辺彩色とは，隣接する枝が同じ色を持たないように枝に色を塗る塗り方のことである．上記の議論と同じように色をラベルだと思うと，枝上に情報が付加されたグラフデータと考えることができる．隣接する枝が同じ色を持たないということは，各頂点に対するある種の非冗長性のような条件を与えているとも考えられる．もともと最適化における割当問題において研究されてきた問題であるので，この種のデータ的なアプローチに関してはこれからの研究が期待される．

グラフの辺彩色で色数が最小な物を求める問題は NP-完全であり，困難な問題である．しかし，グラフが 2 部グラフであれば，グラフの最大次数と同じ色数である辺彩色が必ず存在することが知られており，マッチングのアルゴリズムを用いて，その１つを多項式時間で求められることも知られている．今回はこの最小色数の辺彩色に注目し，与えられた 2 部グラフのすべての最小色数辺彩色を効率よく列挙するアルゴリズムを開発した．

この問題に対しては既存のアルゴリズムが存在するが，そのアルゴリズムは基本的に１つの辺彩色あたり 枝数の線形時間よりも真に長い時間かかる計算量になっている．これは，辺彩色を求めるアルゴリズムの基本的な性質から来ており，辺彩色を求めるアルゴリズムの観点からは改良は難しいように見える．しかし，今回の研究では，探索全体での計算時間に着目し，探索を行う木構造のルート上で，葉のレベルに近い部分が全体の計算時間を占め，かつその部分では辺彩色１つあたりの計算量が頂点数の線形となっていることを証明した．このため，アルゴリズム的に複雑な技法を用いることなく単純な改良のみで，計算量を頂点数に比例する時間まで，劇的に小さくすることに成功した．このような解析を中心としたアルゴリズムの高速化は，実用上効率の良いアルゴリズムと理論的な計算量との乖離を埋めるという意味で非常に有効な技術であり，今回の研究もこの点に対する貢献が大きいと考えている．

３つ目の問題は，入力した半順序集合に対して，そのトポロジカルオーダリングをすべて列挙する問題である．トポロジカルオーダリングとは，集合の要素を半順序の順序での逆転が生じないよう並べる並べ方のことである．半順序を有向グラフで表現していると考えれば，トポロジカルオーダリングとは，必ず有向枝の向きが右から左になるように，頂点を直線上に並べる並べ方と考えてよい．この問題に対しても既存の手法が存在する．既存の手法はトポロジカルオーダリング全体の集合を含む集合を考え，その集合の上に直線型の探索ルートを構築している．この手法だと，１つのオーダリングを１回訪れることなり，また，探索ルートが直線であるため，応用上での取り回しに問題がある．今回の研究では，トポロジカルオーダリングの集合上に木構造型の探索ルートを構築することに成功した．計算量は，既存手法では１つあたり平均定数時間であったのが，本研究でのアルゴリズムは１つあたり真に定数時間となっており，改善がなされている．

本年度の列挙アルゴリズムに関する研究は以上である．本年度の研究ではこの他にも，列挙的なアプローチを用いていくつかの最適化問題の研究を行っている．以下でそれを解説する．

平面巡回セールスマン問題とは，与えられた２次元上の地点をすべて通り，もとの地点に戻ってくるようなルートの中で最短なものを求める問題である．入力した地点の凸包を取ったときに，そ

の凸包の外周に含まれない地点を内点と呼ぶ．今回の研究では，内点の数がある小さな数 k で抑えられるような場合に注目し，$O(k!kn)$ 時間と $O(k)$ メモリで最短ルートを求めるアルゴリズムと，$O(2^k k^2 n)$ 時間と $O(2^k kn)$ メモリで動くアルゴリズムを開発した．

また，有向マトロイドにおける実現性にかかわる問題においても，マトロイドのランクが 4 であり，かつ要素数が 8 である場合について，どのような性質が成り立つかを研究した．今後有向マトロイドの列挙問題と関連し，より大きな部分での性質を明らかにできることが期待される．

研究業績一覧

学術論文

1. Shin-ichi Nakano, Takeaki Uno:
"Generating Colored Trees", 31st International Workshop on Graph-Theoretic Concepts in Computer Science, Lecture Notes in Computer Science, 3787, 249-260, 2005 年 12 月.
概要: A c-tree is a tree such that each vertex has a color c in $\{c_1, c_2, ..., c_m\}$. The problem of enumerating all c-trees with at most n vertices without repetition has an application to data mining problem of tree structured patterns, however no efficient algorithm, which generates each tree in constant time on average, is known. In this paper we give a simple algorithm for enumerating c-trees with at most n vertices and diameter d. Our algorithm generates each c-tree in constant time on average. By using the algorithm for each diameter $2, 3, ..., n-1$, we can generate all c-trees with at most n vertices.

2. Yoshio Okamoto, Takeaki Uno, Ryuhei Uehara:
"Linear-Time Counting Algorithms for Independent Sets in Chordal Graphs", 31st International Workshop on Graph-Theoretic Concepts in Computer Science, Lecture Notes in Computer Science, 3787, 433-444, 2005 年 12 月.
概要: We study some counting and enumeration problems for chordal graphs, especially concerning independent sets. We first provide the following efficient algorithms for a chordal graph: (1) a linear-time algorithm for counting the number of independent sets; (2) a linear-time algorithm for counting the number of maximum independent sets; (3) a polynomial-time algorithm for counting the number of independent sets of a fixed size. With similar ideas, we show that enumeration (namely, listing) of the independent sets, the maximum independent sets, and the independent sets of a fixed size in a chordal graph can be done in constant amortized time per output. On the other hand, we prove that the following problems for a chordal graph are # P-complete: (1) counting the number of maximal independent sets; (2) counting the number of minimum maximal independent sets. With similar ideas, we also show that finding a minimum weighted maximal independent set in a chordal graph is NP-hard, and even hard to approximate.

3. Hiroaki Arimura, Takeaki Uno:
"An Output-Polynomial Time Algorithm for Mining Closed Frequent Ranked Tree Patterns", Lecture Notes in Artificial Intelligence, 3625, 1-19, 2005 年 8 月.
概要: Frequent closed pattern discovery is one of the most important topics in the studies of the compact representation for data mining. In this paper, we consider the frequent closed pattern discovery problem for a class of structured data, called attribute trees (AT), which is a subclass of labeled ordered trees and can be also regarded as a fragment of description logic with functional roles only. We present an efficient algorithm for discovering all frequent closed patterns appearing in a given

collection of attribute trees. By using a new enumeration method, called the prefix-preserving closure extension, which enable efficient depth-first search over all closed patterns without duplicates, we show that this algorithm works in polynomial time both in the total size of the input database and the number of output trees generated by the algorithm. To our knowledge, this is one of the first result for output-sensitive algorithms for frequent closed substructure disocvery from trees and graphs.

4. Yasuko Matsui, Takeaki Uno:
"On the Enumeration of Bipartite Minimum Edge Colorings", to appear in the conference proceedings on Graph Theory 2004, 2005 年.
概要: For a bipartite graph $G = (V, E)$, an edge coloring of G is a coloring of the edges of G such that any two adjacent edges are colored in different colors. In this paper, we consider the problem of enumerating all edge colorings with the fewest number of colors. We propose a simple polynomial delay algorithm whose amortized time complexity is $O(|V|)$ per output, whereas the previous fastest algorithm took $O(|E| \log |V|)$ time per output. Although the delay of the algorithm is $O(|E||V|)$, the delay of our algorithm can be reduced to $O(|V|)$ by using a simple modification with a queue of polynomial size. We show an improvement to reduce the space complexity from $O(|V||E|)$ to $O(|E|+|V|)$. Furthermore, we obtain a lower bound $(|E| - |\hat{V}| + 1) \max\{2^{\Delta-3}, 2(|\hat{V}|/2+1)^{\Delta-3}/(\Delta-1)\}/\Delta$ of the number of edge colorings included in G, where Δ is the maximum degree and $\hat{V}$ is the set of vertices of the maximum degree.

5. Shin-ichiro Kawano and Shin-ichi Nakano:
"Constant Time Generation of Set Partitions", IEICE TRANS. FUNDAMENTALS, E88-A, 930-934, 2005 年.
概要: 集合 $\{1, 2, \cdots, n\}$ の k 個の集合への分割を列挙する簡単かつ高速なアルゴリズムを与える．そのような分割の個数は第二種のスターリング数として知られている．我々のアルゴリズムは，各分割を，分割1つあたり定数時間で，重複も抜けもなく生成するが，既知のアルゴリズムは，各分割を，分割1つあたり"平均"定数時間で生成するものしか知られていない．各 $k = 1, 2, \cdots, n$ について，分割を列挙することにより，集合 $\{1, 2, \cdots, n\}$ のすべての分割も列挙できる．そのような分割の個数はベル数として知られている．

6. Shin-ichiro Kawano and Shin-ichi Nakano:
"Generating All Series-parallel Graphs", 電子情報通信学会英文論文誌, 離散数学とその応用小特集号, E88-A, 1129-1135, 2005 年.
概要: 本論文は高々m 本の辺からなるすべての直並列グラフを列挙するアルゴリズムを与える．このアルゴリズムは各直並列グラフを，グラフ1つあたり，平均定数時間で生成する．

7. Vladimir G. Deineko, Michael Hoffmann, Yoshio Okamoto and Gerhard J. Woeginger:
"The traveling salesman problem with few inner points", Operations Research Letters, 31, 106-110, 2006 年.
概要: We propose two algorithms for the planar Euclidean traveling salesman problem. The first runs in $O(k!kn)$ time and $O(k)$ space, and the second runs in $O(2^k k^2 n)$ time and $O(2^k kn)$ space, where n denotes the number of input points and k denotes the number of points interior to the convex hull.

研究会等

1. 小野顕光, 中野眞一:
"Constant Time Generation of Linear Extensions", 電子情報通信学会コンピュテーション研究会 COMP2005-16, 2005-16, 2005 年.

概要: 半順序集合 $\mathcal{P}$ が与えられたときに, すべてのトポロジカルソートを生成する幾つかのアルゴリズムが知られている.) 既知のアルゴリズムで最も高速なものは, 各トポロジカルソートを “平均” 定数時間で生成する. 本文は, 各トポロジカルソートを定数時間で生成するアルゴリズムを与える. 既知のアルゴリズムは, 各トポロジカルソートを丁度 2 回づつ生成し, そのうちの一方のみを出力するのに対し, 我々のアルゴリズムは各トポロジカルソートを丁度 1 回づつ生成する.

2. 山中克久, 川野晋一郎, 菊地洋右, 中野眞一: “整数分割の列挙”, 情報処理学会アルゴリズム研究会, 104, 2006 年.
概要: 本文では, 正の整数 n の整数分割を列挙するアルゴリズムを与える. この問題は, 組み合わせ論において基本的な問題の 1 つであり, 長い間, 広く研究されてきた. これまで, 整数分割を 1 つ当たり平均定数時間で列挙する方法しか知られていなかった. 我々は, 与えられた整数の整数分割を, 最悪でも 1 つ当たり定数時間で重複なく列挙するアルゴリズムを提案する. また, 条件付きの整数分割を定数時間で列挙するアルゴリズムをいくつか与える.

3. Hiroki Nakayama, Sonoko Moriyama, Komei Fukuda and Yoshio Okamoto: “Comparing the strengths of the non-realizability certificates for oriented matroids”, Proceedings of 4th Japanese-Hungarian Symposium on Discrete Mathematics and its Applications, 243–249, 2005 年.
概要: An oriented matroid is a combinatorial abstraction of a vector configuration in a real vector space. An oriented matroid is *realizable* if it is obtained from a vector configuration. Deciding realizability of an oriented matroid is known to be NP-hard. There are several classes of non-realizable oriented matroids which admit succinct certificates derived from the non-Euclidean, the non-Shannon, the non-HK, the non-HK* methods, and the method of biquadratic final polynomials. In the present paper we focus on OM(4,8), the class of rank-4 oriented matroids on an 8-element ground set. We report the complete classification of OM(4,8) with respect to the five non-realizability certificates. In particular, the result shows the superiority of the certificate using biquadratic final polynomials to the other certificates, both in uniform and non-uniform cases.

学会大会等

1. 松井 泰子: “On the Groebner walks”, International conference on Theoreitical Effectivity and Practical Effectivity of Groebner Bases, 2005 年 8 月.

2. 松井 泰子: “On Junction Tree Algorithms”, 2nd Pacific Workshop on Discrete Mathematics, 2005 年 12 月.

3. 松井 泰子: “An Algorithm for Enumerating All Tree Matchings for Ordered Trees”, 37th Southeastern International Conference on Combinatorics, Graph Theory and Computing, 2006 年 3 月.

4. 清見 礼, 宇野 毅明, 松井 知己: “電力取引における約定量決定問題の高速解法”, 日本オペレーションズ・リサーチ秋季研究発表会, 2005 年 9 月.

C05: 幾つかの画像関連問題の計算複雑度の解析と効率的な解決法の提案

浅野 哲夫 † 上原 隆平 † 元木光雄 † 小保方 幸次 ‡ 河村 泰之 §

† 北陸先端科学技術大学院大学・情報科学研究科
〒 923-1292 石川県能美市旭台
{t-asano, uehara, mmotoki}@jaist.ac.jp

‡ 一関工業高等専門学校・制御情報工学科
〒 021-8511 一関市萩荘字高梨
obokata@ichinoseki.ac.jp

§ 石川工業高等専門学校・電子情報工学科
〒 929-0392 石川県河北郡津幡町北中条タ 1
kawamura@ishikawa-nct.ac.jp

1 はじめに

最近のディジタルカメラに代表される画像入力装置の普及は目を見張るものがある．それに伴って計算機で画像を処理する機会が飛躍的に増大しているが，入力装置の性能向上は必然的にデータ量増大を招き，従来からの素朴なアルゴリズムでは妥当な時間内に処理することが困難になりつつあるのが現状である．将来を展望したとき，データ量の爆発により処理不能に陥る危険性があり，今のうちに計算量の理論に基づいて計算困難度を数学的に解析し，それに基づいてアルゴリズムを開発することが急務である．

このような観点から，本研究では，アルゴリズム理論の立場から画像に関連する諸問題に取り組んだ．学術的にはコンピュータビジョンやコンピュータグラフィックスの分野がこれに密接に関連しているが，これらの分野では問題を数学的に定式化して，その計算複雑度を解析することは余り一般的ではない．むしろ，計算機実験を通して人間の目視による判断が優先される傾向にある．本研究では画像に関連する様々な問題について，その本質を数学的に定式化することから始めて，計算複雑度を解析し，最終的には効率の良いアルゴリズムを開発することを目指している．

上記の目標を達成するために，本年度から新たに３名の研究者をグループに迎え入れた．同じ講座の助教授である上原隆平，一関高等専門学校・制御情報工学科の小保方幸次，それに石川工業高等専門学校・電子情報工学科の河村泰之である．上原は，グラフ理論面からの貢献を，小保方は画像の領域分割などでの理論と実験に関する研究を，河村はディスクレパンシ理論に基づいた一様点配置問題に関する研究を担当する．

点配置問題に関しては，ディスクレパンシの基準に基づいた方式の理論を構成した後，実験的にも予想を超える成果を得ることができた．この結果は電子情報通信学会の論文誌に投稿した．また画像のディジタルハーフトーニングについては世界的に関心を集め，年度内に国際会議での招待講演を二回行った．反響は高く，この分野の研究が盛んになるものと期待できる．適応型メッシュ生成については，初期の理論結果を得ることができた．指紋同定に関しては指圧による変形も考慮した新たな手法を提案し，国際会議で発表するとともに，電子情報通信学会においても論文の形で発表した．以下では，指紋同定に関する研究について詳しく述べる．

2 A Combinatorial Approach to Fingerprint Analysis using Euclidean Distance Transform

2.1 Introduction

Automatic fingerprint identification systems (AFIS) are used for personal identification. Fingerprints have the properties of distinctiveness or individuality, and persistence over time.

These properties make fingerprints suitable for biometric uses. AFISs are usually based on minutiae matching [7, 11, 12]. Minutiae, or Galton's characteristics [9] are local discontinuities in terms of terminations and bifurcations of the ridge flow patterns that constitute a fingerprint. These two types of minutiae have been considered by the Federal Bureau of Investigation for identification purposes [17]. AFIS based on minutiae matching involves different stages (see 図 2.1(a) for an illustration): (i) fingerprint image acquisition; (ii) preprocessing of the fingerprint image; (iii) feature extraction (e.g. minutiae) from the image; (iv) matching of fingerprint images for identification. A detailed and insightful discussion on all these steps can be found in [11, 13], and as such to avoid repetition, we refer the reader to them. Our work in this paper focusses on binarization and minutiae extraction preceded by an enhancement step (see Fig. 2.1(b)). Below we briefly discuss the enhancement method we used.

2.2 Enhancement of Fingerprint Images

Fingerprint images require specialized enhancement techniques owing to their inherent characteristics like a high noise content. The much widely used PCASYS package [4] uses an enhancement algorithm described earlier [2]. It involves cutting out subregions of the images (a 32×32 block to be specific), taking their FFT and suppression of a band of low and high frequency components followed by some non-linear operations in the frequency domain and transforming the images back to the spatial domain. This algorithm was also used by Kovács-Vajna [12]. We have also used this enhancement algorithm in our work owing to its simplicity and elegance.

The preprocessing phase is known to consume over 95% of the total time of fingerprint identification and verification [5]. That is the reason a considerable amount of research has been focussed on this area.

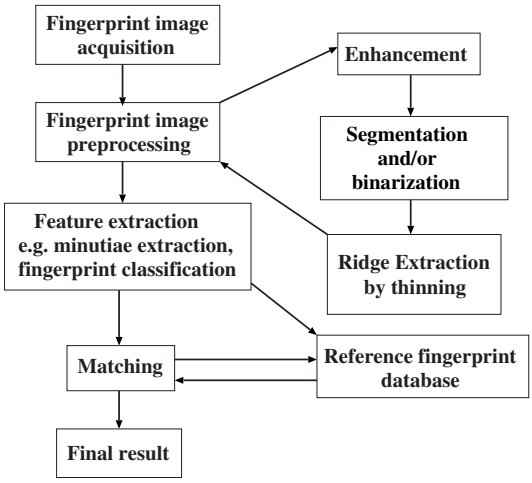
2.3 Our Work

Most of the previous algorithms designed for fingerprint binarization [6, 14, 15] are heuristics, in that they do not start with a definition of an optimal threshold. In contrast, we define a condition for an optimal threshold based on equal widths of ridges and valleys and then design a combinatorial algorithm for finding such an optimal threshold. Width is estimated using EDT. Most of the current fingerprint methods that use binarization perform thinning to get a 1-pixel thick ridge (see 図 2.1(a)). Then, minutiae are detected from the thinned image. We show that by using EDT values one can straightaway detect minutiae from the binarized image without applying any sort of thinning. Most of the methods developed in fingerprint analysis use arbitrarily selected parameters and in many cases they are not justified; it is just experimentally selected. Our work depends minimally on an arbitrary choice of parameters because EDT value adapt itself to the data. The highlights of our work are: (i) a deterministic algorithm for binarization; (ii) minutiae detection without thinning and (iii) minimal use of arbitrary parameters.

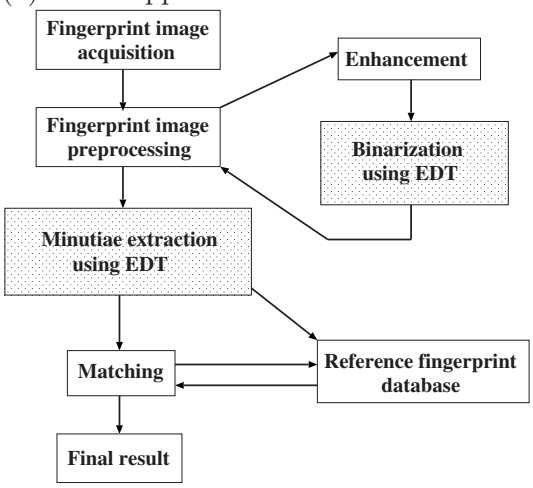
2.4 The Binarization Algorithm

Euclidean Distance Transform

A two-dimensional binary image I of $N \times N$ pixels is a matrix of size $N \times N$ whose entries are 0 or 1. The pixel in a row i and column j is associated with the Cartesian co-ordinate (i, j). The EDT of a binary image I is defined in [3] as an assignment to each background pixel (0) (i, j) a value equal to the Euclidean distance between (i, j) and the closest feature pixel (1). Breu et al. [3] proposed an optimal $O(N \times N)$ algorithm



(a) Usual approaches.



(b) Our approach.

図 2.1: Two flowcharts showing the different phases in fingerprint analysis taken by (a) usual approaches and (b) our method. In (b) the highlighted modules show the area of our work.

using Voronoi diagrams. In [10], Hirata and Katoh give a much simpler algorithm using envelope of parabolas with the same complexity as [3] for finding EDT. In keeping with the above, we define two types of EDT values. The first one $DT_{0,1}$ is the same as the above. The second one is $DT_{1,0}$ which is the value assigned to a 1 pixel equal to the Euclidean distance to the nearest 0 pixel. Using the results given in [10], we have the following fact:

Fact 1 *Both $DT_{1,0}$ and $DT_{0,1}$ can be computed in optimal time $\theta(N^2)$ for an $N \times N$ binary image. Also, the values of both $DT_{1,0}$ and $DT_{0,1}$ are greater than or equal to* 1.

2.5 Euclidean Distance Transform and Width

Fingerprint images are characterized by almost equal width ridges and valleys. We will use this particular characteristic of the fingerprint image for binarization. Measuring the width for arbitrary shapes is a difficult, non-trivial problem. In this section, we model the problem in continuous domain to show how EDT can be used to find equal width ridges and valleys.

Model in the continuous domain

The fingerprint image can be modeled. In the continuous domain, the image is a continuous function $f : (x, y) \rightarrow I\!R$. A cross section of this function along a direction perpendicular to the ridge increases (decreases) till it reaches the ridge point (valley) which is a maxima (minima). Let $t \in [0, M]$ be a threshold, such that if $f \geq t$, it is mapped to 1, else to 0. The highlighted part shown in the middle is the part mapped to 0. After thresholding, the parts would be rectangles. Consider such a rectangular object $ABCD$ of width w and height h, with $h > w$. The medial axis of this object divides the shape into regions such that the nearest boundary line from any point in the region is determined. The total EDT value for region 1 is $\int_0^{w_i/2} \int_{-y+w_i/2}^{y+(h-w_i/2)} (w_i/2 - y)\, dxdy = (w_i^2 h)/8 - w_i^3/12$. Similarly, the total EDT value for region 3 is $\int_{x-w_i/2}^{-x+w_i/2} \int_0^{w_i/2} x\, dxdy = w_i^3/24$. So, the total EDT value $\phi_{dt}(w_i)$ of the rectangle is $w_i^2 h/4 - w_i^3/12 = w_i^2/4(h - w_i/3)$. Note that, the total EDT value increases (decreases) with the increase (decrease) of width because $\phi_{dt}(w_i)' > 0$ and $h > w$. Now, the total distance transform $DT_{1,0}$ is $w_1^2 h/4 - w_1^3/12 + w_3^2 h/4 - w_3^3/12$ and the total distance transform $DT_{0,1}$ is $w_2^2 h/4 - w_2^3/12$. Now, as t increases, both w_1 and w_3 decrease and

w_2 increases. This implies that with increase of t, $DT_{1,0}$ decreases and $DT_{0,1}$ increases. So, $DT_{1,0}$ and $DT_{0,1}$ can intersect only once and evidently, $DT_{1,0}$ is equal to $DT_{0,1}$ when $w_1 = w_2$. That is, the optimal value of threshold is reached when $DT_{0,1} = DT_{1,0}$, implying $w_1 = w_2$. This simple analysis shows that the total of EDT values can be used as a measure of finding a threshold that gives equal width ridges and valleys. So, more formally we have the following definition for the optimal threshold.

Definition 1 *The optimal threshold is a value $t \in [0, M]$ that binarizes the image such that the ridge width is equal to the valley width or sum total of EDT values are equal.*

Discrete image and Euclidean distance transform

In the discrete model, the co-ordinates are discrete given by the pixel locations. So, the observations from the previous subsection do not directly apply. But, the crucial observation from the previous subsection is that sum total of $DT_{1,0}$ values decreases with t and the sum total of $DT_{0,1}$ values increases with t.

Lemma 1 *The sum total of $DT_{1,0}$ values decreases with the threshold t. Similarly, the sum total of $DT_{0,1}$ values increase with the threshold t.*

The proof is easy. We know that each of the EDT values in the discrete domain is greater than or equal to 1. So, with the threshold t increasing, pixels in the binary image move from the regions of 1 to 0, thus making $DT_{1,0}$ and $DT_{0,1}$ decreasing and increasing respectively. Then, the optimal threshold t can be computed from the intersection of these two curves. But, in the discrete case, we may not be able to locate a single value, where the functions of sum total of $DT_{1,0}$ and $DT_{0,1}$ meet. So, we modify the definition of the optimal threshold in the discrete case as follows.

Definition 2 *The optimal threshold can be two values t_1 and t_2 such that $t_2 - t_1 = 1$ and the sum total of $DT_{1,0}$ values is greater than the sum total of $DT_{1,0}$ values at t_1 and their relation reverses at t_2.*

2.6 Algorithm for Binarization

To take care of different contrast and intensity across different image regions, we apply local thresholding. We cut out 32×32 sub-blocks of the image region and apply the enhancement algorithm due to [2] followed by our binarization algorithm. Due to the monotonically increasing (decreasing) property of the sum total of $DT_{0,1}$ ($DT_{1,0}$) with the threshold t ($t \in [0, M-1]$), we can employ a binary search to find the optimal threshold according to Def. 2. For the pseudocode, see [1].

Theorem 1 *The binarization algorithm under Definition 2 runs in time $O(N^2 \log M)$.*

The binary search is employed $O(\log M)$ times and the dominant computation is the computation of EDT and its sum which takes $O(N^2)$ time (see Fact 1). Thus the total time complexity of the binarization process is $O(N^2 \log M)$. With M, the number of gray levels, being a constant for all practical purposes, the algorithm for binarization runs in time that is linear in the number of pixel entries, which is $O(N^2)$.

Remark 1 *Note that the monotonic curves corresponding to sum of $DT_{1,0}$ and $DT_{0,1}$ may not intersect when sum of $DT_{1,0}$ is always greater than sum of $DT_{0,1}$. This happens for image blocks which are noisy or do not have a proper gray level distribution, like a fingerprint image. We characterize such blocks as non-binarizable blocks. Thus, our binarization algorithm has an added property of segmenting the fingerprint image region.*

3 Previous binarization algorithms and comparisons

Here, we review three previous works and compare these methods with ours.

3.1 Binarization algorithm of Moayer and Fu

Moayer and Fu [14] proposed an iterative algorithm using repeated convolution by a Laplacian operator and a pair of global dynamic thresholds that are progressively moved towards an unique value. The pair of global dynamic thresholds changes with each iteration and controls the convergence rate to the binary pattern. This method, which requires repeated convolution operations, is time consuming and the final result depends on the choice of the pair of dynamic thresholds and some other design parameters. As local information can not be dealt with well, some impulsive noise needing further preprocessing will always remain.

3.2 Binarization algorithm of Coetzee and Botha

Coetzee and Botha [6] proposed an algorithm that generates the resultant binary image as a logical OR of two binary images. One binary image is obtained by a local threshold on the gray scale image and the other binary image is obtained by filling in the area delimited by the edges. The efficiency of this algorithm depends heavily on the efficiency of the edge finding algorithm to find delimiting edges. As this method uses local thresholds, the results are fairly clear. But, on the flip side, this method uses many arbitrary parameters: (i) the authors use a $2d \times 2d$ (adaptive) window with $d = 2$; (ii) in the gray-scale window, they chose a threshold of 0.6 of the maximum gray value (see Ps. 1443 and 1444 of [6]). The choice of none of these parameters is explained. In effect, our experiments show that a threshold of 0.4 of the maximum gray value works better. Also, as the algorithm uses two windows (gray-scale and edge), the running time is prohibitively long.

3.3 Binarization algorithm of Ratha et al.

Ratha et al. [15] proposed a binarization approach based on peak detection in the gray-level profiles along sections orthogonal to the ridge orientation. The gray-level profiles are obtained by projection of the pixel intensities onto the central section. This algorithm has two positive factors: (i) the orientation field computed for binarization is also used for the following steps; (ii) this algorithm is the fastest among all of the four methods (including ours) we compared. This method uses a fixed length line segment in certain orientations to binarize, and as such generates the following drawbacks: (i) If the ridges are very close in the image, the binarized ridges are merged together; (ii) Most of the bifurcations and even some ridges are broken by the oriented line segments. Again, like the other two algorithms, this method depends on many arbitrary parameters (see P. 1667 of [15]). Also, the authors did not mention anything about the size of the one-dimensional averaging mask used (see P. 1664 of [15]). This heuristic algorithm, though working well in practice, has a deficiency that it does not retain the full width of the ridges, and as such is not a true binary reflection of the original fingerprint image.

3.4 Comparisons

There are two distinct features of our binarization algorithm compared to the other three methods: (i) as we view binarization as an optimization process, we start with a very clear definition of an optimal threshold; this in turn, allows us to design a truly deterministic algorithm; (ii) our algorithm uses no arbitrary pa-

rameter; the choice of a 32×32 window for local thresholding is dictated by the algorithm for enhancement in [2, 4]. As there is no mathematical way of comparing the results, below we give qualitative comparisons.

Fingerprint images used

We used the fingerprint images from (i) NIST Special Database 4[16], (ii) NIST Special Database 14[4], (iii) Database B1 of FVC2000[8], (iv) Database B2 of FVC2000[8] and (v) fingerprint images scanned by the FUJITSU Fingerprint Sensor (model: FS-210u). The images of (i) and (ii) are of size 480×512. The images of (iii) and (v) are of size 300×300 and (iv) are of size 364×256. All of the images are of 500 dpi resolution. From each database, two images of good quality and two images of bad quality (four in all) were manually selected, thus making 20 images. For each data set, the two images on the left are of good quality and the other two on the right are of bad quality. The quality was determined manually.

Qualitative comparison

First of all, the images were enhanced using the enhancement algorithm of [2]. Then, we ran all the four binarization algorithms on these 20 enhanced images on a Sun Blade 150, sparc, Solaris 5.9, 550 MHz. For a qualitative comparison, we did the following. We asked 5 unbiased volunteers conversant with fingerprint technology to rank the resulting binarized images. Obviously, we kept the identity of the authors of all the algorithms a secret from them! It can be seen that on an average the users ranked the output of our binarization algorithm better than others. As to time, our deterministic algorithm ranks second; the fastest being the algorithm from Ratha et al. [15].

4 Minutiae Detection using Euclidean distance transform

Most of the minutiae detection algorithms find out the minutiae from the one-pixel thick ridge image obtained by thinning after binarization (see, for example, [7]). Once our binarization process finishes, we have a matrix with each ridge pixel having a corresponding EDT value. Our goal is now to exploit this information to detect minutiae directly from the thick ridges of the binary image without thinning. This will be useful for saving time in real world application. In most cases the location of the minutiae will not be exact the same in different versions of the same fingerprint owing to distortion, so it makes sense to find out a small region of connected pixels in which the minutiae lies. Our goal, then, is to find these minutiae regions for further matching. The minutiae treated will be bifurcation and termination.

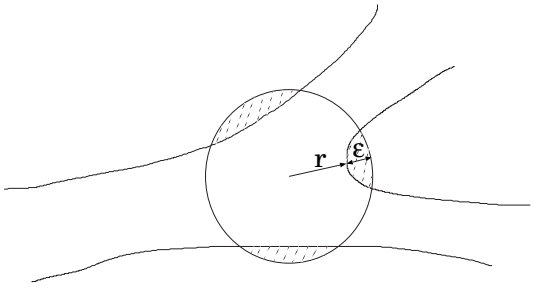
4.1 Detecting bifurcation minutiae

Bifurcation minutiae in the continuous domain

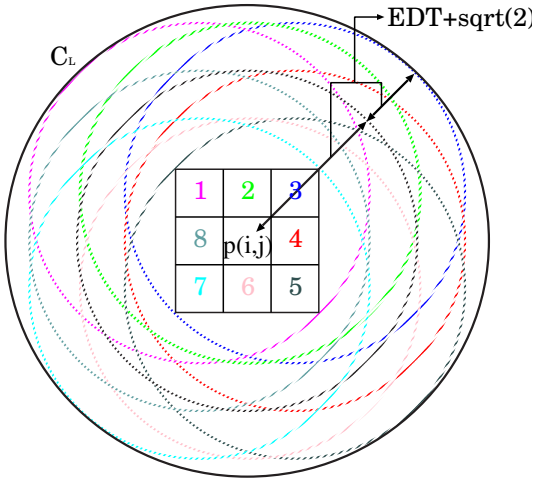
We first show how EDT can be used for finding a bifurcation minutia in the continuous domain in the following observation.

Observation 1 *If we draw a circle C centered at a bifurcation point in the continuous domain with a radius $r + \epsilon$ (where r is the EDT value in the continuous domain and ϵ is an arbitrarily small positive number), then C must contain three background components. See 図 2.2(a) for an illustration.*

Loosely speaking, this bifurcation point corresponds to the bifurcation in the medial axis of the continuous structure. Next, follows a discussion on carrying forward Observation 1 in the continuous domain to the discrete domain.



(a) Bifurcation in the continuous domain; the background components are shown shaded.



(b) Circles formed by the EDT value; the circle C_L is the smallest radius circle covering all the 9 EDT circles (shown dotted).

図 2.2: Finding bifurcation minutiae.

Bifurcation minutiae in the discrete domain

The issue here is to find out an appropriate radius for a circle so that Observation 1 holds in the discrete domain.

Definition 3 *An EDT circle is a circle centered at a grid point (i, j) with a radius r, where r is the EDT value of the grid point (i, j).*

EDT in the discrete domain has a geometric significance as mentioned in the following fact.

Fact 2 *For a ridge pixel p_i having an EDT value r, if we draw a circle C centered at p_i with a radius r, then there will be at least one valley pixel on the circumference of C.*

The radii of two EDT circles whose centers lie in the 8-neighborhood of each other cannot be arbitrary. The following Observation is easy to follow.

Observation 2 *Let the EDT value at a grid point (i, j) and any of its 8-neighbors be r and $r_i, (i = 1, \ldots, 8)$ respectively. Then, surely $r - \sqrt{2} \leq r_i \leq r + \sqrt{2}$.*

The equality is attained when (i, j), any r_i and the pixel that contributes to the EDT value at (i, j) lie on a straight line.

Unlike in a continuous domain, where a point can be chosen as mentioned in Observation 1, it is very difficult to choose a unique pixel as a bifurcation in a discrete digital image. This happens because the medial axis is not uniquely defined for a digital image. So, we mark a set of 9 connected pixels as a region where a bifurcation lies.

Observation 3 *If there is a bifurcation region in a 3×3 window of pixels, there will be three background components of connected pixels inside the union of those 9 EDT circles. See* 図 *2.2(b) for the union of the 9 EDT circles.*

This observation is true because in whatever way a bifurcation enters or leaves the 3×3 region, it divides the 3×3 region into three regions and in each region there will be at least one pixel; and the *EDT* circle centered at this pixel will have three different background components. But, finding out the correct union of these 9 circles is somewhat time consuming. So, we will find out a circle C_L with the least radius centered at (i, j) that covers the union of the 9 *EDT* circles centered at (i, j) and its 8 neighbors.

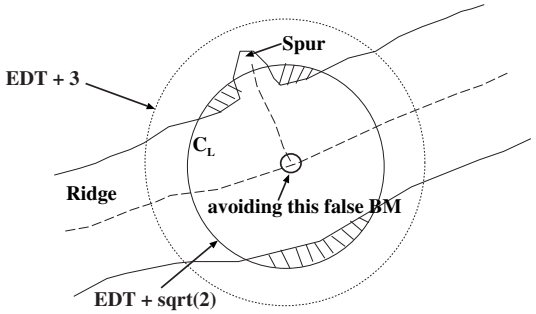
Lemma 2 *The radius of the circle C_L is given by the EDT value plus $\sqrt{2}$.*

The proof follows from Fact 2, Observations 2 and 3.

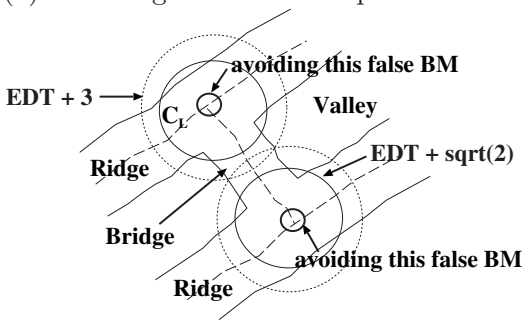
So, to test for a bifurcation region, we form the circle C_L; and if in this circle there are three separate background components, we mark the pixels in this region as bifurcation.

Avoiding spurs and bridges to find bifurcation minutiae

The theory developed earlier for detecting bifurcation fails when there are spurs or bridges, which are deformities in the ridge structure. A *spur* [13] is a small protrusion from the original ridge and gives rise to a false minutia. A *bridge* [13] is a structure that joins two ridges across a valley and gives rise to two false minutiae. See 図 2.3(a) and (b) for examples. To avoid the false minutiae thus generated, we developed the following heuristic. Note that, in the case of spurs, the circle C_L is such that it will cut the spur and generate a bifurcation. To avoid that, we increase the radius of C_L, to find only two connected components and avoid this false bifurcation. In case of bridges, if the radius of C_L is increased appropriately, then both the false minutiae can be removed by detecting the intersection of two such circles. In massive experiments, statistics show the average width of ridges (valleys) is around $5 \sim 6$ pixels wide in 300×300, 500 dpi image. [Note that, from our binarization algorithm, we can estimate the width as average of the EDT values.] So, we increase the radius of C_L and make the new radius as $EDT + 3$ ($3 = \lceil (5/2) \rceil = \lceil (6/2) \rceil$). We now apply the same method of the previous subsection with a new circle C'_L whose radius is $EDT + 3$. The only modification is that we detect the intersection of C'_Ls to avoid bridges. See 図 2.3(a) and (b) for an illustration of spur and bridge removal respectively.



(a) Avoiding detection of spurs as bifurcation.



(b) Avoiding detection of bridges as bifurcation.

図 2.3: Finding correct bifurcation minutiae(BM) by avoiding spurs and bridges.

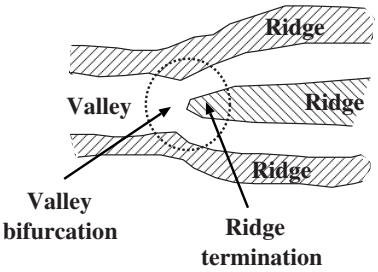
4.2 Detecting termination minutiae

There is a widely held belief that a ridge termination minutiae is a dual of a valley bifurcation minutiae as pointed out in [13] (see Pg. 85-86 of [13] and 図 2.4(a)). With this duality principle in place, we thought that the methodology developed for detecting ridge bifurcation could simply be applied to detect valley bifurcation and hence, ridge termination. But, during our experiments on different data sets, we came across a counter example to this duality principle as shown in 図 2.4(b), where a ridge termination does not correspond to a valley bifurcation. So, we developed the following heuristic method to detect such minutiae. The heuristic method can to some extent differentiate between spurs [13] and real termination minutiae.

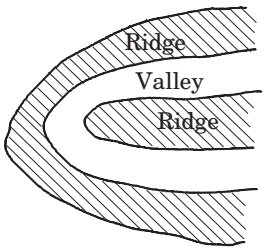
Refer to 図 2.4(c) for the following part of the discussion. We use the circle C'_L defined for determining bifurcation minutiae to detect the termination minutiae.

Observation 4 *A ridge termination minutiae has the following two properties: (i) it is surrounded by a single component of valley pixels inside the union circle and (ii) the length of the elongated part of the ridge termination (estimated by $\overline{bd}$) is greater than the width of the ridge (estimated by $\overline{ac}$) inside the union circle.*

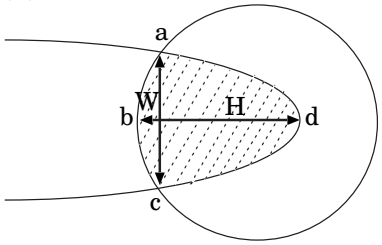
Based on the above observation, our heuristic method for finding a termination is as follows:



(a) The duality relation between ridge termination and valley bifurcation.



(b) A counterexample where duality fails.



(c) Finding termination minutiae.

図 2.4: Finding termination minutiae.

1. Find the two intersection points of the ridge with the union circle (a and c), and compute the length W of the line segment $\overline{ac}$.

2. Find the middle point b of the arc ac of the union circle; and the farthest point d on the ridge boundary from b. Compute the length H of $\overline{bd}$.

3. If $H > W$, then the origin of the union circle is a termination minutiae.

We could remove many spurs in our heuristic for finding terminations because spurs do not satisfy the structural information stated in Observation 4.

4.3 Minutiae detection results

The bifurcation and termination minutiae detected by our algorithm were compared manually with the minutiae present in the enhanced images and the results are given in Table. It can be seen that even for bad quality fingerprint images, our total error is within acceptable limits. Another interesting point to note is that there is no error for exchanging termination and bifurcation minutiae. The time taken for minutiae detection averages 0.177 sec. on an IBM x40, inter pentium M, WinXP, 1.4GHz.

4.4 Conclusion

In this paper, we focussed on binarization and minutiae extraction of fingerprints using a Euclidean distance transform. The particular choice of EDT helped us in developing a deterministic algorithm for binarization. We used the same EDT to find bifurcation and termination minutiae. Working with the original binary image (not the thinned one) has its added advantage: spurs and bridges can be removed in the same phase as minutiae detection. The most notable distinction of our work is that it uses a minimum of arbitrarily selected parameters.

参考文献

[1] Liang, X., Bishnu, A., and Asano, T. "A Near-linear Time Algorithm for Binarization of Fingerprint Images using Distance Transform", 10th *IWCIA*, pp. 197-208, LNCS vol. 3322, Auckland, Dec., 2004.

[2] *Automated Classification System Reader Project (ACS)*, Technical Report, DeLaRue Printrak Inc., Feb., 1985.

[3] Breu, H., Gil, J., Kirkpatrick, D., and Werman, M., "Linear Time Euclidean Distance Transform Algorithms", *IEEE Trans. PAMI*, vol. 17, no. 5, pp. 529-533, 1995.

[4] Candela, G. T., Grother, P. J., Watson, C. I., Wilkinson, R. A. and Wilson, C. L., *PCASYS - A Pattern-Level Classification Automation System for Fingerprints*, NISTIR 5647, National Institute of Standards and Technology, August, 1995.

[5] Chang, J. -H., Fan, K. -C., "Fingerprint Ridge Allocation in Direct Gray-Scale Domain", *Pattern Recognition*, vol. 34, no. 10, pp. 1907-1925, 2001.

[6] Coetzee, L., and Botha, E. C., "Fingerprint Recognition in Low Quality Images", *Pattern Recognition*, vol. 26, no. 10, pp. 1441-1460, 1993.

[7] Farina, A., Zs. M. Kovács-Vajna, Zs., M. and Leone, A., "Fingerprint Minutiae Extraction from Skeletonized Binary Images", *Pattern Recognition*, vol. 32, pp. 877-889, 1999.

[8] Fingerprint Verification Competition, 2000, http://bias.csr.unibo.it/fvc2000/download.asp.

[9] Galton, F., *Fingerprints*, London: Macmillan, 1892.

[10] Hirata, T., and Katoh, T., "An Algorithm for Euclidean distance transformation", *SIGAL Technical Report of IPS of Japan*, 94-AL-41-4, pp. 25-31, September, 1994.

[11] Jain, A. K., Hong, L., Pankanti, S. and Bolle, R., "An Identity-Authentication System Using Fingerprints", *Proc. of IEEE*, vol. 85, no. 9, pp. 1365-1388, 1997.

[12] Kovács-Vajna, Z. M., "A Fingerprint Verification System Based on Triangular Matching and Dynamic Time Warping", *IEEE Trans. PAMI*, vol. 22, no. 11, pp. 1266-1276, 2000.

[13] Maltoni, D., Maio, D., Jain, A. K., and Prabhakar, S., *Handbook of Fingerprint Recognition*, Springer-Verlag, New York, 2003.

[14] Moayer, B. and Fu, K., "A Tree System Approach for Fingerprint Pattern Recognition", *IEEE Trans. PAMI*, vol. 8, no. 3, pp. 376-388, 1986.

[15] Ratha N. K., Chen, S. Y., and Jain, A. K., "Adaptive Flow Orientation-Based Feature Extraction in Fingerprint Images", *Pattern Recognition*, vol. 28, no. 11, pp. 1657-1672, 1995.

[16] Watson, C. I., Wilson, C. L., *Fingerprint Database*, National Institute of Standards and Technology, Special Database 4, FPDB, April, 1992.

[17] Wegstein, J. H., *An Automated Fingerprint Identification System*, US Government Publication, Washington, 1982.

研究業績一覧

著書

1. 浅野哲夫:
"アルゴリズム・サイエンス・シリーズ「入り口からの超入門」", 共立出版, 2006 年.
概要: 本特定研究のグループでアルゴリズム・サイエンス・シリーズと題してシリーズ本を出版することになったが，本書はその第 1 弾である．この研究プロジェクトには様々な目標があるが，特に重視しているのが「社会的評価基準」である．数学的に高度な結果を導くだけではなく，分かりやすさと実用性も備えた成果を出すことも重要な目標としている．その一環として，アルゴリズムの重要性とアルゴリズム研究の楽しさを世の中に伝えるというのが本書の役割である．

2. 浅野哲夫:
"アルゴリズム・サイエンス・シリーズ「計算幾何：理論の基礎から実装まで」", 共立出版, 2006 年予定.
概要: 計算幾何学とは，幾何的な計算問題を計算機を用いて効率よく解くための算法を開発するとともに，幾何的な計算問題の本質的

な計算困難度を数学的に解析するための学問分野である．本書では，計算幾何学の代表的な問題の紹介から始めて，効率の良い算法の開発図式をわかりやすく解説することを主たる目標とした．また，幾何データを取り扱うためのデータ構造についても触れている．実用に供するために，多数のプログラムを掲載していることも特徴の一つである．

学術論文

1. X. Liang, T. Asano:
   "Linear Time Algorithm for Binary Fingerprint Image Denoising using Distance Transform", 電子情報通信学会論文誌 D, 採録決定, .
   概要: Fingerprints are useful for biometric purposes because of their well known properties of distinctiveness and persistence over time. However, owing to skin conditions or incorrect finger pressure, original fingerprint images always contain noise. Especially, some of them contain useless components, which are often mistaken for the terminations that are an essential minutia of a fingerprint. Mathematical Morphology (MM) is a powerful tool in image processing. In this paper, we propose a linear time algorithm to eliminate impulsive noise and useless components, which employs generalized and ordinary morphological operators based on Euclidean distance transform. There are two contributions. The first is the simple and efficient MM method to eliminate impulsive noise, which can be restricted to a minimum number of pixels. We know the performance of MM is heavily dependent on structuring elements (SEs), but finding an optimal SE is a difficult and nontrivial task. So the second contribution is providing an automatic approach for choosing appropriate SEs to eliminate useless components. We have developed a novel algorithm for the binarization of fingerprint images. The information of distance transform values can be obtained directly from the binarization phase. The results show that using this method on fingerprint images with impulsive noise and useless components is faster than existing denoising methods and achieves better quality than earlier methods.

2. B. Aronov, T. Asano, Y. Kikuchi, S. C. Nandy, S. Sasahara, and T. Uno:
   "A Generalization of Magic Squares with Applications to Digital Halftoning", Theory of Computing System, 採録決定.
   概要: A semimagic square of order n is an $n \times n$ matrix containing the integers $0, ..., n^2?1$ arranged in such a way that each row and column add up to the same value. We generalize this notion to that of a zero $k \times k$ discrepancy matrix by replacing the requirement that the sum of each row and each column be the same by that of requiring that the sum of the entries in each $k \times k$ square contiguous submatrix be the same. We show that such matrices exist if k and n are both even, and do not if k and n are are relatively prime. An application to digital halftoning is also mentioned.

3. S. Sasahara and T. Asano:
   "New Dispersed-dot halftoning technique by elimination of unstable pixels for electrophotography", Journal of Electronic Imaging, 2005.
   概要: In this paper, we propose an algorithm that adaptively arranges or grows clusters according to tone slope of the cluster-dot halftoning by bubble packing. This technique locates small cluster regions to increase effective resolution on the portion of rapid tone change, and locates large cluster regions to increase effective tone scale on the portion of mild tone change to achieve a good balance between effective resolution and effective tone scale. Since

the clusters are arranged irregularly, our technique has an effect of suppressing interference with regular patterns, such as Moire, and produces a good tone reproduction without occurring artifacts.

4. T. Asano, M. de Berg, O. Cheong, H. Everett, H. Haverkort, N. Katoh, and A. Wolff: "Optimal Spanners for Axis-Aligned Buildings", Computational Geometry: Theory and Applications, 30, 1, 2005.
   概要: Given a set of axis-parallel buildings (rectangles) in the plane, we connect them with tunnels so that we don't get cold while walking from one to the other. This paper presents an efficient algorithm for choosing the bridges such that their dilation is optimal.

5. B. Aronov, T. Asano, N. Katoh, K. Mehlhorn, and T. Tokuyama:
   "Polyline fitting of planar points under min-sum criterion", International Journal on Computational Geometry and Applications, 採録決定.
   概要: Fitting a curve of a certain type to a given set of points in the plane is a basic problem in statistics and has numerous applications. We consider fitting a polyline with k joints under the min-sum criteria with respect to L_1- and L_2-metrics, which are more appropriate measures than uniform and Hausdorff metrics in statistical context. We present efficient algorithms for the 1-joint versions of the problem and fully polynomial-time approximation schemes for the general k-joint versions.

6. T. Asano, P. Evans, R. Uehara, G. Valiente: "Site consistency in phylogenetic networks with recombination", In Iliopoulos, C.S., Park, K., Steinh ¨ ofel, K., eds.: Algorithmics in Bioinformatics, College Publications, 6, 2006.
   概要: 分子生物学における問題は，文字列上の問題として定式化できる．進化木における，具体的な問題に対して，効率の良いアルゴリズムを構築した．

7. T. Asano, J. Matousek, and T. Tokuyama: "The Distance Trisector Curve", ACM Symposium on Computing Theory, 発表予定.
   概要: Given points p and q in the plane, we are interested in separating them by two curves C_1 and C_2 such that every point of C_1 has equal distance to p and to C_2, and every point of C_2 has equal distance to C_1 and to q. We show by elementary geometric means that such C_1 and C_2 exist and are unique. Moreover, for $p = (0, 1)$ and $q = (0, -1)$, C_1 is the graph of a function $f\ R \to R$, C_2 is the graph of $-f$, and f is convex and analytic (i.e., given by a convergent power series at a neighborhood of every point). We conjecture that f is not expressible by elementary functions and, in particular, not algebraic.

8. T.Asano, S. Choe, S. Hashima, Y. Kikuchi, and S.-C. Sung:
   "Distributing Distinct Integers Uniformly over a Square Matrix with Application to Digital Halftoning", 7th Hellenic European Conference on Computer Mathematics and its Applications, 2005.
   概要: This paper considers how to distribute n^2 integers between 0 and $n^2 - 1$ as uniformly as possible over an $n \times n$ square matrix. We introduce a discrepancy-based measure to evaluate the uniformity. More precisely, we take a sum of matrix elements over every $k \times k$ contiguous submatrix and define the discrepancy of the matrix as the largest difference among those sums. It is known that if n and k are both even integers then we can construct zero-discrepancy matrices. In this paper we present a scheme for achieving a new discrepancy bound $2n$ when n is odd and k is 2. This is an improvement from the previous bound $4n$.

We borrow basic ideas behind orthogonal Latin squares and semi-magic squares. An n-ary number system also plays an important part. This problem is closely related to digital halftoning. Low discrepancy matrices would improve the quality of commonly used Ordered Dither Algorithm.

9. X. Liang, K. Kotani and T. Asano:
"Automatically Choosing Appropriately-Sized Structuring Elements to Eliminate Useless Components in Fingerprint Image", Proc. Visual Communications and Image Processing 2005, 5960, 2005.
概要: Fingerprints are useful for biometric purposes because of their well known properties of distinctiveness and persistence over time. However, owing to skin condition or incorrect finger pressure, some fingerprint images contain useless components. They are often mistaken for the terminations that are an essential minutia of a fingerprint. Mathematical Morphology (MM) is one powerful tool in image processing. The performance of MM is heavily dependent on structuring elements (SEs), but finding an optimal SE is a difficult and nontrivial task. In this work, we focus on automatically choosing an appropriate SE for eliminating useless components of fingerprint images using linear time Euclidean distance transform algorithm. We exploit the property that these useless components are thinner than fingerprint ridges. So, we estimate the width of useless components and fingerprint ridges using Euclidean distance transform values, and then provide a linear time algorithm to eliminate the useless components. We have developed a novel algorithm for the binarization of fingerprint images. The information of distance transform values can be obtained directly from the binarization phase. The results show that using this method on fingerprint images with useless components is faster than existing methods and achieves better quality than earlier methods.

10. S. Teramoto, T. Asano, B. Doerr, and N. Katoh:
"Inserting Points Uniformly at Every Instance", Proc. 2005 Korea Japan Joint Workshop on Algorithms and Computation, 2005.
概要: A problem of arranging n points as uniformly as possible, which is equivalent to that of packing n equal and non-overlapping circles in a unit square, is frequently asked. In this paper we generalize this problem in such a way that points be inserted one by one with uniformity preserved at every instance. Our criteria on uniformity is to minimize the gap ratio (which is the maximum gap over the minimum gap) at every point insertion. We present a linear time algorithm for finding an optimal n-point sequence with the maximum gap ratio bounded by $2^{\lfloor n/2 \rfloor/(\lfloor n/2 \rfloor+1)}$ in the 1-dimensional case. We describe how hard the same problem is for a point set in the plane and propose a local search heuristics for finding a good solution.

11. R. Uehara and T. Uno:
"Canonical Tree Representation of Distance Hereditary Graphs and Its Applications Authors", IEICE Technical Report, COMP2005-61, 2006.
概要: 距離遺伝的グラフとは，部分グラフにおいて距離が不変なグラフであり，幾何的なモデルを持つ．このグラフクラスの認識と同型性を高速に行なう線形時間かつ線形領域で動作するアルゴリズムを開発した．認識アルゴリズムは既存のものよりも単純であり，同型性を判定するアルゴリズムは未解決問題を解決したものである．

研究会等

1. S. Teramoto and R. Uehara:
   “Voronoi game on graphs and its complexity”, IPSJ SIG Technical Report, 2006-AL-104-2, 2006.
   概要: ボロノイ図とは領域を分割する概念であり，計算幾何学における基本概念の一つである．ボロノイゲームとはこれを二人ゲームとして定式化したものである．ここではこれを離散的なゲームとして定式化し，先手が有利になる場合と，そのときの必勝戦略を示した．

2. R. Uehara and Y. Uno:
   “Laminar Structure of Ptolemaic Graphs and Its Applications”, IEICE Technical Report, COMP2005-30, 2005.
   概要: プトレマイオスグラフとは，トレミーの不等式によって特徴づけられる幾何的特徴を持つグラフのクラスである．このグラフクラスに,『極大クリークのラミナー性』という新しい特徴づけを与えた．新しい特徴づけに基づいた，さまざまな問題に対する効率の良いアルゴリズムも提案した．

C06: グラフ構造を有する問題に対する近似アルゴリズムの設計

永持 仁 † 軽野 義行 ‡ 宇野 裕之 §

† 京都大学 大学院 情報学研究科
〒 606-8501 京都市左京区吉田本町
nag@amp.i.kyoto-u.ac.jp

‡ 京都工芸繊維大学 工芸学部 機械システム工学科
〒 606-8585 京都市左京区松ヶ崎橋上町
karuno@kit.ac.jp

§ 大阪府立大学 理学系研究科 情報数理科学専攻
〒 599-8531 堺市学園町 1-1
uno@mi.s.osakafu-u.ac.jp

1 はじめに

本研究では，グラフ構造を持つ離散最適化問題を中心としてスケジューリング問題，図形充填問題などの問題に対して厳密解法（多項式時間アルゴリズム，分枝限定法），理論保障付き近似アルゴリズムの開発を行う．

通信網，電力網，交通網，VLSI の配線，スケジューリング問題，地理情報システム等の多くのシステム工学的，情報工学的諸問題に対するアルゴリズムを設計する場合には，これらを離散最適化問題として定式化することで，問題の持つ計算の複雑さの解明や高度な数学的解法の適用が可能となる．しかし，一般には，複雑な要求条件を含む現実の問題を離散最適化問題として定式化した場合には，分岐限定法や整数計画法といった離散最適化の汎用アルゴリズムしか適用できず，このままでは計算効率のよいアルゴリズムを得ることはできない．一方，遺伝アルゴリズム，シミュレーティッド・アニーリング法，タブーサーチ法などの計算の発見的手法に基づくソフトウエアも開発されているが，常に良質な答えを出力するという理論的な保証はなされていない．そこで，常に，最適解に対する近似の程度が理論的に抑えられているような答えを出力する，理論保障付き近似アルゴリズムの開発が望まれる．本研究では，グラフアルゴリズムを中心的な道具として，離散最適化問題に対する理論保証付きアルゴリズムの開発を行う．対象とする問題は，グラフの問題に限らず，グラフ論的手法の適用できる種々の問題を含む．

初年度は，グラフ連結度問題，スケジューリング問題などにおいて近似アルゴリズムの開発や理論的基盤に関して研究成果を挙げた．今年度は，これらの研究課題をについて研究を進展させると同時に，最近重要性が高まっている情報の可視化において有用な技術となるグラフの描画問題に関する研究成果を得ることができた．今年度までに得られた研究成果を以下の四つのカテゴリーに分類して報告する．

- グラフ連結度問題
- 図形処理に関する問題
- スケジューリング問題
- 最長路問題
- グラフのランキング問題

2 グラフ連結度問題

2.1 ネットワーク設計

指定された連結度を持つグラフを構成する問題はネットワーク設計問題として従来から盛んに研究されている．本研究では，与えられたグラフに対して要求された連結度を満たすために必要最小量の枝を付加する連結度増大問題においていくつかの新しい結果を得た．

無向多重グラフ $G = (V, E)$ が与えられたときに，二つの整数 $k, \ell > 0$ に対して，グラフを ℓ-枝連結かつ k-点連結である多重グラフにするために付加する枝の集合を最小にする問題を取り扱った

(T. Ishii, H. Nagamochi, T. Ibaraki, Augmenting a $(k-1)$-Vertex-Connected Multigraph to an ℓ-Edge-Connected and k-Vertex-Connected Multigraph, Algorithmica, vol. 44, pp. 257-280, 2006)．この研究では，与えられたグラフが $(k-1)$-点連結であるとき，ℓ-枝連結かつ k-点連結である多重グラフにするためには最適値より僅かに高々$\max\{\ell+1, 2k-4\}$ 本多い枝の集合を $O(\min\{k, \sqrt{n}\}kn^3+n^4)$ 時間で求められることを示した（$n=|V|$）．

連結度増大問題の中でも 2 節点間ごとに局所連結度の要求が指定されている問題は取り扱いがさらに困難になる．単純連結グラフ $G=(V,E)$ と 2 点対の集合 R が与えられたときに，新しい枝の集合 F で最小のものを G に付加し，得られるグラフ $G+F$ が単純でかつどの対 $(u,v)\in R$ に対しても u と v の間に 2 本の内素なパスを持つように増大させる問題を取り扱った (H. Nagamochi, A (4/3)-Approximation for the Minimum 2-Local-Vertex-Connectivity Augmentation in a Connected Graph, J. Algorithms, vol. 56, pp. 77–95, 2005)．この問題の NP-困難性および (3/2) 倍近似アルゴリズムの存在は，既に我々の先行研究で証明済みであり，本研究では，グラフ構造に関する精巧な分解方法により最適値の下界を評価する議論を強化することができ，その結果，さらに近似精度を高めた (4/3) 倍近似アルゴリズムを開発することに成功した．また，計算時間は $O(|E|+|R|)$，つまり線形時間である．この成果に対しては，日本オペレーションズ・リサーチ学会より平成 17 年度文献賞が与えられている．

ネットワーク設計問題においては連結度の要求以外にも直径を小さくすることが求められることが多い．連結度と直径の両者を同時に考慮したグラフの増大問題に対する研究成果はまだ少ない．与えらたグラフ $G=(V,E)$ に枝を最小本数付加して，その直径を指定された整数 $D\geq 1$ 以下にする問題は，グラフ G が任意であれば，$P=NP$ でない限り，定数倍近似のアルゴリズムが存在しないことが知られている．また，グラフ G が森であり，$D\geq 3$ が奇数である場合に，問題が定数倍近似可能であるかどうかも未解決であったが，本研究において，この疑問に対して肯定的な答えを与えた (T. Ishii, S. Yamamoto, H. Nagamochi, Augmenting Forests to Meet Odd Diameter Requirements, Discrete Optimization (掲載予定))．具体的には，グラフ G が森であり，$D\geq 3$ が奇数である問題に対して，$O(|V|^3)$ 時間の 8 倍近似アルゴリズムを見出した．さらに，増大されたグラフが直径制約以外にも 2 点連結であることを要求にとして加えた場合には，4 倍近似の答えを線形時間で求められることを示した．

2.2 グラフ分割問題

枝に重みを持つ無向グラフの節点集合を k 個の部分集合へ分割し，異なる部分集合を接続する枝の集合を k-カットと呼ぶ．重み最小の 2-カットを求める問題は $O(nm)$ 時間程度で解けることが知られているが，k を変数と見たときには，最小 k-カット問題は NP-困難になることが分かっている．$O(knm)$ 時間の 2 倍近似アルゴリズムも知られている．ここでは，最小 k-カットを厳密に求めるためのアルゴリズムの計算量について研究を行った．これまで，計算量が $O(n^{O(k)})$ であるアルゴリズムとしては答えに誤りを許すモンテカルロ型の確率アルゴリズムが設計されているが，決定性アルゴリズムの計算量としては $O(n^{O(k^2)})$ が最良であり，両者の大きな隔たりは長い間埋められなかった．本研究では，初めて最小 k-カットを厳密に求める決定性アルゴリズムの計算量を $O(n^{O(k)})$ に軽減することに成功した (Y. Kamidoi, N. Yoshida, H. Nagamochi, A Deterministic Algorithm for Finding All Minimum k-Way Cuts, 4th Japanese-Hungarian Symposium on Discrete Mathematics and Its Applications, pp. 224–233, 2005)．我々は，与えられた最小 k-カットの問題例を高々$O(n^{2k-5})$ 個の最小 $(\lfloor(k+\sqrt{k})/2\rfloor+1)$-カットの問題例に帰着できることを証明し，この事実に基づく分割統治法型のアルゴリズムを設計した．提案したアルゴリズムの計算量は，$O(n^{4k/(1-1.71/\sqrt{k})-31})$ であり，すべての最適解を求めることもできるのが特徴である．

以下では，グラフ上の資源集合分割問題に対して得られた結果を紹介する．この問題は，連結なグラフ $G=(V,E)$ といくつかの互いに素な節点の部分集合 $T_1, T_2, \ldots, T_k$ （資源集合と呼ぶ）を入力とし，出力としては，節点 V を 2 分割した部

分集合 V_1，V_2 で次の 2 条件を満たすものを求めることである．

(1) V_1, V_2 はいずれも G から連結な部分グラフを誘導する（すなわち，V_1, V_2 間の枝を削除してもグラフは連結である）．

(2) 各資源集合 T_j, $j = 1, 2, \ldots, k$ は均等分割される．つまり，$|V_1 \cap T_j| = |V_2 \cap T_j| = |T_j|/2$ が成立する（簡単のため各 $|T_j|$ は偶数と仮定する）．

この問題は $k = 1$ であっても NP-困難であることが知られているが，我々の研究では，グラフ G にある程度高い点連結度 $f(k)$ が仮定されていれば常に条件 (1),(2) を同時に満たす均等分割が存在すると予想されている．実際，$k = 2$ の場合には，グラフが 3 点連結であれば必ず条件 (1),(2) を満たす均等分割が存在することを我々の先行研究で証明している (H. Nagamochi, T. Jordan, Y. Nakao and T. Ibaraki, Convex embeddings and bisections of 3-connected graphs, Combinatorica, vol.22, no.4 (2002) 537–554)．この証明では，幾何学的な手法を用いる点が特徴である．与えられたグラフをいったん平面に埋め込み，そこで組み合わせ幾何の手法であるハムサンドイッチカットを用いて，平面に埋め込まれた資源集合を均等分割する．ここでの要点は，平面に埋め込まれたグラフを直線でどう分割しても，分割されたいずれの領域内においてもグラフが連結であるようにうまく埋め込むことである．我々の先行研究では，3 点連結グラフであれば「凸埋め込み」という直線分割に対し連結性を保持できる埋め込み方法の存在を証明し，これに基づく $O(|V|^2 \log |V|)$ 時間，$O(|V| + |E|)$ 領域のアルゴリズムを提案した．しかし，これは計算モデルとして理想的な数値計算ができることを仮定しており，実際に計算機上で実装した場合には丸め誤差により計算が破綻する可能性がある．実際にこのアルゴリズムを素朴な方法で実装した場合に，ある程度の規模の問題例になると計算が正常に進行しなくなることを確認した．本研究では，計算誤差をまったく伴わない新しいアルゴリズムとそのためのデータ構造を開発した (H. Nagamochi, K. Iwata, T. Ishii, A Robust Algorithm for Bisecting a Triconnected Graph with Two Resource Sets, Theoretical Computer Science A, vol. 341, pp. 364–378, 2005)．提案する方法は，座標位置に基づく平面幾何の情報を管理する代わりに，均等分割に必要な 2 点の間の相対位置の情報を順序集合のみで管理することで，座標を維持する必要をなくし，高々$|V|$ 程度までの整数値のみで計算の進行が制御可能になった．提案法の計算時間，計算領域は，ともに $O(|V|^2)$ である．計算時間は改良されているが，計算領域は，先行結果の $O(|V| + |E|)$ よりも一見悪く見える．先行結果では，モデルとして無限精度の数値が維持できることを仮定しており，改良した方法では，高々$|V|$ 程度までの整数値のみで十分であるので，計算機上での計算領域としては，改善されていると考えられる．

資源集合をもつグラフの均等分割問題については $k \geq 3$ の場合には未解決であり，k に対して，入力グラフ G が $(k+1)$-点連結であれば条件 (1),(2) を満たす均等分割が存在することが予想されていた．本研究では，において，$k = 3$ の場合には一般にはこの予想は正しくないことを反例を構成して証明し，一方で，$k = 3$ の場合には，入力グラフ G が 4-点連結であり，かつ 4 点の完全グラフ K_4 を部分グラフとして含む場合には，必ず条件 (1),(2) を満たす均等分割が存在し，そのような分割を求める $O(|V|^3 \log |V|)$ 時間のアルゴリズムを与えた (T. Ishii, K. Iwata, H. Nagamochi, Bisecting a Four-Connected Graph with Three Resource Sets, The The 16th Annual International Symposium on Algorithms and Computation (ISAAC 2005), Lecture Notes in Computer Science, Springer-Verlag vol. 3827, pp. 176–185, 2005)．さらに，この結果が枝集合版の資源集合の均等分割問題に拡張できることも示した．枝集合の資源集合の均等分割問題は以下のように定義される．入力として，連結なグラフ $G = (V, E)$ といくつかの互いに素な枝の部分集合 $F_1, F_2, \ldots, F_k$（資源集合と呼ぶ）が与えられ，出力は，次の 2 条件を満たす枝集合 E の 2 分割集合 E_1，E_2 である．

(1) E_1, E_2 はいずれも G から連結な部分グラフを誘導する．

(2) 各資源集合 F_j, $j = 1, 2, \ldots, k$ は均等分割される．つまり，$|E_1 \cap F_j| = |E_2 \cap F_j| = |F_j|/2$

が成立する（簡単のため各 $|F_j|$ は偶数と仮定する）.

枝集合の資源集合の均等分割問題に対しては，$k = 1, 2, 3$ のときは，グラフが $(k+1)$-枝連結であることが十分条件であることを証明した.

3　図形処理に関する問題

3.1　グラフ描画問題

グラフの自動描画は電子回路設計や部屋の間取などの他，最近注目されている地理情報の表現など情報の可視化技術の確立のための核として重要な役割を果たしている．以下では，本研究で得られた「２階層描画問題」,「クラスタ付き平面グラフ描画問題」に対する結果を報告する.

非閉路的有向グラフを平面内に描画する方法として日本人研究者の開発した Sugiyama 法がよく知られている．この方法では，平行な直線をいくつか用意し，グラフの節点集合を直線の数の部分集合に分離して，各部分集合の節点を対応させる直線上に配置し，枝をその両端点をつなぐ直線分で描くことで階層状のグラフ描画を得ることができる．このとき，線分同士が交差する点の個数が得られた描画の質を決める尺度として用いられる．通常，各階層内での節点の配列順は自由に変えることができるので，描画全体での交差点数を最小にするように各階層において最適となる節点の配列を求めることが望まれる．しかし，一般に，多層の問題を一度に取り扱うことは計算量的に困難な問題であり，２階層問題における数学的な構造が現在研究されている．２階層の描画であっても，２層内の節点の配列をどちらも自由に変更することが許されている問題設定の場合には最適解の $O(\log n)$ 程度の近似精度しか得られていない．これに対し，２層のうち１層内の節点の配置順を固定した場合には，３倍近似アルゴリズムが [P. Eades and N. C. Wormald, Edge Crossing in Drawing Bipartite Graphs, Algorithmica, vol. 11, pp. 379-403, 1994] により 10 年前に提案されていた．本研究では，１層固定の２階層描画に対して近似精度を 1.4664 に大きく改善することに成功した (H. Nagamochi, An Improved Bound on the One-Sided Minimum Crossing Number in Two-Layered Drawings, Discrete and Computational Geometry, vol. 33, pp. 569–591, 2005)．提案法は，交差点数最小化問題に対する確率的なアルゴリズムの設計を平面上のある種の図形の最適設計問題に変換するという独特な議論に基づいている．提案法は $O(n \log n)$ 時間で実行できるラスベガス型確率アルゴリズムであるが，これを脱ランダム化し決定性の 1.4664 近似アルゴリズムが得られることも示している.

平面上に交差なく描画できる平面グラフについては様々な描画表現やそのためのアルゴリズムが研究されている．入力として，平面グラフと節点の部分集合の作るクラスタを考え，グラフの描画の中に，クラスタを不必要な枝交差なしに描く問題はさらに広い用途を持つ．与えられるクラスタの集合は，どの二つのクラスタも交差しないと仮定する（すなわちクラスタ集合はラミナ族）．クラスタ集合を持つ平面グラフをクラスタ付きグラフを呼ぶ．このとき，次の条件を満足する直線描画の存在を議論するのが基本的な問題設定である.

(i) グラフの各枝を直線分で，各クラスタを多角形で描く.

(ii) 枝同士の交差はない.

(iii) クラスタを表現する多角形同士は交差しない.

(v) 多角形と枝は必要なら１度だけ交差を許す.

さらに，グラフの内面やクラスタを表す多角形を凸にできればさらに望ましい．クラスタ付きグラフに対する直線描画で各クラスタを凸多角形で表現できるかという問題に対して，本研究では各クラスタが連結部分グラフを誘導する場合，これを肯定的に解決した (P. Eades, Q. Feng, X. Lin, H. Nagamochi, Straight-Line Drawing Algorithms for Hierarchical Graphs and Clustered Graphs, Algorithmica, vol. 44, pp. 1-32, 2006)．この研究では，クラスタ付きグラフの研究に先立って，階層型平面グラフに対する直線描画の存在について議論を行っている．それは，クラスタ付きグラフの凸描画問題は，階層型平面グラフの非交差直線描画問題に帰着すれば解けることを示したからである．階層型平面グラフとは，グラフの節点集合の分割を持ち，それぞれの節点集合は x, y-平面

において同じ y 座標を持つことが指定され，同じ部分集合内での節点の持つ x-座標は未決定であるがそれらの大小関係は（グラフ全体が枝交差を生じないように）定められている．ここでの研究課題は，各部分集合内の節点の x-座標をうまく固定し，グラフの枝をその両端点をつなぐ直線分で描いたときに，枝同士の交差を発生させないことである．この問題に対して $c-st-$ 番号付けという節点のラベル付けを考案し，階層型平面グラフは必ず非交差直線描画を持つことを証明し，線形時間のアルゴリズムを与えた．この結果に基づき，クラスタ付きグラフの凸描画問題もまた線形時間で解くことができることを示した．

我々は，クラスタ付きグラフに対して，各クラスタが連結部分グラフを誘導する場合，クラスタの多角形を凸する直線描画が存在することを示したが，クラスタが誘導する部分グラフの境界自体は凸多角形になるとは限らない．もし，クラスタが誘導する部分グラフの境界自体を常に凸にすることができれば，クラスタ自体の多角形を特別に計算する必要がなくなる．そこで，そのような描画の存在について研究を行った．明らかな必要条件としては，各クラスタが誘導する部分グラフは，単に連結であるだけでなく，２点連結であることが必要である．この必要な仮定の下で，クラスタ付きグラフに対する直線描画でクラスタが誘導する部分グラフの境界に凸にするものが存在することを示した (H. Nagamochi, K. Kuroya, Drawing c-Planar Biconnected Clustered Graphs, Discrete Applied Mathematics (掲載予定))．

3.2 図形パッキング問題

本研究では，平面図形を矩形の容器内にパッキングする問題に対して，厳密解法とヒューリスティックの両方のアプローチからアルゴリズムの設計を進めている．以下では，本研究で得られた矩形を容器内に最適に配置する厳密解法の結果について報告する (T. Imamichi, M. Kenmochi, K. Nonobe, M. Yagiura, H. Nagamochi, Branch-and-bound Algorithms for Rectangular Strip Packing and Perfect Packing Problems, ESICUP (EURO Special Interest Group on Cutting and Packing) 2nd Meeting, 2005)．矩形パッキング問題 (two dimensional rectangle packing problem) は, 与えられた複数の矩形を, 互いに重なり合うことなく目的関数値が最小となるように平面上に配置する問題である．この種の問題に対する解法は鉄鋼業や繊維産業で素材の切断を効率よく行うために応用されているだけでなく, スケジューリング問題など, 現実の世界において広く応用されている．通常, 矩形の辺が垂直か水平となるような配置のみを考え, 矩形の 90 度回転を許可するか否か, 詰め込む容器の幅が予め決められているか否かなど, パッキングの規則についていくつか選択肢がある．目的関数としても様々な種類が考えられ, 与えられたすべての矩形を, 幅の固定された容器に高さが最小となるように詰め込む問題を特にストリップパッキング問題 (two dimensional strip packing problem) と呼ぶ．ストリップパッキング問題は NP 困難であることが知られており, 今日までに多くの研究がなされている．

ストリップパッキング問題に対する発見的アルゴリズムとして有名なものの一つとして, 1980 年に Baker らが提案した bottom-left (BL) 法が挙げられる．1983 年には Chazelle が bottom-left-fill (BLF) 法について研究をしている．また, 近年では 1996 年に Jakobs が, 1999 年に Liu と Teng がそれぞれ BL 法と遺伝アルゴリズムを用いたメタ解法の研究を行っており, BL 法はこれまで多くの研究の基となっている．また, 2004 年に Burke らによって, best-fit と呼ばれる新たな発見的アルゴリズムも開発された．メタ解法の研究も盛んであり, 先に挙げたに加え, Hopper と Turton による研究, 今堀らによる研究などが挙げられる．厳密解法に対しては, 2003 年の Martello らによる, 矩形の回転を許可しない場合に対する分枝限定法の研究がある．現実の応用においては, 矩形数が数十程度までの中小規模の問題例が対象となる事例が多数存在し, 問題規模が小さいときには近似解法よりも厳密解法の方が優れた性能を示す傾向が強いことが多くの問題に対して確認されている．厳密解法に対しては, 2003 年の Martello らによる, 矩形の回転を許可しない場合に対する分枝限定法の研究がある．本研究では, 矩形数が中規模までのストリップパッキング問題に焦点を置き, 厳密解を求めることを目的とした．矩形の向きに関し

ては, 90 度回転を許可する場合と許可しない場合の両方を考える.

まず, より制限のある問題として完全パッキング (perfect packing) と呼ばれる問題を扱う. 完全パッキング問題とは, 与えられたすべての矩形を幅と高さの決まった容器に隙間なく敷き詰めることができるか否かを判定する問題である. 完全パッキング問題に対しては, 2004 年に Lesh らが回転を許可しない場合に対して矩形数 29 までの問題例を解いている. 本研究では, 完全パッキング問題に分枝限定法を適用することを考え, BL 法の考え方を用いた分枝規則と, 矩形の配置が常に階段状となるように配置していく分枝規則の 2 種類を試みた. さらに, 限定操作として, 動的計画法 (dynamic programming, DP) を用いる方法を提案した. 次に, 一般のストリップパッキング問題に対して, そのアルゴリズムを適用する方法として, 完全パッキング問題への変換と階段状を維持する分枝の拡張を与えた.

計算実験を行い, 完全パッキング問題に対しては, 階段上を維持する分枝と動的計画法による限定操作を用いて従来の研究を改善する矩形数 49 までの問題例が解けることを確認した. また, 一般のストリップパッキング問題に対して, 無駄なスペースを小さくできる (すなわち完全パッキングに近い) 問題例が効果的に解けることを示すことができた.

4 スケジューリング問題

スケジューリングの問題では，配送スケジューリングと機械スケジューリングを取り上げ，それらに対する近似アルゴリズムの設計を検討している．配送スケジューリングでは，搬送車両の走行経路がグラフで表される．また，機械スケジューリングでは，ジョブショップ問題に対する隣接グラフのように，ジョブの移動経路を表すためにしばしばグラフが用いられる．スケジューリング問題では，ジョブの処理順序が主要な決定事項のひとつであるが，優れた近似性能を実現するためには，アルゴリズムの設計において，それらのグラフ構造も考慮に入れることが必要である．

4.1 配送スケジューリング

複数台の搬送車両が，与えられた走行経路上の配送作業（すなわち，ジョブ）を分担して処理する際に，各車両への負荷があらかじめ定められた上限値（以下，容量という）を超えないようにしながら，使用する車両数を最小にする問題を考え，グラフ理論的なアプローチを行う．まず，走行経路を各枝と点に非負重みを持つ連結グラフ $G = (V, E)$ によりモデル化する．枝 $e \in E$ および点 $v \in V$ の重みをそれぞれ $w(w)$，$h(v)$ と表す．ここで，$w(e)$ は車両が枝 e を通過するときの移動コスト（移動時間）を意味し，$h(v)$ は点において行う作業に対するコスト（作業時間）を表す．各車両の容量を d，デポの役割をする点を r とし，車両数を表す整数を p とする．

つぎに，配送スケジューリング問題を部分木被覆問題に置き換える．部分木被覆問題とは，与えられたグラフをいくつかの部分木に分割する問題であり，いくつかのバリエーションがある．容量制約付き部分木被覆問題 (the capacitated subtree cover problem: CSC) とは，点集合 V の p 分割 $\mathcal{X} = \{X_1, X_2, \ldots, X_p\}$ と p 個の部分木 $T_1, T_2, \ldots, T_p$（ただし，各 T_i は $X_i \subseteq V(T_i)$ および $w(T_i) + h(X_i) \leq d$ を満たすもの）を実行可能解とし，部分木の数 p を最小にすることを目的とする．ここで，部分木 T_i のコストは，T_i の枝の重み和 $w(T_i)$ と X_i の点の重み和 $h(X_i)$ の合計として定義される．この問題にデポを考慮することで定義される容量制約付き根付き部分木被覆問題 (the capacitated rooted-subtree cover problem: CRSC) とは，点の点集合 V の p 分割 $\mathcal{X} = \{X_1, X_2, \ldots, X_p\}$ と p 個の部分木 $T_1, T_2, \ldots, T_p$（ただし，各 T_i は $X_i \cup \{r\} \subseteq V(T_i)$ および $w(T_i) + h(X_i) \leq d$ を満たすもの）を実行可能解とし，部分木の数 p を最小にすることを目的とする．なお，部分木に容量制約がない代わりに，与えられた整数 p に対して，部分木の最大コストを最小にすることを目的とした問題は，ミニマックス部分木被覆問題 (the minmax subtree cover problem: MSC) と呼ばれる．デポを考慮する場合は，ミニマックス根付き部分木被覆問題 (the minmax rooted-subtree problem: MRSC) と呼ばれる．

部分木被覆問題への置き換えは，各車両のおこ

なう配送作業（が存在する点の集合）に誘導される部分グラフを一つの部分木で近似できないか，という考えに動機づけられている．実際，走行経路が木グラフで与えられるとき，問題 MSC に対する定数倍近似アルゴリズムを用いることによって，デポなしメイクスパン最小化配送スケジューリング問題に対しては 5 倍近似アルゴリズムを構成でき，また，問題 MRSC に対する定数倍近似アルゴリズムを用いることによって，デポありメイクスパン最小化配送スケジューリング問題に対しては 3 倍近似アルゴリズムを構成できる．

車両数最小化問題の検討準備のため，本研究課題では問題 CSC と CRSC を取り上げている．車両数最小化は各配送作業の完了時刻に関する直接的な関数ではなく，過去の配送スケジューリングに対する近似アルゴリズムの研究では殆ど扱われていないようである．これは，メイクスパンや最大ツアー時間などの目的関数に比べて，下界値の導出が難しいと考えられていたからである．本研究課題では，昨年度，与えられたグラフが木である場合，問題 CSC に対するひとつの下界値計算法を与えた．この下界値は，木グラフにおける問題 MSC の上界値計算法をサブルーチンとして用いている．この結果から，木グラフにおける問題 CSC に対して，3 倍近似アルゴリズムが導かれた．また，この結果は，部分木のコストと部分木の数とのひとつの相互関係を示している．

本年度は，一般グラフにおける問題 CSC に対する近似アルゴリズムの設計に取り組み，結論から言えば，ある定数倍近似アルゴリズムを提案した．この近似アルゴリズムでは，最近示された一般グラフにおける問題 MSC に対する $(4+\varepsilon)$ 倍近似アルゴリズム（G. Even, N. Garg, J. Könemann, R. Ravi and A. Sinha, *Oper. Res. Lett.* 32 (2004) 309–315）の前処理を活用している（ここで ε はあらかじめ定められる任意の正数であり，この大きさによってアルゴリズムの計算手間が変化する）．提案アルゴリズムでは，与えられたグラフが木構造を持たない場合，それをいくつかの成分に分け，各成分における最小木を求めることによって，一般グラフの問題を木グラフの問題に帰着させるアプローチを取っている．前処理は，容量 d を超える重みの枝を取り除き，与えられたグラフをいくつかの成分に分ける．これは，そのような枝が問題 CSC の最適解において使われることは有り得ないからである．木グラフにおける問題 MSC の上界値計算法をサブルーチンとして用いると，各成分に割り当てられるべき最小の部分木数のたかだか 7 倍で，すべての部分木のコストが容量以下に収まることが言える．最終的に，一般グラフにおける問題 CSC に対する 7 倍近似アルゴリズムが得られる．各車両の負荷として移動時間と作業時間をカウントする場合には，この部分木被覆問題に対する結果が車両数最小化問題における近似アルゴリズムの設計に重要な役割を果すと考えられる．

なお，一般グラフにおける問題 CRSC に対しても，問題 CSC と同様のアプローチで近似アルゴリズムを設計した．すべての部分木がデポを含まなければならないという厳しい制約条件のため，こちらは定数倍近似とはならなかったが，データ依存の近似比は得ることができた．

4.2 機械スケジューリング

機械スケジューリング問題において現れる重要なグラフ構造のひとつとして，ショップスケジューリング問題におけるジョブの移動経路が挙げられる．代表的なショップモデルとして，オープンショップ問題，ジョブショップ問題，フローショップ問題などがある．オープンショップ問題では，各ジョブは複数の機械を訪問しながらそれらの上で処理を受けなければならないが，機械の訪問順序（すなわち，そのジョブの移動経路）はあらかじめ定められているのではなく，スケジューラが決定する．ジョブショップ問題でも，各ジョブは複数の機械で処理を受けなければならないが，その訪問順序はあらかじめ定められている．ジョブショップ問題において，すべてのジョブの訪問順序が同一であるとき，その問題は特別にフローショップ問題と呼ばれる．

本研究課題で扱っているショップ問題のひとつに，タイムラグを考慮した 2 機械フローショップ問題がある．タイムラグは，切削加工前後の中間作業あるいはベルトコンベアの搬送時間等に対応することから，FMC (flexible manufacturing cell) スケジューリングの基本モデルのひとつともされる．この問題に対しては，$O(n \log n)$ 時間で動作

する 2 倍近似アルゴリズムおよび多項式時間近似スキーム（以下，PTAS と略記）の存在が知られていた (それぞれ M. Dell'Amico, *Operations Research*, 44 (1996) 777–787, L. A. Hall, *Mathematical Programming*, 82 (1998) 175–190)．ここで n はジョブ数を表している．後に我々も，$O(n \log n)$ 時間で動作する 11/6 倍近似アルゴリズムを与えた．

2 倍未満の近似比の達成のひとつのポイントは，非順列スケジュールの活用である．非順列スケジュールとは，機械毎にジョブの処理順序が異なるスケジュールのことをいう．すべての機械においてジョブの処理順序が同じであるならば，それは順列スケジュールであるという．タイムラグを考慮した 2 機械フローショップ問題に対しては，最適順列スケジュールを求める $O(n \log n)$ 時間アルゴリズムが知られている．もちろん，最適順列スケジュールを元々の問題の近似解として用いることは可能であるが，その近似比は 2 であって，それ以上改善することはできない（これが前述の 2 倍近似アルゴリズムに相当する）．

比喩的な表現ではあるが，非順列スケジュールでは，タイムチャートにおいて二つのジョブの移動経路が交差するといえる．そして，最適化に効果がありそうな交差として，一方のジョブのタイムラグが長い場合を挙げることができる（前述の 2 倍近似アルゴリズムの最悪ケースの最適解がそのようなスケジュールになっている）．特に 11/6 倍近似アルゴリズムでは，ある適切なしきい値を導入することにより，長いタイムラグを持つジョブとそうでないジョブを区別して，意図的にそのような移動経路の交差を生じさせている．

現時点で，理論的な近似精度の観点からは PTAS が最も優れているが，計算手間や実装の容易性の観点からは，必ずしも実用的とは言えない部分がある．一方で，長いタイムラグを持つジョブを識別するための前述のしきい値は効率よく計算することができるので，それはいわゆるメタ戦略に組み込むことができる．メタ戦略によって理論的な近似精度が改善できるわけではないが，機械間のバッファの有限性やロボットによる搬送時間など，FMC 特有の制約条件を満足するようなヒューリスティックが構築できる．実際，本年度はこの方面からアプローチして，計算実験を積み重ねている最中である．もちろん，PTAS の実用性向上は重要なので，検討すべき課題を再整理しておく必要がある．

5 最長路問題

最長路 (閉路) 問題とは, 無向グラフ G と, その枝集合 $E(G)$ に対する実数値の重みが与えられたときに, 重みの和が最大となる路 (閉路) およびその長さを求める最適化問題である. 過去の多くの研究には, 最短の経路を対象にしたものが多い. たとえば, グラフにハミルトン性を仮定して最短のハミルトン閉路を求める問題は, 代表的な NP 困難問題として知られる巡回セールスマン問題であり, 近似可能性や, ある程度大規模な問題に対する実用的に高速な厳密アルゴリズムなど, 数多くの結果が知られている.

これに対して, 巡回セールスマン問題の一部を特別な場合として含み, いくつもの実用的な応用を持つ最長路問題は, 理論的にも非常に興味深いにもかかわらず, 過去にあまり多くの関連研究が見られない.

本研究課題のテーマは近似アルゴリズムの設計であるが, この問題に対しては, 必ずしも近似解法だけに限定せず, 厳密解法の開発をも目指す.

5.1 入力を限定するアプローチ

一般の入力に対して NP 困難な組合せ最適化問題においては, 精度の保証はないが実用的には十分な精度の解を与えるヒューリスティクスの開発や, 精度が保証された近似アルゴリズムの設計などの対策が考えられる. 他方, 実際には限られたグラフや重みのみが入力として出現することも多く, ここでは, 入力として与えられるグラフクラスを制限することによって厳密解を得ることを目指す. このためには, さまざまなグラフクラスやその応用を熟知した上で, アルゴリズム設計に有用な性質や特徴づけを得る必要がある. われわれは, すでに木やブロックグラフが持つ性質を利用して, これらに対する最長路問題を解く厳密アルゴリズムを開発しており, ここでは新たに Ptolemaic グラフと呼ばれるクラスを対象とし, その性質を調査した.

Ptolemaic グラフとは, グラフの任意の 4 点 x, y, z, w 間の距離に, トレミーの不等式 (ptolemaic inequality) $d(x,y)d(z,w) \leq d(x,z)d(y,w)$ が成り立つグラフをいい, このグラフクラスは, コーダルグラフと距離遺伝グラフの交わりと一致することが知られている. また Ptolemaic グラフは, われわれが過去に対象としたブロックグラフを特別な場合として含む.

われわれは, この Ptolemaic グラフに対する新しい特徴づけを与えた. それは, クリークのラミナー構造にもとづくものであり, グラフ G の極大クリークの空でない交わりの集合族を $\mathcal{C}(G)$ として, $\mathcal{C}(G)$ 上に定義されるあるグラフを $T(\mathcal{C}(G))$ としたとき, G が Ptolemaic グラフであるための必要十分条件は $T(\mathcal{C}(G))$ が木であるというものである. この結果から, Ptolemaic グラフに対する正準木表現 (クリークラミナー木) $T(\mathcal{C}(G))$ が得られる. このクリークラミナー木は, Ptolemaic グラフの交モデルにもなっており, 辞書式幅優先探索 (LexBFS) によって得られる完全点消去順序 (perfect elimination ordering) から, 線形時間で構築することができる.

したがって, このクリークラミナー木を用いることにより, Ptolemaic グラフの認識問題および同型性判定問題を線形時間で解くことができる. さらに, ハミルトン閉路問題も線形時間で解くことに成功した. このことは, Ptolemaic グラフに対する最長路問題を解く大きな手がかりであり, 次年度以降の解決が期待できる.

6 グラフのランキング問題

グラフの点ランキングとは, グラフの点に対して整数値を割り当てるラベリング $r : V \to R_+$ で, 同じラベル i を持つ 2 点間の任意の路には, i より大きなラベル j を持つ点が必ず存在するという条件を満たすものである. これは, 互いに干渉しあう仕事は同時に実行できないという制約のもとに, その仕事の完了時刻 (ステップ数) を最小にするという問題を定式化している. しかしながら, それぱかりではなく, 点彩色問題の一般化にもなっており, 理論的にも非常に興味深い問題であり, 過去に多数の研究がある. またすべての定義において, 点を枝で置き換えた枝ランキング問題も同様に定義され, これも並列処理ステップ最小化に応用がある.

われわれは過去に, この枝ランキング問題に対して, より自然な形で並列処理ステップを最小化する問題を表現するモデルとなる「最小枝ランキング全域木問題 (MERST)」を定義し, これに対してさまざまな理論的な解析や, 近似アルゴリズムの提案などを行ってきている. それらは例えば, MERST の NP 困難性や, 近似比 $\frac{\min\{(\Delta^*-1)\log n/\Delta^*, \Delta^*-1\}}{\log(\Delta^*+1)-1}$ (ただし, n は点数, Δ^* は最大次数最小全域木の最大の次数) を持つ近似アルゴリズムなどである. また, 入力となるグラフクラスを制限することによる厳密アルゴリズムとして, 入力がしきい値グラフである場合の MERST に対して, 線形時間のアルゴリズムを提案している.

この問題に対する本年度の成果は, 新たに split グラフと呼ばれるクラスに対する厳密アルゴリズムを提案したことである. Split グラフとは, グラフの点集合 V が, クリーク K と独立点集合 S に分割可能なグラフとして定義される. このグラフの全域木を考えるとき, クリーク K 内の点は任意の順序で連続して接続できることを利用すると, 問題 MERST の解は, 最大流問題 (の変種) を解くことで導かれることが判明し, その結果, MERST に対する多項式時間アルゴリズムを得た.

この点/辺ランキング問題に対しては, われわれが提案した最小ランク全域木問題以外にも, さまざまなバリエーションを考えることができ, それらが今後の課題となる.

7 おわりに

本研究では，グラフ構造を有する離散最適化問題に対する理論保証付きアルゴリズムの開発を行った．対象とする問題は，グラフの問題に限らず，スケジューリング問題，図形処理問題など多岐にわたる．それぞれの分野の問題は，その問題特有の構造があるが，単に，分野個別の議論を行うのではなく，異なる分野における有用な手法を他の分野で適用することで問題を解決することを目指す．例えば，本研究で進めている配送スケジューリング問題に対する近似アルゴリズムはスケジューリング理論とグラフ理論の両方の研究手法を適用することで設計されている．グラフの資

源つき２分割問題は，問題を幾何の変換し，組み合わせ幾何学の手法を適用することで解決している．この一方で，アルゴリズムの設計において有用な性質や設計手法などは，異なる分野においても本質的に共通であることも多い．そのような，共通のアルゴリズム設計技術を抽出し，一般的な概念へ拡張することも本研究の目指す方向である．

研究業績一覧

学術論文

1. H. Nagamochi:
   "An Improved Bound on the One-Sided Minimum Crossing Number in Two-Layered Drawings", Discrete and Computational Geometry, 33, 569-591, 2005.
   概 要: Given a bipartite graph $G = (V, W, E)$, a 2-layered drawing consists of placing nodes in the first node set V on a straight line L_1 and placing nodes in the second node set W on a parallel line L_2. The one-sided crossing minimization problem asks to find an ordering of nodes in V to be placed on L_1 so that the number of arc crossings is minimized. In this paper, we a 1.4664-approximation algorithm for this problem. This improves the previously best bound 3 due to P. Eades and N. C. Wormald [Edge crossing in drawing bipartite graphs, Algorithmica 11 (1994), 379-403].

2. P. Eades, Q. Feng, X. Lin, H. Nagamochi:
   "Straight-Line Drawing Algorithms for Hierarchical Graphs and Clustered Graphs", Algorithmica, 44, 1-32, 2006.
   概要: Hierarchical graphs and clustered graphs are useful nonclassical graph models for structured relational information. Hierarchical graphs are graphs with layering structures; clustered graphs are graphs with recursive clustering structures. Both have applications in CASE tools, software visualization, and VLSI design. Drawing algorithms for hierarchical graphs have been well investigated. However, the problem of straight-line representation has not been solved completely. In this paper, we answer the question: does every planar hierarchical graph admit a planar straight-line hierarchical drawing? We present an algorithm that constructs such drawings in linear time. Also, we answer a basic question for clustered graphs, that is, does every planar clustered graph admit a planar straight-line drawing with clusters drawn as convex polygons? We provide a method for such drawings based on our algorithm for hierarchical graphs.

3. T. Ishii, H. Nagamochi, T. Ibaraki:
   "Augmenting a $(k-1)$-Vertex-Connected Multigraph to an ℓ-Edge-Connected and k-Vertex-Connected Multigraph", Algorithmica, 44, 257-280, 2006.
   概要: For two integers $k, \ell > 0$ and an undirected multigraph $G = (V, E)$, we consider the problem of augmenting G by the smallest number of new edges to obtain an ℓ-edge-connected and k-vertex-connected multigraph. In this paper, we show that a $(k-1)$-vertex-connected multigraph G can be made ℓ-edge-connected and k-vertex-connected by adding at most $\max\{\ell+1, 2k-4\}$ surplus edges over the optimum in $O(\min\{k, \sqrt{n}\}kn^3 + n^4)$ time, where $n = |V|$.

4. Y. Karuno, H. Nagamochi:
   "Scheduling Vehicles on Trees", Pacific Journal of Optimization, 1, 527-543, 2005.
   概要: The vehicle scheduling problem consists of a set of n jobs which are located at different vertices in a given graph. Each job is characterized by a release time, a handling time and a due date (or a deadline). There are m $(1 \le m \le n)$ identical vehicles on the graph to process the jobs. The problem asks to find a routing schedule of the

m vehicles that minimizes a given objective function. Graphs are restricted to paths or trees in some applications, and thus the problem on these graphs has been studied extensively. In this paper, we give a brief review of approximation algorithms to the problem on paths or trees obtained by the previous work. As a closely related topic, we also discuss the subtree cover problem where a given edge-weighted tree with n weighted vertices is partitioned into a number of subtrees so as to minimize a given objective. In this paper, we propose an $O(n^3 \log n)$ time 3-approximation algorithm to the problem of minimizing the number of subtrees, where the weight of each subtree must not exceed a specified capacity.

5. H. Nagamochi:
"A $\frac{4}{3}$-Approximation for the Minimum 2-Local-Vertex-Connectivity Augmentation in a Connected Graph", J. Algorithms, 56, 77-95, 2005.
概要: Given a simple connected graph $G = (V, E)$ and a set R of pairs of vertices, we consider the problem of augmenting G by a smallest set F of new edges such that the resulting graph $G + F$ remains simple and has at least two internally disjoint paths between u and v for each pair $(u, v) \in R$. The problem is known to be NP-hard, and a 3/2-approximation algorithm has been obtained so far. In this paper, we introduce new stronger lower bounds on the optimal value, and propose an $O(|E|+|R|)$ time 4/3-approximation algorithm to the problem.

6. H. Nagamochi:
"Approximating the Minmax Rooted-Subtree Cover Problem", IEICE Transactions, E88-A, 1335-1338, 2005.
概要: Let $G = (V, E)$ be a connected graph such that each edge $e \in E$ and each vertex $v \in V$ are weighted by nonnegative reals $w(e)$ and $h(v)$, respectively. Let r be a vertex designated as a root, and p be a positive integer. The minmax rooted-subtree cover problem (MRSC) asks to find a partition $\mathcal{X} = \{X_1, X_2, \ldots, X_p\}$ of V and a set of p subtrees $T_1, T_2, \ldots, T_p$ such that each T_i contains $X_i \cup \{r\}$ so as to minimize the maximum cost of the subtrees, where the cost of T_i is defined to be the sum of the weights of edges in T_i and the weights of vertices in X_i. Similarly, the minmax rooted-cycle cover problem (MRCC) asks to find a partition $\mathcal{X} = \{X_1, X_2, \ldots, X_p\}$ of V and a set of p cycles $C_1, C_2, \ldots, C_p$ such that C_i contains $X_i \cup \{r\}$ so as to minimize the maximum cost of the cycles, where the cost of C_i is defined analogously with the MRSC. In this paper, we first propose a $(3 - 2/(p + 1))$-approximation algorithm to the MRSC with a general graph G, and we then give a $(6 - 4/(p + 1))$-approximation algorithm to the MRCC with a metric (G, w).

7. 石井 利昌, 永持 仁, 高橋 健吾, 西垣 豊, 武田 真人:
"タンク繰りにおける経路探索法", システム制御情報学会誌, 18, 213-221, 2005.
概要: 石油化学事業において, 石油化学プラントを効率的に運用するための生産計画の最適化が要求されている. 生産計画の最適化を考慮する際, プラントへ原料をいかに効率よく供給するかは, 重要な課題の一つである. 通常, 購入された原料は, まず, 港から一時的に複数の貯蔵用タンクに受け入れられ, その後生産計画に従って, プラントへ供給される. この際, 配管網上で, 港-タンク間, タンク-タンク間, またはタンク-プラント間において, 互いに途中の配管を共有しない 2 本以上の経路を見つけることが求められる. 本研究では, この配管網上での経路探索問題に対し, 配管網をグラフに置き換えることで, グラフ理論を用いた解法を提案する. 我々の解法では, 効率的に問題を解くために, 要求されうる全ての経路をあらかじめ木状のデータ構造に蓄える. 提案アルゴリズムの有効性につい

ては, 昭和電工 (株) における事例を基に, 計算機実験により検証する.

8. H. Nagamochi:
"Packing Unit Squares in a Rectangle", The Electronic Journal of Combinatorics, 12, R37, 2005.
概要: For a positive integer N, let $s(N)$ be the side length of the minimum square into which N unit squares can be packed. This paper shows that, for given real numbers $a, b \geq 2$, no more than $ab - (a + 1 - \lceil a \rceil) - (b + 1 - \lceil b \rceil)$ unit squares can be packed in any $a' \times b'$ rectangle R with $a' < a$ and $b' < b$. From this, we can deduce that, for any integer $N \geq 4$, $s(N) \geq \min\{\lceil \sqrt{N} \rceil, \sqrt{N - 2\lfloor \sqrt{N} \rfloor + 1} + 1\}$. In particular, for any integer $n \geq 2$, $s(n^2) = s(n^2 - 1) = s(n^2 - 2) = n$ holds.

9. H. Nagamochi, K. Iwata, T. Ishii:
"A Robust Algorithm for Bisecting a Triconnected Graph with Two Resource Sets", Theoretical Computer Science A, 341, 364-378, 2005.
概要: Given two disjoint subsets T_1 and T_2 of nodes in a 3-connected graph $G = (V, E)$ with a node set V and an arc set E, where $|T_1|$ and $|T_2|$ are even numbers, it is known that V can be partitioned into two sets V_1 and V_2 such that the graphs induced by V_1 and V_2 are both connected and $|V_1 \cap T_j| = |V_2 \cap T_j| = |T_j|/2$ holds for each $j = 1, 2$. An $O(|V|^2 \log |V|)$ time and $O(|V| + |E|)$ space algorithm for finding such a bipartition has been proposed based on a geometric argument, where G is embedded in the plane $\Re^2$ and the node set is bipartitioned by a ham-sandwich cut on the embedding. A naive implementation of the algorithm, however, requires high precision real arithmetic to distinguish two close points in a large set of points on $\Re^2$. In this paper, we propose an $O(|V|^2)$ time and space algorithm to the problem. The new algorithm, which remains to be based on the geometric embedding, can construct a solution purely combinatorially in the sense that it does not require computing actual embedded points in $\Re^2$ and thereby no longer needs to store any real number for embedded points. Although the new algorithm seems to need more space complexity, it can be implemented only with $|V|$ linked lists such that each element stores an integer in $[1, |V|]$.

10. H. Nagamochi:
"Increasing the Edge-Connectivity by Contracting a Vertex Subset", IEICE Transactions on Information and Systems, E89-D, 744-750, 2006.
概要: Let $G = (V, E)$ be an edge weighted graph with n vertices and m edges. For a given integer p with $1 < p < n$, we call a set $X \subseteq V$ of p vertices a p-maximizer if X has a property that the edge-connectivity of the graph obtained by contracting X into a single vertex is no less than that of the graph obtained by contracting any other subset of p vertices. In this paper, we first show that there always exists an ordering $v_1, v_2, \ldots, v_n$ of vertices in V such that, for each $i = 2, 3, \ldots, n - 1$, set $\{v_1, v_2, \ldots, v_i\}$ is an i-maximizer. We give an $O(mn + n^2 \log n)$ time algorithm for finding such an ordering and then show an application to the source location problem.

11. H. Nagamochi, K. Kuroya:
"Drawing c-Planar Biconnected Clustered Graphs", Discrete Applied Mathematics, (掲載予定).
概要: In a graph, a cluster is a set of vertices, and two clusters are said to be non-intersecting if they are disjoint or one of them is contained in the other. A clustered graph C consists of a graph G and a set of non-intersecting clusters. In this paper, we assume that C has a compound planar drawing and each cluster induces a

biconnected subgraph. Then we show that such a clustered graph admits a drawing in the plane such that (i) edges are drawn as straight line segments with no edge crossing, and (ii) the boundary of the biconnected subgraph induced by each cluster is a convex polygon.

12. H. Nagamochi:
"Sparse Connectivity Certificates via MA Orderings in Graphs", Discrete Applied Mathematics, (掲載予定).
概要: For an undirected multigraph $G = (V, E)$, let α be a positive integer weight function on V. For a positive integer k, G is called (k, α)-connected if any two vertices $u, v \in V$ remain connected after removal of any pair (Z, E') of a vertex subset $Z \subseteq V - \{u, v\}$ and an edge subset $E' \subseteq E$ such that $\sum_{v \in Z} \alpha(v) + |E'| < k$. The (k, α)-connectivity is an extension of several common generalizations of edge-connectivity and vertex-connectivity. Given a (k, α)-connected graph G, we show that a (k, α)-connected spanning subgraph of G with $O(k|V|)$ edges can be found in linear time by using MA orderings. We also show that properties on removal cycles and preservation of minimum cuts can be extended in the (k, α)-connectivity.

13. H. Ito, H. Nagamochi:
"Two Equivalent Measures on Weighted Hypergraphs", Discrete Applied Mathematics, (掲載予定).
概要: Let $H = (N, E, w)$ be a hypergraph with a node set $N = \{0, 1, \ldots, n-1\}$, a hyperedge set $E \subseteq 2^N$, and real edge-weights $w(e)$ for $e \in E$. Given a convex n-gon P in the plane with vertices $x_0, x_1, \ldots, x_{n-1}$ which are arranged in this order clockwisely, let each node $i \in N$ correspond to the vertex x_i and define the area $A_P(H)$ of H on P by the sum of the weighted areas of convex hulls for all hyperedges in H. For $0 \le i < j < k \le n-1$, a convex three-cut $C(i, j, k)$ of N is $\{\{i, \ldots, j-1\}, \{j, \ldots, k-1\}, \{k, \ldots, n-1, 0, \ldots, i-1\}\}$ and its size $c_H(i, j, k)$ in H is defined as the sum of weights of edges $e \in E$ such that e contains at least one node from each of $\{i, \ldots, j-1\}$, $\{j, \ldots, k-1\}$ and $\{k, \ldots, n-1, 0, \ldots, i-1\}$. We show that the following two conditions are equivalent:

- $A_P(H) \le A_P(H')$ for all convex n-gons P.
- $c_H(i, j, k) \le c_{H'}(i, j, k)$ for all convex three-cuts $C(i, j, k)$.

From this property, a polynomial time algorithm for determining whether or not given weighted hypergraphs H and H' satisfy "$A_P(H) \le A_P(H')$ for all convex n-gons P" is immediately obtained.

14. H. Nagamochi:
"A Fast Edge-Splitting Algorithm in Edge-Weighted Graphs", Inst. Electron. Inform. Comm. Eng. Trans. Fundamentals, (掲載予定).
概要: Let H be a graph with a designated vertex s, where edges are weighted by non-negative reals. Splitting edges $e = \{u, s\}$ and $e' = \{s, v\}$ at s is an operation that reduces the weight of each of e and e' by a real $\delta > 0$ while increasing the weight of edge $\{u, v\}$ by δ. It is known that all edges incident to s can be split off while preserving the edge-connectivity of H and that such a complete splitting is used to solve many connectivity problems. In this paper, we give an $O(mn + n^2 \log n)$ time algorithm for finding a complete splitting in a graph with n vertices and m edges.

15. T. Ishii, S. Yamamoto, H. Nagamochi:
"Augmenting Forests to Meet Odd Diameter Requirements", Discrete Optimization, (掲載予定).
概要: Given a graph $G = (V, E)$ and an

integer $D \geq 1$, we consider the problem of augmenting G by the smallest number of new edges so that the diameter becomes at most D. It is known that no constant approximation algorithms to this problem with an arbitrary graph G can be obtained unless $P = NP$. For a forest G and an odd $D \geq 3$, it was open whether the problem is approximable within a constant factor. In this paper, we give the first constant factor approximation algorithm to the problem with a forest G and an odd D; our algorithm delivers an 8-approximate solution in $O(|V|^3)$ time. We also show that a 4-approximate solution to the problem with a forest G and an odd D can be obtained in linear time if an augmented graph is additionally required to be biconnected.

16. H. Nagamochi, T. Kawada:
"Minmax Subtree Cover Problem on Cacti", Discrete Applied Mathematics, (掲載予定).
概要: Let $G = (V, E)$ be a connected graph such that edges and vertices are weighted by nonnegative reals. Let p be a positive integer. The minmax subtree cover problem (MSC) asks to find a pair $(\mathcal{X}, \mathcal{T})$ of a partition $\mathcal{X} = \{X_1, X_2, \ldots, X_p\}$ of V and a set $\mathcal{T}$ of p subtrees $T_1, T_2, \ldots, T_p$, each T_i containing X_i so as to minimize the maximum cost of the subtrees, where the cost of T_i is defined to be the sum of the weights of edges in T_i and the weights of vertices in X_i. In this paper, we propose an $O(p^2 n)$ time $(4 - 4/(p+1))$-approximation algorithm for the MSC when G is a cactus.

17. 軽野 義行, 永持 仁, 大嶋 芳行:
"食品の袋詰め最適化問題に対する動的計画法", 日本機会学会論文集, (掲載予定).
概要: In this paper, we deal with a food packing problem in an automated food packing system. The packing system has n hoppers, where an item is thrown into each hopper. An integer weight w_i and a priority γ_i are associated with each item i, where any w_i is assumed to be bounded by an integer w_{max}. Given a set I of n items in the hoppers, the packing system chooses a subset I' $(\subseteq I)$ of items, and puts them into a package with a specified target weight B. After that, the packing system updates the set I by taking the union of the remaining items in $I - I'$ and new items thrown into empty hoppers. Repeating these operations, it makes a large number of packages one by one. In the packing system, an item may be left in a hopper for a long time until it is chosen. The priority γ_i is introduced to avoid such a situation, if possible. The packing problem is formulated as a lexicographic bi-criteria discrete optimization problem, where the first objective is to minimize $\sum_{i \in I'} w_i$ such that $\sum_{i \in I'} w_i \geq B$ must be satisfied, and the second is to maximize $\sum_{i \in I'} \gamma_i$. In this paper, we propose an $O(n^2 w_{max})$ time algorithm based on dynamic programming to the packing problem. We also examine the performance of the proposed approach by means of numerical experiments, and report the results.

18. Kazuhisa Makino, Yushi Uno, Toshihide Ibaraki:
"Minimum Edge Ranking Spanning Trees of Split Graphs", Discrete Applied Mathematics, (to appear).
概要: Given a graph G, the minimum edge ranking spanning tree problem (MERST) is to find a spanning tree of G whose edge ranking is minimum. However, this problem is known to be NP-hard for general graphs. In this paper, we show that the problem MERST has a polynomial time algorithm for split graphs, which have useful applications in practice. The result is also significant in the sense that this is a first non-trivial graph class for which the problem MERST is found to be polynomially

solvable. We also show that the problem MERST for threshold graphs can be solved in linear time, where threshold graphs are known to be split.

研究会等

1. Ryuhei Uehara, Yushi Uno:
"Laminar Structure of Ptolemaic Graphs with Applications", Lecture Notes in Computer Science, Springer, 3827, 186–195, 2005.
概要: Ptolemaic graphs are graphs that satisfy the Ptolemaic inequality for any four vertices. The graph class coincides with the intersection of chordal graphs and distance hereditary graphs. The graph class can also be seen as a natural generalization of block graphs (and hence trees). In this paper, a new characterization of ptolemaic graphs is presented. It is a laminar structure of cliques, which leads us to a canonical tree representation. The tree representation gives a simple intersection model for ptolemaic graphs. The tree representation is constructed in linear time from a perfect elimination ordering obtained by the lexicographic breadth first search. Hence the recognition and the graph isomorphism for ptolemaic graphs can be solved in linear time. Using the tree representation, we also give an efficient algorithm for the Hamiltonian cycle problem.

2. T. Ishii, K. Iwata, H. Nagamochi:
"Bisecting a Four-Connected Graph with Three Resource Sets", 4th Japanese-Hungarian Symposium on Discrete Mathematics and Its Applications, 107-113, 2005.
概要: Let $G = (V, E)$ be an undirected graph with a node set V and an arc set E. G has k pairwise disjoint subsets $T_1, T_2, \ldots, T_k$ of nodes, called resource sets, where $|T_i|$ is even for each i. The partition problem with k resource sets asks to find a partition V_1 and V_2 of the node set V such that the graphs induced by V_1 and V_2 are both connected and $|V_1 \cap T_i| = |V_2 \cap T_i| = |T_i|/2$ holds for each $i = 1, 2, \ldots, k$. The problem of testing whether such a bisection exists is known to be NP-hard even in the case of $k = 1$. On the other hand, it is known that if G is $(k+1)$-connected for $k = 1, 2$, then a bisection exists for any given resource sets, and it has been conjectured that for $k \geq 3$, a $(k + 1)$-connected graph admits a bisection. In this paper, we show that for $k = 3$, the conjecture does not hold, while if G is 4-connected and has K_4 as its subgraph, then a bisection exists and it can be found in $O(|V|^3 \log |V|)$ time.

3. K. Haraguchi, H. Nagamochi, T. Ibaraki:
"Compactness of Classifiers by Iterative Compositions of Features", 4th Japanese-Hungarian Symposium on Discrete Mathematics and Its Applications, 92-98, 2005.
概要: Classification is one of the most important issues in machine learning. In an n-dimensional binary space $\{0,1\}^n$, we are given a set of examples $x \in \{0,1\}^n$, where each example x is labeled as $y(x)$ by a Boolean function $y : \{0,1\}^n \mapsto \{0,1\}$, called an oracle, and the classification problem asks to find a classifier c, a Boolean function $c : \{0,1\}^n \mapsto \{0,1\}$ that is (approximately) identical to y. We assume that y is a compact concept in the spirit of Occam's Razor. For constructing classifiers on computers, we use a representation model L which provides forms for classifiers that can be implemented on computers, where the complexity of representation is determined as its length on a computer. From our assumption on oracles, we wish to construct a classifier c with small complexity. In this paper, we discuss two representation models, iteratively composed features and decision trees, and prove that, for any classifier c, the former has a representation which is

at least as compact as that by the latter.

4. T. Fukunaga, H. Nagamochi:
"Edge Packing Problem with Edge Capacity Constraints", 4th Japanese-Hungarian Symposium on Discrete Mathematics and Its Applications, 69-75, 2005.
概要: The edge dominating set problem is one of the fundamental covering problems in the field of combinatorial optimization. In this paper, we consider a packing version of this problem. Given a graph with an edge cost, the problem asks to find a maximum cost edge set such that each edge in the graph is adjacent to at most one edge in the set. We show inapproximability of the problem by a reduction from the independent set problem. We also consider a capacitated case of this problem and propose an approximation algorithm based on a relation between two polytopes for an LP relaxation of the problem and the capacitated b-matching problem.

5. Y. Kamidoi, N. Yoshida, H. Nagamochi:
"A Deterministic Algorithm for Finding All Minimum k-Way Cuts", 4th Japanese-Hungarian Symposium on Discrete Mathematics and Its Applications, 224-233, 2005.
概要: Let $G = (V, E)$ be an edge-weighted undirected graph with n vertices and m edges. We present a deterministic algorithm to compute a minimum k-way cut of G for a given k $(5 \leq k \leq n-1)$. Our algorithm is a divide-and-conquer method which consists of a procedure that reduces an instance of the minimum k-way cut problem to $O(n^{2k-5})$ instances of the minimum $(\lfloor (k+\sqrt{k})/2 \rfloor + 1)$-way cut problem, and can be implemented to run in $O(n^{4k/(1-1.71/\sqrt{k})-31})$ time.

6. T. Imamichi, M. Kenmochi, K. Nonobe, M. Yagiura, H. Nagamochi:
"Branch-and-bound Algorithms for Rectangular Strip Packing and Perfect Packing Problems", ESICUP (EURO Special Interest Group on Cutting and Packing) 2nd Meeting, 2005.
概要: The rectangular strip packing problem asks for a placement of given rectangles without any overlap into a container of a fixed width, where the objective is to minimize the height of the container. The perfect packing problem, a special case of the strip packing, asks to determine whether given rectangles can be packed into a container of a fixed width and height without any waste space. We consider various types of branch-and-bound algorithms for these problems with and without rotations. We first develop a branch-and-bound algorithm to the strip packing problem based on sequence pair coding scheme, which represents the relative placement relations of rectangles. This scheme is general, but the resulting algorithm could solve small instances with up to 11 rectangles in practical time. We then consider the perfect packing problem and examine various branching rules and bounding operations. As for branching rules we consider two strategies called bottom-left and staircase placement. Bottom-left placement is to place rectangles one by one at the bottom-left point in the available space, where each branch corresponds to a rectangle. Staircase placement is to place rectangles keeping the entire shape of placed rectangles forming a staircase, where each branch corresponds to a corner on the stairs. As for bounding operations we consider three methods called dynamic programming (DP) cut, linear programming (LP) cut and active node combination (ANC) cut. DP cut examines whether we can fill all gaps of the empty space with dynamic programming. LP cut solves the LP relaxation problem of an integer programming formulation of the packing problem to check its feasibility. ANC

cut combines the current node with other active nodes to tighten the feasibility test by DP cut. We conducted computational experiments on benchmark instances to examine all combinations of the above operations and observed the following. (1) Feasible instances are in many cases much easier than infeasible ones, because we can stop the search immediately after a feasible solution is found, while as to infeasible instances we must conclude infeasibility for entire search space. (2) Effective method is different depending on the feasibility of instances. (3) Our algorithm outperforms existing algorithms for the perfect packing problem without rotation, solving almost all benchmark instances with up to 49 rectangles within reasonable computation time.

7. M. Kenmochi, T. Imamichi, K. Nonobe, M. Yagiura, H. Nagamochi:
"Exact Algorithms for the 2-Dimensional Strip Packing Problem with Rotations", The IFORS Triennial 2005 Conference, 2005.
概要: We examine various strategies for exact approaches to the 2-dimensional strip packing problem (2SP) with rotations and propose a new branching rule in branch-and-bound algorithms for the perfect packing problem (PP), which is a special case of 2SP. This rule is very effective especially for feasible instances of PP.

8. M. Nishihara, M. Yagiura, T. Ibaraki, H. Nagamochi:
"The Relation Between Option Pricing and Optimization Problems", The IFORS Triennial 2005 Conference, 2005.
概要: We investigate the option pricing problem based only on the no-arbitrage assumption, without assuming any stochastic model. We theoretically extend Bertsimas and Popescu's results that the problem can be solved efficiently via convex programming. Furthermore we confirm that our results are practical from computational results using real data.

9. H. Nagamochi:
"Heuristics for the Minmax Subtree Cover in Graphs", The IFORS Triennial 2005 Conference, 2005.
概要: Given an edge-weighted graph and an integer k, the minmax tree cover problem asks to find a set of k subtrees of the graph such that the union of the subtrees covers all vertices and the maximum weight of the subtrees is minimized. This talk surveys constant factor approximation algorithms for this problem.

10. T. Fukunaga, H. Nagamochi:
"Approximation Algorithms for the b-Edge Dominating Set Problem and Its Related Problems", The Eleventh International Computing and Combinatorics Conference (COCOON 2005), Lecture Notes in Computer Science, Springer-Verlag, 3595, 747-756, 2005.
概要: The edge dominating set problem is one of the fundamental covering problems in the field of combinatorial optimization. In this paper, we consider the b-edge dominating set problem, a generalized version of the edge dominating set problem. In this version, we are given a simple undirected graph $G = (V, E)$ and a demand vector $b \in Z_+^E$. A set F of edges in G is called a b-edge dominating set if each edge $e \in E$ is adjacent to at least $b(e)$ edges in F, where we allow F to contain multiple copies of edges in E. Given a cost vector $w \in R_+^E$, the problem asks to find a minimum cost of a b-edge dominating set. We first show that there is a $\frac{8}{3}$-approximation algorithm for this problem. We then consider approximation algorithms for other related problems.

11. T. Ishii, K. Iwata, H. Nagamochi:
"Bisecting a Four-Connected Graph with

Three Resource Sets", The The 16th Annual International Symposium on Algorithms and Computation (ISAAC 2005), Lecture Notes in Computer Science, Springer-Verlag, 3827, 176-185, 2005.

概要: Let $G = (V, E)$ be an undirected graph with a node set V and an arc set E. G has k pairwise disjoint subsets $T_1, T_2, \ldots, T_k$ of nodes, called resource sets, where $|T_i|$ is even for each i. The partition problem with k resource sets asks to find a partition V_1 and V_2 of the node set V such that the graphs induced by V_1 and V_2 are both connected and $|V_1 \cap T_i| = |V_2 \cap T_i| = |T_i|/2$ holds for each $i = 1, 2, \ldots, k$. It is known that if G is $(k+1)$-connected for $k = 1, 2$, then a bisection exists for any given resource sets, and it has been conjectured that for $k \geq 3$, a $(k+1)$-connected graph admits a bisection. In this paper, we show that for $k = 3$, the conjecture does not hold, while if G is 4-connected and has K_4 as its subgraph, then a bisection exists and it can be found in $O(|V|^3 \log |V|)$ time. Moreover, we show that for an arc-version of the problem, the $(k+1)$-edge-connectivity suffices for $k = 1, 2, 3$.

12. Y. Karuno, H. Nagamochi:
"Minimizing Capacitated Tree Covers of Graphs", Third International Conference on Innovative Applications of Information Technology for the Developing World (Asian Applied Computing Conference (AACC 2005)), 2005.

概要: Let $G = (V, E)$ be a simple connected graph such that each vertex $v \in V$ and each edge $e \in E$ are weighted by non-negative reals $h(v)$ and $w(e)$, respectively. The capacitated subtree cover problem asks to find a partition $\mathcal{X} = \{X_1, X_2, \ldots, X_p\}$ of V and a set $\mathcal{T} = \{T_1, T_2, \ldots, T_p\}$ of p subtrees such that each T_i contains X_i so that the cost of each T_i must not exceed a specified capacity d (> 0), where the cost of each T_i is defined by the sum of weights of edges in T_i and weights of vertices in X_i. The objective is to minimize the number p $(= |\mathcal{X}| = |\mathcal{T}|)$ of subtrees. In this paper, we propose a constant factor approximation algorithm to the problem.

13. Y. Koga, M. Yagiura, K. Nonobe, T. Imamichi, H. Nagamochi, T. Ibaraki:
"Efficient Branch-and-bound Algorithms for Weighted MAX-2-SAT", Third International Conference on Innovative Applications of Information Technology for the Developing World (Asian Applied Computing Conference (AACC 2005)), 2005.

概要: Given a set of m clauses on n propositional variables, where each clause contains at most two literals and is weighted by a positive real, MAX-2-SAT asks to find a truth assignment that maximizes the total weight of satisfied clauses. In this paper, we propose two branch-and-bound algorithms for MAX-2-SAT. Our algorithm features two new transformation rules and two efficient algorithms for computing lower bounds. Computational comparisons on benchmark instances disclose that these algorithms are highly effective in reducing the number of search tree nodes as well as computation time of a branch-and-bound algorithm to MAX-2-SAT.

14. K. Haraguchi, H. Nagamochi, T. Ibaraki:
"Experimental Studies on Representation Complexity and Error Rates of Iteratively Composed Features", Third International Conference on Innovative Applications of Information Technology for the Developing World (Asian Applied Computing Conference (AACC 2005)), 2005.

概要: We consider constructing a classifier $c : \{0,1\}^n \mapsto \{0,1\}$ from a training set of n-dimensional binary vectors. A classifier is usually represented by a representation

model such as decision tree (DT) and iteratively composed feature (ICF). In this paper, we discuss the following issues through computational experiments: 1) relation between the representation complexity γ, the error on the training set e and the expected error E of an ICF classifier and 2) comparison between ICF and DT. For 1), we observe that a simpler ICF is more likely to attain a small E, among the ICFs having the same e. For 2), we see that DTs generated by C4.5 and ICFs generated by our algorithm are competitive in terms of E.

15. Y. Uno:
"An experimental study on the Web graph", The IFORS Triennial 2005 Conference, 2005.
概要: The Web graph is a digraph induced by the hyperlink structure of WWW, and a large amount of research has revealed its complex topology. We present some new experimental observations on the topological structure of the Web graph that have not been reported so far. These results will give suggestions for designing web algorithms.

C07: Web コンテンツ活用に関連した離散最適化問題の研究

増山 繁 † 梅村 恭司 ‡ 中山 慎一 § 本間 宏利 ¶ 石井 利昌 ‡ 相田 慎 †

† 豊橋技術科学大学知識情報工学系
〒 441-8580 豊橋市天伯町雲雀ヶ丘 1-1
{masuyama,aida}@tutkie.tut.ac.jp

‡ 豊橋技術科学大学情報工学系
〒 441-8580 豊橋市天伯町雲雀ヶ丘 1-1
{umemura,ishii}@ics.tut.ac.jp

§ 徳島大学総合科学部
〒 770-8502 徳島市南常三島町 1-1
shin@ias.tokushima-u.ac.jp

¶ 釧路工業高等専門学校 情報工学科
〒 084-0916 釧路市大楽毛西 2 丁目 32-1
honma@info.kushiro-ct.ac.jp

1 はじめに

本グループでは、Web 上に存在する膨大な量の情報を活用するための技術的問題を離散最適化問題として定式化し、それに対し、実用的観点からみて有効かつ適切なアルゴリズムを開発することを目的とする。特に、以下の 2 つの項目に重点をおいて研究を実施してきている。

1. 要約、検索などの、 Web コンテンツを知的活動において活用するのを支援するための基本技術の確立

2. Web コンテンツ配信方法を求める問題のグラフ理論的定式化とその解法

1 の細目は以下の通りである。

1.1. ユーザの個別の情報要求に適合した要約手法、及び、分類手法とそのアルゴリズムの開発

1.2. Web データから人間が気づかない未知の知識を発見、獲得する手法の開発

2 の細目は以下の通りである。

2.1. コンテンツ配信問題に対する計算量の解明と効果的解法の提案

2.2. コンテンツ配信の基盤となる、ネットワーク信頼性等、高度情報通信網に関連した諸問題の定式化とそのアルゴリズム

平成１７年度に得られた主な成果は以下のとおりである。

- Web コンテンツ活用に関連したテキストからの情報抽出及びテキスト自動要約
  - 交通事故事例に含まれる事故原因表現の新聞記事からの抽出
  - 可読性の向上を目的とした片仮名表記外来語の換言知識獲得
  - 略語とその原型語との対応関係のコーパスからの自動獲得手法の改良
  - ユーザの要約要求を反映するためにユーザとのインタラクションを導入した複数文書要約システム
- Web コンテンツ配信と関連した問題、および、その基盤としての高度情報通信網に関連した問題
  - 最小節点ランキング全域木問題の計算複雑度
  - 外平面グラフ上での最小節点ランキング全域木問題に対する多項式時間アルゴリズム
  - モバイルエージェント実行計画問題について

以下では、主としてこれらの成果について紹介する。

2 Web コンテンツ活用に関連した情報抽出及びテキスト自動要約

2.1 交通事故事例に含まれる事故原因表現の新聞記事からの抽出 [学術論文 4]

自動車の保有台数は，年々増加の一途をたどり，平成 13 年には 8,972 万台と，国民 1.4 人に 1 台の

割合となった．それに伴い，交通事故が大きな社会問題となっている．事故統計によれば，道路交通事故発生件数は昭和 45 年の 720,880 件を最高に，一旦は減少した．しかし，昭和 50 年代半ばから再び増加傾向を示し，平成 5 年には昭和 45 年の件数を上回る．その後，増加の一途をたどり，平成 16 年には，952,191 件に達している．

交通事故低減に向けた効果的な対策のために，事故原因の分析が重要であることに疑問の余地はない．そのためのデータとして代表的なものは交通事故統計年報である．同事故統計は，発生時間帯別や当事者の年齢別など事故を様々な角度から集計しており，マクロ分析と呼ばれている．その中で，上記目的にあった集計には，道路形状別・昼夜別・事故類型別全事故件数，法令違反別・当事者別全事故件数，当事者別・行動類型別死亡事故件数などがある．例えば，事故類型別の集計では，事故を「出会い頭」,「追越・追抜時」等，36 種類の類型に分類して集計している．しかし，なぜ，出会い頭あるいは追越・追抜で事故になったかという原因は，このデータだけでは分からない．

マクロ分析に対してミクロ分析がある．資料は，出会い頭事故をミクロ事故調査により，詳細に分析したものである．事故原因をドライバの「認知エラー」,「判断・予測エラー」で大別し，それぞれの原因を数項目に分類して分析している．このようなミクロ分析は，当事者の聞き取り調査によって初めて可能となった分析であり価値の高いものである．しかし，交通事故防止に関する研究のため，自分の研究テーマに沿った観点で分析したくても，同資料に開示された以上のことは不明である．しかし，同資料は公的な組織による交通事故現場での詳細な調査に基づくものであり，このようなデータを追加収集することは容易ではない．

一方，近年のインターネットの普及などにより大量の電子テキストが利用可能となった．その中にあるニュース記事や Web ページなどに，膨大な交通事故のテキスト情報が含まれている．そこで，情報検索・情報抽出などの言語処理技術を利用して，交通事故に関する大量のテキスト情報を抽出し，さらに，事故原因に関する情報を抽出できれば，従来のマクロ分析，ミクロ分析を補完する有用な情報になり得ると期待できる．本論文では，新聞記事の電子テキストデータに含まれる交通事故を扱った記事[1]から，事故原因に関する情報として事故原因を表す表現（例えば,「ハンドル操作を誤った」）を自動的に抽出する手法を提案する．

2.2 可読性の向上を目的とした片仮名表記外来語の換言知識獲得 [学術論文 2]

外来語である片仮名語、特に英語を語源とした片仮名語の和語または漢語への換言のための知識獲得に関する研究を行なった。近年、公的文書等における難解な片仮名語の乱用が問題視されている。片仮名語の大部分は英単語に基づく外来語であり、従来日本語で用いられてきた語彙に換言可能な場合も多い。換言とは、ある言語表現の意味内容を保持したまま別の表現へと言い替えることであり、自然言語処理のための要素技術として今後ますます重要になると認識されている。換言するための知識は人手で作成することもできるが、実用的な質と量を満たすためには多大な労力を要する。そのため、換言知識は可能な限り自動的に獲得することが望ましい。以上より、本研究では、難解な片仮名語をより理解し易い語へと言い替えるための換言知識を自動的に獲得することを目的としている。手順としては、まず、片仮名語の元になった英単語を復元する。そして、得られた英単語の日本語訳を辞書によって獲得し、候補を絞り込む。実験の結果、英単語復元は再現率 82.2%、精度 81.1%を得、換言候補獲得については再現率 14.6%、精度 70.8%となった。

近年、日本語の公的文書において片仮名語が多用されるようになり、文書可読性の低下が問題となっている。国立国語研究所は、自治体の広報紙等で用いられることの多い難解な外来語である片仮名語に対して、より理解しやすい語への換言例を作成し、文書可読性の向上を推奨している。換言とは、ある言語表現の意味内容を保持したまま、別の表現へと言い替えることであり、その有用性が最近注目されている。同所は、今後も半年に５０語程度ずつ換言例を追加するとしている。このような手順をとっている理由としては、一度にすべての換言知識を整備することが困難であること、

[1]なお，本論文における交通事故事例は道路交通事故に限る．

外来語である片仮名語には新語が多いため、ある時点で換言知識を十分に整備したとしても、次の年には知識の追加や更新が必要になること等があげられている。２００４年１２月現在で提案されている語は１４１語であり、日常的に用いられている片仮名語に比べると、はるかに少ない。より大量の換言知識を整備するために、全ての換言規則を人手で作成するのではなく、ある程度自動的に取得することが望ましい。

本研究では、片仮名語からの換言知識を自動獲得するための手法を考案した。その際に、片仮名語の性質に特化した手法を用いることで性能の向上を試みた。

換言知識の自動獲得の研究としては、他にも、パラレルコーパスを用いたものがある。しかし、一般に大量のパラレルコーパスを利用することは困難であり、獲得された換言知識の量は少ない。特に、片仮名語に関しては、パラレルコーパス自体が入手困難であるため、本研究では考慮していない。また、久光らは、括弧表現を利用して換言事例を自動獲得している。この方法も、獲得される知識の量は多くないが、単一のコーパスから知識獲得が可能であることや、獲得された知識の正解率が高いこと等の利点もある。そのため、本研究では、この研究に基づく手法も併用している。

換言の必要がある片仮名語の大部分は、英語に基づく外来語である。つまり、その片仮名語が日本語の語彙中では新語･未知語だったとしても、元となった英単語は、英語の語彙中で既知の場合が多い。そのため、日英翻訳のための辞書を用いて、英単語から日本語訳を獲得することができる。そこで、片仮名語から元になった英単語を復元する。一般に、ひとつの英単語に相当する日本語訳は、数十語程度獲得されるので、その中から最もふさわしい一語に絞り込むために、統計的手法を併用する。英単語が復元できなかった場合の換言候補はコーパス中の全名詞とする。以上が、本手法の主要部分の概要である。また、難解な片仮名語は新聞記事中で補足説明されている場合がある。本手法では、これらの情報も利用し、換言知識獲得の手助けとした。

実験の結果、英単語復元は再現率 82.2%, 精度 81.1%を得、換言候補獲得については再現率 14.6%、精度 70.8%となった。

2.3 略語とその原型語との対応関係のコーパスからの自動獲得手法の改良 [学術論文 3]

日本語には，ある名詞から一部の文字を省略することで意味内容を保ったまま別の表現に変換する事例が多く存在し，一般に略語と定義される．例えば,「原発」は,「原子力発電所」の略語であり,「原子力発電所」からいくつかの文字が省略されているにもかかわらず，同一の意味を持つ．また，複合名詞から一部の名詞が省略されても意味が変わらない，あるいは，読み手が省略された名詞を推定できる場合が存在する．例えば「バブル経済崩壊」から「経済」が省略されて「バブル崩壊」と表記されても，一般知識から「経済」を推定することができる．このような名詞と略語との対応も要約や検索において有用な知識であるため，抽出対象とする．そのため，本稿では，複合名詞から名詞が省略された場合も同じく略語と定義し，略語とそれに対応した元の語との対応関係をコーパスから自動的に獲得する手法を提案する．(以降，略語に対応した元の語を原型語と定義する．)

略語とその原型語との対応関係を取得できれば，情報検索や文書要約において有用である．

- 検索：検索キーワードとして略語を入力した場合でも，その略語に対応する原型語を含む文書も検索できるようになる．新しい略語は常に発生し続けるため，人手による登録では多大な労力が必要となる．本手法はコーパスに含まれている略語とその原型語との対応を自動的に取得できるので，インターネットのニュース記事等をコーパスに使用すれば，最新の略語と原型語との対応も獲得可能である．

- 要約： 名詞の略語は元の名詞から一部の文字が削除された表現であるので，文字数が少なくなるにもかかわらず同一の意味をもつ名詞である．そのため，文中の名詞を略語に置き換えることによる文内要約に利用できる．また，複数文書要約においては異った文書中で略語とその原型語が混在している場合があり，冗長性の削除のために略語とその原型語を認識できる必要がある．

略語とその原型語との対応関係の獲得は言い換え

知識獲得の一種である．なぜなら，略語と原型語は表記が異なるにもかかわらず同じ意味を持つからである．

言い換え知識獲得は，例えばシソーラスの構築や語のクラスタリングといった研究とは同じ意味を持つ表現を獲得しなければならないという点で異なる．言い換え知識獲得の研究としてさまざまな手法が提案されている．例えば，原著に対する複数の翻訳本から言い換え知識を獲得する手法,「サ変名詞+する」から動詞相当句へ言い換える手法,「A が V する B」のような動詞連体修飾表現を「A の B」へ言い換える手法などがある．本手法は略語と原型語との対応関係をコーパスから獲得する手法であり，それに対応した手法を開発する必要がある．

関連研究として，括弧表現から語の対応を自動抽出する手法が提案されている．例えば「朝鮮民主主義人民共和国（北朝鮮）」から「朝鮮民主主義人民共和国」と「北朝鮮」との語の対応を獲得している．この手法により本稿で述べる手法では獲得できない対応を獲得することができるが，コーパスに括弧表現として記載されている対応しか獲得できない．例えば，コーパスに「原子力発電所(原発)」という文字列が出現しないと,「原子力発電所」とその略語「原発」との対応は獲得できない．しかし，その略語が一般的に知られている表現であれば，名詞 (略語) の表現はコーパス中に出現しないと考える．それに対して，本手法では括弧表現のような特別な文構造を必要としないため,「原子力発電所」とその略語「原発」との対応を獲得できる．

英語の略語復元に関する関連研究として，プログラムソースに出現する略語を規則に基づいて復元する手法が提案されている．日本語の略語復元に関する関連研究として，入力された略語を復元規則に基づいて復元する手法が提案されている．また，入力されたカタカナ語の省略形を WEB 文書を使用して推定する手法が提案されている．それらに対して，本手法は日本語の略語とそれに対応する元の語との対応をコーパスから取得する手法であり，入力された略語を元の語へ復元する研究ではない．そのため，コーパスに出現する各名詞が略語か原型語であるかどうかの情報は与えられていないことを手法の前提としている．また，本手法ではカタカナ語の省略形以外にも，漢字による略語と原型語との対応も取得する．しかし，3.1 節でも述べるが，表層的な文字情報による規則のみで不適切な略語候補と原型語候補との対応を排除し，略語とその原型語との対応を取得することは困難であると考える．そのため，本手法では，コーパスに含まれる名詞対から規則を適用して略語候補と原型語の候補との対応を取得し，その後，略語候補と原型語候補の類似度を統計情報を使用して計算し，類似度が高い略語候補と原型語候補との対応を略語と原型語との対応として取得する．

英語における略語と原型語との対応のコーパスからの取得の先行研究としては，一方は略語を多く含み，もう一方は略語が少ない同一ドメインの文書群を 2 つ用意し，略語を多く含む文書における未知語は何かの略語である可能性があるとして，もう一方の文書群から対応する名詞を抽出する手法が提案されている．しかし，この手法では同一ドメインの略語を多く含むコーパスと含まないコーパスを共に用意しなければならない．そのため，そのようなコーパス対の入手が必ずしも可能であるとは限らない上，ドメインが限定されるため，そのドメインにおける略語と原型語との対応しか抽出できない．

それらの先行研究に対して，我々は，以前に単一のコーパスから略語と原型語との対応を抽出する試みを行なった．この手法は，日本語における名詞の文字情報による規則を用いて，略語候補と原型語候補との対応をコーパスから探索する．そして，略語候補と原型語候補の名詞間類似度を計算し，ある閾値より名詞間類似度が高い対応を略語と原型語との対応として取得する．我々の既提案手法は，単一のコーパスから名詞と略語との対応を抽出することを試みるため，ドメインに依存しない略語を抽出可能であった．また，文内の構造は用いないため，例えば括弧表現のような特殊な構造をしていなくても，略語と原型語との対応を抽出可能である．本稿で提案する手法は，我々の既提案手法を改良し，既提案手法に比べて同一の再現率において高い精度を目指したものである．

本手法と既提案手法とでは，名詞間類似度の計算手法が異なる．既提案手法は，正しい略語と原型語の対応でも低い類似度が割り当てられること

がある．既提案手法では略語候補，原型語候補が出現する文に含まれる全ての名詞を取得し，それを意味属性に汎化する．そして，その意味属性に付与された重みを要素としたベクトルを生成し，ベクトル間の余弦を略語候補と原型語候補の類似度とする．しかし，略語候補や原型語候補と関連が低い名詞の意味属性をも要素とするため，多くの非零要素を持つベクトルが生成される．そのため，たとえ正しい略語と原型語の対応でも低い類似度が割り当てられることがある．それに対して，本手法は，略語候補や原型語候補に対するベクトルを生成する際に，略語候補や原型語候補を含む文書から名詞を取得する．そして，略語候補や原型語候補に関連のある名詞を抽出する処理を行い，無関係な名詞によるベクトル成分への悪影響を抑制する．評価の結果，既提案手法より同一の再現率において高い精度を達成した．また，提案した手法のより詳細な実験を行い，本手法の有効性を確認した．

2.4 ユーザの要約要求を反映するためにユーザとのインタラクションを導入した複数文書要約システム [学術論文 5]

近年のコンピュータ，および，情報通信技術の進歩により，膨大な量の機械可読な情報を簡単に得ることができるようになった．しかしながら，それは情報の爆発を招き，不必要な情報や冗長な情報も多く含まれるようになった．この情報爆発の問題を解決するために，文書中の不必要な情報を除去し，重要な情報のみを取り出す文書自動要約の必要性が高まっている)．従来，文書自動要約とは，主として１つの文書から１つの要約を自動的に生成する技術であった．しかしながら，人間が知的な活動を行うためには１つの文書の要約を生成するよりも，ある事柄に関連した複数の文書から１つの要約を生成する技術 (すなわち，複数文書要約技術) の方がより重要である．なぜなら，人間の限られた情報処理能力では，検索結果などで得られた関連した多くの文書を読むのに多大な時間が必要であり，それらを１つの要約にまとめることで読む時間の大幅な削減が可能になるからである．特に，ある検索要求の検索結果として得られた文書集合に対する複数文書要約を生成することで，ユーザの負担もなく素早く検索結果の内容を確認できることから，実用性，将来性ともに期待できる技術である．そのため，複数文書要約技術の確立が強く望まれており，近年，盛んに研究されている．

本論文では，複数文書要約とは，検索要求に適合する文書集合から，指定された長さの１つの要約を作成するタスクと定義する．そのため，要約対象となる文書集合は１つの検索要求の話題に関連している文書集合である．(例えば，天体望遠鏡「すばる」の試験観測開始に関する文書集合，タンザニア，ケニアでの米国大使館爆破事件に関する文書集合など．) ところが，検索要求に適合する文書集合から１つの要約を生成するとはいえ，その文書集合には多くの内容が含まれており，文書集合に含まれる各文書の内容は一様ではない．例えば,「ソニーのＡＩＢＯ発売に関する文書集合」には，ＡＩＢＯの動作に関するものや販売方法に関するものなど，様々な内容が含まれている．この文書集合から生成される要約は，これらの内容を全て盛り込んでいることが望ましいが，全ての内容を含む要約を少ない文字数で生成することは困難である．さらに，重要な情報として認識される内容は，ユーザによって異なる．これは，検索要求に適合する文書集合に含まれるいくつかの情報の中で，ユーザが知りたい情報がユーザごとに異ることが１つの原因である．例えば,「ソニーのＡＩＢＯ発売に関する文書集合」を要約する場合,「アイボの機能」に関する情報が知りたいユーザと「アイボの販売方法」に関する情報が知りたいユーザでは，そのユーザにとって生成される要約に含まれるべき情報が異なる．

本論文では，複数文書要約において，ユーザが知りたい情報を「要約要求」と定義し，要約要求を反映した要約 (すなわち，ユーザが知りたい情報を含む要約) を生成するために，ユーザとのインタラクションを導入した複数文書要約システムを提案する．具体的には，まず，要約対象となる文書集合から，検索要求の話題と関連した k 個のキーワードを自動的に抽出し，ユーザに提示する．ユーザは提示されたキーワードの中から自分の要約要求に適したキーワードを選択する．本複数文書要約システムは，ユーザが選択したキーワードを使用して要約を生成することで，ユーザの要約

要求を反映した要約を生成する．本複数文書要約システムは，次の 4 つの処理で構成される．

キーワード抽出： 要約対象である，ある検索要求に適合する文書集合から，その検索要求の話題と関連したキーワードを抽出する．(抽出されたキーワードをユーザに提示する．)

重要文抽出： ユーザによって選択されたキーワードを使用して，要約対象の文書集合から重要文を抽出する．

冗長情報除去： 文書集合から抽出された重要文の集合には同じ内容を含む文が含まれている．そのため，抽出された重要文集合に含まれている，冗長な情報を含む文を削除する．

文圧縮： 抽出された重要文の中に含まれる不要な部分 (動詞連体修飾節) を除去し，1 文の文字数を減らすことで，文を圧縮する．

複数の文書が含まれる 1 つの文書集合に対して，キーワード抽出，重要文抽出，冗長情報除去，文圧縮を行い，1 つの要約が生成される．

本複数文書要約システムは，検索と要約の評価のためのワークショップ NTCIR4 [2] における要約タスク (以降，TSC3) に参加し，複数文書要約タスクにおいて良い成績を達成したことを示す．

2.5 その他

その他、以下について予備的結果をえた。

1. Weblog 内のリンクに対する感情推定の試みー Web コミュニティ発見法改善の基礎としてー

Web 上の情報量の増加と Weblog などの簡易な情報発信手段の普及によって、Web 上のリンクを単に「リンク先ページへの信頼」と解釈することはできなくなってきた。Web 上のリンクに込められた感情を知ることによって、より密に連携した Web コミュニティを発見することが可能になると考えられる。そこで本研究では、Weblog 内のリンクに対して、教師付き学習によって感情スコアを推定することを試みた。肯定的文書、否定的文書間の表現の偏りや、Weblog 特有の文書構造を考慮した結果、ピアソンの相関係数で 0.45 程度と、かなりの相関をもって推測可能であることがわかった。

2. 学生レポート採点支援のためのレポート類似部分発見手法

近年の情報技術の発達により，レポートの剽窃が非常に容易なものとなり問題と なっている．本研究では Smith-Waterman アルゴリズムを基礎とした，さまざまな「類似」を検出できるレポート類似部分発見法を考案した．そして，現実に提出されたレポートを含めた文書集合に対して実験を行った結果，F 値 $= 1$ となり，完全に剽窃レポートを検出することに成功した．

3. 文書頻度計数の線形時間アルゴリズムの実装と評価

統計的自然言語処理において，文字列を特徴付ける統計量として，文字列の出現頻度や文字列の現れる文書の総数などが用いられる。しかし，単純な方法では文書集合中のすべての任意文字列に対して，これらの統計量を計算するには $O(N^2)$ のメモリを必要とし，大規模なコーパスに対しては実際的でない。本稿では，Range Minimum Query のアルゴリズムを用いて $O(N)$ のメモリ空間と $O(N)$ の時間で，すべての任意文字列の重複条件付き文書頻度を求めるアルゴリズムを実装し，評価した。

3 Web コンテンツ配信と関連した問題、および、その基盤としての高度情報通信網に関連した問題

3.1 最小節点ランキング全域木問題の計算複雑度 [学術論文 6]

グラフ G の節点ランキングとは、同じラベルをもつ任意の 2 節点を結ぶ路上に必ず両端の節点のラベルより大きなラベルをもつ節点が存在するように節点にラベルを振ることである。グラフ G の節点ランキングのうち、最大ラベルが最小となるものを最小節点ランキングという。与えられたグラフの全域木のうち、最小節点ランキングが最小となるものを求める問題を最小節点ランキング全域木問題 (MVRST: minimum vertex ranking spanning tree) という。この問題は、VLSI 設計、

[2] http://research.nii.ac.jp/ntcir/workshop/work-ja.html

データ配信におけるサーバの配置問題、センサネットワークにおけるデータ処理プロセッサの配置等への応用が考えられる。

まず、３次元マッチング問題が決定問題版のMVRST へ多項式時間帰着可能であることを示すことにより、MVRST が NP 困難であることを示した。また、グラフ G の、直径が最小となる全域木を求めるというアイデアに基づいた近似率 $\frac{\lfloor \frac{1}{2}(\ell+3) \rfloor}{\lceil \log_2(\ell+2) \rceil}$ の近似アルゴリズムを提案した。

一方、置換グラフに対し、長さ４以上の単純閉路を含まないなどの性質を用いることで、動的計画法に基づく $O(n^3)$ 時間のアルゴリズムを開発した。

3.2 外平面グラフ上で最小節点ランキング全域木問題を解く多項式時間アルゴリズム [学術論文 7]

前節で示したように最小節点ランキング全域木問題が一般には NP 困難であるが、グラフのクラスを外平面グラフに限定することで多項式時間のアルゴリズムをえた。本アルゴリズムは動的計画法に基づいている。

3.3 モバイルエージェント実行計画問題について [学術論文 1]

モバイルエージェント実行計画問題を定式化し、各エージェントの通信するエージェント数を２に制限した場合ですら強 NP 完全であることを証明した。また、NP 完全である範囲や、近似アルゴリズムについての検討を行なった。

マルチエージェントシステムは、特に人工知能の分野で精力的に研究されてきた。エージェントとはプロセスなどのような動作主体 (computational entity) のことである。モバイルエージェントとは、任意のホストに移動可能なエージェントのことで、分散環境におけるプロセスマイグレーションの概念とほぼ同じである。マルチエージェントシステムにおけるモバイルエージェントの移動性に関する研究は、通信コストの削減を目的としている。しかし、あるホストに膨大な数のエージェントが集中すればそのホストは過負荷となることより、CPU コストと通信コストの両方のバランスをとるようにホストにエージェントを配置することによって、効率的な実行を目指すことが必要になる。通常、CPU コストの最大値を最小にするように設計されたこの種の配置最適化は、マルチプロセッサ上でのタスクスケジューリングの形式で表される。よって、よって、モバイルエージェントタスクに対応させ、ホストをプロセッサに対応されることにより、モバイルエージェントの負荷分散を達成することを、マルチプロセッサにおけるタスクスケジューリングの拡張とみなすことができる。しかし、従来のタスクスケジューリング問題では、モバイルエージェントの相互通信と移動について考慮することはできない。そこで、新たにこのような問題をモバイルエージェント実行計画問題として定義して、その計算複雑度を解析する。

マルチプロセッサ上のタスクスケジューリングは３０年以上の間研究されている。従来の研究では、CPU コストのバランスをとることや、タスク間の関係（半順序関係など）が着目されてきた。また、従来の研究により、タスクが preemptive でなければ問題はマルチプロセッサスケジューリングとなり、強 NP 完全となることが知られている。なお、タスクが preemptive の場合は、多項式時間で最適なスケジュールを得ることができる。

その一方で、モバイルエージェントシステム上でのシステム全体の観点からの負荷分散の研究は全くされてこなかった。この理由はエージェントが自律的存在であるためだと推察される。エージェントの移動の最適化に関して従来からいくつかの研究がなされているが、それらはすべて個々のエージェント移動に焦点を当てて研究したもので、システム全体の性能に関する研究ではない。例えば、データのリモートアクセス、メッセージ交換、プロセスマイグレーションの性能比較、一連のタスクのためのエージェント移動スケジュールタスクとエージェントの旅程 (itinerary) を考慮したモバイルエージェントの選択などである。これらは、モバイルエージェントの相互通信を考えずに、エージェントとホストとの相互通信のみを考え、エージェントの移動スケジュールのみを最適化しようとしたものである。システム管理エージェントに関しては、そのような定式化は適切であり有用であるが、実際の多くのエージェントシステム（たとえば、情報交換や契約など）では、

エージェントの相互通信を必要とする。もちろん、エージェント間での通信に関する研究（たとえば、契約ネットなど）は多く行なわれているが、これらの研究は負荷分散に焦点を合せていない。

システム全体の性能向上を目指すのは、個々のエージェント利益を平均的に良く保つと予想できることより妥当である。そこで、システム全体の仕事の完了時間を最小にすることを目的とする、モバイルエージェントの相互通信に関する要素を定式化に取り込む。

モバイルエージェントは preemptive タスクとみなすことができる。よって、エージェント間に通信が全くないなら、多項式時間で最適な配置を得ることができる。しかし、エージェントが互いに通信するとき、これを得ることができるかどうかは分かっていない。本研究では、エージェントがお互いに通信する場合には、時間最適な配置を求めることは強 NP 完全であることを証明した。具体的には、CPU コストと実行途中のエージェントの移動の考慮を不要にし、さらに、各エージェントの通信相手が丁度二つのエージェントになるように制限した問題が強 NP 完全であることを証明した。通常、エージェントは限られた数 ($O(1)$) のエージェントとのみ通信するため、この制限は現実のモバイルエージェントシステムの環境を反映している。この成果は、エージェントがお互いに通信する必要があるほぼすべての実際の状況に対し、最適なエージェントの配置を与えるどのような効率的なアルゴリズムもないであろうということを示したことになる。

3.4 その他

その他、他グループのメンバーとの共同研究として以下の成果を得た。

1. 2 種類の資源集合を持つ 3 連結グラフを 2 分割する頑健なアルゴリズム [学術論文 8]
2. タンク繰りにおける経路探索法 [学術論文 9]
3. 最小数の枝付加による $(k-1)$ 節点連結多重グラフから 1 枝連結かつ k 節点連結多重グラフへの変換 [学術論文 10]
4. 森への枝付加により奇数長の直径 D を実現する 8 近似アルゴリズムの考案 [学術論文 11]

研究業績一覧

学術論文

1. Atsushi Sasaki, Tadashi Araragi, Shigeru Masuyama, Keizo Miyata:
“Formulation of Mobile Agents Allocation and its Strong NP-Completeness”, IEICE Trans. Inf. and Systems, Vol.E88-D, No.5, pp.1060-1063, 2005 年 5 月.
概要: We formally define the mobile agent allocation problems from a system-wide viewpoint and then prove that it is strongly NP-complete even if each agent communicates only with two agents. This is the first formal definition for acheduling mobile agents from the viewpoint of load balancing, which enables us to discuss its properties on a rigorous basis. The problem is recognized as preemptive scheduling with independent tasks that require mutual communication. The result implies that almost all subproblems of mobile agent allocation, which require mutual communication agents, are strongly NP-complete.

2. 吉田辰巳, 遠間　雄二, 増山 繁, 酒井 浩之:
“ 可読性の向上を目的とした片仮名表記外来語の換言知識獲得”, 電子情報通信学会論文誌 D-II, Vol.J88-D-II, No.7, pp.1060-1063, 2005 年 5 月.
概要: 本論文では, 外来語である片仮名語, 特に英語を語源とした片仮名語の和語または漢語への換言のための知識獲得に関する研究を行なった結果を報告した. 近年, 公的文書等における難解な片仮名語の乱用が問題視されている. 片仮名語の大部分は英単語に基づく外来語であり, 従来日本語で用いられてきた語彙に換言可能な場合も多い. 換言とは, ある言語表現の意味内容を保持したまま, 別の表現へと言い替えることである. 自然言語処理のための要素技術として, 今後ますます重要になると認識されている. 換言するための知識は人手で作成することもできるが, 実用的な質と量を満たすためには多大な労力を要

する．そのため, 換言知識は可能な限り自動的に獲得することが望ましい．以上より, 本研究では, 難解な片仮名語をより理解し易い語へと言い替えるための換言知識を自動的に獲得することを目的としている．手順としては, まず, 片仮名語の元になった英単語を復元する．そして, 得られた英単語の日本語訳を辞書によって獲得し, 候補を絞り込む．実験の結果, 英単語復元は再現率 82.2%, 精度 81.1%を得, 換言候補獲得については再現率 14.6%, 精度 70.8%となった．

3. 酒井 浩之, 増山 繁:
“略語とその原型語との対応関係のコーパスからの自動獲得手法の改良”, 自然言語処理, Vol.12, No.5, pp.207-231, 2005 年 10 月.
概要: 略語とその略語に対する元の語 (原型語と定義) との対応関係を，コーパスから自動的に獲得する手法を提案する．本手法は，同一の再現率においてより高い精度を達成できるように，我々の既提案手法を改良したものである．このような知識は，情報検索や文書要約などにおいて有用である．本手法は，まず，略語候補とそれに対応した原型語の候補を，それらを構成している文字情報から獲得する．そして，略語候補と原型語の候補の名詞間類似度を計算することで，略語とその原型語との対応関係を取得する．例えば，略語「原発」に対して，原型語「原子力発電所」のような対応関係を取得できる．なお、本手法はコーパスに出現する各名詞が略語か原型語であるかどうかの情報が与えられていることを前提としていない。評価の結果，名詞間類似度の閾値を 0.4 に設定した場合，精度 73.4% の結果を得た．本手法と既提案手法とを比較した結果，同一の再現率においてより高い精度を達成し，既提案手法よりも有効な手法であることを確認した．

4. 酒井 浩之, 梅村 祥之, 増山 繁:
“交通事故事例に含まれる事故原因表現の新聞記事からの抽出”, 自然言語処理, （掲載予定）.
概要: 新聞記事に含まれる交通事故事例の記事から事故原因を表す表現 (例えば,「ハンドル操作を誤った」) を自動的に抽出する手法を提案する．抽出結果に基づき交通事故事例の原因を分析することで，例えば交通事故防止装置の開発に役立てることができる．本手法では，まず，前処理として Support Vector Machines(SVM) を用いて新聞記事コーパスから交通事故事例の記事を抽出し，抽出された交通事故事例の記事から事故原因を表す表現を，新聞記事コーパスから得られる統計的な情報を使用して抽出する．具体的には，事故原因を表す表現がいくつか係る表現を種表現と定義して人手で 1 つ与え，種表現に係っている事故原因表現を自動的に取得する．そして，取得したいくつかの事故原因表現から自動的に種表現を取得し，さらに，取得した種表現から再び事故原因表現を取得する．このプロセスを繰り返すことで，事故原因表現，および，その種表現を取得していく．本手法を評価したところ，事故原因表現抽出の精度は 77.2% であり，再現率は 38.6% であった．また，事故原因表現，および，種表現を共に含んでいる文，もしくは，事故原因表現に「らしい」が追加された表現を含む文を原因文と定義し，その抽出精度，再現率を求めたところ，精度が 87.2%，再現率が 40.8% であった．

5. 酒井 浩之, 増山 繁:
“ユーザの要約要求を反映するためにユーザとのインタラクションを導入した複数文書要約システム”, 日本知能情報ファジィ学会誌, （掲載予定）.
概要: 本論文では，ユーザの要約要求を反映するためにユーザとのインタラクションを導入した複数文書要約手法を提案する．従来，文書自動要約とは，主として 1 つの文書から 1 つの要約を自動的に生成する技術であった．しかしながら，人間が知的な活動を行うためには 1 つの文書の要約を生成するよりも，ある事柄に関連した複数の文書から 1 つの要約を生成する技術 (すなわち，複数文書要約技術) の方がより重要である．なぜなら，人間の限られた情報処理能力では，検索結果などで得られた関連した多くの文書を読むのに多大な時間が必要であり，それらを 1 つの要約

にまとめることで読む時間の大幅な削減が可能になるからである．しかしながら，一般にユーザごとに興味のある情報が異なるため，ユーザによって必要な情報が異なる．そこで，本論文では，複数文書要約においてユーザが知りたい情報を “要約要求” と定義し，ユーザの要約要求を考慮しそれに適合した要約を生成できる複数文書要約手法を提案する．具体的には，要約対象となる，ある事柄に関連した複数文書からその事柄に関連のあるキーワードを抽出しユーザに提示する．ユーザは提示されたキーワードから要約要求に適したキーワードを選択する．その選択されたキーワードによって生成される要約が変化する．提案した要約手法の評価のために，国立情報学研究所主催の，検索と要約の評価のためのワークショップ NTCIR4 における要約タスク (TSC3) に参加した．その結果，複数文書要約タスクにおいて良好な成績を得ることができた．なお，TSC3 へは，本システムによってスコア付けされたキーワードのうち上位 12 個を必ず選択するように変更することで，ユーザとのインタラクションを行わない複数文書要約システムとして参加した．また，ユーザとのインタラクションによる複数文書要約への効果を評価し，提案手法の有効性を確認した．

6. Keizo Miyata, Shigeru Masuyama, Shin-ichi Nakayama, Liang Zhao:
“ NP-hardness proof and an approximation algorithm for the maximum vertex ranking spanning tree problem”, Discrete Applied Mathematics, （掲載予定）.
概要: The minimum vertex ranking spanning tree problem (MVRST) is to find spanning tree of G whose vertex ranking is minimum. In this paper, we show that MVRST is NP-hard. To prove this, we polynomially reduce the 3-dimensional matching problem to MVRST. Moreover, we present an approximation algorithm for MVRST.

7. Shin-ichi Nakayama, Shigeru Masuyama:
“ A Polynomial Time Algorithm for Obtaining a Minimum Vertex Ranking Spanning Tree in Outerplanar Graphs(invited paper)”, IEICE Trans. Inf. and Systems, （掲載予定）.
概要: The minimum vertex ranking spanning tree problem is to find a spanning tree of G where vertex ranking is minimum. This problem is NP-hard and no polynomial time algorithm for solving it is known for non-trivial classes of graphs other than interval graphs. This paper proposes a polynomial time algorithm for solving the minimum vertex ranking spanning tree problem on outerplanar graphs.

8. Hiroshi Nagamochi, Kengo Iwata, and Toshimasa Ishii:
“A robust algorithm for bisecting a triconnected graph with two resource sets”, Theoretical Computer Science A, vol. 341, 364-378, 2005 年 6 月.
概要: Given two disjoint subsets T_1 and T_2 of nodes in an undirected 3-connected graph $G = (V, E)$ with a node set V and an arc set E, where $|T_1|$ and $|T_2|$ are even numbers, it is known that V can be partitioned into two sets V_1 and V_2 such that the graphs induced by V_1 and V_2 are both connected and $|V_1 \cap T_j| = |V_2 \cap T_j| = |T_j|/2$ holds for each $j = 1, 2$. An $O(|V|^2 \log |V|)$ time and $O(|V|+|E|)$ space algorithm for finding such a bipartition has been proposed based on a geometric argument, where G is embedded in the plane $\Re^2$ and the node set is bipartitioned by a ham-sandwich cut on the embedding. A naive implementation of the algorithm, however, requires high precision real arithmetic to distinguish two close points in a large set of points on $\Re^2$. In this paper, we propose an $O(|V|^2)$ time and space algorithm to the problem. The new algorithm, which remains to be based on the geometric embedding, can construct a solution purely combinatorically in the sense that it does not require computing ac-

tual embedded points in $\Re^2$ and thereby no longer needs to store any real number for embedded points. Although the new algorithm seems to need more space complexity, it can be implemented only with $|V|$ linked lists such that each element stores an integer in $[1, |V|]$.

9. 石井利昌，永持仁，高橋健吾, 西垣豊, 武田真人:
“タンク繰りにおける経路探索法”, システム制御情報学会論文誌, vol.18, no.6, 213-221, 2005 年 6 月.
概要: 石油化学事業においては, 石油化学プラントを最適な生産計画に従って効率的に運用することが要求されている．最適な生産計画を立案するためには，原料を貯蔵タンクを介しプラントへ効率よく供給するための経路取りの計算が必要である．通常, 購入された原料は, まず，港から一時的に複数の貯蔵用タンクに受け入れられ, その後生産計画に従って, プラントへ供給される．この際，配管網上で，港-タンク間，タンク-タンク間，またはタンク-プラント間において，互いに途中の配管を共有しない複数本の経路を見つけることが求められる．本研究では, この配管網上での経路探索問題をグラフモデルにより表現し，グラフアルゴリズムに基づいた解法を提案する．我々の解法では，要求されうる全ての経路をあらかじめ木状のデータ構造に蓄えておき，経路生成時にこのデータ構造を参照することにより計算時間の短縮を図る．提案アルゴリズムの有効性については, 昭和電工 (株) における事例を基に, 計算機実験により検証した.

10. Toshimasa Ishii, Hiroshi Nagamochi, and Toshihide Ibaraki:
“Augmenting a (k-1)-vertex-connected multigraph to an l-edge-connected and k-vertex-connected multigraph”, Algorithmica, （掲載予定）.
概要: For two integers $k, \ell > 0$ and an undirected multigraph $G = (V, E)$, we consider the problem of augmenting G by the smallest number of new edges to obtain an ℓ-edge-connected and k-vertex-connected multigraph. In this paper, we show that a $(k-1)$-vertex-connected multigraph G can be made ℓ-edge-connected and k-vertex-connected by adding at most $\max\{\ell+1, 2k-4\}$surplus edges over the optimum in $O(\min\{k, \sqrt{n}\}kn^3 + n^4)$ time, where $n = |V|$.

11. Toshimasa Ishii, Shigeyuki Yamamoto and Hiroshi Nagamochi:
“Augmenting Forests to Meet Odd Diameter Requirements”, Discrete Optimization, （掲載予定）.
概要: Given a graph $G = (V, E)$ and an integer $D \geq 1$, we consider the problem of augmenting G by the smallest number of new edges so that the diameter becomes at most D. It is known that no constant approximation algorithms to this problem with an arbitrary graph G can be obtained unless $P = NP$. For a forest G and an odd $D \geq 3$, it was open whether the problem is approximable within a constant factor. In this paper, we give the first constant factor approximation algorithm to the problem with a forest G and an odd D; our algorithm delivers an 8-approximate solution in $O(|V|^3)$ time. We also show that a 4-approximate solution to the problem with a forest G and an odd D can be obtained in linear time if the augmented graph is additionally required to be biconnected.

研究会等

1. 佐々木淳，櫟粛之，増山繁:
“ 非同期分散分枝限定法の基本構造と可能性”, 第 18 回 回路とシステム軽井沢ワークショップ論文集, pp.259-264, 2005 年 4 月.
概要: 分散システムにおいて, 各変数がタスクに対応し, その値がそのタスクの割り当て先ホストを示すような負荷分散問題を解くための新しい非同期分散分子限定方を提案する.

これは, NP 困難な離散最適化問題に対して非同期完全分散システムで近似解でない厳密な最適解を求める最初の最適化分散アルゴリズムである. これは従来の分散最適化アルゴリズムに比べて高い柔軟性と頑健性をもつ. そのアイデアには, 分枝限定法, 分割統治法, および, 局所探索法における λ-Opt 近傍の考え方を複合させている. 本手法は, 今後の拡張により, 大規模動的分散システムにおいて有用になり得る.

2. Shin-ichi Nakayama, Shigeru Masuyama: "n $O(n^3)$ Time Algorithm for Obtaining the Minimum Vertex Ranking Spanning Tree on Permutation Graphs", Proc. of the 4th Japanese-Hungarian Symposium on Discrete Mathematics and its Applications, pp.250-256, 2005 年 6 月.
概要: The minimum vertex ranking spanning tree problem is to find a spanning tree of G whose vertex ranking is minimum. This paper proposes an $O(n^3)$ time algorithm for solving the minimum vertex ranking spanning tree problem on a permutation graph.

3. 酒井 浩之, 梅村祥之, 増山 繁:
" 新聞記事からの交通事故事例および事故原因表現の抽出", 情報処理学会研究報告, 2005-FI-80 2005-NL-169, pp.85-92. 2005, 2005 年 9 月.
概要: 新聞記事から交通事故事例の記事を抽出し, さらに, その中から事故原因を表す表現 (例えば,「ハンドル操作を誤った」) を自動的に抽出する手法を提案する. 本手法では, まず, Support Vector Machine(SVM) を用いて新聞記事コーパスから交通事故事例の記事を抽出する. そして, 抽出された交通事故事例の記事から事故原因を表す表現を抽出する. 具体的には, 事故原因を表す表現がいくつか係る表現を種表現と定義して人手で 1 つ与え, 種表現に係っている事故原因表現を自動的に取得する. つぎに, 取得したいくつかの事故原因表現から自動的に種表現を取得し, さらに, 取得した種表現から再び事故原因表現を取得する. このプロセスを繰り返すことで, 事故原因表現, および, その種表現を取得していく. 本手法を評価したところ, 交通事故事例抽出は精度 82.0%, 再現率 84.3% であった. また, 事故原因表現, および, 種表現を共に含んでいる文を原因文と定義し, その抽精度, 再現率を求めたところ, 精度が 77.7%, 再現率が 39.8% であった.

4. 松田耕史, 山本悠二, 酒井浩之, 増山繁:
"Weblog 内のリンクに対する感情推定の試み ー Web コミュニティ発見法改善の基礎としてー", 電子情報通信学会技術研究報告, NLC2005, pp.85-92, 2006 年 2 月.
概要: Web 上の情報量の増加と Weblog などの簡易な情報発信手段の普及によって、Web 上のリンクを単に「リンク先ページへの信頼」と解釈することはできなくなってきた。Web 上のリンクに込められた感情を知ることによって、より密に連携した Web コミュニティを発見することが可能になると考えられる。そこで本研究では、Weblog 内のリンクに対して、教師付き学習によって感情スコアを推定することを試みた。肯定的文書、否定的文書間の表現の偏りや、Weblog 特有の文書構造を考慮した結果、ピアソンの相関係数で 0.45 程度と、かなりの相関をもって推測可能であることがわかった。

5. 太田貴久, 増山繁:
"学生レポート採点支援のためのレポート類似部分発見手法", 電子情報通信学会技術研究報告, NLC2005, pp.37-42, 2006 年 2 月.
概要: 近年の情報技術の発達により, レポートの剽窃が非常に容易なものとなり問題となっている. 本研究では Smith-Waterman アルゴリズムを基礎とした, さまざまな「類似」を検出できるレポート類似部分発見法を考案した. そして, 現実に提出されたレポートを含めた文書集合に対して実験を行った結果, F 値 = 1 となり, 完全に剽窃レポートを検出することに成功した.

6. 尾田晃, 梅村恭司:
"文書頻度計数の線形時間アルゴリズムの実装と評価", 情報処理学会　バイオ情報学

研究会, 2005-BIO-3, 95-98, 2005/12/22.
概要: 統計的自然言語処理において，文字列を特徴付ける統計量として，文字列の出現頻度や文字列の現れる文書の総数などが用いられる。しかし，単純な方法では文書集合中のすべての任意文字列に対して，これらの統計量を計算するには $O(N^2)$ のメモリを必要とし，大規模なコーパスに対しては実際的でない。本稿では，Range Minimum Query のアルゴリズムを用いて $O(N)$ のメモリ空間と $O(N)$ の時間で，すべての任意文字列の重複条件付き文書頻度を求めるアルゴリズムを実装し，評価する

7. Toshimasa Ishii, Kengo Iwata and Hiroshi Nagamochi:
"Bisecting a four-connected graph with three resource sets", Proceedings of the 4th Japanese-Hungarian Symposium on Discrete Mathematics and Its Applications, 巻号, 107-113, 2005 年 6 月.
概要: Let $G = (V, E)$ be an undirected graph with a node set V and an arc set E. G has k pairwise disjoint subsets $T_1, T_2, \ldots, T_k$ of nodes, called resource sets, where $|T_i|$ is even for each i. The partition problem with k resource sets asks to find a partition V_1 and V_2 of the node set V such that the graphs induced by V_1 and V_2 are both connected and $|V_1 \cap T_i| = |V_2 \cap T_i| = |T_i|/2$ holds for each $i = 1, 2, \ldots, k$. The problem of testing whether such a bisection exists is known to be NP-hard even in the case of $k = 1$. On the other hand, it is known that if G is $(k+1)$-connected for $k = 1, 2$, then a bisection exists for any given resource sets, and it has been conjectured that for $k \geq 3$, a $(k+1)$-connected graph admits a bisection. In this paper, we show that for $k = 3$, the conjecture does not hold, while if G is 4-connected and has K_4 as its subgraph, then a bisection exists and it can be found in $O(|V|^3 \log |V|)$ time. Moreover, we show that for an arc-version of the problem, the $(k+1)$-edge-connectivity suffices for $k = 1, 2, 3$.

8. Toshimasa Ishii, Kengo Iwata and Hiroshi Nagamochi:
"Bisecting a four-connected graph with three resource sets", The The 16th Annual International Symposium on Algorithms and Computation (ISAAC 2005), 176-185, 2005 年 12 月.
概要: Let $G = (V, E)$ be an undirected graph with a node set V and an arc set E. G has k pairwise disjoint subsets $T_1, T_2, \ldots, T_k$ of nodes, called resource sets, where $|T_i|$ is even for each i. The partition problem with k resource sets asks to find a partition V_1 and V_2 of the node set V such that the graphs induced by V_1 and V_2 are both connected and $|V_1 \cap T_i| = |V_2 \cap T_i| = |T_i|/2$ holds for each $i = 1, 2, \ldots, k$. The problem of testing whether such a bisection exists is known to be NP-hard even in the case of $k = 1$. On the other hand, it is known that if G is $(k+1)$-connected for $k = 1, 2$, then a bisection exists for any given resource sets, and it has been conjectured that for $k \geq 3$, a $(k+1)$-connected graph admits a bisection. In this paper, we show that for $k = 3$, the conjecture does not hold, while if G is 4-connected and has K_4 as its subgraph, then a bisection exists and it can be found in $O(|V|^3 \log |V|)$ time. Moreover, we show that for an arc-version of the problem, the $(k+1)$-edge-connectivity suffices for $k = 1, 2, 3$.

学会大会等

1. Shigeru Masuyama:
"On the minimum vertex ranking spanning tree problem", IFORS2005, 2005 年 7 月.

2. 横田隼, 酒井浩之, 増山繁:
"質問応答システムのための Web 掲示板からの質問記事抽出", 言語処理学会第 12 回年次大会発表論文集, pp.332-335, 2006 年 3 月.

3. 宮本雅人, 酒井浩之, 増山繁:
“論文 LATEX 原稿からのプレゼンテーション資料自動生成”, 言語処理学会第 12 回年次大会発表論文集, pp.640-643, 2006 年 3 月.

4. 山本悠二, 増山繁, 増山繁:
“小説自動要約のための隣接文間の結束性判定手法”, 言語処理学会第 12 回年次大会発表論文集, pp.1083-1086, 2006 年 3 月.

5. 石井利昌，岩田健吾，永持仁:
“資源節点集合を持つグラフを均等分割する問題について”, 日本オペレーションズ・リサーチ学会アルゴリズム研究部会, 2005 年 11 月.

6. 石井利昌，岩田健吾，永持仁:
“3 つの資源節点集合を持つ 4 点連結グラフを均等分割する問題について”,「特定領域研究」新世代の計算限界 平成 17 年度 第 2 回全体会議, 2005 年 11 月.

C08: 高性能近似アルゴリズムの設計法に関する研究

平田　富夫 †　藤戸　敏弘 ‡　和田幸一 §　小野　孝男 †

† 名古屋大学 大学院 情報科学研究科
〒 464-8603 名古屋市千種区不老町
{hirata,ono}@is.nagoya-u.ac.jp

‡ 豊橋技術科学大学 情報工学系
〒 441-8580　豊橋市天伯町雲雀ヶ丘 1-1
fujito@ics.tut.ac.jp

§ 名古屋工業大学情報工学専攻
〒 466-8555 名古屋市御器所町
wada@nitec.ac.jp

1　はじめに

グラフ問題や組合せ問題のような離散構造をもつ問題のほとんどは NP 完全（最適化問題の場合は NP 困難）であり, 現在の計算機では計算時間が膨大になり手に負えない問題である．しかし, たとえ NP 困難であっても, 計算機を用いてなんとか解かなければならない離散最適化問題が情報処理の現場ではますます増えている．たとえば, OR の分野では, より大規模なネットワーク上での資源割当て問題やスケジューリング問題を解かなければならない．また, 人工知能の分野では推論処理のような高度な計算を要求する問題がつぎつぎと発生している．このような現実を踏まえ, たとえ求まる解が最適ではなくとも, それに十分近いことを保証できる近似アルゴリズムの設計論が今日の重要な研究テーマとなっている．本研究の目的は, グラフの彩色問題と集合被覆問題を中心とした代表的離散最適化問題に対する高性能近似アルゴリズムを開発するとともに, これまでに提案されている近似アルゴリズムを設計手法の立場から調査・分類し一般的設計法を構築することである．

本年度の研究成果は以下のようである．グラフ問題に関しては、ある制限された最小重み木状被覆問題に対し近似アルゴリズムを与えた。一般化された彩色問題に対し高性能な近似アルゴリズムを開発した。 グラフの辺縮約問題に関して近似困難性を示した。集合被覆問題に関しては、重みつき集合被覆問題および集合多重被覆問題に関して成果を得た。この他, 公開鍵暗号系において重要な演算であるスカラー倍計算の効率的なアルゴリズムを与えた．また, 画像処理で有用な距離変換を効率よく求めるハードウェアアルゴリズムのＶＬＳＩ設計を行った．以下では主な研究成果に関して詳細を述べる．

2　グラフ問題

2.1　最小重み木状被覆問題の近似

グラフの基本問題としてよく知られている**頂点被覆問題**では，頂点はそれに接続する辺を**被覆する**といい，グラフ $G = (V, E)$ の任意の辺が頂点集合 $C \subseteq V$ のある頂点により被覆されるとき，C は G の頂点被覆であるという．このとき最小頂点被覆問題とは，位数が最小な頂点被覆を求める問題である．より一般的には，各頂点に非負重み $c : V \to \mathbb{R}_+$ が割り当られたグラフ G が与えられ，頂点集合 U の重みを U 内の頂点の重みの総和 $\sum_{v \in U} c(v)$ とするとき，最小重みの頂点被覆を求める問題を**最小重み頂点被覆問題**という．

被覆という概念が，頂点と辺の接続関係に関するものであるのに対し，辺同士（もしくは頂点同士）の隣接関係には支配が用いられる．辺はそれに隣接する他の辺を**支配する**といい，辺集合 $F \subseteq E$ に属さない G の任意辺が F のある辺に支配されるとき，F を G の**辺支配集合**という．頂点被覆問題と同様に，各辺に非負重み $c : E \to \mathbb{R}_+$ が割り当られたグラフ G が与えられたとき，最小重みの辺支配集合を求める問題を**最小重み辺支配集合問題**という．

これらのグラフ問題が様々な応用分野で現れるとき，求める解が “連結性” をも有していること

が望まれる局面がある．つまり，単に頂点被覆であるだけでなく，連結部分グラフを誘導するような頂点集合を必要とする**連結頂点被覆問題**や，連結な辺支配集合をその解とする**連結辺支配集合問題**の解決が求められる．当然ながら，非負重みは連結頂点被覆問題では頂点に，そして連結辺支配集合問題では辺に割り当てられ，それぞれ最小重みの解を求めることをその目的とする．連結グラフ G における**木状被覆**とは，頂点集合が G の頂点被覆となるような木のことをいうが，連結辺支配集合問題が重み最小の木状被覆を求める問題に他ならないため，同問題は，**木状被覆問題** (*Tree Cover* 問題) とも呼ばれる．また，木には常に頂点数＝辺数＋1 の関係があるため，“重みなし” 木状被覆問題と “重みなし” 連結頂点被覆問題が等価であることも見てとれる．

これまでに挙げた問題はいずれも NP 困難であることが知られており，そのためこれまでにも様々な効率的近似手法が研究されてきた．連結頂点被覆の NP 困難性は，頂点被覆からの多項式時間還元により示されるが，それが近似保証を保存することも知られており, よって前者の（多項式時間）近似は後者のそれと同等以上に難しいといえる．更に前述の通り，重みなしの場合で連結頂点被覆と木状被覆とが等価であることから，木状被覆問題の近似も頂点被覆のそれと同等以上に困難である．これまで上記問題に対して得られている主な（多項式時間）近似保証は次の通りである．まず最も有名な頂点被覆問題に対しては，2 倍近似が早くから知られており，現在最良の結果は $2-(1-o(1))\frac{\ln\ln n}{\ln n}$ [23] である．辺支配集合問題に対しても，簡単なアルゴリズムにより 2 倍近似が可能であることが，重みなしの場合に以前から知られていたが，任意重みの場合も 2 倍近似できることが最近示されている [15]. 同様に，木状被覆問題（即ち連結辺支配集合問題）も重みなしの場合 2 倍近似できることが簡単なアルゴリズムで示すことができる [34]．一方，任意重みをもつ木状被覆問題に対しては，まず 3.55 倍近似が示され [2]，その後 $3+\epsilon$ まで改善され [29, 14]，これが現在のところ最良結果である．つまり，連結辺支配集合問題では（辺支配集合問題のときと違い），一様重みの場合ほど良い近似保証が任意重みの下ではまだ得られていない．更に悪いことには，現在最良の $(3+\epsilon)$ 倍近似アルゴリズム [29, 14] は，多項式時間とはいえとても実用的であるとはいえない．というのも，そこでは指数オーダーサイズの線形計画問題を厳密に解く必要があり，そのためには楕円体法に頼らざるを得ないからである．

本研究では，最小重み連結辺支配集合問題に対してより良い近似アルゴリズムの開発へ向けて，まずは 2 倍以上の開きのある重みが 2 種類だけ与えられる木状被覆問題を考えた．このように制限された最小重み辺支配集合問題に対し，主双対法に基づく近似アルゴリズムを設計し，最大フロー問題の解法と同じ計算量で，2 倍近似保証することが可能であることを示した．

2.2 一般化彩色問題の近似アルゴリズム

defective coloring に関して David Karger は次のような問題を提起した：n 頂点のグラフを $O(n^\epsilon)$ 色で彩色する頂点彩色アルゴリズムに基づき常に $(O((n/d)^\epsilon), d)$-defective coloring が可能であることを，一般的な議論によって示すことができるだろうか．ここで (k,d)**-defective coloring** とは，与えられたグラフの頂点集合を，誘導する部分グラフの最大次数がたかだか d であるような部分集合（これを d**-defected 独立集合**と呼ぶ）の k 個の直和に分解することである．0-defected 独立集合とは普通の独立集合のことであり，従って (k,d)-defective coloring は k-彩色を一般化した概念である．与えられたグラフに (k,d)-defective coloring が存在するかどうかを答える問題である (k,d)**-defective coloring 問題**は，任意の $k \geq 3$ と $d \geq 0$ に対し NP-完全であることが示されている．

本研究では，最大次数が Δ のグラフに対し $O(\Delta^\alpha)$ 色で彩色するアルゴリズムが存在するという仮定の元で defective coloring が常に可能であることを示す．特に，任意の $k \geq 3$ に対し，$O(n^\epsilon)$ 色で彩色する近似アルゴリズムを使って k-彩色可能なグラフに対する $(O((n/d)^\epsilon), d)$-defective coloring が可能であることを示す．これは，Karger の問題に対し部分的ではあるが肯定的に答える結果である．この結果を導くにあたり，我々は Lovász による **defective 彩色数**の上界に関する結果を一般化した．つまり，Lovász は最大次数 Δ のグ

ラフ（これは $\Delta+1$ 色で彩色可能である）が任意の定数 d に対し $(\lceil\Delta/d\rceil, d)$-defective 彩色可能であることを示したが，我々は最大次数 Δ のグラフを $O(\Delta^\alpha)$ 色で彩色することができれば任意の d に対して $(O((\Delta/d)^\alpha, d)$-defective 彩色可能であることを証明した．この成果に関しては付録で詳細に紹介する．

2.3 辺縮約問題の近似困難性

グラフのある性質 P に対し，その性質を満たさないグラフから，P を満たすグラフを構成することを考える．そのためには，頂点の削除，辺の削除，または辺の縮約が考えられる．最小個数の頂点，辺を削除して P を満たすグラフを構成する問題はそれぞれ（性質 P に関する）頂点削除問題，辺削除問題と呼ばれ，性質 P が non-trivial で hereditary である場合，どちらの近似困難比率も明らかになっている．

一方，縮約しなければならない辺の最小個数を求める問題を（性質 P に関する）辺縮約問題と呼ぶ．性質 P が縮約に対し hereditary であり，3-connected グラフによって決定される場合，この問題は NP 完全であることがわかっているが，その近似困難な比率に関しては今まで知られていなかった．

本研究では，MAX E3-SAT の問題例から，ギャップ保存リダクションにより連結点被覆問題の問題例を構成し，さらに辺縮約問題の問題例にリダクションを行うことにより，辺縮約問題の近似困難な比率を求める．

3 集合問題

3.1 集合被覆問題に対する近似アルゴリズム

実用上様々な応用をもつ**集合被覆問題（*SC*）**は，よく知られた組合せ最適化問題で，次のように定義される：n 個の要素から成る台集合 U，U の部分集合の族 $\mathcal{F}$，各部分集合 $S\in\mathcal{F}$ に割り当てられた非負コスト c_S とが与えられたとき，$\bigcup_{S\in\mathcal{F}'} S = U$ となるような最小コストの部分集合族 $\mathcal{F}'$ が求められる．SC において，どの部分集合もその位数が k 以下である場合，それを k **集合被覆問題（*k-SC*）**と呼ぶ．$k\geq 3$ であれば k-SC でも NP 困難であるだけでなく，APX 困難でもあることが知られている [33].

直感的に最も自然かつ単純な SC に対するヒューリスティックである貪欲法は，U の要素すべてが被覆されるまで，コスト的に最も効率の良い部分集合を選択する操作を繰り返す．ここで，各集合 S のある時点での “効率” とは，コスト c_S を，S 内で未被覆な要素数で割ったもので，S を用いて新たに被覆するのに 1 個当りに要するコストである．一様コストのもと，この手法の SC に対する近似保証が $H(n)=\sum_{i=1}^{n}(1/i)$ であり，k-SC に対しては $H(k)$ であることを最初に示したのは Johnson である [27]．Lovász は小数被覆を用いて同じ結果を導いているが [31]，線形計画の双対性を利用することで，任意重み k-SC に対しても同じ近似保証 $H(k)$ が成り立つことが，Chvátal により後に示された [6]．更に，対話証明による近似困難性の結果より，この SC に対する貪欲法の近似保証が望みうる限界にほぼ近いこともわかっている [13].

重みなし k-SC に対しては，貪欲法の改良版により近似保証 $H(k)-1/6$ が得られ [20]，更に様々な局所探索の手法を取り入れることで，$H(k)-11/42, H(k)-1/3$ [21, 22] へと改善され，現在最良の近似保証は $H(k)-1/2$ である [11]．k-SC に対応する充填問題は k 集合充填問題（k-SP）であるが，貪欲法の近似保証が k であるのに対し，重みなしの場合で $k/2+\epsilon$ [26]，重みありの場合でも $(k+1)/2$ [4] という，より良い近似保証が知られている．ところが，重みあり k-SC に対しては貪欲法による $H(k)$ が依然としてベストなままである．本研究では，異なる重みの間には 2 倍以上の開きがあるように制限された重みつき 3-SC に対し，貪欲法を改良することで近似保証 $H(k)-1/6$ が得られることを示した．アルゴリズムは，Goldschmidt らによる貪欲法の変形版 [20] を一般化したものである．が，彼らのものを含め，貪欲法より優れたアルゴリズム [21, 22, 11] がすべて組合せ論的に解析されているのに対し，我々は k-SC の線形計画緩和とその双対計画を用いた Chvátal のアプローチ [6] を踏襲している．特に，解析だけでなくアルゴリズム設計においても，Galai [17, 18] と

Edmonds [12] によるグラフの分割定理がキーとなっている.

3.2 集合多重被覆問題に対する近似アルゴリズム

前出の集合被覆問題の自然な一般化である**集合多重被覆問題（*MC*）**とは，SC を次のように拡張した問題である．台集合 U の各要素 u には入力時に**被覆要求**と呼ばれる非負整数 r_u が割り当てられ，各 u を（少なくとも）r_u 回被覆する解（部分集合族）が求められる．どの部分集合の位数も k 以下であるとき，同問題は k **集合多重被覆（*k*-*MC*）**と呼ばれる．通常の SC は，MC において $r_u \equiv 1$ $(\forall u \in U)$ と制限した場合に相当するが，これを任意の $r_u \geq 0$ に拡張すると，許される被覆の仕方によって，MC には二通りの問題設定が考えられる. つまり，どの部分集合も 1 度だけしか使えないもの（**制約付き** *MC*) と，何度使っても構わないもの（**制約なし** *MC*）とである．SC に対する貪欲法は，いずれの MC に対しても SC に対するのと同等の近似性能を発揮することが知られているが [10]，一方，それを凌駕する近似手法は k-MC に対しても知られていない. しかしながら，制約なし k-MC の場合，k-SC へ “非多項式的” に還元することができ，例えば Goldschmidt らの変形版貪欲法 [20] を適用し，$H(k)$ より良い近似保証を得ることもできる．これに対し，制約付き k-MC にはそのような還元が知られていず，k-SC に関する既知結果をどのように利用できるかは不明である.

本研究では，集合多重被覆問題の近似に関する上述の状況を背景に，制約付き k-MC に対し，貪欲法よりも優れた近似アルゴリズムの開発を目指した．その方法として，まず k-SC に対する Goldschmidt らの変形版貪欲法 [20] を，制約付き k-MC 用に一般化した．その中で，制約付き k-MC は最終的に制約付き 2-MC まで還元されるのであるが，この問題は次の 2 点から多項式時間可解であることがいえる：1) 制約付き 2-MC は**単純 b 辺被覆（*simple b-edge cover, SbEC*）**というグラフ問題と等価である，2)SbEC は $O(mn \log n)$ 時間で解ける [16]．双対フィット法による，k-MC に対する通常の貪欲法の解析は，Vazirani の教科書 [36] に詳しいが，我々も双対フィット法により変形版貪欲法を解析した．そのため，SbEC の線形計画による記述 [7, 35] と，その双対計画の最適解が有する構造特性を詳細に調べた．これらの特性を利用してある変数値を丸め，SbEC の双対最適解を k-MC の双対解へフィットさせることで，k-MC に対する変形版貪欲法の近似保証として $H(k) - 1/6$ が得られることを示した.

4 付録：k-彩色可能なグラフに対する近似 defective coloring

defective coloring に関して David Karger は次のような問題を提起した: n 頂点のグラフを $O(n^\epsilon)$ 色で彩色する頂点彩色アルゴリズムに基づき常に $(O((n/d)^\epsilon), d)$-defective coloring が可能であることを, 一般的な議論によって示すことができるだろうか. 以下では, 最大次数が Δ のグラフに対し $O(\Delta^\alpha)$ 色で彩色するアルゴリズムが存在するという仮定の元で defective coloring が常に可能であることを示す. 特に, 任意の $k \geq 3$ に対し, $O(n^\epsilon)$ 色で彩色する近似アルゴリズムを使って k-彩色可能なグラフに対する $(O((n/d)^\epsilon), d)$-defective coloring が可能であることを示す. これは, Karger の問題に対し部分的ではあるが肯定的に答える結果である. 以下で議論の詳細について述べる。

4.1 Introduction

グラフ $G = (V, E)$ に対する頂点彩色とは, 頂点に色を割当ててどの辺も両端点が同じ色にならないようにすることである. G の**彩色数** ($\chi(G)$ で表す) は頂点彩色が可能な最小の色数である. $\chi(G)$ の値を決定する問題は NP-困難であることが知られている [19]. 頂点彩色では各色クラスに属する頂点が独立集合になっていなければならないが, この条件を緩和した次の問題を考える: グラフ G と (彩色の欠陥/defect と呼ばれる) 定数 d が与えられたときに, 各色クラスに属する頂点によって誘導されるどの部分グラフの最大次数もたかだか d であるようにグラフの各頂点に色を割当てることはできるだろうか. このような彩色を defective

coloring と呼ぶ.

Definition 1.1 グラフ G の (k,d)-defective coloring とは, どの頂点 v についても同じ色であるような隣接頂点がたかだか d 個しかないように G の頂点に k 個の色を割当てることである. *defective* **彩色数** $\chi_d(G)$ とは, G の (k,d)-defective coloring が存在する最小の k の値である.

Definition 1.2 グラフ $G=(V,E)$ に (k,d)-defective coloring が存在するならば, G は (k,d) 色で defective coloring 可能であるという. このとき頂点集合 V を k 個の部分集合に分割することができ, そのそれぞれによって誘導される部分グラフはいずれも最大次数がたかだか d である. このような部分集合を d-defected 独立集合と呼ぶ.

defective coloring 問題は Andrews and Jacobson[1], Harary and Jones[25], Cowen, Cowen and Woodall[8] らによって独立に提案された. Cowen, Goddard and Jesurum[9] は任意の $k \geq 3$ と $d \geq 0$ に対し一般的なグラフの (k,d)-defective coloring 問題が NP-完全であることを示した. さらに, 彼らは任意の定数 defect d に対し P $\neq$ NP ならば defective 彩色数を n^ϵ 倍以内では近似できないような定数 $\epsilon > 0$ が存在することも証明した. 一方で彼らは, 3-彩色可能なグラフに対しては知られているほとんどの近似アルゴリズムが defective coloring に拡張できることも示している. 特に, Wigderson のアルゴリズム [37] を一般化して $(O((n/d)^{1/2}),d)$-defective coloring 可能な $O(\Delta|E|)$ 時間アルゴリズムを導いた. また, Karger, Motwani, Sudan のアルゴリズム [28] を拡張して 3-彩色可能なグラフに対する $(\tilde{O}((n/d)^{1/4}),d)$-defective coloring 可能な多項式時間アルゴリズムを示した. ここで $\tilde{O}$ は log の多項式倍を無視していることを表している. [9] の最後の節には未解決問題がいくつか挙げられている. そのうちの 1 つ, 次の問題が David Karger によって提起された: n 頂点のグラフを $O(n^\epsilon)$ 色で彩色する近似アルゴリズムに基づき, 常に $(O((n/d)^\epsilon),d)$-defective coloring が可能であることを, 一般的な議論によって証明することができるだろうか.

$O(n^\epsilon)$-彩色から直接 $(O((n/d)^\epsilon),d)$-defective coloring を求めるのは簡単ではないように思われる. Xie, Ono and Hirata は, 最大次数が Δ の任意の k-彩色可能なグラフに対し, $O(\Delta^{1-x/k})$-彩色を $O(n^{C_k})$-彩色に変換できることを示した [38]. ここで $k \geq 3$ と定数 $2 < x < 3$ に対し $C_k \leq 1-(x+0.928)/(k+1)$ である. この結果により, $O(\Delta^\alpha)$-彩色を元にして defective coloring においても同様の結果が得られるのではないかと考えられる. この考察に基づき, 本論文では次のような問題を考えることにより Karger の問題に対し部分的に答を与える: $O(\Delta^\alpha)$-彩色アルゴリズムが存在すると仮定する. このとき, $O(n^\epsilon)$-彩色及び $(O((n/d)^\epsilon),d)$-defective coloring は常に可能だろうか. 3-彩色可能なグラフに対しては, $O(\Delta^\alpha)$-彩色アルゴリズムの存在を仮定すると簡単に $O(n^{1-1/(\alpha+1)})$-彩色と $(O((n/d)^{1-1/(\alpha+1)}),d)$-defective coloring が得られる. 我々は $\alpha = 1-x/k$ に対しこの結果を任意の k-彩色可能なグラフに一般化し, $O(n^{C_k})$-彩色及び $(O((n/d)^{C_k}),d)$-defective coloring 可能であることを示す. ここで $k \geq 3$, $0 \leq x < 3$ に対し $C_k \leq 1-(x+0.928)/(k+1)$ である.

本論文は, 以下次のように構成される. まず II 節では $O(\Delta^\alpha)$-彩色から $(O((\Delta/d)^\alpha),d)$-defective coloring が得られることを示す. 次に III 節 IV 節で 3-彩色可能なグラフに対する結果を拡張し, さらに任意の k-彩色可能なグラフに一般化する. 最後に V 節でまとめを行う.

4.2 Relationship between Proper Coloring and Defective Coloring

Lovász[30] は一般的なグラフに対し defective 彩色数の上界を与えた:

Theorem 2.1 [30] 任意の k に対し, $|E|$ 本の辺を持ち最大次数が Δ であるどんなグラフも $(k,\lfloor\Delta/k\rfloor)$-defective coloring 可能である. さらに, この defective coloring は $O(\Delta|E|)$ 時間で求めることができる.

Proof: まず各頂点に k 色を任意に割当てる.

色 i が割当てられた頂点の集合を V_i で表す. 頂点集合 V は $V = V_1 \cup V_2 \cup \cdots \cup V_k$ と分割することができる. 頂点 v に対し, その隣接頂点で集合 V_i に属するものの個数を $d_v(V_i)$ で表す. ここで頂点 $u \in V_i$ は色 i を割当てられた隣接頂点が $\lfloor \Delta/k \rfloor$ 個より多い, つまり $d_u(V_i) \geq \lfloor \Delta/k \rfloor + 1$ を満たすと仮定する. G の頂点に対する任意の k-彩色において $d_u(V_j) \leq \lfloor \Delta/k \rfloor$ を満たす色クラス V_j が必ず存在する. そこで u の色を i から j に変える. この操作により端点が同じ色であるような辺は $d_u(V_i) - d_u(V_j) \geq (\lfloor \Delta/k \rfloor + 1) - \lfloor \Delta/k \rfloor = 1$ 本減少する. 従ってこのように頂点の色を変えていくことにより $(k, \lfloor \Delta/k \rfloor)$-defective coloring が得られ, そのときに必要な色の変更回数はたかだか $|E|$ 回である.

この Lovász の定理から次の定理を得ることができる. 後の節で示す結果はこの定理に基づいている:

Theorem 2.2 最大次数 Δ の任意のグラフを $O(\Delta^\alpha)$ 色で彩色可能であると仮定する. このとき, 任意の定数 $d \geq 1$ に対し $(O((\Delta/d)^\alpha), d)$-defective coloring 可能である.

Proof: $c = \lceil \Delta/d \rceil$ とおく. 与えられたグラフ $G = (V, E)$ に対し, Lovász のアルゴリズムにより (c, d)-defective coloring を求め, 頂点集合を割当てられた色によって $V = V_1 \cup V_2 \cup \cdots \cup V_c$ と分割する. V_i は色 i を割当てられた頂点の集合である.

この分割に基づき, 次のようにグラフ $G' = (V', E')$ を構築する: 頂点集合 V_i に対しグラフ G' の頂点 $v'_i \in V'$ を割当てる. 従って $V' = \{v'_1, \ldots, v'_c\}$ である. そして, 元のグラフ G において V_i と V_j の間に辺がある, つまり $u \in V_i$, $v \in V_j$ であるような辺 (u, v) が存在するときに v'_i と v'_j をつなぐ辺 $e'_{ij} \in E'$ を加える. この新しいグラフ=G' における最大次数を Δ' で表す. G' は $O((\Delta')^\alpha) \leq O((\lceil \Delta/d \rceil - 1)^\alpha) < O((\Delta/d)^\alpha)$ 色で彩色可能である. そこで, この彩色において v'_i に割当てられた色を, 全ての頂点 $v \in V_i$ に対し改めて割当てる.

G' において 2 頂点 v'_i, v'_j が隣接していればこれらに同じ色が割当てられることはない. 従って, V_i と V_j の間に辺が存在すれば V_i に属する頂点と V_j に属する頂点に同じ色が割当てられることもない. これは, 元のグラフ G の頂点に対し色を割当て直したあとでも defect d が変化しないことを意味し, よって G に対する $(O(\Delta/d)^\alpha), d)$-defective coloring が得られた.

4.3 Defective Coloring for 3-colorable Graphs

General Results

まず 3-彩色可能なグラフに対して考える.

Corollary 3.1 最大次数が Δ である任意の 3-彩色可能なグラフに対して $O(\Delta^\alpha)$ 色で彩色するアルゴリズムが存在すると仮定する. このとき $O(n^\epsilon)$ 彩色及び $(O((n/d)^\epsilon), d)$-defective coloring が可能である. ここで $\epsilon = 1 - 1/(\alpha + 1)$ である.

系 3.1 を使うことにより, [9] の次の結果が直ちに得られる: Wigderson のアルゴリズム $(\alpha = 1)$ は任意の 3-彩色可能なグラフを $O(n^{1/2})$ 色で彩色することができ, また $(O((n/d)^{1/2}), d)$-defective coloring を見付けることもできる. KMS アルゴリズム $(\alpha = 1/3)$ では, 3-彩色可能な任意のグラフを $(\tilde{O}((n/d)^{1/4}), d)$-defective coloring 可能である.

Extentions of Blum and Karger's Results

1997 年に, Blum and Karger[5] は 3-彩色可能なグラフを $\tilde{O}(n^{3/14})$ 色で彩色する多項式時間アルゴリズムを提案した. これは現在でも最良の結果である. 証明の概要を後に記すが, 最後の部分を変更するだけで $(\tilde{O}((n/d)^{3/14}), d)$-defective coloring に拡張することができる. 本論文では他の部分で用いられている記号との混同を避けるため, [5] とは異なる記号を用いることにする. すなわち [5] において α, δ, n^ρ で表されている値を, 本論文ではそれぞれ β, ϑ, δ と表記する.

Definition 3.2 [5] 頂点 v に対しその次数を $d(v)$, 隣接頂点の集合を $N(v)$ で表す. 頂点集合 S, $T \subseteq V$ に対し $d_T(v) = |N(v) \cap T|$, $D_T(S) = \sum_{v \in S} d_T(v)$ と定義する. さらに, 頂点集合 S に属する頂点の次数の和を $D(S) = D_V(S)$ で表す. 今 G は 3-彩色可能であり, G の 3-彩色によって頂点集合 V を 3 個の独立集合 V_1, V_2, V_3 に分割することができる. これらの独立集合のうち $D(V_i) \geq D(V)/3$, つまり $D(V_i) \geq D(V - V_i)/2$ と満たす V_i を特に R で表す.

Definition 3.3 [5] $\vartheta = \vartheta(n) = 1/(5 \log n)$ とし, $j = 0, 1, \ldots$ に対し $I_j = \{v \in V | (1+\vartheta)^i \leq d(v) < (1+\vartheta)^{i+1}\}$ と定義する. つまり, 次数が 1 以上の頂点をビン I_j につめ, どのビンにおいても次数がたかだか $1+\vartheta$ 倍以内であるようにする. ここで頂点集合 S に対しその隣接頂点の集合を $N(S) = \bigcup_{v \in S} N(v)$ で, また $i = 0, 1, \ldots$ に対し $N_i(S) = \{v \in N(S) | (1+\vartheta)^i \leq d_s(v) < (1+\vartheta)^{i+1}\}$ で定義する. $N_i(S)$ は $N(S)$ の部分集合であり, その頂点は S に属する $(1+\vartheta)^i$ 個以上 $(1+\vartheta)^{i+1}$ 個未満の頂点と隣接する.

Lemma 3.4 [5] 3-彩色可能な n 頂点のグラフ $G = (V, E)$ において, 以下のいずれかの条件を満たす頂点 (集合) を見付けることができれば G の $O(n^\beta)$ 彩色が可能である:

1. 大きさ $\Omega(n^{1-\beta})$ の独立集合
2. いかなる G の 3-彩色においても同じ色であるような 2 個の頂点
3. 隣接頂点が $O(|S|n^\beta)$ 個であるような独立集合 S
4. $|N(u) \cap N(v)| = \Omega(n^{1-2\beta})$ であるような 2 頂点 u, v

Theorem 3.5[5] 3-彩色可能な n 頂点の任意のグラフ $G = (V, E)$ において $v \in R$ と $j \in \{0, 1, \ldots, \log_{1+\vartheta} n\}$ をうまく選ぶことにより集合 $S = N(v) \cap I_j$ が以下の条件を満たすようにできる:

$$
\begin{aligned}
|S| &\geq \frac{\vartheta^2 D(R)}{|R| \log_{1+\vartheta} n}, \\
D_R(S) &\geq \frac{1}{2}(1 - 3\vartheta) D(S).
\end{aligned}
$$

Theorem 3.6[5] 3-彩色可能な n 頂点グラフ $G = (V, E)$ と $\lambda \in [0, 1]$ が与えられたとする. このとき, $D_R(S) \geq \lambda D(S)$ であるような任意の集合 S に対し $T = N_i(S)$ が以下の条件を満たす $i < \log_{1+\vartheta} n$ が存在する:

$$
\begin{aligned}
D_T(S) &\geq \frac{\vartheta D_R(S)}{\log_{1+\vartheta} S}, \\
\frac{|T \cap R|}{|T|} &\geq (1 - 2\vartheta)\lambda.
\end{aligned}
$$

Theorem 3.7 [5] 3-彩色可能な n 頂点グラフ $G = (V, E)$ において以下の条件を満たす頂点集合 S, T が与えられたとする:

1. S を 2 色で彩色するような G の 3-彩色が存在し,
2. $D_T(S) = \Omega(|S| n^{1-2\beta} \log^2 n)$, かつ
3. $[D_T(S)]^3 = \Omega\left(\left[|S| + \max_{v \in S} d_T(v)\right] \times \left[|S||T^2 n^{1-2\beta} \log n + |T||S|^2 n\right.\right.$

このとき, G の $O(n^\beta)$-彩色が可能である.
G を 3-彩色可能なグラフとし, G から次数がたかだか δ である頂点を逐次削除することにより最終的に得られるグラフを G' とする (頂点を削除するごとに次数は変化する). 定理 3.5, 3.6 から G' のある頂点 v と適当な値 $i, j \in \{0, \ldots, \log_{1+\vartheta} n\}$ に対し, 集合 $S = N(v) \cap I_j$, $T = N_i(S)$ は次の性質を満たす:

$$
\begin{aligned}
\frac{|T \cap R|}{|T|} &\geq \frac{1}{2}(1 - 2\vartheta)(1 - 3\vartheta) \geq \frac{1}{2}\left(1 - \frac{1}{\log n}\right), \\
D_T(S) &= \Omega\left(\frac{\vartheta D(S)}{\log_{1+\vartheta} n}\right) = \Omega\left(\frac{\vartheta \delta |S|}{\log_{1+\vartheta} n}\right) \quad (2.23)
\end{aligned}
$$

$|T| = \Omega(n^{1-\beta})$ と仮定する. このとき T は大きさが少なくとも $(1/2)|T|(1 - 1/\log n)$ の独立集合を含んでいるので, Bar-Yehuda and Even[3] と Monien and Speckenmeyer[32] によって独立

に開発された頂点被覆アルゴリズムによって, T に含まれる大きさ $|T|/\log|T|$ の独立集合を見付けることができる. 従って補題 3.4(1) から G の $\tilde{O}(n^{\beta})$-彩色を見付けることができる.

一方 $|T| = o(n^{1-\beta})$ と仮定すると定理 3.7 を用いてやはり G の $\tilde{O}(n^{\beta})$-彩色を見付けることができる. 元々の証明では

$$n^{4\rho} = \tilde{\Omega}(n^{3-4\beta} + n^{\rho+3-5\beta})$$

であることを用いて定理 3.7(3) から [5] の最後を式を導いている.

本論文では n^{ρ} を δ と表記しているため, この式は

$$\delta^4 = \tilde{\Omega}(n^{3-4\beta} + \delta n^{3-5\beta})$$

と書くことができる.

$\delta^4 = \delta n^{3-5\beta}$ ならば $n^{\beta} = (n/\delta)^{3/5}$ である. 従って, $\delta \geq n^{3/8}$ ならば $n^{3-4\beta} = n^{3/5}\delta^{12/5} \leq \delta^4$ となる. 同時に, 式 $n^{1-2\beta} = \delta(\delta/n)^{1/5} \leq \delta$ から定理 3.7(2) が成り立つ. なぜなら, 定理 3.7(2) は (1) より弱いからである. また, S がある頂点の隣接頂点集合の部分集合であることから定理 3.7(1) も成り立つ. ここでは詳細を省くが定理 3.7(3) から式 (2) を導くことができ, 従って S と T が G' に関して定理 3.7 の全ての条件を満たすことがわかる. つまり G に対しても定理 3.7 の全ての条件を満たす. 証明は [5] に述べられている.

G の平均次数がたかだか 2δ であるときには, 次数が 2δ より小さい頂点が少なくとも $n/2$ 個存在する. これらの頂点によって誘導される部分グラフの最大次数は明らかに 2δ であり, 定理 2.2 から KMS アルゴリズム [28] を使うことによりこの部分グラフを $(\tilde{O}((\delta/d)^{1/3}), d)$-defective coloring することができる. よって大きさ $\tilde{\Omega}(n(d/\delta)^{1/3})$ の d-defected 独立集合が得られる. この d-defected 独立集合の全ての頂点に同じ色を割当て, 残りのグラフに対して新たな色で同じ操作を繰り返す. これで G を $(\tilde{O}((\delta/d)^{1/3}), d)$-defective coloring することができる. 等式 $(n/\delta)^{3/5} = (\delta/d)^{1/3}$ が成り立つときには 3-彩色可能なグラフを $(\tilde{O}((n/d)^{3/14}), d)$-defective coloring するという目的が達成できる. [5] の $\tilde{O}(n^{2/9})$-彩色に基づく別の結果からはより簡単に $(\tilde{O}((n/d)^{2/9}), d)$-defective coloring が得られるがここでは省略する.

4.4 General Results for k-colrable Graphs

The $O(n^{\frac{x+0.928}{k+1}})$-proper Coloring

この節では 3-彩色可能なグラフに対する結果を $k > 3$ に拡張する. 既に触れたように, Xie, Ono and Hirata[38] はある仮定のもとで $O(\Delta^{\alpha})$-彩色から $O(n^{\varepsilon})$-彩色が得られることを示した. [38] では $2 < x < 3$ に対してこの結果を示したが, 簡単にわかるように $0 \leq x < 3$ というより一般的な条件に拡張することができる. そこで拡張した結果を次に示す.

Corollary 4.1 [38] 最大次数 Δ の k-彩色可能なグラフを $O(\Delta^{1-x/k})$ 色で彩色するアルゴリズム A が存在すると仮定する. ここで $k \geq 3$ かつ $0 \leq x < 3$ とする. このとき n 頂点の k-彩色可能なグラフを $O(n^{C_k})$ 色で彩色するアルゴリズム B を構成することができる. ここで $C_k \leq 1 - (x + 0.928)/(k + 1)$ である.

Generalization for Defective Coloring

任意の k-彩色可能なグラフにおいて, どの頂点 v についてもその隣接頂点 $N(v)$ で誘導される部分グラフ $G_{N(v)}$ は $(k-1)$-彩色可能である. この事実を用いるため, $\alpha = 1 - x/k$ として定理 2.2 を書き直す. 新たな式を用いると, 次の系 4.2 が証明できる.

Theorem 2.2' 最大次数が Δ の k-彩色可能なグラフに対して $O(\Delta^{1-x/k})$ 色で彩色できると仮定する. このとき, 任意の定数 $d \geq 1$ に対し $(O((\Delta/d)^{1-x/k}), d)$-defective coloring 可能である.

Corollary 4.2 最大次数が Δ の k-彩色可能なグラフを $O(\Delta^{1-x/k})$ 色で彩色するアルゴリズム A が存在すると仮定する. ここで $k \geq 3$ かつ $0 \leq x < 3$ である. このとき, n 頂点の k-彩色可能なグ

ラフを $O(n^{C_k})$ 色で彩色し, また $(O((n/d)^{C_k}), d)$-defective coloring を見付けるアルゴリズム B が存在する. ここで $C_k \leq 1 - (x + 0.928)/(k + 1)$ である.

いくつかの近似アルゴリズムに対しては, 直接 defective coloring を見付けるように修正できることに注意する. 例えば Wigderson のアルゴリズム ($x = 0$) から直ちに $(O((n/d)^{1-1/(k-1)}), d)$-defective coloring が, また KMS アルゴリズム ($x = 2$) に対しても $(O((n/d)^{1-3/(k+1)}), d)$-defective coloring が得られる.

4.5 Concluding remarks

本研究では, 最大次数 Δ のグラフを $O(\Delta^{\alpha})$ 色で彩色するアルゴリズムが存在すると仮定して Karger の問に対する回答を与えた. 特に, $k \geq 3$ のときには任意の k-彩色可能なグラフに対する $O(\Delta^{1-x/k})$ 彩色アルゴリズム ($0 \leq x < 3$) から $O(n^{C_k})$ 彩色アルゴリズムと $(O((n/d)^{C_k}), d)$-defective coloring アルゴリズムが得られることを示した. ここで $C_k \leq 1 - (x + 0.928)/(k + 1)$ である. 例えば Wigderson のアルゴリズムでは $x = 0$ であり, $O(n^{1-1/(k-1)})$ 色で彩色可能であるが, このアルゴリズムを拡張することで $(O((n/d)^{1-1/(k-1)}), d)$-defective coloring を見付けることができる. また, KMS アルゴリズムでは $x = 2$ であり, $\tilde{O}(n^{1-3/(k+1)})$ 色での彩色から $(\tilde{O}((n/d)^{1-3/(k+1)}), d)$-defective coloring を得ることができる.

3-彩色可能なグラフに対しては, Blum and Karger の $\tilde{O}(n^{3/14})$ 彩色アルゴリズムから $(\tilde{O}((n/d)^{3/14}), d)$-defective coloring が得られることも示した. これに関連して, k-彩色可能なグラフに対する Halperin *et al.* の結果 [24] が defective coloring に対しても適用できるかどうかが興味の持たれるところである.

参考文献

[1] J. Andrews and M. Jacobson. On a generalization of chromatic number. *Congressus Number*, (47):33–48, 1985.

[2] E.M. Arkin, M.M. Halldórsson and R. Hassin, "Approximating the tree and tour covers of a graph," *Inform. Process. Lett.*, Vol. 47, pp. 275–282, 1993.

[3] R. Bar-Yehuda and S. Even. A local-ratio theorem for approximating the weighted vertex cover problem. *Annals of Discrete Mathematics*, (25):27–46, 1985.

[4] P. Berman, "A $d/2$ approximation for maximum weight independent set in d-claw free graphs," *Nordic J. Comput.*, Vol. 7, No. 3, pp. 178–184, 2000.

[5] A. Blum and D. Karger. An $\tilde{O}(n^{3/14})$-coloring algorithm for 3-colorable graphs. *Information Processing Letters*, 61:49–53, 1997.

[6] V. Chvátal, "A greedy heuristic for the set-covering problem," *Math. Oper. Res.*, Vol. 4, No. 3, pp. 233–235, 1979.

[7] W. Cook, W.R. Pulleyblank, "Linear systems for constrained matching problems," *Math. Oper. Res.*, Vol. 12, pp. 97–120, 1987.

[8] L. Cowen, R. Cowen, and D. Woodall. Defective colorings of graphs in surfaces: partitions into subgraphs of bounded valence. *Journal of Graph Theory*, (10):187–195, 1986.

[9] L. J. Cowen, W. Goddard, and C. E. Jesurum. Coloring with defect. *Proc. 8th Ann. ACM-SIAM Symp. on Discrete Algorithms*, pages 548–557, 1997.

[10] G. Dobson, "Worst-case analysis of greedy heuristics for integer programming with nonnegative data," *Math. Oper. Res.*, Vol. 7, No. 4, pp. 515–531, 1982.

[11] R. Duh, M. Fürer, "Approximation of k-set cover by semi-local optimization," in *Proc.*

29th Annual ACM Symp. Theory of Computing, pp. 256–264, 1997.

[12] J. Edmonds, "Paths, trees and flowers," *Canad. J. Math.*, Vol. 17, pp. 449–467, 1965.

[13] U. Feige, "A threshold of $\ln n$ for approximating set cover," *J. ACM*, Vol. 45, No. 4, pp. 634–652, 1998.

[14] T. Fujito, "On approximability of the independent/connected edge dominating set problems," *Inform. Process. Lett.*, Vol. 79, No. 6, pp. 261–266, 2001.

[15] T. Fujito, H. Nagamochi, "A 2-approximation algorithm for the minimum weight edge dominating set problem," *Discrete Appl. Math.*, Vol. 118, pp. 199–207, 2002.

[16] H.N. Gabow, "An efficient reduction technique for degree-constrained subgraph and bidirected network flow problems," in *Proc. 15th ACM Symp. Theory of Computing*, pp. 448–456, 1983.

[17] T. Gallai, "Kritische Graphen II," *Magyar Tud. Akad. Mat. Kutató Int. Közl.*, Vol. 8, pp. 373–395, 1963.

[18] T. Gallai, "Maximale Systeme unabhängiger Kanten," *Magyar Tud. Akad. Mat. Kutató Int. Közl.*, Vol. 9, pp. 401–413, 1964.

[19] M.R. Garey and D.S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness.* Freeman and Company, 1979.

[20] O. Goldschmidt, D.S. Hochbaum, G. Yu, "A modified greedy heuristic for the Set Covering problem with improved worst case bound," *Inform. Process. Lett.*, Vol. 48, pp. 305–310, 1993.

[21] M.M. Halldórsson, "Approximating discrete collections via local improvements," in *Proc. 6th Annual ACM-SIAM Symp. Discrete Algorithms*, pp. 160–169, 1995.

[22] M.M. Halldórsson, "Approximating k-set cover and complementary graph coloring," in *Proc. IPCO V*, pp. 118–131, 1996.

[23] E. Halperin, "Improved approximation algorithms for the vertex cover problem in graphs and hypergraphs," *SIAM J. Comput.*, Vol. 31, No. 5, pp. 1608-1623, 2002.

[24] E. Halperin, R. Nathaniel, and U. Zwick. Coloring k-colorable graphs using small palettes. *Proceedings of the Twelfth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 319–326, 2001.

[25] F. Harary and K. Jones. Conditional colorability II: Bipartite variations. *Congressus Number*, (50):105–218, 1985.

[26] C.A.J. Hurkens, A. Schrijver, "On the size of systems of sets every t of which have an SDR, with an application to the worst-case ratio of heuristics for packing problems," *SIAM J. Discrete Math.*, Vol. 2, No. 1, pp. 68–72, 1989.

[27] D.S. Johnson, "Approximation algorithms for combinatorial problems," *J. Comput. System Sci.*, Vol. 9, pp. 256–278, 1974.

[28] D. Karger, R. Motwani, and M. Sudan. Approximate graph coloring by semidefinite programming. *Journal of the ACM*, 45:246–265, 1998.

[29] J. Könemann, G. Konjevod, O. Parekh, A. Sinha, "Improved approximations for tour and tree covers," *Algorithmica*, Vol. 38, No. 3, pp. 441–449, 2003.

[30] L. Lovász. On decompositions of graphs. *Studia Sci. Math. Hungar.*, 1:237–238, 1966.

[31] L. Lovász, “On the ratio of optimal integral and fractional covers,” *Discrete Math.*, Vol. 13, pp. 383–390, 1975.

[32] B. Monien and E. Spechenmeyer. Ramsey numbers and an approximation algorithm for the vertex cover problem. *Acta Informatica*, (22):125–123, 1985.

[33] C. Papadimitriou, M. Yannakakis, “Optimization, approximation and complexity classes,” *J. Comput. System Sci.*, Vol. 43, pp. 425–440, 1991.

[34] C. Savage, “Depth-first search and the vertex cover problem,” *Inform. Process. Lett.*, Vol. 14, No. 5, pp. 233–235, 1982.

[35] A. Schrijver, *Combinatorial Optimization (vol.A)*, Springer, Berlin, 2003.

[36] V. Vazirani, *Approximation Algorithms*, Springer, Berlin, 2001.

[37] A. Wigderson. Improving the performance guarantee for approximate graph coloring. *Information Processing Letters*, 30:729–735, 1983.

[38] X. Xie, T. Ono, and T. Hirata. On approximation algorithms for coloring k-colorable graphs. *IEICE Trans.*, E86-A(5):1046–1051, 2003.

研究業績一覧

学術論文

1. A. Kako,T. Ono, T. Hirata, M. Halldorsson:
   “Approximation Algorithms for the Weighted Independent Set Problem”, Lecture Notes in Computer Science, 3787, 341–350, 2005.
   概要: In the unweighted case, approximation ratio for the independent set problem has been analyzed in terms ofthe graph parameters such as the number of vertices, maximum degree, and average degree. In the weighted case, no corresponding results are possible for average degree, since inserting the vertices with small weight decreases the average degree arbitrarily without significantly changing the approximation ratio. In this paper, we introduce weighted measures, namely “weighted” average degree and “weighted” inductiveness, and analyze algorithms for the weighted independent set problem in terms of these parameters.

2. 勝谷裕樹, 小野孝男, 平田富夫:
   “グラフ論的手法を用いた {2,3}-EC-SNDP に対する近似アルゴリズム”, 電子情報通信学会論文誌, J86-D-I, 11, 1679–1686, 2005.
   概要: ネットワーク設計問題のひとつに Survival Network Design Problem(SNDP) と呼ばれる問題がある．本研究では, {2,3}-EC-SNDP に対し, 深さ優先探索と極大全域森を組み合わせたアルゴリズムを提案し, その近似比率が $\frac{7}{3}$ となることを示す．また, このアルゴリズムを改良し近似比率が 2 となることを示す.

3. D. Adachi, T. Hirata:
   “Refined Computation for Points of the form 2^kP Based on Montgomery Trick”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E89-A, 1, 334–339, 2006.
   概要: This paper focuses on algorithms for an efficient scalar multiplication. We propose two algorithms for computing points of the form 2^kP in affine coordinates. One works for $k = 2$, and the other works for arbitrary natural number k. The efficiency of these algorithms is based on a trade-off between a field inversion and several field multiplications. We apply Montgomery trick to implement this trade-off. Since a field inversion is usually more expensive than 10 field multiplications, our algorithms are efficient

in comparison with existing ones.

4. T. Fujito, H. Kurahashi:
"A Better-than-Greedy Algorithm for k-Set Multicover", Lecture Notes in Computer Science, 3879, 176–189, 2006.
概要: The set multicover (MC) problem is a natural extension of the set cover problem such that each element requires to be covered a prescribed number of times (instead of just once as in set cover). The k-set multicover (k-MC) problem is a variant in which every subset is of size at most k. Due to the multiple coverage requirement, two versions of MC have been studied; the one in which each subset can be chosen only once (*constrained MC*) and the other in which each subset can be chosen any number of times (*unconstrained MC*). For both versions the best approximation algorithm known so far is the classical greedy heuristic, whose performance ratio is $H(k)$, where $H(k) = \sum_{i=1}^{k}(1/i)$. It is no hard, however, to come up with a natural modification of the greedy algorithm such that the resulting performance is never worse, but could also be strictly better. This paper will verify that this is indeed the case by showing that such a modification leads to an improved performance ratio of $H(k) - 1/6$ for both versions of k-MC.

5. T. Fujito, T. Okumura:
"A Modified Greedy Algorithm for Dispersively Weighted 3-Set Cover", Discrete Applied Mathematics, （印刷中）.
概要: The set cover problem is that of computing a minimum weight subfamily $\mathcal{F}'$, given a family $\mathcal{F}$ of weighted subsets of a base set U, such that every element of U is covered by some subset in $\mathcal{F}'$. The k-set cover problem is a variant in which every subset is of size at most k. It has been long known that the problem can be approximated within a factor of $H(k) = \sum_{i=1}^{k}(1/i)$ by the greedy heuristic, but no better bound has been shown except for the case of unweighted subsets. In this paper we consider approximation of a restricted version of the weighted 3-set cover problem, as a first step towards better approximation of general k-set cover problem, where any two distinct subset costs differ by a multiplicative factor of at least 2. It will be shown, via LP duality, that an improved approximation bound of $H(3) - 1/6$ can be attained, when the greedy heuristic is suitably modified for this case. A key to our algorithm design and analysis is the Gallai-Edmonds structure theorem for maximum matchings
.

6. T. Doi, T. Fujito:
"A Primal-Dual Method for Approximating Tree Cover with Two Weights", Discrete Applied Mathematics, （掲載予定）.
概要: The *tree cover (TC)* problem is to compute a minimum weight connected edge set, given a connected and edge-weighted graph G, such that its vertex set forms a vertex cover for G. Unlike related problems of vertex cover or edge dominating set, weighted TC is not yet known to be approximable in polynomial time as good as the unweighted version is. Moreover, the best approximation algorithm known so far for weighted TC is far from practical in its efficiency. In this paper we consider a restricted version of weighted TC, as a first step towards better approximation of general TC, where only two edge weights differing by at least a factor of 2 are available. It will be shown that a factor 2 approximation can be attained efficiently (in the complexity of max flow) in this case by a primal-dual method. Even under the limited weights as such, the primal-dual arguments used will be seen quite involved, having a nontrivial style of dual assignments as an essential part in it, unlike the case of

uniform weights.

7. 山中，伊藤，片山，犬塚，和田:
“軸の方向に関する共有知識を持たない自律分散ロボット群に対する形状形成アルゴリズム”, 電子情報通信学会論文誌, J88-D-I、4, 739–750, 2005.
概要: 自律分散ロボット群とは，各ロボットが自律的，協調的に動作することにより，全体として一つの問題を解決するロボット群である．これまでに自律分散ロボットを理論的なモデルで抽象化し，一点集合問題，形状形成問題など様々な問題に適用する研究が行なわれている．本論文で扱う形状形成問題とは，任意の位置に配置されたロボット群が特定の形状を形成する問題である．形状を形成するとは，入力形状を平行移動して，回転，拡大縮小，反転させたものとロボットの配置が一致することをいう．形状形成問題に関する研究してしては，ロボットに与える共通知識の量による，任意の形状に対する形成可能性について議論されている．本研究では，以前の動作で得られた情報を記憶できないロボットを対象にし，ロボット間で共有する座標系に関する知識が従来よりも少ない場合において任意の形状を形成することができるアルゴリズムを提案し，その正当性を証明する．

8. H. Zheng, S. Omura, J. Uchida, K. Wada:
“An optimal certificate dispersal algorithm for mobile ad hoc networks”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E88-A、4, 1627–1273, 2005.
概要: In this paper, we focus on the problem that in an ad hoc network, how to send a message securely between two users using the certificate dispersal system. In this system, special data called certificate is issued between two users and these issued certificates are stored among the network. Our final purpose on this certificate dispersal problem is to construct certificate graphs with lower dispersability cost which indicates the average number of certificates stored in each node in an ad hoc network. As our first step, when a certificate graph is given, we construct two efficient certificate dispersal algorithms for strongly connected graphs and directed graphs in this paper. We can show that for a strongly connected graph $G = (V, E)$ and a directed graph $H = (V', E')$, new upper bounds on dispersability cost on the average number of certificates stored in one node are $O(D_G + |E|/|V|)$ and $O(p_G d_{max} + |E'|/|V'|)$ respectively, where D_G is the diameter of G, d_{max} is the maximum diameter of strongly connected components of H and p_G is the number of strongly connected components of H. Furthermore, we give some new lower bounds for the problem and we also show that our algorithms are optimal for several graph classes.

9. H. Zheng, S. Omura, K. Wada:
“An approximation algorithm for minimum certificate dispersal problems”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E88-A、2, 551–558, 2006.
概要: We consider a network, where a special data called certificate is issued between two users, and all certificates issued by the users in the network can be represented by a directed graph. For any two users u and v, when u needs to send a message to v securely, v's public-key is needed. The user u can obtain v's public-key using the certificates stored in u and v. We need to disperse the certificates to the users such that when a user wants to send a message to the other user securely, there are enough certificates in them to get the reliable public-key. In this paper, when a certificate graph and a set of communication requests are given, we consider the problem to disperse the certificates among the nodes in the network, such that the communication requests are satisfied and the total number of certificates

stored in the nodes is minimized. We formulate this problem as MINIMUM CERTIFICATE DISPERSAL (MDC for short). We show that MDC is NP-complete, even if its input graph is restricted to a strongly connected graph. We also present a polynomial 2-approximation algorithm MinPivot for strongly connected graphs, when the communication requests satisfy some restrictions. We introduce some graph classes for which MinPivot can compute optimal dispersals, such as trees, rings, some Cartesian products of graphs.

研究会等

1. H. Otsuki, T. Hirata:
"Inapproximability of the Edge Contraction Problem", 2005 Korea-Japan Joint Workshop On Algorithms and Computation, 84–88, 2005, 8.
概要: For a property π on graphs, the edge-contraction problem with respect to π is defined as a problem of finding a set of edges of minimum cardinality whose contraction results in a graph satisfying the property π. This paper gives a lower bound for the approximation ratio for the problem for any property π that is hereditary on contractions and determined by biconnected components.

2. J. Uchida, I. A. K. M. Muzaidal, Y. Katayama, W. Chen, K. Wada:
"Construction and maintenamce of a cluster-based architecture for sensor networks", 39th Hawaii International Conference on System Science, 1-10, 2006.
概要: A sensor network is a collection of transmitter-receiver devices (referred to as nodes). We assume that each node synchronizes and performs transmission or reception per round. In this paper, we consider the construction and maintenance of a cluster-based architecture for a sensor network, with two atomic operations node-move-in and node-move-out which are performed by appearance and disappearance of a node. In our proposed architecture, a deterministic broadcasting can be done in $O(p)$ rounds, where p is the number of clusters. We present a randomized algorithm for a node-move-in and a deterministic algorithm for a node-move-out, which work in $O(q)$ expected rounds and $O(|T|)$ rounds, respectively, where q is the number of neighbors in the network of the joining node and T is a subtree of the architecture whose root is the leaving node. We also provide some alternative algorithms for the operations.

C09: ネットワーク問題のモデル化とアルゴリズムの研究

伊藤 大雄 † 岩間 一雄 † 増澤 利光 ‡ 宮崎 修一 § 堀山 貴史 †

† 京都大学 大学院 情報学研究科
〒 606-8501 京都市左京区吉田本町
{itohiro,iwama,horiyama}@kuis.kyoto-u.ac.jp

‡ 大阪大学 大学院 情報科学研究科
〒 560-8531 豊中市待兼山町 1-3
masuzawa@ist.osaka-u.ac.jp

§ 京都大学 学術情報メディアセンター
〒 606-8501 京都市左京区吉田本町
shuichi@media.kyoto-u.ac.jp

1 はじめに

グラフは接続関係を表現する抽象モデルとして有用であり，古くから盛んに研究されている数学的対象である．特に近年は，計算機やインターネットの急速な発展に伴い，これらを対象としたグラフ問題に対するアルゴリズム研究が盛んになってきている．例えば，ネットワークの信頼性やルーティングの効率化，論理回路の最小化や基盤への埋め込みと言った問題はその典型例である．

本研究の目的は，ネットワークや計算機上での問題をグラフ問題としてモデル化し，そのアルゴリズム開発の研究を行うことである．ただし，本研究では，例えばルーティング問題を取り扱う場合にはルータの構造を特徴付けるグラフのみを考えるなど，入力を現実的なものに絞ることにより，アルゴリズムの効率化を目指している．以下，各節で，平成 17 年度の結果を述べる．

2 各種グラフの平均ストレッチ

我々が日々通信に使用している様々な情報伝達ネットワークの性能は，単に拠点間を結ぶ回線の性能だけでなく，そのネットワークの形状に深く依存している．そのため，たとえ拠点間の回線が高い性能を有していたとしても，ネットワークの構成法によりその性能を十分に発揮できない場合がある．多数のネットワークを接続して通信を行う場合には端末間で情報を伝達する経路を定めるためにルーティングテーブルが必要であるが，ネットワーク上には物理的な閉路が存在する場合が数多く存在し，これがルーティングテーブルを作成する上で障害となる．

そこで予めネットワーク上に閉路の存在しないスパニングツリー（全域木）を設定し，ネットワーク上の最短経路ではなく閉路の存在しない全域木を既定の経路として定めることにより前述した問題を回避することができる．しかしながら，閉路の存在するネットワーク中に全域木を設定することにより端末間の距離は明らかに以前より増加してしまい，ネットワークの性能が低下してしまう．本研究では，ネットワークの性能を評価する指標に平均ストレッチを用いた．あるグラフ G について G の全頂点を含む部分グラフ H を考えるとき，G における各頂点間の距離と H における各頂点間の距離の比をストレッチと呼ぶ．平均ストレッチとはこれらを平均したものである．ストレッチは “グラフ H 上ではグラフ G 上の何倍遠回りしなくてはいけないのか” ということに対応するため，G に対する H の性能を表現する指標として重要視されている．

本研究では平均ストレッチの特徴，特に定数上限の存在性を扱った．閉路を含むグラフのうち最も単純な重みなしリング状グラフと完全グラフについて，グラフのサイズに関わらず平均ストレッチの上限を定数で抑えることのできる全域木の構成法を示した．また，より多くの閉路を含むグラフの例として格子状グラフを扱い，我々は二次元格子状グラフについて，そのサイズに関わらず平均ストレッチの上限が定数であるような全域木の構成法およびその上限値を示した．さらに，d 次元に拡張した格子状グラフについて，そのサイズ

に対して対数関数的に増加する平均ストレッチの上限を示した．

3　孤立 2 部クリークの列挙

Web から情報を得る手法には，テキストに基づく検索方法と，HITS や PageRank のようにリンクの構造に基づく手法がある．リンク構造に基づいた情報検索手法とはグループ内で密にリンクされている Web ページのグループを見つけるというものであり，このアイデアはそのような Web ページ群はお互いに類似した内容を扱うページ群なのではないだろうかというものである．リンク構造に基づく手法は，Web ページを頂点，Web リンクを枝に対応させた Web グラフと呼ばれるグラフを用いて議論される．

密にリンクされた Web ページ群の Web グラフ上での表現の例として，クリーク（完全グラフ）や 2 部クリーク（完全 2 部グラフ）などが挙げられる．しかし，このようなものを求める問題（最大のもの，極大のものを列挙する）のほとんどは難しく，良い近似方法もない．

本研究では「孤立した」2 部クリークを扱った．部分グラフが「孤立している」とは，内部で密にリンクされているだけでなく，その部分グラフと外部とのリンクが少ないことをいう．この孤立しているという条件を用いることで多くの問題が簡単になり，孤立した 2 部クリークを枝数の線形時間で列挙することが可能になることを示した．また，この孤立条件を少し変えるだけで問題は難しくなり，線形時間での列挙は不可能となることも示した．

4　3-正則グラフ上の行商人問題に対するアルゴリズムの改良

本研究では入力を次数 3 の正則グラフに限定した形での行商人問題に対するアルゴリズムの改良を行った．行商人問題 (巡回セールスマン問題) は最も有名な NP 完全問題の一つである．一般のグラフに対する行商人問題のアルゴリズムとしては，1962 年に発表された動的計画法による $O(n^2 2^n)$ 時間アルゴリズムが知られているが，それ以降改善されたアルゴリズムは見つかっていない．

一方，一般の行商人問題に対して各種制限を加えた問題に対しても広く研究されている．本研究の対象である，与えられるグラフを次数 3 の正則グラフに限定した行商人問題もその一つである．本問題も一般の行商人問題と同じく NP 完全問題であり，Eppstein による $2^{n/3} \approx 1.2599^n$ 時間アルゴリズムが知られている．本研究ではこれを 1.2569^n に改良した．

5　単位円盤グラフ上の高速アルゴリズム

単位円盤グラフは平面上で大きさの等しい円盤によってできる交差グラフであり，円盤がグラフの頂点に対応し，円盤の対が交わるか接するとき，またそのときに限りそれらの円盤に対応する頂点の対を辺で接続することによって得られる．単位円盤グラフは通信可能領域がすべて等しい無線端末で構成されるネットワークと自然な対応があり，実用的にも重要である．本研究では，単位円盤グラフ上の最大独立集合問題を解く多項式時間近似スキーム (PTAS) を示した．

6　最大被覆供給点配置問題に対する多項式時間アルゴリズム

k を正整数とする．グラフにおいて供給点と呼ばれる節点の集合を定めたときに，$k-1$ 本の辺を任意にグラフから除去しても供給点集合と節点 v との間にパスが必ず確保されるとき，供給点は節点 v をカバーすると呼ぶ．この概念はネットワークの耐故障性を計る尺度として重要であり，この尺度を用いた問題として供給点配置問題が知られている．供給点配置問題とは，与えられたグラフの全ての節点をカバーするような最小個数の供給点配置を決定する問題であり，耐故障性に優れたネットワークを実現する上で重要な問題である．

本研究では，この問題と深い関係を持つ最大被覆供給点配置問題という問題を提案した．この問題は，与えられたグラフに対し，限られた数の供給点を配置して最大数の節点をカバーする問題で

ある．本問題は，配置可能なサーバ数に制限がある場合での耐故障性に優れたネットワーク設計に重要となる．これら二つの問題は，集合被覆問題と最大被覆問題という二つの NP 困難問題と同様の関係を持っており，前者には供給点配置問題，後者には最大被覆供給点配置問題が対応する．なお，集合被覆問題と最大被覆問題では近似困難性が異なる．

供給点配置問題では多項式時間アルゴリズムが既に知られている．研究の目標は，最大被覆供給点配置問題に対する多項式時間アルゴリズムの発見，もしくは NP 困難性の証明である．本研究では，まず連結グラフに対し $k = 2$ の場合と $k = 3$ の場合に対する多項式時間アルゴリズムをそれぞれ与えた．次に非連結グラフに対する多項式時間アルゴリズムが連結グラフに対するものに還元できることを一般的に示し，その結果の一つとして，$k = 2$，$k = 3$ それぞれの場合について非連結グラフに対する多項式時間アルゴリズムを得た．また，入力を木と高連結なグラフに制限した本問題に対してそれぞれ多項式時間アルゴリズムを与えた．

さらに本研究では，本問題を一般化した二つの問題が NP 完全であることを示した．一つは入力を有向グラフとした問題である．もう一つは，供給点の配置コストが各節点に与えられているとして，配置できる供給点を数ではなくコストによって制限した問題である．なお，これらと同様の一般化を供給点配置問題に施した場合においては多項式時間アルゴリズムの存在が示されている．

7 平面グラフ上の Hajós Calculus

3 彩色不能なグラフの族を構成する非決定性手続きとして Hajós Calculus が知られている．このグラフ構成法によって任意の 3 彩色不能なグラフが多項式ステップで構成可能ならば NP=co-NP となる．しかし，現在に至るまで多項式ステップで構成されないグラフの族は知られていない．我々はこの問題を考えるにあたり，平面グラフにおける 3 彩色不能なグラフの構成法，すなわち構成される過程のすべてのグラフが平面的である構成法を提案した．

8 分散データ構造スキップグラフの探索頻度偏りを考慮した拡張

スキップグラフは資源の検索・挿入・削除を $O(\log n)$(n は資源数) で実行可能な分散データ構造であり，故障耐性，負荷分散特性に優れている．スキップグラフでは全資源を対等に扱っているため，各資源に対するアクセス頻度に偏りのあるシステムにおける検索時間は最適ではない．そこで，本研究ではアクセス頻度の偏りに対応するため，各資源に対して検索頻度に応じた重みを付加し，重みの大きい資源に対しては高速にアクセス可能となるようにスキップグラフを拡張した．

本研究では，ある資源 i の重みを $w(i)$，全資源の重み総和を W とした際に，資源 i の検索時間が $O(\log(W/w(i)))$ となるような重み付け手法を提案した．また，資源の検索頻度が既知の場合に重みを割り当てる際，各資源の重みの比を検索頻度の比と同じに設定する事で検索時間が最小となることを示した．この方法は理論的に最適であるが，メンテナンスコストの観点からは実用的ではない．そこで，メンテナンスコストを考慮した重み付け手法もあわせて提案し，その有効性をシミュレーションにより評価した．

9 根付き木ネットワーク上において局所情報のみで負荷分散を実現する自己安定アルゴリズム

自己安定アルゴリズムとは，任意のネットワーク状況からアルゴリズムの実行を開始したとしても，やがてあらかじめ与えられたネットワーク状況に到達する（解を求める）アルゴリズムである．本研究では，木ネットワーク中の各プロセスに任意の負荷（整数）が与えられると，やがて任意のプロセス間の負荷の差が高々1（1-balancing）になる自己安定アルゴリズムを提案した．また，提案アルゴリズムは負荷を表す情報のみで 1-balancing を実現している．

10 無線ネットワークにおける距離 2 の彩色を利用した TDMA スケジュール手法

無線ネットワークにおける通信方式として，衝突なし通信を実現する TDMA（時分割多重）通信がよく用いられている．効率的な TDMA 通信を実現するには，各ノードが送受信するタイミングを決める TDMA スケジューリングが重要である．これまでにいくつかの TDMA スケジューリングが提案されているが，それらの手法は，帯域の利用率が低い，各ノードの送信帯域の最小保証値が示されていないなどの問題を有している．そこで本研究では，距離 2 の彩色結果を利用した帯域の利用率の高い TDMA スケジューリングを提案した．また，提案手法における各ノードの送信帯域の最小保証値を示した．さらに，シミュレーションによって，既存の TDMA スケジューリングに比べ，提案手法が帯域の高い利用率を達成していることを示した．

11 共有メモリ型スイッチにおけるオンラインバッファ管理アルゴリズムの競合比の改良

近年，ネットワークの運用において QoS(Quality of Service) の保証が主要な論点となっている．これを実現するために定式化した問題がオンラインバッファ管理問題であり，スイッチなどのキュー管理をオンライン問題として定式化したものである．本問題には様々なモデルが考案されている．本研究ではその中の 1 つである共有メモリ型スイッチを扱ったモデルを取り上げた．このモデルの目的はスループットの最大化であり，本研究の成果として，グリーディアルゴリズムの競合比の上限を 2 から $2 - 1/N$ に改良した．ここで，N はスイッチの出力ポート数である．

12 オンラインアルゴリズムにおける競合比の自動解析

将来の入力が未知の状況をモデル化したオンライン問題において，アルゴリズムの性能を評価する手法として，競合比解析が用いられる．この解析は，一般に人手による証明という形でなされるが，ある種の問題に対しては，よりタイトな競合比を得るために膨大な数の場合分けを必要とし，全ての場合を列挙するのは事実上困難となる．本研究では，そのような問題に対し，競合比解析の計算機による自動化手法を提案し，実際にオンラインナップザック問題と k- サーバ問題に対して解析を行う．

オンラインナップザック問題は，サイズ 1 以下のアイテムが次々と与えられ，各段階でアイテムをナップザックに保持するか捨てるかを決めることを繰り返し，入力の終了時点でのアイテムサイズを最大化する問題である．本稿では，オンラインナップザック問題の，特にナップザックの数が 2 で，ナップザック間のアイテムの入れ替えを許したモデルについて考察する．このモデルの競合比は，従来の結果では上限が 1.3334，下限が 1.2808 であり，上下限に開きがあった．この上下限の差を縮めるためには，解析に膨大な数の場合分けが必要となるアルゴリズムを設計しなければならない．本研究では，この問題に対して計算機による競合比の自動解析を提案した．自動解析の主なアイデアは次の通りである．第一に，そのアルゴリズムの実行中の，ビンの中身やアイテムサイズに関する条件式等の途中経過の情報を「状態」として表す．そして，基礎となるアルゴリズムを元に，状態遷移図を作成する．次に，生成した状態遷移図の各状態について，次の性質を持った不等式の組を生成する．その不等式の組は，もし解を持たなければ競合比はある値以下である．この不等式の組の解が存在しないことを Mathematica を用いて確認する．この手法により，このモデルの競合比の上限と下限が 1.3012 で一致することを証明した．

13　2 種類の商品を扱う正直なオークション

本研究においては，入札を一回だけ行い，ある入札者の入札額は他の入札者にはわからない秘密入札であるオークションを扱う．オークションのアルゴリズムを考案するに当たって，正直なオークションという概念を導入する．正直なオークションとは，入札者が商品に対して思っている真実の利用価値を自分の入札として「正直に」入札したときに，その入札者の利益が最も大きくなるようなオークションのことである．また，あるオークションが正直であることとオークションが入札独立であることは同値であることが示されている．オークションが入札独立であるということは，ある入札者が落札に成功したとき，落札額がその入札者の入札額に依存せずに決定されるということである．

ここでは，オークションを競売人の立場に立って設計することを考える．すなわち，オークションの売上を最大化することが目的となる．また販売する商品としては，複製に手間やコストのかからないデジタル商品，例えば有料テレビ番組やインターネットからダウンロードできる音楽ファイルのようなものを仮定する．競売人側は商品を無限に供給できるが，各入札者が購入する商品は 1 種類につき高々1 個までとする．

最近の研究では，競合比の下界が 2.42 であることが示されている．また，現在のところ最良の競合比 3.39 を実現する CORE オークションというアルゴリズムが発表されている．しかしながら，これらの研究成果はいずれも 1 種類の商品を扱うオークションについてのものであり，同じ前提条件における複数種類の商品を扱ったオークションに関する研究は少ない．

そこで，本研究においては既存の 1 種類の商品を扱う正直なオークションを 2 種類の商品を扱えるよう拡張した．加えて，それぞれのモデルにおいて競合比を新たに定義し，新しく考案したオークションの評価を行った．その結果，どちらのモデルにおいても定数の競合比を持つオークションを得ることができた．

14　消費電力抑制のためのジョブスケジューリング

モバイル情報機器の電池駆動時間向上のため，プロセッサ速度の効率的な動的制御が求められている．従来のモデルでは各ジョブには完了期限が設定されてきたが，モバイル機器上で完了期限は通常与えられない．我々は完了期限を無くした上で，ジョブの滞在時間と消費電力量の和をコストとするモデルを提案する．そしてフェーズ制の均衡アルゴリズムを設計した．解析の結果，このアルゴリズムが有界な競合比を持つことを示した．またオフラインの場合に対して，最適スケジュールを出力する多項式時間アルゴリズムを与えた．

15　組合せ二段回路の最大動作率

回路の消費電力には回路への入力変化あたりの平均消費電力と最大消費電力とが存在するが，前者の測定と比べ後者を正確に測定することは困難である．これは考慮すべきパラメータが多いこと，またパラメータ自身が取る値域の広さが故に全域的，網羅的な探索が事実上不可能であるためである．

この困難さに対して回路モデルおよび電力消費モデルを高度に抽象化し，近年発展が著しい分野であるグラフ理論や SAT の問題に還元するアプローチが存在する．これはその問題に対して解の品質が保証された近似アルゴリズムを適用することによりある程度の誤差を許し，実用的な時間で最大消費電力を見積もろうというものである．しかしながら，高度に抽象化されたモデルにおいても回路の最大消費電力を高い精度で求めることは依然として困難である．

その一方で，回路規模に対する回路の最大消費電力に非自明な下限の存在が言えるならば，それにより最大消費電力の見積もりに際して確実なバイアスを考えることが可能となる．本研究ではこのような考えに基づき，回路の最大消費電力を回路規模に対する比で表現し，回路の入力 n をパラメータとしてその下限を示す．

本研究で扱ったのは各頂点の入り次数が 0，1，2 のいずれかに制限された有向グラフ $G = (V, E)$ で表現される n 入力二段の組合せ論理回路で，2

入力の AND ゲートと NOT ゲートから構成される．回路の電力消費モデルはゲートの出力変化によるもののみに単純化し，各ゲートの消費電力の和と等しいとする．また各ゲートの消費電力は等しいとする．そのような回路モデル，電力消費モデルの下で回路の最大電力消費率を定義し，まず 4 入力の回路について上下段，および回路全体での最大電力消費率の最小値の下限を示した．またその下限を実現する回路も併せて示し，各下限がタイトであることを示した．次いでこの結果を一般化し，n 入力回路における最大電力消費率の最小値の上限を与える回路の構成法と，それにより構成される回路が与える最大電力消費率を示した．その後 n 入力回路における最大電力消費率の最小値の下限を示した．

16 否定数を限定した回路計算量の下界

回路計算量とは，ある論理関数を計算する論理回路を考えたときに，最も小さい回路に含まれる素子の個数のことである．回路計算量は，P 対 NP 問題に対する有力なアプローチであると考えられており，NP に含まれる論理関数に対して多項式を越えるサイズの回路計算量の下界を示すことができれば，P $\neq$ NP を示したことになるが，特に制限を加えない一般の回路においては現在のところ線形サイズの下界しか示されていない．そのような現状の中で，否定素子数を $\lceil \log(n+1) \rceil$ に限定した回路において $\omega(n \log(n))$ の下界を示すことができれば，一般の回路における同等の下界を示したことになることが知られており，本研究では，否定数を $\log(n+1)$（ただし，$n+1$ は 2 の累乗）に限定した回路計算量の下界に関する研究を行なった．

否定数を $\lceil \log(n+1) \rceil - 1$ に限定した回路については既に指数サイズの下界が示されているが，ここでの否定素子一つの差は大きく $\lceil \log(n+1) \rceil$ に限定した回路では線形サイズの下界しか示されていない．本研究では，否定数を $\log(n+1)$（ただし，$n+1$ は 2 の累乗）に限定した回路における n 入力 2 出力論理関数 (PARITY, ¬PARITY) の回路計算量の下界が $5n-c$ であることを示した．否定数を $\log(n+1)-1$ に限定した回路では，パリティ関数の回路計算量の下界が $4n + 3\log(n+1) - c$ となることが既に知られているが，これを元にさらに改良を加えることで証明を行なった．

17 3SAT の計算時間の改良に向けて

CNF 論理式の充足可能性問題（SAT）は和積形のブール式が与えられた時，全ての節を真にする，つまり式全体を真にする様な変数への真理値割り当てが存在するかどうかを問う問題である．典型的な NP 問題で，答えが yes であることを示すのは式全体を真にする真偽値の割り当て（証拠）を示せば良いが，no であることを示すのは一般には困難である．NP 完全性が最初に証明された問題としても有名である．LSI の設計検証等多くの実用的応用があり，人工知能分野だけでなく，計算量理論，離散アルゴリズム，設計自動化の分野で最も活発に研究されている問題の一つである．各節に含まれるリテラルの数が高々k 個である CNF 論理式 (k-CNF 論理式) の充足可能性問題は k-SAT と呼ばれる． 特に NP 完全性が成立する最小の $k = 3$ の場合が重要であり，3SAT の計算時間の改善を目指して活発な研究が行なわれている． 我々は 3SAT に対するアルゴリズムを提案し最悪の場合の解析を行なった． 現在，最高速のアルゴリズムは我々が提案したもので，その計算時間は 1.323^n である．本研究では，この計算時間のさらなる改良を目指し，新たなアルゴリズムを提案・解析した．改良のアイデアを以下に述べる．本研究では高速なアルゴリズムのひとつである PPSZ アルゴリズムの性質に着目した．一般に SAT アルゴリズムは n 個の変数に対する真偽値の割り当てを求める必要があるが，PPSZ においてはおよそ $0.4n$ 個の変数に対する正しい割り当てを求めることができれば，多項式時間で n 個の変数全ての割り当てに拡張できるという性質がある．この $0.4n$ 個の変数に対する割り当てを高速に求めることができれば，現在最速のアルゴリズムを改良できる．元の PPSZ ではこの部分を総当り探索で求めており，その計算時間がボトルネックとなっていた．本研究では総当りの代わりに Schoening のアルゴリズムを用いた探索を提案した．提案したアルゴリズムをある仮定の下で

解析した結果，3SAT の最悪計算時間の改良を達成することができた．

18　論理式の解密度の濃縮

与えられた論理式 f に対して，次の条件を満たす論理式 g を考える．(i) もし f が充足不能ならば g は充足不能である．(ii) もし f が充足可能ならば g は充足可能で，f よりも “易しい” 式である．易しさの尺度として，我々は論理式の解密度を用いる．解密度は，n を論理式の変数の個数として，(論理式の充足解の個数)/2^n で定義される．我々は，与えられる論理式 f が 3-CNF，出力すべき論理式 g が AND, OR, NOT で構成される論理式である問題を扱う．この問題にはふたつの方法が考えられる．g を得るために変数を減らす方法と，変数を増やす方法である．それらの方法は SAT アルゴリズムに基づいているが，よりよい SAT アルゴリズムが必ずしもよりよい解密度を濃縮するアルゴリズムではないことを示した．

19　量子ネットワークコーディング

量子情報は連続であるため，古典情報と比べて取り扱いが非常に難しいことがしばしばある．その典型例は情報の複製である．古典のディジタル情報を複製することは容易だが，量子においては情報の完全な複製は不可能であることが知られている．本研究では量子ネットワークコーディングが可能かどうか議論した．ネットワークコーディングとは近年 Ahlswede らにより導入された概念である．これは，いわゆる液体をネットワークに流す場合と異なり，(古典) 情報をネットワークに流す場合は適切なコーディングを行うことによりボトルネックとなる枝容量を越えた情報を送ることが可能となるというものである．本研究では量子情報の複製の場合と同様，情報の近似を許せば量子ネットワークコーディングが可能であることを示した．対象としたネットワークモデルはバタフライと呼ばれるものである．このネットワークには 2 つのパス s_1 から t_1 と s_2 から t_2 が存在し，これらのパスはボトルネックとなる容量 1 の枝を共有している．古典情報の場合，ネットワークコーディングにより我々はそれぞれのパスに 1 ビットずつ流すことができる．本研究では量子情報の場合に，それぞれのパスに任意の量子状態を流しそれぞれの受信者が得る量子状態と送られた状態のフィデリティが 1/2 より大きくできることを示した．ここでフィデリティとは 2 つの量子状態の距離を測る単位で 1 のとき 2 つは同じ状態，1/2 のとき 2 つはランダムな関係にあるようなものである．また片方のパスには古典情報を流す場合，得られる量子状態のフィデリティは 2/3 に改良されること，あるいはそれぞれの量子状態が有限の状態数のときも同様の改良ができることを示した．この結果を利用して s_1 から t_1(s_2 から t_2 も同様) に 2 ビットの古典情報を送ったとき，片方のビットのみなら復元できるというプロトコルを設計することも可能となった．

20　安定結婚問題に対する近似アルゴリズム

安定結婚問題とは，Gale と Shapley によって提唱されたマッチング問題である．この問題では，N 要素同士の 2 つの集合 (例えば，男性と女性) と，各個人の異性に対する希望リストが与えられる．男性 m が女性 w_2 よりも w_1 の方を好む時，$w_1 \succ_m w_2$ と表記する．また，マッチング M に対して男性 m とマッチしている相手の女性を $M(m)$ と表記する．ここで，あるマッチング M において，$w \neq M(m)$ であり，$w \succ_m M(m)$ かつ $m \succ_w M(w)$ であるような (m, w) を M の blocking pair と呼ぶ．blocking pair の存在しないマッチングを安定マッチングといい，安定マッチングを求める問題を安定結婚問題という．安定結婚問題の任意の例題に対して安定マッチングが存在することは，Gale と Shapley によって 1962 年に示されており，安定マッチングを $O(N^2)$ 時間で求めるアルゴリズム (Gale-Shapley アルゴリズム) も示されている．

安定結婚問題の現実世界での応用として，アメリカでは研修医を病院に割り当てる NRMP というマッチングシステムにこの問題が使われている．同様のシステムはカナダやスコットランドでも取り入れられており，日本でも 2004 年度の研修医配属から安定結婚問題が利用され始めた．

安定結婚問題の拡張として，希望リスト内に全員の名前を含まなくても良い不完全リストと，希

望リスト内での同順位を許す同順位リストの二つの拡張が考えられるが，片方の拡張の下では，安定マッチングは全て同サイズであり，安定マッチングは多項式時間で求めることができる．ところが，これらの両方の拡張を同時に施すと，一つの例題に対して異なったサイズの安定マッチングが存在する可能性があり，その最大サイズの安定マッチングを見つける問題 (MAX SMTI) は APX 完全であることが知られている．MAX SMTI に対して，近似度 2 を達成するアルゴリズムの存在は自明である．現在知られている最良の近似アルゴリズムは，近似度 $2-c\frac{\log N}{N}$(N は入力における男性の数，c は任意の正定数) のアルゴリズムである．本研究ではこの近似度を $2-c\frac{1}{\sqrt{N}}$(c は $c \leq \frac{1}{4\sqrt{6}}$ を満たす正定数) に改良した．

21　半順序付き集合ゲームの必勝法

組み合わせゲームの 1 つに，Poset(半順序付き集合) Game と呼ばれるものが知られている．このゲームは以下のようなものである．まず，半順序付き集合が入力として与えられる．(1) 2 人のプレイヤーは交互に集合の要素を 1 つずつ選んでいく．(2) 選んだ要素と，その要素より大きい要素を全て消さなくてはならない．(3) 選ぶ要素の無くなったプレイヤーの負け．Poset Game は単一の祖先 (毒節点) を持つ dag（非閉路的有向グラフ）で表現できる．このゲームは有名な Nim から未解決の Chomp まで多様なゲームを含み，これらの研究からは様々な興味深い結果が得られている．本研究では Poset Game を拡張し，毒節点が複数あり，しかも毒に重みを持たせ，与えられた体力を越えて毒を取った競技者が負けるとしたゲームを扱った．この拡張したゲームの必勝手順を多項式時間で得る方法について考察した．

22　FDB を用いた接続ポート固有の IP アドレスリースが可能な DHCP サーバの設計と実装

ネットワーク障害の解析のため，あるホストの IP アドレスや MAC アドレスからそれが存在する場所を探す必要が生じることがある．しかし，DHCP を用いた情報コンセントでは IP アドレスは物理的な端末の位置と無関係に割り当てられるためこの作業は困難である．そこで，本研究では個々の情報コンセントに対して固定的に IP アドレスを割り当てる DHCP サーバを開発した．この DHCP サーバは SNMP を用いてスイッチングハブの MAC アドレスフォワーディングテーブル (FDB) を取得し，割り当て対象端末の接続したポートを知る．本システムでは，ネットワーク管理者は容易に特定の DHCP クライアントの設置場所に到達することが可能となる．

研究業績一覧

学術論文

1. Taisuke Izumi, and Toshimitsu Masuzawa: “An improved algorithm for adaptive condition-based consensus”, Proceedings of the 12th Colloquium on Structural Information and Communication Complexity (SIROCCO 2005), LNCS 3499, pp.170-184, 2005 年 5 月.
   概要: Condition-Based Approach studies restrictions on the inputs of a distributed problem, called conditions, to circumvent several impossibility results. Especially, for the synchronous consensus problem, the relation between conditions and time complexity bounds has been studied. In our previous work, we introduced the adaptiveness on time complexity of the condition-based approach, and established the adaptive condition-based approach: It classifies all possible input vectors into the hierarchical sequence of conditions according to their difficulty called legality level. For such hierarchy, adaptive algorithms achieve time complexity depending on the legality level of input vectors. In this paper, we propose an improved version of the adaptive condition-based algorithms for synchronous consensus that achieves better time complexity than the previous one. On the

assumption that majority of processes are correct, the proposed algorithm terminates within $\min\{f+2, t+1\} - l$ rounds if $l < f$, where f and t is the actual and the maximum numbers of faults respectively, and l is the legality level of input vectors. Moreover, the algorithm terminates in 1 round if $l \geq t$ and $f = 0$, and terminates within 2 rounds if $l \geq f$ holds. Compared with our previous algorithm, the proposed algorithm improves time complexity by one round in the case of $f = t$ and $l > f$.

2. Y. Hanatani, T. Horiyama, and K. Iwama: "Hajós Calculus on Planar Graphs", Proc. the 4th Japanese-Hungarian Symposium on Discrete Mathematics and Its Applications, pp.76–83, 2005 年 6 月.
概要: The Hajós calculus is a nondeterministic procedure which generates the class of non-3-colorable graphs. If all non-3-colorable graphs can be constructed in polynomial steps by the calculus, NP = co-NP holds. Up to date, however, it remains open whether there exists a family of graphs that can be generated in polynomial steps. To attack this problem, we propose two graph calculi PHC and PHC* that generate non-3-colorable planar graphs, where intermediate graphs in the calculi are also restricted to be planar. Then we prove that PHC and PHC* are sound and complete. We also show that PHC* can polynomially simulate PHC.

3. H. Ito, G. Nakamura, and S. Takata: "Chomp with Poison-Strewn Chocolates", Proc. the 4th Japanese-Hungarian Symposium on Discrete Mathematics and Its Applications, pp.336–343, 2005 年 6 月.
概要:

4. Tomoko Suzuki, Taisuke Izumi, Fukuhito Ooshita, and Toshimitsu Masuzawa: " Self-adaptation of mobile agent population in dynamic networks: a biologically inspired approach", Proceedings of the 2nd IEEE International Conference on Autonomic Computing (ICAC-05), pp.374-375, 2005 年 6 月.
概要: Mobile agent is one of the most promising paradigms to support autonomic computing in a large scale ofdistributed system with diversity: mobile agents traverse the distributed system and carry out a sophisticated task at each node adaptively. In mobile-agent-based systems, a larger number of agents generally require shorter time to complete the whole task but consume more resources. Therefore, it is indispensable to keep an appropriate number of agents for its application. In this paper, we consider the mobile agent population control problem in dynamic networks: it requires to adjust the number of agents to a constant fraction of the current network size.We propose algorithms inspired by a biological paradigm and show by simulations that the proposed algorithms realizeself-adaptation of mobile agent population in dynamic networks.

5. Tomoko Suzuki, Taisuke Izumi, Fukuhito Ooshita, and Toshimitsu Masuzawa: "Biologically inspired self-adaptation of mobile agent population", Proceedings of the 3rd Workshop on Self-adaptive and Autonomic Computing (DEXA International Workshop), pp.170-174, 2005 年 8 月.
概要: Mobile agent is one of the most promising paradigms to support autonomic computing in a large scale of distributed system with diversity: mobile agents traverse the distributed system and carry out a sophisticated task at each node adaptively. In mobile-agent-based systems, a larger number of agents generally require shorter time to complete the whole task but consume more resources (e.g., processing power and network bandwidth). Therefore, it is indispensable to keep an appropriate number of agents for its application. In this

paper, we consider the mobile agent population control problem in dynamic networks: it requires to adjust the number of agents to a constant fraction of the current network size. We propose algorithms inspired by a biological paradigm and show by simulations that the proposed algorithms realize self-adaptation of mobile agent population in dynamic networks.

6. W. W. Bein, K. Iwama, L. L. Larmore, and J. Noga:
"The Delayed k-Server Problem", Proc. the 15th International Symposium on Fundamentals of Computation Theory (FCT 2005), pp.281–292, 2005 年 8 月.
概要: We introduce a new version of the server problem: the delayed server problem. In this problem, once a server moves to serve a request, it must wait for one round to move again, but could serve a repeated request to the same point. We show that the delayed k-server problem is equivalent to the $(k-1)$-server problem in the uniform case, but not in general.

7. K. Iwama, A. Lingas, and M. Okita:
"Max-stretch Reduction for Tree Spanners", Proc. the 9th International Workshopon Algorithms and Data Structures (WADS 2005), pp.122–133, 2005 年 8 月.
概要: A tree t-spanner T of a graph G is a spanning tree of G whose max-stretch is t, i.e., the distance between any two vertices in T is at most t times their distance in G. If G has a tree t-spanner but not a tree $(t-1)$-spanner, then G is said to have max-stretch of t. In this paper, we study the Max-Stretch Reduction Problem: for an unweighted graph $G=(V,E)$, find a set of edges not in E originally whose insertion into G can decrease the max-stretch of G. Our results are as follows: (i) For a ring graph, we give a linear-time algorithm which inserts k edges improving the max-stretch optimally. (ii) For a grid graph, we give a nearly optimal max-stretch reduction algorithm which preserves the structure of the grid. (iii) In the general case, we show that it is NP-hard to decide, for a given graph G and its spanning tree of max-stretch t, whether or not one-edge insertion can decrease the max-stretch to $t-1$. (iv) Finally, we show that ! the max-stretch of an arbitrary graph on n vertices can be reduced to $s' \geq 2$ by inserting $O(n/s')$ edges, which can be determined in linear time, and observe that this number of edges is optimal up to a constant.

8. Toshimitsu Masuzawa, and Hirotsugu Kakugawa:
"Self-stabilization in spite of frequent changes of networks: Case study of mutual exclusion on dynamic rings", Proceedings of the 7th International Symposium on Self-Stabilizing Systems (SSS), LNCS 3764, pp.183-197, 2005 年 10 月.
概要: It is generally said that a self-stabilizing protocol is inefficient in distributed systems with frequent faults or topological changes and, what is worse, it might never converge to its intended behavior forever. Its main reason is that a new fault or topological change brings the system into an unexpected configuration, and thus, the system restarts convergence to its intended behavior *from scratch*. But the reasoning seems too pessimistic. This paper provides a novel observation about self-stabilization on frequently changing networks: by quantifying influence of steps of a self-stabilizing protocol and that of a topological change, efficiency of the convergence can be estimated with considering topological changes that occur during the convergence. To show the feasibility and effectiveness of the approach, this paper presents a simple self-stabilizing mutual exclusion protocol on a dynamic ring where

processes can join and leave the ring at any time. This paper clarifies what restrictions on frequency of joins and leaves are sufficient to guarantee the convergence and to guarantee the intended behavior after the convergence. The restrictions are not strict and thus the protocol can complete convergence and can continue its intended behavior on a frequently changing ring.

9. X. Han, K. Iwama, and G. Zhang:
"On-line Removable Square Packing", Proc. the 3rd International Workshop on Approximation and Online Algorithms (WAOA 2005), LNCS 3879, pp.216–229, 2005年10月.
概要: The online removable square packing problem is a two-dimensional version of the online removable Knapsack problem. For a sequence of squares with side length at most 1, we are requested to pack a subset of them into a unit square in an online fashion where the online player can decide whether to take the current square or not and which squares currently in the unit square to remove. The goal is to maximize the total packed area. Our results include: (i) Any online algorithm cannot achieve a better competitive ratio than 2.618. (ii) The matching upper bound is achieved by a relatively simple online algorithm if repacking is allowed. (iii) Without repacking, we can achieve an upper bound of 3.0 by using the concept of bricks by Januszewski and Lassak. (iv) The offline version of the problem admits a PTAS.

10. H. Ito, K. Iwama, and T. Osumi:
"Linear-Time Enumeration of Isolated Cliques", Proc. the 13th Annual European Symposium on Algorithms (ESA 2005), LNCS 3669, pp.119–130, 2005年10月.
概要: For a given graph G of n vertices and m edges, a clique S of size k is said to be c-isolated if there are at most ck outgoing edges from S. It is shown that this parameter c is an interesting measure which governs the complexity of finding cliques. In particular, if c is a constant, then we can enumerate all c-isolated maximal cliques in linear time, and if $c = O(\log n)$, then we can enumerate all c-isolated maximal cliques in polynomial time. Note that there is a graph which has a superlinear number of c-isolated cliques if c is not a constant, and there is a graph which has a superpolynomial number of c-isolated cliques if $c = \omega(\log n)$. In this sense our algorithm is optimal for the linear-time and polynomial-time enumeration of c-isolated cliques.

11. J. Akiyama, H. Fukuda, H. Ito, and G. Nakamura:
"Infinite Series of Generalized Gospher Space Filling Curves", Abstracts of the China-Japan Conference on Discrete Geometry, Combinatorics, and Graph Theory (CJCDGCGT) 2005, pp.6–8, 2005年11月.
概要:

12. H. Ito:
"Transformation of Simple Graphs Preserving Cut-Size Order and Their Simpleness", Abstracts of the China-Japan Conference on Discrete Geometry, Combinatorics, and Graph Theory (CJCDGCGT) 2005, pp.12–14, 2005年11月.
概要:

13. Toshimitsu Masuzawa, and Sebastien Tixeuil:
"A self-stabilizing link-coloring protocol resilient to unbounded byzantine faults in arbitrary networks", Proceedings of the 9th International Conference on Principles of Distributed Systems (OPODIS 2005), pp.283-298, 2005年12月.
概要: Self-stabilizing protocols can tolerate any type and any number of transient faults. However, in general, self-stabilizing protocols provide no guarantee about

their behavior against permanent faults. This paper proposes a self-stabilizing link-coloring protocol resilient to (permanent) Byzantine faults in arbitrary networks. The protocol assumes the central daemon, and uses $2\Delta - 1$ colors where Δ is the maximum degree in the network. This protocol guarantees that any link (u, v) between non faulty processes u and v is assigned a color within $2\Delta + 2$ rounds and its color remains unchanged thereafter. Our protocol is Byzantine insensitive in the sense that the subsystem of correct processes remains operating properly in spite of unbounded Byzantine faults.

14. K. Iwama, S. Miyazaki, and N. Yamauchi: "A $(2 - c\frac{1}{\sqrt{N}})$-Approximation Algorithm for the Stable Marriage Problem", Proc. the 16th Annual International Symposium on Algorithms and Computation (ISAAC 2005), LNCS 3827, pp.902–914, 2005 年 12 月.
概要: We consider the problem of finding a stable matching of maximum size when both ties and unacceptable partners are allowed in preference lists. This problem is NP-hard and the current best known approximation algorithm achieves the approximation ratio $2 - c\frac{\log N}{N}$, where c is an arbitrary positive constant and N is the number of men in an input. In this paper, we improve the ratio to $2 - c\frac{1}{\sqrt{N}}$, where c is a constant such that $c \leq \frac{1}{4\sqrt{6}}$.

15. Tomoko Suzuki, Taisuke Izumi, Fukuhito Ooshita, Hirotsugu Kakugawa, and Toshimitsu Masuzawa:
"Bio-inspired replica density control in dynamic networks", Proceedings of the 2nd International Workshop on Biologically Inspired Approaches to Advanced Information Technology (Bio-ADIT 2006), LNCS 3853, pp.281-293, 2006 年 1 月.
概要: Resource replication is a crucial technique for improving system performance of distributed applications with shared resources. A larger number of replicas require shorter time to reach a replica of the requested resource, but consume more storage of hosts. Therefore, it is indispensable to adjust the number of replicas appropriately for its application. This paper considers the problem for controlling the density of replicas adaptively in dynamic networks. The goal of the problem is to adjust the number of replicas to a constant fraction of the current network size. This paper proposes algorithm inspired by the single species population model, which is a well-known population ecology model. The simulation results show that the proposed algorithm realize self-adaptation of the replica density in dynamic networks.

16. Taisuke Izumi and Toshimitsu Masuzawa:
"An interest-based peer clustering algorithm using ant paradigm", Proceedings of the 2nd International Workshop on Biologically Inspired Approaches to Advanced Information Technology (Bio-ADIT 2006), LNCS 3853, pp.379-386, 2006 年 1 月.
概要: The interest-based clustering is one of promising approaches to achieve low-cost search in peer-to-peer file sharing. It organizes the logical overlay network where peers having similar interests are closely located. In this paper, we propose an interest-based peer clustering algorithm using ant paradigm. Our algorithm is inspired by the ant-based clustering algorithm, which is one of heuristic methods to categorize many data items. We also evaluate this algorithm by simulations.

17. M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita:
"Quantum Network Coding", Proc. the 9th Workshop on Quantum Information Processing (QIP2006), 2006 年 1 月.

概要: Since quantum information is continuous, its handling is sometimes surprisingly harder than the classical counterpart. A typical example is cloning; making a copy of digital information is straightforward but it is not possible exactly for quantum information. The question in this talk is whether or not "quantum" network coding is possible. Its classical counterpart is another good example to show that digital information flow can be done much more efficiently than conventional (say, liquid) flow. Our answer to the question is similar to the case of cloning, namely, it is shown that quantum network coding is possible if approximation is allowed, by using a simple network model called Butterfly. In this network, there are two flow paths, s_1 to t_1 and s_2 to t_2, which shares a single bottleneck channel of capacity one. In the classical case, we can send two bits simultaneously, one for each path, in spite of the bottleneck. Our results for quantum network coding include: (i) We can send any quantum state $|\psi_1\rangle$ from s_1 to t_1 and $|\psi_2\rangle$ from s_2 to t_2 simultaneously with a fidelity strictly greater than 1/2. (ii) If one of $|\psi_1\rangle$ and $|\psi_2\rangle$ is classical, then the fidelity can be improved to 2/3. (iii) Similar improvement is also possible if $|\psi_1\rangle$ and $|\psi_2\rangle$ are restricted to only a finite number of (previously known) states. This allows us to design an interesting protocol which can send two classical bits from s_1 to t_1 (similarly from s_2 to t_2) but only one of them should be recovered.

18. Hirotsugu Kakugawa, and Toshimitsu Masuzawa:
"A self-stabilizing distributed algorithm for 5-spanner", Proceedings of the IASTED International Conference on Networks and Communication Systems (NCS), 2005 年 3 月.
概要: Self-stabilization is a theoretical framework of non-masking fault-tolerant distributed algorithms. A self-stabilizing system tolerates any kind and any finite number of transient faults, such as message loss, memory corruption, and topology change. Because message loss and topology change occur so frequently in mobile ad hoc networks, distributed algorithms on them should tolerate such events. In this paper, we propose a self-stabilizing distributed algorithm for computing a 5-spanner, which can be used, for example, as a basis for computing virtual backbone or routing in mobile ad hoc networks.

19. Taisuke Izumi, and Toshimitsu Masuzawa:
"Condition adaptation in synchronous consensus", IEEE Transactions on Computers, (刊行予定).
概要: The condition-based approach is one of sophisticated methods to overcome several impossibility results in distributed consensus problem (e.g., impossibility of fault tolerance in asynchronous consensus, or time complexity lower bounds in synchronous consensus). It introduces conditions on input vectors to specify subsets of all possible input vectors to consensus algorithms, and condition-based algorithms can circumvent the impossibility if actual input vectors satisfy a particular condition. In this paper, we present a new condition-based paradigm for synchronous consensus. We newly introduce the concept of adaptation on the time complexity of condition-based algorithms, and present the adaptive condition-based approach to synchronous consensus. In our approach, all possible input vectors are classified into hierarchical conditions according to their difficulty called the legality level. Execution time of adaptive condition-based algorithms depends on the legality level of input vectors.

20. Y. Hanatani, T. Horiyama, and K. Iwama: "Density Condensation of Boolean Formulas", Discrete Applied Mathematics, （刊行予定）.
概要: We consider problems of reasoning with a knowledge-base, which is represented by an ordered binary decision diagram (OBDD), for two cases of general and Horn knowledge-bases. Our main results say that both finding a model of a knowledge-base and deducing from a knowledge-base can be done in linear time for a general knowledge-base, but that abduction is NP-complete even for a Horn knowledge-base. Then, we consider abduction when its assumption set consists of all propositional literals (i.e., an answer for a given query is allowed to include any positive literals), and show that it can be done in polynomial time if the knowledge-base is Horn, while it remains NP-complete for the general case. Some other solvable cases are also discussed.

21. Y. Asahiro, T. Horiyama, K. Makino, H. Ono, T. Sakuma, and M. Yamashita: "How to Collect Balls Moving in the Euclidean Plane", Discrete Applied Mathematics, （刊行予定）.
概要:

22. H. Ito, and H. Nagamochi: "Two Equivalent Measures on Weighted Hypergraphs", Discrete Applied Mathematics, （刊行予定）.
概要:

23. H. Ito, K. Iwama, and T. Tamura: "Efficient Methods for Determining DNA Probe Orders", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.E88-A, no.5, （刊行予定）.
概要: In STS-based mapping, it is necessary to obtain the correct order of probes in a DNA sequence from a given set of fragments or an equivalently a hybridization matrix A. It is well-known that the problem is formulated as the combinatorial problem of obtaining a permutation of A's columns so that the resulting matrix has a consecutive-one property. If the data (the hybridization matrix) is error free and includes enough information, then the above column order uniquely determines the correct order of the probes. Unfortunately this does not hold if the data include errors, and this has been a popular research target in computational biology. Even if there is no error, ambiguities in the probe order may still remain. This in fact happens because of the lack of some information regarding the data, but almost no further investigation has previously been made. In this paper, we define a measure of such imperfectness of the data as the minimum amount of the additional fragment! s that are needed to uniquely fix the probe order. Polynomial-time algorithms to compute such additional fragments of the minimum cost are presented. A computer simulation using genes of human chromosome 20 is also noted.

24. K. Sugihara, and H. Ito: "Maximum-Cover Source Location Problems", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.E88-A, no.5, （刊行予定）.
概要: Given a graph $G = (V, E)$, a set of vertices $S \subseteq V$ covers $v \in V$ if the edge connectivity between S and v is at least a given number k. Vertices in S are called sources. The source location problem is a problem of finding a minimum-size source set covering all vertices of a given graph. This paper presents a new variation of the problem, called maximum-cover source-location problem, which finds a source set S with a given size p, maximizing the sum of the weight of vertices covered by S. It presents an $O(np + m + n \log n)$-time algorithm for

$k = 2$, where $n = |V|$ and $m = |E|$. Especially it runs linear time if G is connected. This algorithm uses a subroutine for finding a subtree with the maximum weight among p-leaf trees of a given vertex-weighted tree. For the problem we give a greedy-based linear-time algorithm, which is an extension of the linear-time algorithm for finding a longest path of a given tree presented by E. W. Dijkstra around 1960. Moreover, we show some polynomial solvable cases, e.g., a given graph is a tree or $(k-1)$-edge-connected, and NP-hard cases, e.g., a vertex-cost function is given or G is a digraph.

25. H. Ito:
"Harary's Generalized Ticktacktoe", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.J88-A, no.6, (刊行予定).
概要:

研究会等

1. 角田大輔, 堀山貴史, 岩間一雄:
"入札額の範囲が制限された正直なオークション", 電子情報通信学会 コンピュテーション研究会, 信学技報, vol.105, COMP2005-6, pp.39–47, 2005 年 4 月.
概要: 1 回入札，秘密入札 (入札額が他人には分からない入札) の 正直なオークション (truthful auction) を扱う．正直なオークションでは，正直に入札すること，すなわち自分にとっての真の利用価値を自分の入札値とすることで，最良の利得を得ることが保証される．正直なオークションを実現するアルゴリズムの性能評価には競合比が用いられ，これまでに下界が 2.42 であることが知られている． また，CORE アルゴリズムが提案されており，競合比 3.39 を達成している． 本報告では，入札額の最大値と最小値の比が高々 r 倍以内である時に，競合比 $\ln r + 1$ を達成するオークションアルゴリズムを提案する．最初に，基本となるアルゴリズムとして，他の入札者の最低入札額を提示額とする最低入札額オークションを示す． このアルゴリズムを拡張することで，最低入札額またはその定数倍の複数の提示額をもつオークションを提案する． 提示額の種類を増化させることで競合比は改善され，確率分布により提示額を決定することで競合比 $\ln r + 1$ を達成する

2. 山内直哉, 宮崎修一, 岩間一雄:
"安定結婚問題に対する局所探索近似アルゴリズムの改良", 電子情報通信学会 コンピュテーション研究会, 信学技報, vol.105, no.72, COMP2005-15, pp.45–51, 2005 年 5 月.
概要: 安定結婚問題において，同順位リストと不完全リストの存在を許した問題に対して最大サイズの安定マッチングを見つける問題を考える． この問題は NP 困難であり，現在知られている最良の近似アルゴリズムは，$(2 - c\frac{\log N}{N})$-近似アルゴリズムである．(ここで，c は任意の正定数であり，N は入力中の男性の数である．) 本論文では，この近似度を $2 - c\frac{1}{N^{\frac{2}{3}}}$ に改良した．(c は $c \leq \frac{1}{2\sqrt[3]{6}}$ を満たす正定数である．)

3. 桝田秀夫, 木村洋介, 大下福仁, 齊藤明紀, 増澤利光:
"FDB を用いた接続ポート固有の IP アドレスリースが可能な DHCP サーバの設計と実装", 情報処理学会研究報告（分散システム/インターネット運用技術 2005-DSM-037）, Vol.2005, No.39, pp.41-46, 2005 年 5 月.
概要: ネットワーク障害解析のためあるホストの IP アドレスや MAC アドレスからそれが存在する場所を探す必要が生じることがある．DHCP を用いた情報コンセントでは IP アドレスは物理的な端末の位置と無関係に割り当てられるためこの作業は困難である．我々は，個々の情報コンセントに対して固定的に IP アドレスを割り当てる DHCP サーバを開発した．この DHCP サーバは SNMP を用いてスイッチングハブの MAC アドレスフォワーディングテーブル (FDB) を取得し，割り当て対象端末の接続したポートを知る．このサーバは，通常のサーバより応答時間が 0.5 秒長い．本システムを利用することで，

ネットワーク管理者は容易に特定の DHCP クライアントの設置場所に到達することができる．

4. Taisuke Izumi, and Toshimitsu Masuzawa: “On solvability of one-step consensus”, 電子情報通信学会技術研究報告 DC2005-8, Vol.105, No.123, pp.7-12, 2005 年 6 月.
概要: While any fault-tolerant asynchronous consensus algorithm requires two communication steps even in failure-free executions, it is known that we can construct the algorithm terminating in one step for some good inputs (e.g. all processes propose a same value). In this paper, we present the necessary and sufficient constraint for the set of inputs for which we can construct the asynchronous consensus algorithm terminating in one step. Our investigation is based on the notion of the condition-based approach: it introduces conditions on input vectors to specify subsets of all possible input vectors and condition-based algorithms can circumvent some impossibility if the actual input vector satisfy a particular condition. More interestingly, conditions treated in this paper are adaptive. That is, we consider hierarchical sequences of conditions whose k-th condition is the set of input vector for which the consensus can be solved in one step even if at most k processes crash. The necessary and sufficient constraint we propose in this paper is one for such condition sequences. In addition, we present several instances of the sufficient condition sequences. Compared with existing constraint for inputs (i.e. all processes propose a same value), all of these instances are more relaxed.

5. 山内由紀子, 中南良浩, 大下福仁, 増澤利光: “無線ネットワークにおける距離 2 の彩色を利用した TDMA スケジュール手法”, 情報処理学会研究報告（マルチメディア通信と分散処理, 2005-DPS-123), Vol.2005, No.58, pp.69-74, 2005 年 6 月.
概要: 無線ネットワークにおける通信方式として，衝突なし通信を実現する TDMA（時分割多重）通信がよく用いられている．効率的な TDMA 通信を実現するには，各ノードが送受信するタイミングを決める TDMA スケジューリングが重要である．これまでにいくつかの TDMA スケジューリングが提案されているが，それらの手法は，帯域の利用率が低い，各ノードの送信帯域の最小保証値が示されていないなどの問題を有する．そこで，本稿では，距離 2 の彩色結果を利用した，帯域の利用率の高い TDMA スケジューリングを提案する．また，提案手法における，各ノードの送信帯域の最小保証値を示す．さらに，シミュレーションによって，既存の TDMA スケジューリングに比べ，提案手法が帯域の高い利用率を達成していることを示す．

6. 小林浩二, 宮崎修一, 岡部寿男: “共有メモリ型スイッチにおけるオンラインバッファ管理アルゴリズムの競合比の改良”, 電子情報通信学会 コンピュテーション研究会, 信学技報, vol.105, no.144, COMP2005-21, pp.17–22, 2005 年 6 月.
概要: オンラインバッファ管理問題は，近年のネットワーク運用における主要な論点となっている QoS (Quality of Service) 保証実現のための，スイッチなどの キュー管理をオンライン問題として定式化した問題であり，様々なモデルが考案されている．本論文ではその中の 1 つである 共有メモリ型スイッチを扱ったモデルを取り上げる． 我々は，アルゴリズム Longest Queue Policy (LQD) の競合比の既知の上限を $2 - 1/N$ に改良した．ここで，N はスイッチの出力ポート数である．

7. 杉原堅也, 伊藤大雄: “最大被覆供給点配置問題に関する考察”, 2005 年夏の LA シンポジウム, pp.25.1–25.12, 2005 年 7 月.
概要: 供給点配置問題とは，グラフ $G = (V, E)$ が与えられたとき，全ての節点を被覆する最小要素の供給点集合 $S \subseteq V$ を見つける問題である．ただし，節点部分集合 $S \subseteq V$ が

節点 $v \in V$ を被覆するとは，S と v の枝連結度が与えられた整数 k 以上となっていることを言う．本稿では，この問題を変形した最大被覆供給点問題を提案し，本問題について考察を行う．本問題は，グラフ G と各節点の重みが与えられたとき，被覆される節点の重みの和が最大となるような要素数が p 個の供給点集合 $S \subseteq V$ をみつける問題である．本稿では，$k = 2$ の場合における $O(np+n\log n+m)$ 時間アルゴリズムを示し，特に G が連結グラフの場合には線形時間アルゴリズムが存在することを示す．このアルゴリズムは，与えられた節点重みの付いた木から葉が p 個の最大重み部分木をみつけるというサブルーチンを用いており，このサブルーチンはダイクストラによる木の最長路を求めるアルゴリズムの拡張となっている．さらに本稿では，G が $(k-1)$-枝連結グラフの場合や木の場合における多項式時間アルゴリズムを示す．また，G が有向グラフの場合，もしくは節点に供給点を配置するコストを与えた場合に本問題が NP-困難となることを示す．

8. 森住大樹, 岩間一雄:
“否定数を $\log(n+1)$ に限定した回路計算量の下界について”， 夏の LA シンポジウム, pp.30.1–30.4, 2005 年 7 月.
概要: 本稿では，否定数を $\log(n+1)$ に限定した回路における n 入力 2 出力論理関数 (PARITY, ¬PARITY) の 回路計算量の下界が $5n-c$ であることを示す． 否定数を限定しない場合の現在知られている最高の下界は $5n-o(n)$ であるが，否定数を限定することによって それより上の下界が得られることも期待できる． 本稿の内容は，$5n-o(n)$ を越えることには至っていないが，より単純な関数を用いてほぼ同等の下界を得るものである． また，否定数を $\lceil\log(n+1)\rceil$ に限定した回路において $\omega(n\log(n))$ の下界を示すことができれば，一般の回路における 同等の下界を示したことになることが知られており，否定数を $\lceil\log(n+1)\rceil$ に限定した回路の回路計算量を 調べることは特別な意味を持つ．

9. 堀山貴史, 中塚裕之, 岩間一雄:
“逆算法に基づく詰将棋の列挙”, 特定領域研究 新世代の計算限界 ミニ研究集会 (組合せゲーム・パズル), 2005 年 9 月.
概要: 近年の計算機の高速化やメモリ量の増加，洗練されたアルゴリズム設計法の発展により，与えられた条件を満たす解を 1 つだけでなく すべて列挙することが，実用上要請されるようになってきている． 本発表では，逆算法による詰将棋の列挙アルゴリズムを提案する． 逆算法により詰め手数の少ないものから順に詰将棋を列挙することで，詰将棋解答プログラムを用いることなく，与えられた条件下で可能な詰将棋を 高速に列挙することができる．

10. Taisuke Izumi, Toshimitsu Masuzawa:
“A weakly-adaptive condition-based consensus algorithm in asynchronous distributed systems”, 電子情報通信学会技術研究報告 COMP2005-34, Vol.105, No.273, pp.43-48, 2005 年 9 月.
概要: While the (uniform) consensus problem is one of fundamental and important problems for designing fault-tolerant distributed systems, it cannot be solved in failure-prone asynchronous distributed systems. To circumvent this impossibility, the condition-based approach is recently introduced. It introduces conditions, which is a subset of all possible inputs, and condition-based algorithms can circumvent the impossibility if actual input belongs to the condition. In existing condition-based consensus algorithms, the size of conditions depends on the maximum number of crash faults. In this paper, we propose the condition-based consensus algorithm whose condition depends on the actual number of crash faults. This algorithm is weakly-adaptive in the following sense: it has a parameter k. The algorithm solves the consensus for more inputs than the existing one if at most k processes actually crash. On the other hand, if more than k processes crash, it solves the

consensus only for less inputs.

11. Tomoko Suzuki, Taisuke Izumi, Fukuhito Ooshita, Hirotsugu Kakugawa, and Toshimitsu Masuzawa:
"A biologically inspired approach to replica control in dynamic networks", 情報処理学会研究報告 (アルゴリズム, 2005-AL-102), Vol.2005, No.91, pp.51-58, 2005 年 9 月.
概要: Resource replication is a crucial technique for improving system performance of distributed application with shared resources. A larger number of replicas require shorter time to reach a replica of the requested resource, but consume more storage of hosts. Therefore, it is indispensable to adjust the number of replicas appropriately for its application. This paper considers the problem for controlling the density of replicas adaptively in dynamic networks. The goal of the problem is to adjust the number of replicas to a constant fraction of the current network size. This paper proposes algorithm inspired by the single species population model, which is a well-known population ecology model. The simulation results show that the proposed algorithm realize self-adaptation of the replica density in dynamic networks.

12. T. Horiyama, K. Iwama, and J. Kawahara:
"Automated Competitive Analysis of Online Problems", 電子情報通信学会 コンピュテーション研究会, 信学技報, vol.105, no.344, COMP2005-45, pp.5–12, 2005 年 10 月.
概要: In this paper we study the 2-Bin Exchangeable Online Knapsack Problem (2EOK) which is an extension of the 2-Bin Removable Online Knapsack Problem. We prove an optimal upper bound of $1/t$ for the competitive ratio of 2EOK, where t is a real root of $4x^3 + 5x^2 - x - 4 = 0$ ($t \approx 0.76850$ and $1/t \approx 1.3012$). To prove this result, we made a full use of computer programs as follows: For the algorithm we wish to prove the upper bound, we first construct an equivalent finite state diagram with about 300 states. Then for each state we generate a finite set of inequalities such that the competitive ratio at that state is at most $1/t$ if the set of inequalities do not have a real solution. The latter can be checked by Mathematica. The number of inequalities generated was approximately 600 in total, and our computation time was 30 minutes using Athlon XP 2600+.

13. 宮崎修一, 久保浩史, 高見好男, 四方敏明, 櫻井恒正, 山元伸幸, 河野典, 江原康生, 高倉弘喜, 沢田篤史, 中村素典, 岡部寿男, 北野正雄:
"KUINS 接続機器登録データベースの概要", 全国共同利用情報基盤センター 研究開発論文集, no.27, pp.47–51, 2005 年 10 月.
概要: 京都大学のキャンパスネットワーク KUINS では、利用されているネットワークやホスト情報を管理するためのデータベースを運用している。本稿では、データベースの仕様、データベースの運用方法、データベースを利用した業務の効率化、データベースの今後の拡張計画などを紹介する。

14. 片山喜章, 増澤利光, 和田幸一:
"根付き木ネットワーク上において局所情報のみで負荷分散を実現する自己安定アルゴリズムについて", 情報処理学会研究報告 (アルゴリズム, 2005-AL-103), Vol.2005, No.110, pp.35-40, 2005 年 11 月.
概要: 自己安定アルゴリズムとは, 任意のネットワーク状況からアルゴリズムの実行を開始しても, やがてあらかじめ与えられたネットワーク状況に到達する (解を求める) アルゴリズムである. 本稿では, 木ネットワーク中の各プロセスに任意の負荷 (整数) が与えられると, やがて任意のプロセス間の負荷の差が高々 1 (1-balancing) になる自己安定アルゴリズムを提案する. また, 提案アルゴリズムは負荷を表す情報のみで 1-balancing を実現した.

15. K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita:

"Transmitting Classical Information on the Quantum Network Efficiently", 電子情報通信学会 コンピュテーション研究会, 信学技報, vol.105, no.499, COMP2005-51, pp.15–20, 2005 年 12 月.
概要: The question in this paper is whether the quantum random access (QRA) coding, given by Ambainis et al., on the *network* is possible. This question is motivated by the network coding introduced by Ahlswede et al., which enables us to send classical information much more efficiently on the network by coding at intermediate nodes. We demonstrate that quantum network coding is possible for the QRA coding, by using a simple network model called the Butterfly network. In this network, there are two flow paths, s_1 to t_1 and s_2 to t_2, which shares a single bottleneck channel of capacity one. In the classical case, we can send two bits simultaneously, one for each path, in spite of the bottleneck. However, the quantum case makes this bottleneck much more severe than in the classical case because of the non-orthogonality of quantum states. We resolve this bottleneck and design a protocol which can send two classical bits from s_1 to t_1 (similarly from s_2 to ! t_2) but only one of them should be recovered.

16. S. Miyazaki, and Y. Okabe:
"Cheat-proof Serverless Network Games", Proc. the 4th International Symposium on Computing and Media Studies, pp.94–101, 2006 年 1 月.
概要: We consider playing online games on peer-to-peer networks, without assuming servers that control the execution of game. In such an environment, players may cheat the opponent by, for example, replacing the cards in hands illegally. The aim of this paper is to examine a possibility of excluding such cheatings. We show that by employing cryptographic techniques such as multiparty protocols, we can exclude some type of cheatings in some level. Finally, based on our discussion, we implement a cheat-proof network "Gunjin-Shogi", which is a kind of Japanese chess.

17. 阿武孝文, 堀山貴史, 岩間一雄:
"二段組合せ回路の最大動作率について", 冬の LA シンポジウム, 京都大学数理解析研究所講究録, pp.29.1–29.7, 2006 年 1 月.
概要: 回路の消費電力は 回路が消費する平均電力と最大電力の二つの観点から問題視される． 本稿では後者の最大電力に注目し，2 入力の AND ゲートと NOT ゲートから構成される 一般の n 入力の二段組合せ回路について，ゲート出力が変化したときのみ電力消費が発生するとして単純にモデル化を行った．更に入力変化に対応する消費電力の指標として回路の動作率を定義し，回路入力 $n > 4$ の場合について回路ごとに異なる最大動作率の下限を n の関数の形で示した． また $n = 4$ の場合には下限を実現する回路を提示し 下限がタイトであることを示した．

18. M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita:
"Efficient Transmission of the Information on the Quantum Network", 冬の LA シンポジウム, 京都大学数理解析研究所講究録, 2006 年 2 月.
概要:

19. 原口高裕, 泉泰介, 角川裕次, 増澤利光:
"分散データ構造スキップグラフの探索頻度偏りを考慮した拡張について", 情報処理学会研究報告（アルゴリズム, 2005-AL-105）, Vol.2006, No.30, pp.33-40, 2006 年 3 月.
概要: スキップグラフは資源の検索・挿入・削除を $O(\log n)$(n は資源数) で実行可能な分散データ構造であり，故障耐性，負荷分散特性に優れている．スキップグラフでは全資源を対等に扱っているため，各資源に対するアクセス頻度に偏りのあるシステムにおける検索時間は最適ではない．そこで本論文ではアクセス頻度の偏りに対応するため，各資源に対して検索頻度に応じた重みを付加し，重みの大きい資源に対しては高速にアクセス可能

となるようにスキップグラフを拡張する．本論文では，ある資源 i の重みを $w(i)$，全資源の重み総和を W とした際に，資源 i の検索時間が $O(\log(W/w(i)))$ となるような重み付け手法を提案する．また，資源の検索頻度が既知の場合に重みを割り当てる際，各資源の重みの比を検索頻度の比と同じに設定する事で検索時間が最小となることを示す．この方法は理論的に最適であるが，メンテナンスコストの観点からは実用的ではない．そこで，メンテナンスコストを考慮した重み付け手法もあわせて提案し，その有効性をシミュレーションにより評価する．

20. Yu Wu, Taisuke Izumi, Fukuhito Oosita, Hirotsugu Kakugawa, and Tosimitsu Masuzawa:
"An adaptive searching protocol in peer-to-peer systems based on probabilistic weak quorum system", 情報処理学会研究報告（アルゴリズム，2005-AL-105），Vol.2006, No.30, pp.41-48, 2006 年 3 月.
概要: In this paper, we propose a new P2P searching protocol: Adaptive Probabilistic Searching Protocol (APSP). It is an efficient extension of the original searching protocol based on Probabilistic Weak Quorum System (PWQS). APSP has much lower message complexity, which is proved the minimum, than the original protocol. And it is adaptive to network dynamics by estimating system parameters with an estimation algorithm we present in this paper. The estimation algorithm require small additional message cost and the simulation result proves its efficiency. With the estimation algorithm, APSP keeps the minimum message cost when network environment changes.

21. Kenya Sugihara, and Hiro Ito:
"Maximum-Cover Source-Location Problem with Objective Edge-Connectivity Three", 電子情報通信学会技術研究報告書 CAS2005-122, Vol. 105, No. 634, pp.25-29, 2006 年 3 月.
概要: Given a graph $G = (V, E)$, a set of vertices $S \subseteq V$ covers a vertex $v \in V$ if the edge-connectivity between S and v is at least a given number k. Vertices in S are called sources. The maximum-cover source-location problem, which is a variation of the source location problem, is to find a source set S with a given size at most p, maximizing the sum of the weight of vertices covered by S. In this paper, we show a polynomial-time algorithm for this problem in the case of $k = 3$ when a vertex-weighted and edge-capacitated undirected graph is input.

22. 高田智史, 伊藤大雄, 中村義作:
"毒まみれ半順序付き集合ゲームの必勝法", 電子情報通信学会技術研究報告書 CAS2005-120, Vol. 105, No. 634, pp.13-18, 2006 年 3 月.
概要: 組み合わせゲームの 1 つに，Poset(半順序付き集合) Game と呼ばれるものがある．Poset Game は有名な Nim から未解決の Chomp まで多様なゲームを含み，この研究から様々な面白い結果が得られている．Poset Game は単一の祖先 (毒節点) を持つ dag で表現できる．これの拡張として，毒節点が複数あり，しかも毒に重みを持たせ，与えられた体力を越えて毒を取った競技者が負けるというゲームが考えられる．我々はこのゲームの多項式時間で必勝手順を得る方法について考察する．

23. X. Han, K. Iwama, and G. Zhang:
"Packing Squares with Profits into a Rectangle", 電子情報通信学会総合大会講演論文集, 2006 年 3 月.
概要: In this paper, we study the following packing problem: Given a list of squares with profits, we are requested to pack a sublist of them into a rectangular bin to make profits in the bin as large as possible. The problem is strongly NP-hard and the best worst case ratio is $2 + \epsilon$ by Jansen and Zhang. Our results are as below: i) we

give a simple approximation algorithm with the worst case ratio $\frac{m+1}{m}+\epsilon$, where m is the number of big items in the optimal packing. ii) and further improve the worst case ratio into $\frac{5}{4}+\epsilon$ which is better than the current best result $2+\epsilon$ by Jansen and Zhang.

24. K. Iwama, and S. Tamaki:
"Increasing the Success Probability of PPSZ-type Satisfiability Testing", 電子情報通信学会 コンピュテーション研究会, 信学技報, vol.105, no.680, COMP2005-63, pp.1–6, 2006 年 3 月.
概要: Recently, [Iwama, Tamaki, SODA04] gave a new worst-case upper bound for 3SAT by modifying the PPSZ-type algorithm in [Paturi et. al., FOCS98] by making use of the local-search-type one in [Schoning, Algorithmica 02]. We propose a different kind of modification in this paper. Recall that the analysis of the first algorithm (denoted by **PPSZ**) assumes that each bit of the initial assignment coincides that of a satisfying assignment with probability one half. Our idea is that if we can increase this probability, i.e., if we can use a "better" initial assignment, then the success probability of **PPSZ** should increase. To get this better assignment we use the second algorithm (denoted by **SCH**). Note that the local search starts with a random assignment and gradually approaches to a satisfying assignment z. In the middle of this process, there should be the moment that the current assignment a^* is close to z and to use **PPSZ** with this assiginment a^* has a better success probability than to continue **SCH**. In this paper we prove that this conjecture is true under some assumption on the uniformity of probability.

C10: 情報基盤アルゴリズムとしてのメタヒューリスティクスの研究

茨木 俊秀 † 藤重 悟 ‡ 柳浦 睦憲 § 野々部 宏司 ¶ 巳波 弘佳 † 梅谷 俊治 ‖

† 関西学院大学 理工学部 情報科学科
〒 669-1337 兵庫県三田市学園 2-1
{ibaraki,miwa}@ksc.kwansei.ac.jp

‡ 京都大学 数理解析研究所
〒 606-8502 京都市左京区北白川追分町
fujishig@kurims.kyoto-u.ac.jp

§ 名古屋大学 大学院 情報科学研究科
〒 464-8603 名古屋市千種区不老町
yagiura@nagoya-u.jp

¶ 法政大学工学部システムデザイン学科
〒 184-8584 東京都小金井市梶野町 3-7-2
nonobe@k.hosei.ac.jp

‖ 電気通信大学電気通信学部システム工学科
〒 182-8585 東京都調布市調布ヶ丘 1-5-1
umetani@se.uec.ac.jp

1 はじめに

現在社会は、情報と通信技術に支えられた高度情報化社会と呼ばれているが、さらに成熟を加えて、知識社会へ変貌していくと言われている。そのためには、数々の課題を解決し、克服していかねばならないが、その過程で生ずる多くの問題が、数理的にはいわゆる組合せ問題、組合せ最適化問題の形に記述されることから、それらの解決を図るためのアルゴリズム研究が求められている。

我々の研究グループは、

1. 社会のさまざまな現象を数理的にモデル化する研究、
2. モデル化された問題を解決するためのアルゴリズムの研究、
3. 効果的なアルゴリズムを開発するための理論的基礎研究,

を行っている。第 1 のタイプの研究は、巳波が中心になって進めており、第 2 のタイプは柳浦、野々部および梅谷が中心、第 3 のタイプは藤重が主に担当している。茨木はこのグループの研究総括を担当しているが、主に第 2 のタイプの研究に参加している。

多くの組合せ問題あるいは組合せ最適化問題は、計算的には困難な問題であって、理論的には NP 完全問題あるいは NP 困難問題のクラスに属する。これらの問題を現実的な意味で解決するには、効果的なアルゴリズムを可能にする数学的構造を見つけ出し、そのような問題へのモデル化を行うか、厳密な最適解の導出を目指すのではなく、良質の近似解を高速に求めるという目標に切り替えて、そのための近似アルゴリズムを開発する、という二つのアプローチが考えられる。近似アルゴリズムの研究は、近年きわめて盛んになっているが、このグループでは、メタヒューリスティクスの枠組みで、局所探索に立脚した種々のアルゴリズムに重心をおき、実用的な利用に耐えるようなアルゴリズムの開発を行ってきた。

本報告では、今年度に得られた研究成果を章ごとに説明する。第 2〜7 章はタイプ 2 の研究、第 8 章はタイプ 1 に分類される。

2 時間枠つき配送計画問題

時間枠つき配送計画問題は，複数台の車両を用いて荷物の集配を行う際，車両の容量や顧客の指定時間枠などの種々の制約を満たしつつ，配送に伴うコストの最小化を図る問題である．これは，宅配などへの直接的な応用だけでなく，種々のスケジューリング問題なども含む非常に汎用性の高

い問題である．この問題に対し，時間枠に関するペナルティ関数を導入した汎用的な問題を提案し，その最小化問題に対して動的計画法に基づく高速なアルゴリズムの開発に成功した．このアイデアを組み込んだメタ戦略アルゴリズムとして，反復局所探索法と適当的多スタート局所探索法の 2 種を提案し，代表的なベンチマーク問題例に対して一定の成果をおさめることに成功した．また，ある企業における在庫計画を含むスケジューリング問題を時間枠つき配送計画問題に定式化することで提案手法を適用し，現実のスケジュールよりも優れたスケジュールを立てることにも成功している．

3　長方形パッキング問題

長方形パッキング問題は，与えられた n 個の長方形を互いに重なりなく配置し，それに伴う種々の目的関数の最適化を図る問題である．目的関数としては，例えば

- 全ての長方形を囲む面積の最小化，
- 幅の決まった容器に全ての長方形を詰め込むときの高さの最小化，
- 大きさの決まった容器に長方形を詰め込むときに利用した容器の数の最小化

など，様々なものがある．本研究ではとくに配置の位置に伴うコストを導入した汎用化を考えた．このようなコストを導入することで，各仕事に最早開始時刻や納期のあるスケジューリング問題の一種などを扱うことができる．この問題において，我々は以前配置コストの最小化に対する高速アルゴリズムの開発に成功していた．今回は，局所探索における探索解とその近傍内の解の構造が近いことを利用し，配置コストの最小値の変化量の計算をさらに高速化することに成功した．これを反復局所探索法に組み込むことで，従来のパッキング問題に対するベンチマーク問題例に対してよりよい成果を上げるとともに，スケジューリング問題に対しても一定の成功を収めることができた．最後に，面積最小化問題の問題例 (長方形数 100) に対する計算結果の例を図 2.1 に示しておく．

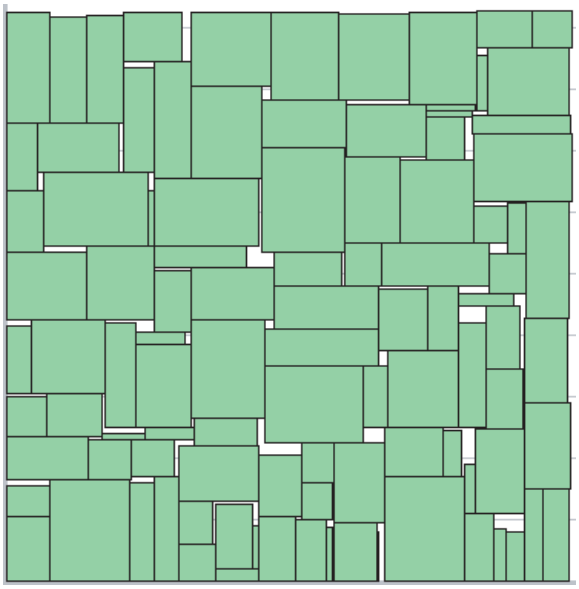


図 2.1: 面積最小化問題に対する計算結果の例（長方形数 100，充填率 96%）

4　一般化割当問題

一般化割当問題は，与えられた n 個の仕事を m 個のエージェントに割り当てる問題である．各仕事とエージェントのペアに対してコストと資源利用量が与えられ，また，各エージェントには利用可能資源量が与えられる．この時，各エージェントにおける資源制約を満たしつつ，割り当てに伴う総コストの最小化を図ることが目的である．割り当てという基本的な構造を対象としているため，様々な問題の基本構造を捉えた問題として非常に重要な問題である．この問題に対しては，我々は以前排除連鎖法 (ejection chains) に基づく高性能アルゴリズムの開発に成功していた．今回は，このアルゴリズムにさらにパス再結合法 (path relinking) などのアイデアを追加することで，大幅な性能改善に成功した．得られたアルゴリズムの性能は極めて高く，$n = 1600$, $m = 80$ までの大規模なベンチマーク問題例に対する計算結果では，現存する他のアルゴリズムの追随を許さない性能を持つことが確認できている．

表 4 に計算結果の一部を示す．比較対象の多い中規模までの問題例に対する計算結果である．表中，PREC は新たに提案した手法であり，それ以外は既存の代表的なメタ戦略アルゴリズム等の比較対象である．表の数値は制限時間内にアルゴ

表 2.1: 一般化割当問題に対するメタ戦略の計算結果 ($n = 100, 200$ の問題例に対して，それぞれ 150 秒，300 秒実行，ただし RLS,CB,DF は除く)

type	n	m	LB	PREC	TSEC	BVDS-l	BVDS-j	VDS	RA	LKGG	NI	RLS	CB	DF	CPLEX
C	100	5	1930	*1931	*1931	*1931	*1931	*1931	1938	*1931	*1931	1942	*1931	*1931	*1931
C	100	10	1400	*1402	*1402	*1402	1403	*1402	1405	1403	1403	1407	1403	*1402	*1402
C	100	20	1242	*1243	*1243	1244	1244	1246	1250	1245	1245	1247	1244	*1243	*1243
C	200	5	3455	*3456	*3456	*3456	3457	3457	3469	3457	3465	3467	3458	3457	*3456
C	200	10	2804	2807	*2806	2809	2808	2809	2835	2812	2817	2818	2814	2807	*2806
C	200	20	2391	*2391	2392	2401	2400	2405	2419	2396	2407	2405	2397	*2391	*2391
D	100	5	6350	*6353	6357	6358	6362	6365	—	6386	6415	6476	6373	6357	6358
D	100	10	6342	6356	6358	6367	6370	6380	6532	6406	6487	6469	6379	*6355	6381
D	100	20	6177	*6211	6221	6275	6245	6284	6428	6297	6368	6358	6269	6220	6280
D	200	5	12741	*12744	12746	12755	12755	12778	—	12788	12973	12923	12796	12747	12750
D	200	10	12426	*12438	12446	12480	12473	†12496	12799	12537	12889	12746	12601	12457	12457
D	200	20	12230	*12269	12284	12440	12318	†12335	12665	12436	12793	12617	12452	12351	12393
E	100	5	12673	*12681	12682	*12681	12682	12685	12917	††12687	‡12686	12836	N.A.	*12681	*12681
E	100	10	11568	*11577	*11577	11585	11599	11585	12047	††11641	‡11590	11780	N.A.	11581	11593
E	100	20	8431	8444	*8443	8499	8484	8490	9004	††8522	‡8509	8717	N.A.	8460	8565
E	200	5	24927	*24930	*24930	24942	24933	24948	25649	††25147	‡24958	25317	N.A.	24931	*24930
E	200	10	23302	23310	*23307	23346	23348	23340	24717	††23567	‡23396	23620	N.A.	23318	23321
E	200	20	22377	*22379	22391	22475	22437	†22452	24117	††22659	‡22551	22779	N.A.	22422	22457

†Sun Ultra 2 Model 2300 で 1,000 秒実行
††Sun Ultra 2 Model 2300 で 20,000 秒実行
‡Sun Ultra 2 Model 2300 で 5,000 秒実行
⋆ 計算時間は文献 [1] を参照
⋆⋆ 文献 [2] の計算結果を引用
⋆⋆⋆ 文献 [3] の結果を引用

リズムが得た最良の目的関数値であり，最小化問題なので値が小さいほどよい（なお LB は最適値の下界値である）.「*」印は表中のアルゴリズムの中で最良の結果が得られたことを示す．表より，PREC の列のほとんどに「*」印がついており，提案手法の性能が極めて高いことが確認できる．

参考文献

[1] Yagiura, M., Ibaraki, T., and Glover, F., An ejection chain approach for the generalized assignment problem, *INFORMS J. on Comput.*, 16, 133, 2004.

[2] Chu, P.C. and Beasley, J.E., A genetic algorithm for the generalized assignment problem, *Computers Oper. Res.*, 24, 17, 1997.

[3] Díaz, J.A. and Fernández, E., A tabu search heuristic for the generalized assignment problem, *Eur. J. Oper. Res.*, 132, 22, 2001.

5 正方形被覆問題

正方形被覆問題は，2 次元平面上に与えられた複数の点すべてを覆い尽くすように，大きさの決まった正方形を配置する問題であり，使用する正方形の数を最小化することが目的である．この問題は，公共施設の配置や VLSI 設計，画像処理分野などに応用を持つ．本研究では，従来の定式化に容量制約を追加した問題を考え，集合被覆アプローチ，メタヒューリスティクスの 2 種類の解法を提案し，その性能を評価するために計算機実験を行った．

集合被覆アプローチは，1 つの正方形で被覆することのできる極大点集合を予めすべて列挙しておき，問題を集合被覆問題として定式化する方法である．極大点集合の列挙には，重み付き極大クリーク列挙に対する出力線形アルゴリズムを用い，効率の良い列挙を行っている．アルゴリズムの性能は，列挙する極大点集合の数に大きく依存することが予想され，計算実験によりこれを確認した．容量制約がない問題例や容量制約が非常に厳しい問題例，点の分布が疎である問題例に対しては，列挙の数が少なく抑えられる傾向にあるため集合被覆アプローチは効果的である．逆に，容量制約

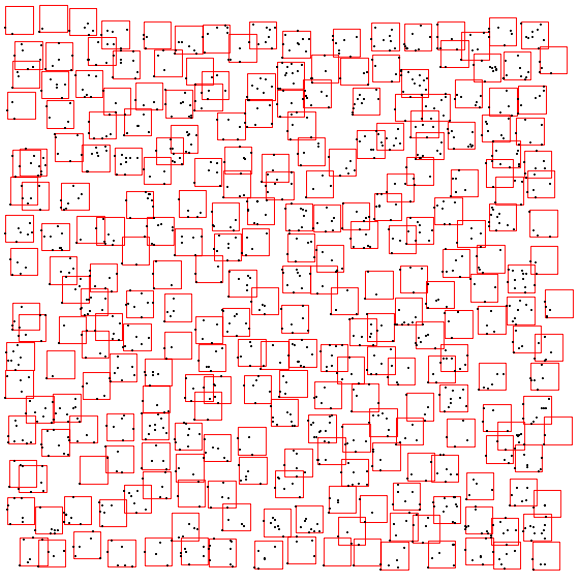


図 2.2: 正方形被覆問題に対する計算結果の例（点数 1600，正方形数 263）

がある程度厳しく，さらに点が平面上密に分布している場合には，列挙すべき極大点集合が多くなり，非実用的となる．

一方，メタヒューリスティクスによるアプローチでは，まず欲張り法を用いて実行可能解を生成した後，正方形の数を 1 つずつ減らしていく．すなわち，実行可能解から正方形を 1 つ取り除いた後，正方形の数を増やすことなく，これが実行可能となるように修正を加える．解の修正にはメタヒューリスティクスを用い，実行可能解を得ることができる限り，正方形を取り除き解を修正する操作を繰り返す．本研究では，アルゴリズムの基本となる局所探索法に，タブー探索，散布探索などのアイデアを取り入れ，高性能化を実現した．また，初期実行可能解を生成するための欲張り法は，近似比 4 を持つものであり，とくに容量制約がない問題例に対しては近似比 2 を持つ．計算実験の結果，メタヒューリスティクスアプローチは，その性能が問題タイプに大きく依存しないことが分かり，集合被覆アプローチが有効に働かないタイプの問題例に対しても良質の解を求めることができた．最後に，点数 1600 の問題例に対する計算結果の例を図 2.2 に示しておく．

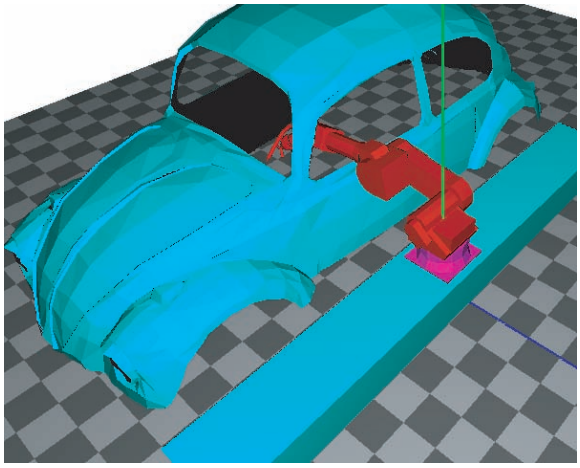


図 2.3: 産業用アームロボットの例 (6 軸)

6　ロボット動作計画問題

ロボット動作計画問題とは，ロボットと障害物の形状と，それらの位置・姿勢が与えられたときに，ロボットの初期姿勢から目的姿勢に至る動作経路を求める問題である．

回転軸を含むロボットの場合，動作経路を求めるために，各々の姿勢に対してロボットと障害物が衝突するかどうかを調べる必要がある．しかし，ロボットの取り得る姿勢の数は，自由度の数に対して指数関数的に増加するため，全ての姿勢を調べることは困難である．そこで，限られた数の姿勢に対してロボットが障害物と衝突するかどうかを調べ，その情報をもとに動作経路の探索を行う確率的・発見的手法がいくつか提案されている．

本研究では，メタヒューリスティクスの 1 つであるパス再結合法の考えにもとづき，初期姿勢・目的姿勢の各々に到達可能な姿勢からなる 2 つ集合を用意し，各集合から仮の初期姿勢と目的姿勢 (もしくは目的姿勢と初期姿勢) の組を選んで局所探索法を適用する手続きを繰返し行う，双方向局所探索法を提案した．また，産業用アームロボット (6 軸)(図 2.3) に対する数値シミュレーションを通じて，提案解法を用いて障害物と衝突しない動作経路を短時間に見つけられることを確かめた．

7　多角形ストリップパッキング問題

多角形ストリップパッキング問題は，n 個の多角形と幅 W(可変)，高さ H (固定) の長方形の母材が与えられた際に，全ての多角形を母材上に互いに重なりなく配置するという制約の下で，必要な母材の幅 W を最小化する問題である．この問題は，機械部品の板取や服の型紙の配置など，実用的な問題とも密接な関わりを持ち，幾何学や組合せ最適化の分野で古くから研究されてきたが，多角形の複雑な形状を扱うのに多大な計算時間を要するため，実用的な解法はほとんどなかった．しかし，近年では，計算幾何や数理計画の分野の発展や，コンピュータの性能の向上も相まって，実用的な規模の例題に対して，歩留りの良い配置計画を求める解法がいくつか提案されている．

本研究では，母材の幅 W を固定した上で，各多角形ペアの重なり度の総和を最小化する問題を考え，誘導局所探索法 (guided local search) に基づくメタヒューリスティクス解法を提案し，その性能を評価するために計算機実験を行った．ここで，各多角形ペアの重なりをなくすために必要な，水平もしくは垂直方向における最小移動距離を重なり度と考える．

メタヒューリスティクス解法では，多角形を一つ選んで，水平・垂直方向へ移動する近傍操作を考え，それらの中で他の多角形との重なり度の総和が最小となる配置へ移動する手続きを繰返し適用することで，新たな近傍解を生成する．今回は，多角形を水平・垂直方向にしか移動しないという，近傍操作の性質を利用して，他の多角形との重なり度の総和が最小となる配置を高速に計算する手法を提案した．また，誘導局所探索法を用いて，評価関数を適応的に変形しながら局所探索法を繰返し適用することで，探索の多様化を実現している．ここでは，各多角形ペアの重なり度に重み係数を掛けた評価関数を考え，直前の局所探索法で得られた解において，重なりを持つ多角形ペアがあれば，その重み係数を増加させて，同一の多角形ペアが重なり続ける状況を回避している．

計算機実験では，いくつかの良く知られたベンチマーク問題例に対して，提案するメタヒューリスティクス解法を適用し，いずれの問題例に対しても 2,3 分程度の計算時間で，最良解に近い充填率の配置計画を求めることができた．最後に，シャツの型紙を配置する問題例 (製品数 99) に対する計算結果を図 2.4 に示しておく．

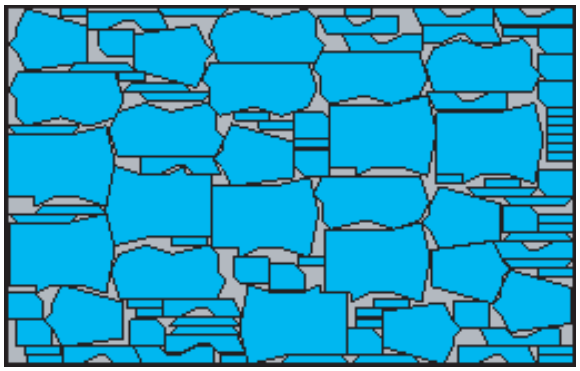


図 2.4: 多角形ストリップパッキング問題に対する計算結果の例（製品数 99，充填率 85%）

8　現実ネットワークのモデル構築

インターネット，Web グラフをはじめ，経済，マーケティング，流行現象，伝染病の伝播，生態系，人間関係など，多くの領域で「ネットワーク」が見られる．近年のコンピュータ技術の発達によるデータ収集・解析能力の向上によって，このような現実のネットワークの性質が詳細に分析できるようになってきた．その結果，現実のネットワークはまったくランダムなネットワークとは異なり，特徴的な性質を持つということが分かってきた．このようなネットワークの特性を調べることにより，様々な応用に際してアルゴリズムを適用する範囲を限定でき計算量の削減につなげられる可能性がある．そこで，本研究では，主に現実のネットワークの特性を反映する適切な数理モデルの構築と解析に重点を置き，その結果として，現実のネットワークにおいて，メタヒューリスティックスをはじめ，様々なアルゴリズムの計算量を削減することを目指している．

本年度は，現実の情報通信ネットワークなどの自律的に形成されるネットワークの特性を反映した形成モデルを解析した．具体的には，携帯電話のトラフィックと加入者数の関係を実データに基づいて解析し，ネットワーク形成モデルを構築した．その結果，携帯電話加入者が形成するネット

ワークを，グラフから次数の高い点が優先的に選び出された点集合から得られる生成部分グラフと捉えることにより，実データの傾向と整合性を持つモデルが得られた．一方，ランダムな点の選択では整合性を持たせることはできない．したがって，携帯電話の加入は，人間関係においてハブとなる人間から優先的に起こったと解釈することができる．また，観測されたグラフ（生成部分グラフ）の次数分布のべき指数から，元のグラフの次数分布のべき指数を推定することもできることを示した．つまり，携帯電話加入者ネットワークデータから人間関係ネットワーク全体の特性を推定できることを示した．

9　むすび

本特定領域2年目として、本年度の研究は、初年度の成果の上に立ってそれらを発展させることに主眼をおいた。その結果、上述の成果について、大部分を論文としてまとめることができた。次年度以降、これらの研究をさらに継続し、多様な問題の解決に利用できるアルゴリズムの理論的基盤の確立と、ソフトウエアとしての開発をさらに進めていく予定である。

研究業績一覧

著書

1. S. Fujishige and M. Yagiura, guest editors: “Pacific Journal of Optimization, Vol. 1, No. 3”, Yokohama Publishers, 2005.

2. T. Ibaraki, K. Nonobe and M. Yagiura, eds.: “Metaheuristics: Progress as Real Problem Solvers”, Springer, NY, 2005.
   概要: The framework of metaheuristics can produce robust and efficient algorithms for many computationally hard problems in real-world applications. This book comprises the papers carefully selected from those presented at the Fifth Metaheuristics International Conference (MIC2003). The book features those papers describing applications of metaheuristics as real problem solving tools, and also contains those discussing methodologies of metaheuristics.

3. S. Imahori, M. Yagiura, H. Nagamochi（分担執筆）:
   “Practical Algorithms for Two-Dimensional Packing”, in: T.F. Gonzalez, ed., Handbook of Approximation Algorithms and Metaheuristics, Chapman & Hall/CRC in the Computer & Information Science Series, （刊行予定）.
   概要: 長方形パッキング問題に対する実用的解法に焦点を当て，調査を行った．とくに，そのような解法の基礎となる解表現に対して詳しく調べ，種々の発見的手法を体系的にまとめた．また，近似度に対する理論的成果の調査も行った．さらに，多角形パッキング問題に対する最近のアルゴリズムの調査結果もまとめた．

4. M. Yagiura and T. Ibaraki（分担執筆）:
   “Generalized Assignment Problem”, in: T.F. Gonzalez, ed., Handbook of Approximation Algorithms and Metaheuristics, Chapman & Hall/CRC in the Computer & Information Science Series, （刊行予定）.
   概要: 一般化割当問題に対する近似解法を中心に，古典的なアルゴリズムから最新のものも含めて調査を行い，代表的なメタ戦略アルゴリズムの比較結果をまとめた．また，分枝限定法に基づく近似解法についても述べ，さらに，近似度に対する理論的な成果に対する調査結果もまとめた．

学術論文

1. E. Boros, T. Ibaraki, H. Ichikawa, K. Nonobe, T. Uno and M. Yagiura:
   “Heuristic approaches to the capacitated square covering problem”, Pacific Journal of Optimization, 1, 465–490, 2005.
   概要: We consider the capacitated square covering problem (CSCP), which is described as follows. Given a set of

points, each having a demand, in the two-dimensional Euclidean plane, we find the minimum number of squares with the same size and capacity to cover all the points under the capacity constraint. As CSCP is NP-hard, we focus on heuristic algorithms in this paper. We first test a set covering approach, in which a CSCP is solved as a set covering problem. Since its performance is not always satisfactory, though it works quite well for a certain type of instances, we then propose a more robust metaheuristic approach. In this approach, starting with a feasible solution using a rather large number of squares, we remove squares one by one. After each removal of a square, the resulting infeasible solution is repaired by a local search method so that it becomes feasible. To increase the performance, we incorporate the idea of tabu search and scatter search as well as an adaptive control mechanism of penalty weights. Computational results on randomly generated instances with up to 1600 points indicate the effectiveness of our approaches.

2. H. Hashimoto, T. Ibaraki, S. Imahori and M. Yagiura:
"The Vehicle Routing Problem with Flexible Time Windows and Traveling Times", Discrete Applied Mathematics, (掲載予定)
.
概要: We generalize the standard vehicle routing problem by allowing soft time window and soft traveling time constraints, where both constraints are treated as cost functions. With the proposed generalization, the problem becomes very general. In our algorithm, we use local search to determine the routes of vehicles. After fixing the route of each vehicle, we must determine the optimal start times of services at visited customers. We show that this subproblem is NP-hard when cost functions are general, but can be efficiently solved with dynamic programming when traveling time cost functions are convex even if time window cost functions are non-convex. We deal with the latter situation in the developed iterated local search algorithm. Finally we report computational results on benchmark instances, and confirm the benefits of the proposed generalization.

3. T. Ibaraki, S. Imahori, M. Kubo, T. Masuda, T. Uno and M. Yagiura:
"Effective Local Search Algorithms for Routing and Scheduling Problems with General Time-Window Constraints", Transportation Science, 39, 206–232, 2005.
概要: We propose local search algorithms for the vehicle routing problem with soft time window constraints. The time window constraint for each customer is treated as a penalty function, which is very general in the sense that it can be non-convex and discontinuous as long as it is piecewise linear. In our algorithm, we use local search to assign customers to vehicles and to find orders of customers for vehicles to visit. It employs an advanced neighborhood, called the cyclic exchange neighborhood, in addition to standard neighborhoods for the vehicle routing problem. After fixing the order of customers for a vehicle to visit, we must determine the optimal start times of processing at customers so that the total penalty is minimized. We show that this problem can be efficiently solved by using dynamic programming, which is then incorporated in our algorithm. We then report computational results for various benchmark instances of the vehicle routing problem. The generality of time window constraints allows us to handle a wide variety of scheduling problems. As such an example, we mention in this paper an application to a production scheduling problem with inventory cost, and report computational results for real

world instances.

4. T. Ibaraki, Yann Vaxès and Xiao-gung Yang:
"Lowering eccentricity of a tree by node-upgrading", Networks, 45, 232-239, 2005.
概要: The eccentricity lowering problem is to reduce the eccentricity of a network by upgrading some nodes (i.e., shrinking the lengths of the edges incident to such nodes). We consider two types of node-upgrading strategies, i.e., a continuous upgrading strategy and a discrete upgrading strategy, where the improvement under the first strategy is a continuous variable, and the improvement under the second strategy is a fixed amount. These problems are hard even to approximate, for general graphs. Therefore we restrict our attention to graphs with simple structures. Assuming that the graph $G = (V, E)$ is a tree, we show that the eccentricity lowering problem under the continuous node-upgrading strategy can be reduced to the eccentricity lowering problem under the continuous edge-upgrading strategy, and can be solved by an $O(|V| \log |V|)$ time algorithm. We also show that the problem for a tree is NP-hard under the discrete upgrading strategy, but admits a fully polynomial approximation scheme, if the graph is a line.

5. S. Imahori, M. Yagiura and T. Ibaraki:
"Improved Local Search Algorithms for the Rectangle Packing Problem with General Spatial Costs", European Journal of Operational Research, 167, 48-67, 2005.
概要: The rectangle packing problem with general spatial costs is to pack given rectangles without overlap in the plane so that the maximum cost of the rectangles is minimized. This problem is very general, and various types of packing problems and scheduling problems can be formulated in this form. For this problem, we have previously presented local search algorithms using a pair of permutations of rectangles to represent a solution. In this paper, we propose speed-up techniques to evaluate solutions in various neighborhoods. Computational results for the rectangle packing problem and a real-world scheduling problem exhibit good prospects of the proposed techniques.

6. S. Imahori, M. Yagiura, S. Umetani, S. Adachi and T. Ibaraki:
"Local Search Algorithms for the Two Dimensional Cutting Stock Problem with a Given Number of Patterns", T. Ibaraki, K. Nonobe and M. Yagiura, eds., Metaheuristics—Progress as Real Problem Solvers, Springer, 181–202, 2005.
概要: We consider the two-dimensional cutting stock problem that arises in many applications in industries. In recent industrial applications, it is argued that the setup cost for changing patterns becomes more dominant and it is impractical to use many different cutting patterns. Therefore, we consider the pattern restricted two-dimensional cutting stock problem, in which the total number of applications of cutting patterns is minimized while the number of different cutting patterns is given as a parameter n. For this problem, we develop local search algorithms. As the neighborhood size plays a crucial role in determining the efficiency of local search, we propose to use linear programming techniques for the purpose of restricting the number of solutions in the neighborhood. In this process, to generate a cutting pattern, it is required to place all the given products (rectangles) into the stock sheet (two-dimensional area) without mutual overlap. For this purpose, we develop a heuristic algorithm using an existing rectangle packing algorithm with the sequence pair coding scheme. Finally, we generate

random test instances of this problem and conduct computational experiments, to evaluate the effectiveness of the proposed algorithms.

7. 今堀慎治，梅谷俊治:
“切出し・詰込み問題とその応用 — (2) 長方形詰込み問題”, オペレーションズ・リサーチ, 50, 335–340, 2005 年 5 月.
概要: 長方形詰込み問題は，様々な大きさの長方形を二次元平面上に重なりなく配置する問題であり，幾何学や組合せ最適化の分野で古くから研究されてきた．本稿では，長方形詰込み問題の様々なバリエーションと解法について解説する．

8. 増田直紀, 巳波弘佳, 今野紀雄:
“構造と機能から見た複雑ネットワーク”, 応用数理, Vol. 16, No. 1, 2006 年 3 月.
概要: ネットワークの研究は，構造の解明と機能の解明に大きく分類できる．前者はスモールワールド性やスケールフリー性など現実のネットワーク形状の特徴の研究が目的である．後者は，ウィルス感染など，ネットワーク上で起こる現象の研究が目的である．構造と機能という二つの観点から，複雑ネットワークに関する研究動向をサーベイし解説した．

9. Y. Matsuoka and S. Fujishige:
“Practical efficiency of maximum flow algorithms using MA orderings and preflows”, Journal of the Operations Research Society of Japan, 48, 297–307, 2005.
概要: 最大隣接順序を用いて藤重によって提案された多項式時間の最大フローアルゴリズムに対して、プリフローの技法を加えて新たなアルゴリズムを考案し、計算機実験によって、その有効性を検証した。

10. K. Nonobe and T. Ibaraki:
“A metaheuristic approach to the resource constrained project scheduling with variable activity durations and convex cost functions”, J. Jozefowska and J. Weglarz (eds.): Perspectives in Modern Project Scheduling, Springer, （出版予定）.
概要: We introduce a generalized model of the resource constrained project scheduling problem (RCPSP). It features that (i) the duration of and (ii) the objective is to minimize a convex function of time-lag costs, where a time-lag cost is charged according to the difference between the san activity is not constant, but can vary in a specified range,tart/completion times of activities. These features achieve the flexibility of the model. It is known that, in the RCPSP, resource constraints can be replaced by some precedence constraints appropriately defined between the activities that require a common scarce resource. If we remove resource constraints by precedence constraints, our problem can be formulated as the dual problem of a minimum cost flow problem, and thus can be solved efficiently. Exploiting this property, we design a heuristic algorithm based on local search. We conducted computational experiments with benchmark instances to minimize the weighted earliness-tardiness costs, as well as instances in which activity-crashing or relaxation of temporal constraints are allowed. These results indicate the usefulness of our generalized RCPSP model and the proposed algorithm.

11. S. Umetani, M. Yagiura and T. Ibaraki:
“One-dimensional cutting stock problem with a given number of setups: A hybrid approach of metaheuristics and linear programming”, Journal of Mathematical Modelling and Algorithms, （掲載予定）.
概要: One-dimensional cutting stock problem (1D-CSP) is one of the representative combinatorial optimization problems, which arises in many industrial applications. Since the setup costs for switching different cutting patterns become more dominant in recent cutting industry, we consider a variant of 1D-CSP, called the pattern restricted problem (PRP), to mini-

mize the number of stock rolls while constraining the number of different cutting patterns within a bound given by users. For this problem, we propose a local search algorithm that alternately uses two types of local search processes with the 1-add neighborhood and the shift neighborhood. To improve the performance of local search, we incorporate it with linear programming (LP) techniques, to reduce the number of solutions in each neighborhood. A sensitivity analysis technique is intorduced to solve a large number of associated LP problems quickly. Through computational experiments, we observe that the new algorithm obtains solutions of better quality than those obtained by other existing approaches.

12. 梅谷俊治，今堀慎治:
“切出し・詰込み問題とその応用 — (1)1 次元資材切出し問題”, オペレーションズ・リサーチ, 50, 270–276, 2005 年 4 月.
概要: いくつかの対象物を，互いに重ならないように与えられた領域内に配置する問題は，切出し・詰込み問題と呼ばれ，多くの分野に応用を持つ代表的な生産計画問題の一つである．本稿では，代表的な切出し・詰込み問題である 1 次元資材切出し問題について解説する．

13. 梅谷俊治，今堀慎治:
“切出し・詰込み問題とその応用 — (3) 多角形詰込み問題”, オペレーションズ・リサーチ , 50, 403–408, 2005 年 6 月.
概要: 多角形詰込み問題は，様々な形状・大きさの多角形を二次元平面状に重なりなく配置する問題であり，機械部品の板取や，服の型紙の配置など，実用的な問題とも密接な関わりを持つ．本稿では，近年，盛んに研究されている，計算幾何や数理計画の手法に基づく実用的な解法を中心に解説する．

14. M. Yagiura, T. Ibaraki and F. Glover:
“A Path Relinking Approach with Ejection Chains for the Generalized Assignment Problem”, European Journal of Operational Research, 169, 548–569, 2006.
概要: The generalized assignment problem is a classical combinatorial optimization problem known to be NP-hard. It can model a variety of real world applications in location, allocation, machine assignment, and supply chains. The problem has been studied since the late 1960s, and computer codes for practical applications emerged in the early 1970s. We propose a new algorithm for this problem that proves to be more effective than previously existing methods. The algorithm features a path relinking approach, which is a mechanism for generating new solutions by combining two or more reference solutions. It also features an ejection chain approach, which is embedded in a neighborhood construction to create more complex and powerful moves. Computational comparisons on benchmark instances show that the method is not only effective in general, but is especially effective for types D and E instances, which are known to be very difficult.

15. M. Yagiura, M. Kishida and T. Ibaraki:
“A 3-Flip Neighborhood Local Search for the Set Covering Problem”, European Journal of Operational Research, 172, 472–499, 2006.
概要: The set covering problem (SCP) calls for a minimum cost family of subsets from n given subsets, which together covers the entire ground set. In this paper, we propose a local search algorithm for SCP, which has the following three characteristics. (1) The use of 3-flip neighborhood, which is the set of solutions obtainable from the current solution by exchanging at most three subsets. As the size of 3-flip neighborhood is $O(n^3)$, the neighborhood search becomes expensive if implemented naively. To overcome this, we propose an efficient implementation that reduces the number of candidates in the

neighborhood without sacrificing the solution quality. (2) We allow the search to visit the infeasible region, and incorporate the strategic oscillation technique realized by adaptive control of penalty weights. (3) The size reduction of the problem by using the information from the Lagrangian relaxation is incorporated, which is indispensable for solving very large instances. According to computational comparisons on benchmark instances with other existing heuristic algorithms for SCP, our algorithm performs quite effectively for various types of problems, especially for very large-scale instances.

研究会等

1. M.Aida, K.Ishibashi, C.Takano, H.Miwa, K.Muranaka, A.Miura:
"Cluster structures in topology of large-scale social networks revealed by traffic data", IEEE GLOBECOM 2005, 2005年11月.
概要: 実際の携帯電話トラフィックデータと整合性のあるネットワーク生成モデルを提案し，その性質を解析した．さらに，観測された部分グラフの次数分布から，元のグラフの次数分布を推定する方法を提案した．

2. D.Harada, T.Ciyonobu, H.Miwa:
"A Probabilistic Analysis of a Network Model Based on a Generalization of the Polya 's Urn Problem", IFORS 2005, 2005年7月.
概要: 現実のネットワークの生成モデルである閾値モデルにおいて，この重み分布が生成されるメカニズムを調べ，重みが「優先的選択」に従って増加する自然なモデルにおいて，重み分布が幾何分布に確率収束することを数学的に厳密に証明した．さらに，重みが幾何分布に従う場合，生成されるグラフがスケールフリーとなることを示した．

3. H. Hashimoto, M. Yagiura and T. Ibaraki:
"An iterated local search algorithm for the time-dependent vehicle routing problem with time windows", Proceedings of the 6th Metaheuristics International Conference (MIC 2005), 506–513, 2005.
概要: We generalize the standard vehicle routing problem with time windows (VRPTW) by allowing both traveling times and traveling costs to be time-dependent, and propose an iterated local search algorithm. Our generalization can treat such situation as rush-hour traffic jam, and moreover, our time window constraint allows each customer to have more than one time window. In our local search procedure, after fixing a route of each vehicle, we must compute an optimal time schedule of each route. We show that this subproblem can be efficiently solved by dynamic programming, which is then incorporated in the local search algorithm. We further propose a filtering method that reduces the sizes of neighborhoods, based on the fact that there are many solutions having no prospect of improvement. Finally, we develop an iterated local search algorithm incorporating all these ingredients. We report computational results on benchmark instances of the VRPTW and artificially generated instances of the time-dependent VRPTW, and discuss the performance of our iterated local search algorithm against existing methods and the benefits of the proposed generalization.

4. S. Imahori, M. Yagiura and T. Ibaraki:
"Variable neighborhood search for the rectangle packing problem", Proceedings of the 6th Metaheuristics International Conference (MIC 2005), 532–537, 2005.
概要: We consider the following rectangle packing problem: Given a set of rectangular items, place all of them into an open-ended two-dimensional bin orthogo-

nally without mutual overlap. This is called the strip packing problem and is known to be NP-hard. For this problem, we propose a variable neighborhood search algorithm based on a coding scheme with a particular grid structure called Bounded Sliceline Grid (BSG). A coded solution is an assignment of rectangular items into BSG, and a placement is computed from a coded solution with a decoding algorithm. In order to find a good coded solution, we use local search technique with some ideas to improve the efficiency; e.g., we utilize the critical paths to reduce the size of a neighborhood without sacrificing the solution quality. Moreover, we propose a new decoding algorithm for local search that can evaluate a coded solution in a neighborhood in amortized constant time.

5. H.Miwa, N.Masuda, N.Konno:
"Scale-free networks and network mining problems", IFORS 2005, 2005 年 7 月.
概要: 現実のネットワークの様々な生成モデルについて解説した．さらに，コミュニティ探索など，複雑ネットワークの研究でよく見られるネットワーク上の最適化問題について解説した.

6. S. Umetani, T. Kurakake, Y. Suzuki and M. Higashi:
"A bi-directional local search for robot motion planning problem with many degrees of freedom", Proceedings of the 6th Metaheuristics International Conference, 878–883, 2005 年 8 月.
概要: The motion planning problem is the problem of finding a collision-free path of a robot from the start configuration to the goal configuration. We consider practical motion planning problems with many degrees of freedom, and propose a variant of the path relinking approach, called the bi-directional local search (BLS). The proposed algorithm repeatedly applies a simple local search between pairs of initiating and guiding configurations. We also develop two heuristic algorithms based on SA and ILS, and compare efficiency of three algorithms through computational experiments on an instance of a welding articulated robot with six degrees of freedom.

学会大会等

1. S. Imahori, M. Yagiura and T. Ibaraki:
"An effective local search algorithm for strip packing problem", The IFORS Triennial 2005 Conference, p. 47, 2005.

2. T. Imamichi, M. Kenmochi, K. Nonobe, M. Yagiura and H. Nagamochi:
"Branch-and-bound algorithms for rectangular strip packing and perfect packing problems", ESICUP (EURO Special Interest Group on Cutting and Packing) 2nd Meeting, p. 23, 2005.

3. M. Kenmochi, T. Imamichi, K. Nonobe, M. Yagiura and H. Nagamochi:
"Exact Algorithms for the 2-Dimensional Strip Packing Problem with Rotations", The IFORS Triennial 2005 Conference, p. 36, 2005.

4. 松本一輝、巳波弘佳、茨木俊秀:
"段ボールの製造工程における順序づけ問題", 日本オペレーションズ・リサーチ学会春季研究発表会, 2006.

5. 松本一輝、巳波弘佳、茨木俊秀:
"段ボールの製造スケジューリング", スケジューリング学会研究発表会, 2005.

6. 野々部宏司:
"資源制約付きスケジューリングによる鋳造日程最適化システムの実現", 日本オペレーションズ・リサーチ学会中部支部シンポジウム「実践的な解法に基づく生産スケジューリング」, 2005.

7. S. Umetani, M. Yagiura, S. Imahori, K. Nonobe, T. Ibaraki and T. Imamich:
“An iterated local search algorithm for irregular packing problem”, The IFORS Triennial 2005 Conference, p. 47, 2005.

8. 柳浦睦憲:
“メタヒューリスティクスによる汎用解法（招待講演）”, 第 36 回システム工学部会研究会「最適化手法の最新動向」, 2005.

9. 柳浦睦憲:
“一般化割当問題に対する効率的メタ戦略アルゴリズム（文献賞受賞招待講演）”, 日本 OR 学会秋期研究発表会, 2005.

C11: 大量データ処理のための領域効率の良いアルゴリズム

定兼 邦彦　山下 雅史　小野 廣隆

九州大学 大学院 システム情報学研究院
〒 812-8581 福岡市東区箱崎 6-10-1
{sada,mak,ono}@csce.kyushu-u.ac.jp

1　はじめに

本研究では大量データ処理のための領域効率の良いアルゴリズムの開発を行っている．従来の研究と異なる点は，領域計算量をビット単位で数え，極限まで計算量を小さくすることを目標としている点である．この場合の極限とは情報理論的下界と呼ばれ，次のように定義される．ある集合 $\mathcal{S}$ に属する要素のうちの 1 つ e を格納するデータ構造のサイズの情報理論的下界 L は，集合 $\mathcal{S}$ の基数を D とすると $L = \log_2 D$ ビットとなる．これは 2 つの異なる要素を区別して格納するには L ビットが必要であるということを意味する．よって領域計算量を削減する際にはこの L まで削減することが目標になる．例えば，$\mathcal{S}$ を n 節点の木全体の集合，$e \in \mathcal{S}$ をある 1 つの木とした場合，$|\mathcal{S}| \approx 4^n$ であるため，$L = 2n - \Theta(\log n)$ となる．集合の要素を列挙することができればそれに順番に番号をつけることで 1 つの要素を L ビットで表現できるが，そのような表現から元の要素を復元したり，圧縮された表現のまま問合せを高速に行えるかどうかはわからない．それを可能とするデータ構造は圧縮データ構造 (succinct data structures) と呼ばれ，現在盛んに研究されている．圧縮データ構造はサイズが $\mathrm{O}(L)$ ビット，または $L + \mathrm{o}(L)$ ビットで，問合せを高速に (定数時間または対数多項式時間で) 実行できるものである．本研究の 1 つ目のテーマは圧縮データ構造の開発およびサイズの解析である．

本研究の 2 つ目のテーマは，計算機に格納できないようなデータの上での演算である．例えば Web グラフはサイズが非常に大きいためグラフ全体を格納するには非常に大量の記憶領域が必要である．そのようなグラフを探索する場合には一度訪れた点を記憶することができないため同じ点を何度も探索してしまう可能性がある．従来はグラフのランダムウォークをすることで解決しているが，同じ点に再度訪れてしまうことを完全に防ぐことはできない．本研究では少ない記憶領域を用いてグラフを探索できるアルゴリズムの開発を行っている．

2　今年度の成果

2.1　透過的データ圧縮

従来の圧縮データ構造では，同じデータに対して同じ問合せを行う場合でも，圧縮手法が異なる場合には問合せのためのデータ構造も異なるものを用いる必要があった．本研究では問合せのためのデータ構造に手を加えることなくデータの圧縮が可能となる汎用的な圧縮法を開発した．

全てのデータは文字列とみなす事ができる．その文字列の長さを n，文字のアルファベットサイズを σ とすると，データの圧縮前のサイズは $n \log_2 \sigma$ ビットとなる．通常のデータ圧縮法ではこの文字列を $nH_k + o(n \log_2 \sigma)$ ビットに圧縮する．ここで H_k は文字列の次数 k の経験的エントロピーであり，$H_k \leq H_{k-1} \leq \cdots H_0 \leq \log_2 \sigma$ である．エントロピーはある仮定の下での圧縮率の下界であるため，この圧縮表現はサイズの点では最適である．しかし従来の圧縮法を用いてデータ構造を圧縮すると問合せ時間が非常に遅くなってしまう．なぜならデータ構造が圧縮してある場合，その一部分のみアクセスしたい場合でも圧縮されたデータ全体を復元する必要があるからである．本研究の圧縮法では，圧縮された文字列の任意の部分を高速に復元できる．具体的には，文字列中の位置が指定されたとき，その位置から始まる部分文字列で長さが $\log n$ ビットのものを定数時間で復元する

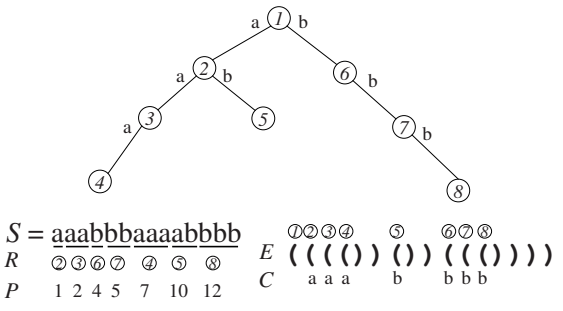


図 2.1: S = aaabbbaaaabbbb に対する提案データ構造.

ことができる．圧縮サイズは $nH_k + o(n \log_2 \sigma)$ ビットであり従来法と漸近的に等しい．

ここで重要なのは，指定された場所の $\log n$ ビットを定数時間で得るという操作は，圧縮されていない文字列中の $\log n$ ビットを単位時間で読み込む操作と同等であるということである．つまり，データは圧縮してあるにもかかわらず圧縮されていないとみなす事ができる．つまりデータ圧縮が透過的になっている．この圧縮法を用いれば，圧縮されていないデータに対して検索を行なうデータ構造があるとすると，それをそのまま圧縮されたデータに対して用いることができ，かつ問合せの計算量も同じである．つまり圧縮されたデータ用に検索のためのデータ構造を作り直す必要がなくなる．

2.2 グラフを効率良く巡回するためのラベル付け法

グラフ上にトークンを巡回させ，グラフの全点に情報を伝えることを考える．グラフは巨大であるため，巡回するためのルートはトークンに格納することができないとする．そこでいかに少ない記憶を用いて効率よく巡回できるかが問題となる．従来手法ではグラフ上に全域木を格納する方法などがあるがその情報をグラフに追加する必要がある．本研究ではグラフに情報を追加せず，またトークンに記憶が必要ない巡回アルゴリズムを提案する．

仮定として，グラフの各点において，そこから d 本の枝が出ているときそれらには 1 から d までの整数のラベルがついているとする．このようなラベル付けは local orientation と呼ばれている．トークンの巡回アルゴリズムは次のようになる．まずある点から出発する場合には 1 のラベルのついている枝をたどる．ある点に到着したとき，到着するときに用いた枝のラベルが i の場合，次の点に出発する場合は $i+1$ のラベルのある枝へ向かう．このアルゴリズムではトークンは記憶を必要としない．トークンがグラフの全点を訪れることができるかどうかはグラフの枝のラベル付けによって決まるが，本研究ではラベル付けをうまく行うと，n 点のどのようなグラフに対しても，全点を訪れる長さ $10n$ 以下のツアーが存在することを示した．

2.3 文書検索のためのデータ構造

文書検索での問合せとしては，ある単語が指定されたときにそれを含んでいる文書を列挙するというものがある．しかし単に列挙してしまうと出力される文書数が多い場合にその中で重要なものを見つけることが難しい．そこで文書にある種のスコアをつけその順序に並び替えるということが行われている．代表的なスコアとしては tf*idf がある．これは文書中の問合せ語の頻度を基にしたスコアである．従来のデータ構造ではこのスコアは特定の単語のみにしか高速に計算できないため，検索精度が落ちている可能性がある．本研究では任意の単語に対するスコアを高速に計算できるデータ構造を開発した．問合せに用いる単語の長さを p，全文書の長さの合計を n，問合せ単語を含む文書の数を q とすると，従来手法では文書ごとに問合せを行なう必要があるため $\mathrm{O}(pq)$ 時間かかってしまうが，これを $\mathrm{O}(p + q \log^{\epsilon} n)$ に改善した ($\epsilon > 0$ は任意の定数)．データ構造のサイズは $\mathrm{O}(1/\epsilon n H_0)$ である．$\epsilon = 1$ の場合，これは文書サイズの約 3 倍であり，非常に小さい．

2.4 動的文書集合のためのデータ構造

文書の集合 (ライブラリ) に対し，文書の挿入削除，およびパタンの検索を効率よく行うデータ構造を開発した．ライブラリ中の文書の長さの合計を n とする．1 つの文書 T の挿入・削除は $\mathrm{O}(|T| \log n)$ で行える．あるパタン P の存在位置

を返す問合せは $O(|P|\log n + occ\log^2 n)$ 時間で行える (occ は P の出現回数)．ライブラリを格納するために必要なスペースは $O(n)$ ビットである (アルファベットサイズは定数とする)．

このようなライブラリのデータ構造のために，本研究では圧縮接尾辞木の新しい表現を開発した．従来法では文字列は静的なものしか扱えなかったが，本研究ではそれを動的な文字列に拡張した．

2.5 圧縮接尾辞配列構築アルゴリズム

圧縮接尾辞配列は文字列検索のためのデータ構造で，長さ n の文字列からのパタン P の検索が $O(|P|\log n)$ 時間で行える．しかしそのサイズは $O(n\log n)$ ビットであり，長い文字列に対しては実用的ではない．圧縮接尾辞配列は接尾辞配列のサイズを圧縮したもので，様々な符号化法が存在しサイズは $O(n\log\sigma)$，$O(nH_0)$，$nH_k + o(n)$ ビットのものが存在する．

圧縮接尾辞配列は接尾辞配列から $O(n)$ 時間で構築することができるが，このような方法では一時的に $O(n\log n)$ ビットの領域が必要となり実用的ではない．本研究では圧縮接尾辞配列を文字列から直接作ることでデータ構造の作成時に必要な領域を削減した．必要な領域は $O(n(H_0+1))$ ビットであり，時間計算量は $O(n\log n)$ である．これらはアルファベットサイズには依存しない．このアルゴリズムにより，ヒトゲノムに対する圧縮接尾辞配列が 3GB のメモリを持つ PC にて 7 時間強で構築できるようになった．従来のアルゴリズムでは時間はほぼ同じだがメモリは 48GB を必要としていた．

3 研究活動

本特定領域のポスドク (4 月〜8 月，9 月からは日本学術振興会外国人特別研究員) である Jesper Jansson と研究を開始した．多くの国際会議や国内研究会に参加し，また発表を行った．本特定領域の全体会議では未解決問題セッションにて「文字列検索における時間と領域のトレードオフ」を主催して議論を行った．また，12 月にシンガポール大学の Wing-Kin Sung 氏，チリ大学の Diego Arroyuelo 氏を九州大学に招き共同研究を行った．3 月の NHC 春学校とワークショップには多くの学生を参加させた．また，定兼は平成 18 年 3 月に「圧縮データ構造の開発」というテーマで船井情報科学奨励賞を受賞した．

研究業績一覧

学術論文

1. Kunihiko Sadakane, Roberto Grossi: "Squeezing Succinct Data Structures into Entropy Bounds", Proc. ACM-SIAM SODA, 1230–1239, Jan. 2006.
   概要: Consider a sequence S of n symbols drawn from an alphabet $\mathcal{A} = \{1, 2, \ldots, \sigma\}$, stored as a binary string of $n\log\sigma$ bits. A *succinct* data structure on S supports a given set of primitive operations on S using just $f(n) = o(n\log\sigma)$ extra bits. We present a technique for transforming succinct data structures (which do not change the binary content of S) into *compressed* data structures using $nH_k + f(n) + O(n(\log\sigma + \log\log_\sigma n + k)/\log_\sigma n)$ bits of space, where $H_k \le \log\sigma$ is the kth-order empirical entropy of S. When $k + \log\sigma = o(\log n)$, we improve the space complexity of the succinct data structure from $n\log\sigma + o(n\log\sigma)$ to $nH_k + o(n\log\sigma)$ bits by keeping S in compressed format, so that any substring of $O(\log_\sigma n)$ symbols in S (i.e. $O(\log n)$ bits) can be decoded on the fly in constant time. Thus, the time complexity of the supported operations does not change asymptotically. Namely, if an operation takes $t(n)$ time in the succinct data structure, it requires $O(t(n))$ time in the resulting compressed data structure. Using this simple approach we improve the space complexity of some of the best known results on succinct data structures. We extend our results to handle another definition of entropy.

2. Stefan Dobrev, Jesper Jansson, Kunihiko Sadakane, Wing-Kin Sung:
"Finding Short Right-Hand-on-the-Wall Walks in Graphs", Proc. of SIROCCO, LNCS 3499, 127–139, May 2005.
概要: We consider the problem of perpetual traversal by a single agent in an anonymous undirected graph G. Our requirements are: (1) deterministic algorithm, (2) each node is visited within $O(n)$ moves, (3) the agent uses no memory, it can use only the label of the link via which it arrived to the current node, (4) no marking of the underlying graph is allowed and (5) no additional information is stored in the graph (e.g. routing tables, spanning tree) except the ability to distinguish between the incident edges (called Local Orientation). This problem is unsolvable, as has been proven even for much less restrictive setting. Our approach is to somewhat relax the requirement (5). We fix the following traversal algorithm: Start by taking the edge with the smallest label. Afterwards, whenever the agent arrives at a node, it continues by taking the successor edge (in the local orientation) to the edge via which it arrived" and ask whether it is possible to choose the local orientations in such a way that the resulting perpetual traversal visits every node in $O(n)$ moves. We give a positive answer to this question, by showing how to construct such local orientations. This leads to an extremely simple, memoryless, yet efficient traversal algorithm.

3. Kunihiko Sadakane:
"Succinct Data Structures for Flexible Text Retrieval Systems", Journal of Discrete Algorithms, (掲載予定).
概要: We propose succinct data structures for text retrieval systems supporting document listing queries and ranking queries based on the *tf*idf* (term frequency times inverse document frequency) scores of documents. Traditional data structures for these problems support queries only for some predetermined keywords. Recently Muthukrishnan proposed a data structure for document listing queries for arbitrary patterns at the cost of data structure size. For computing the *tf*idf* scores there has been no efficient data structures for arbitrary patterns. Our new data structures support these queries using small space. The space is only $2/\epsilon$ times the size of compressed documents plus $10n$ bits for a document collection of length n, for any $0 < \epsilon \leq 1$. This is much smaller than the previous $\mathrm{O}(n \log n)$ bit data structures. Query time is $\mathrm{O}(m + q \log^{\epsilon} n)$ for listing and computing *tf*idf* scores for all q documents containing a given pattern of length m. Our data structures are flexible in a sense that they support queries for arbitrary patterns.

4. Ho-Leung Chan, Wing-Kai Hon, Tak-Wah Lam, Kunihiko Sadakane:
"Compressed Indexes for Dynamic Text Collections", ACM Transactions on Algorithms, (掲載予定).
概要: Let T be a string with n characters over an alphabet of constant size. The recent breakthrough on compressed indexing allows us to build an index for T in optimal space (i.e., $O(n)$ bits), while supporting very efficient pattern matching. Yet the compressed nature of such indexes also makes them difficult to update dynamically. This paper extends the work on optimal-space indexing to a dynamic collection of texts. Our first result is a compressed solution to the *library management* problem, where we show an index of $O(n)$ bits for a text collection $\mathcal{L}$ of total length n, which can be updated in $O(|T| \log n)$ time when a text T is inserted or deleted from $\mathcal{L}$; also, the index supports searching the occurrences of any pattern P in all texts in $\mathcal{L}$ in $O(|P| \log n + occ \log^2 n)$ time, where *occ*

is the number of occurrences. Our second result is a compressed solution to the *dictionary matching* problem, where we show an index of $O(d)$ bits for a pattern collection $\mathcal{D}$ of total length d, which can be updated in $O(|P| \log^2 d)$ time when a pattern P is inserted or deleted from $\mathcal{D}$; also, the index supports searching the occurrences of all patterns of $\mathcal{D}$ in any text T in $O\big((|T| + occ) \log^2 d\big)$ time. When compared with the $O(d \log d)$-bit suffix tree based solution of Amir *et al.*, the compact solution increases the query time by roughly a factor of $\log d$ only. The solution of the dictionary matching problem is based on a new compressed representation of a suffix tree. Precisely, we give an $O(n)$-bit representation of a suffix tree for a dynamic collection of texts whose total length is n, which supports insertion and deletion of a text T in $O(|T| \log^2 n)$ time, as well as all suffix tree traversal operations, including forward and backward suffix links. This work can be regarded as a generalization of the compressed representation of static texts. In the study of the above result, we also derive the first $O(n)$-bit representation for maintaining n pairs of balanced parentheses in $O(\log n / \log \log n)$ time per operation, matching the time complexity of the previous $O(n \log n)$-bit solution.

5. Wing-Kai Hon, Tak-Wah Lam, Kunihiko Sadakane, Wing-Kin Sung, Siu-Ming Yiu:
"A Space and Time Efficient Algorithm for Constructing Compressed Suffix Arrays", Algorithmica, (掲載予定).
概要: With the first human DNA being decoded into a sequence of about 2.8 billion characters, many biological research has been centered on analyzing this sequence. Theoretically speaking, it is now feasible to accommodate an index for human DNA in the main memory so that any pattern can be located efficiently. This is due to the recent breakthrough on compressed suffix arrays, which reduces the space requirement from $O(n \log n)$ bits to $O(n)$ bits for indexing a text of n characters. However, constructing compressed suffix arrays is still not an easy task because we still have to compute suffix arrays first and need a working memory of $O(nlogn)$ bits (i.e., more than 13 Gigabytes for human DNA). This paper initiates the study of constructing compressed suffix arrays directly from the text. The main contribution is a construction algorithm that uses only $O(n)$ bits of working memory, and the time complexity is $O(nlogn)$. Our construction algorithm is also time and space efficient for texts with large alphabets such as Chinese or Japanese. Precisely, when the alphabet size is $|\Sigma|$, the working space becomes $O(n(H_0 + 1))$ bits, where H_0 denotes the order-0 entropy of the text and it is at most $\log |\Sigma|$; for the time complexity, it remains $O(nlogn)$ which is independent of $|\Sigma|$.

研究会等

1. Hirotaka Ono, Sung-Hoon Park, Masafumi Yamashita:
"Failure Detectors for the Leader Election with Bounded Faulty Processes", 電子情報通信学会COMP研究会, COMP2005-55, 43–46, 2005年12月.
概要: Determining the "weakest" failure detectors is a central topic in asynchronous fault-tolerant distributed system, and indeed the weakest failure detectors have been proposed for several fundamental problems such as Consensus, Non-Blocking Atomic Commit, and Leader Election. We consider failure detectors to solve the leader election problem with f faulty processes, under the assumption that future never affect the output of a failure detector. Sabel et. al. showed the weakest failure detector for the

leader election is $\mathcal{P}$, perfect failure detector, with any number of faulty processes under some restricted conditions, and Delporte-Gallet et.al. showed the result holds under more realistic constraints. In this paper, we propose a new failure detector class $\mathcal{M}$ to solve the leader election with less than $\lceil n/2 \rceil$ faulty processes, and show that $\mathcal{M}$ is strictly weaker than $\mathcal{P}$. That is, there is a hardness gap of the leader election with respect to the number of faulty processes.

3.　各種資料

特定領域研究

「新世代の計算限界」ニュースレター　　第 3 号　　2005/7/11

はじめに

このニュースレターは，特定領域・新世代の計算限界のメンバーの情報交換と交流を目的とした情報発信誌です．毎回，いくつかの研究関連の記事と，特定領域のスケジュール・活動報告と，各研究者の活動予定などをお送りいたします．今回は，東北大学徳山豪先生の経験談と，6月に行われた全体会議，幹事会の報告を行います．

1. 「群れ派」の研究の仕方　　ー 徳山 豪 (東北大学)

2. 第2回全体会議を振り返って　　ー 浅野 哲夫 (JAIST)

3. 2005年度第1回幹事会議事録　　ー 事務局

4. イベントカレンダー ＋ 事務連絡

5. このニュースレターについて

「群れ派」の研究の仕方　　徳山 豪 (東北大学)

最近は「引きこもり」や「ネットが友達」など一人でいるのが居るのがいいという方も結構いるらしいが，私は典型的な「群れ派」である．特定研究のおかげでいろいろな人の考えが聞けて，おしゃべりが出来るのは楽しくて仕方が無い．そういう場では少々躁状態になるので，声がでかくて「うざったい」(特に岩間さんや西関先生と一緒だと)が，暖かくお許しいただけるとありがたい．大体が教授室に1時間とじっとしていられないで学生研究室をうろうろしているので，学生には(だれも口に出して言わないが)うっとうしい存在である．そんな性格なので，一人でコツコツ本や論文を読んで勉強するのは苦手で，常に人との関りが幸運をもたらしている．宇野さんのリクエストもあり，そんな話(記憶が薄れているので，意図せずフィクションが入ったらごめんなさい)をしてみる．

食事とドライブ

楽しいおしゃべりの相手というと，浅野哲夫先生(二人の取り決めにより，「浅野さん」と書く)がなんといっても第一である．1988年にはじめての海外出張でイリノイ大学でのACMのSCG(計算幾何学シンポジウム)に行ったのがお付き合いのはじまり．日本でもお会いしたことはあったのだが，当時私は純粋数学(代数的群論)から計算機科学に転向して1年経たないほどの新米で，大先生相手に気後れして直接お話をしたことがなかった．
イリノイ大学のあるアーバナ・シャンペーンというところは平らな大地以外に何にも無いところで，しかも会議参加者は見知らぬ人ばかり．大体が食事をする場所も近くにない．うろうろしていると，うしろから「こんにちは」の声がして，黒いサングラスを掛けたヒゲの先生がニコニコしている．「タご

飯，どうします？　みんなと一緒に行きません？　僕，レンタカーしてるから．」うれしかったなあ．なんといっても人間は食べることが一番．　おまけに，後でIBMのWatson研究所でホストをしてくれたAlok Aggarwalや，研究での転換のきっかけをくれたMicha Sharirら有名人たくさんに紹介してもらった．結局会議期間中ずっと浅野さんの車に同乗したのだが，気に入ってもらえたらしく，「せっかくだから，一緒に研究しましょう．2次元のハッシュ問題だけど，興味ある？」この研究は後で「トポロジカルウォーク」というアイデアを生み，私の出世作（1991SCG）になったのだが，浅野さんとの出会いが無ければ今の半分も研究人生が楽しくなかっただろうと思う．

話のついでだが，この会議で，「ちょっといいか」といって，話しかけてきた二十歳くらいのパデュー大学の中国人学生が居た．テーブルで無理やり向かい合わせたかと思うと，いきなり「計算幾何学の並列アルゴリズムに将来性はあると思うか，返答は如何に」と質問してくる．なんだなんだと思いながら適当に答えていると，「Thank you , 参考になった」といって握手してバイバイである．この生意気な学生はDanny Chen．当時はまだ論文も無い学生だったが，今ではトップクラスの研究者で，貴重な共同研究者である．

講演依頼は喜んで受けよう

STOC-FOCS-SODAとよく言うが，こういった会議に最初に論文を通すのが難しい．私の場合は，山下雅史先生と渡辺治先生のおかげである．といっても共同研究ではなく，駆け出しの研究者だった私に，「ランダムアルゴリズムについての一時間講演をお願い．絶対いい講演ができるから．」とおだてながら迫ったのがこのお二人（詳細は忘れたが，IEICE関係で，聴衆はずいぶんたくさん居た）．　当時ランダムアルゴリズムが世界的にブレイクし，反面日本ではあまり研究者が居なかったことは事実だが，ともかく自分でランダムアルゴリズムを設計したことが無い人間が「良い講演」をするのは難しいし，オリジナルな結果がまったく無いチュートリアルをするのは恥ずかしいと思った．講演期日までの間，柄にもなく一生懸命にさせられた結果が，割り当てや輸送問題を計算幾何学のランダムアルゴリズム手法で解く（問題自体は研究中だったが，ランダムというのは考えても居なかった）というもの．幸運なことにいい問題に当たった（1991SCG,1992SODA）が，講演を断っていたら運はめぐってこなかったろう．

人の話に首を突っ込むと

誰かが面白そうな（研究の）話をしているときに，話に加わりたいが邪魔をすると悪いなと思うかもしれない．IBMの東京基礎研究所で入社4年目くらいの頃，当時の上司の岩野さんと加藤直樹先生（これも加藤さんと呼ぶ）は頻繁に共同研究をしていた．ちょうど私の研究も軌道に乗って，翌年からアメリカ赴任という状況だったが，加藤さんが岩野さんを訪れて来た．ご挨拶でもしようと二人の話している会議室に（呼ばれもしないのに）行くと，なにやら面白げな話をしている．ぐずぐずしている間に，「徳山さんは専門家だから，聞いてよ」というのでありがたく参加すると，幾何学的な動的最小木とパラメトリックなマトロイドについての加藤さんの知識と発見の話題である．O(n^4) がマトロイドの理論で O(n^3) になるらしい．その場で考えてみると，計算幾何学のテクニックでも O(n^3) になるし，両方を組み合わせると O(n^2) にも出来るようである．わずか1時間ほどの Discussionで出来た論文が，「動く点集合の最小木について」（1992FOCS）．さらに，関連するテーマで，たくさん（1995SODA,1999SODA,1999FOCS,2001SCG）論文を書いた．結論として，人の話には遠慮なく首を突っ込むべきである．

朝目覚めると

「ワーム食べませんか？」玉木さんと最初に会ったときに彼が言った言葉である．1992のFOCSで，ワームホールラウティングの講演をした直後，講演に使った（したがってOHP のガラスの上をのたくりまわった）グミキャンディーのミミズのおもちゃを半分にちぎって，片方を銜えながら．こん

な面白い人がIBMの研究所にやってきて，2年間同室だったのだから，いい研究ができないわけがない．まず手始めにということで，Micha Sharirと学会のlunchで一緒したときに「解くべきなのだが，まったく手掛りがない」といわれて挑戦し続けていた「放物線のレベル問題」について玉木さんに話すと，Lovaszのマッチングとカバーリングの双対定理という道具を使って，あららというちに解けてしまったのはおどろいた（1995SCG）．私一人では3年間うまくいかなかったのに．　また或る時，国際会議で同室して，時差のせいで朝（？）3時に目覚めると，玉木さんなにやら思索にふけっている．「目が覚めましたか，ちょっと一緒に考えませんか？」．こちらは目覚めただけで起きたわけではないのだが，一緒につきあう．これで出来たのが1997年のISAACで最優秀論文賞をもらった研究（なんだか，私はサンチョ・パンザみたい）．

さて，玉木さんと私ではタイプはだいぶ違う．共通の趣味である囲碁を打つと良くわかるのだが，私は直感派で諦めが良く，玉木さんは論理（読み）を積み重ねないと納得しない．囲碁は個人ゲームだが，研究は協力して出来るので，違うタイプが重なると相乗効果で大変よろしい．考えてみると，「浅野－加藤－玉木－徳山」は4人ともタイプはそれぞれ違うように思う（どう違うかは，皆さんで判断してください）．浅野さんがリーダーシップを取って，この4人で合宿をしたりして，随分楽しく共同研究をしてきたものである．

研究のエピソードは書き出すと尽きないのだが，残りはまたの機会にしようと思う．

第2回全体会議を振り返って　浅野 哲夫 (JAIST)

去る6月16日から2日間に亘って開催された第2回の全体会議について報告します．昨年，特定研究がスタートして以来，平成16年10月に東北大学で開かれた第1回の全体会議，今年の2月に京都で開かれた国際会議に引き続いての会合ですが，最初の2回についてはまだ成果を出せる状況にないということもあって，招待講演を主とする構成になっていました．代表幹事の伊藤先生から，東京電機大学の築地先生と一緒に次回の全体会議を計画するように言われたとき，どのようなコンセプトにするか色々と考えました．まず考えたことは，特定研究にとって最も重要なことは何かでした．とにかく偉大な成果を出すことが要求されている訳ですが，特定研究としての成果というのは，単独では難しかった問題を特定研究のグループの力を借りて初めて解くことに成功したというものであることが望ましい訳です．つまり，うまくコラボレーションができたかどうかが問われる訳です．もちろん，理論のことですから，何度も集まったから必ず成果が出るという保証は何もありませんが，社会に対しては，少なくともコラボレーションがうまく行くように最大限の努力はしたということが見えなければならないと考えた訳です．では，そのためにはどうすればいいかですが，コラボレーションを成功させるためには，まず我々のグループの中でどんな成果があるのか，誰がどんな研究を行っているのかを知ることが肝腎です．ということで，まずは全ての研究班に自分たちの研究を紹介してもらおうという考えに至りました．もちろん，全員に話をしてもらうのが最適ですが，そうすると時間が2日では全く足りないので，ポスターの形式にしました．コラボレーションの切っ掛けは，日常会話に近い，ちょっとした会話の中から生まれるものだと個人的に信じているので（とにかく，興味ある共通の話題がないことにはやる気が起きないので），とにかくインフォーマルな会話の時間を大切にしたかったのです．

もう一つの視点は，私がこのコミュニティーが好きなのは，日本の社会にしては珍しく年齢の壁が高くないことです．理論をやっていると，どうしても若い人の集中力には負けるから，経験が豊富だというだけで威張ることができません．これが年齢を余り感じることなく誰とでも話せる雰囲気を醸し出しているのだと思います．いつの間にか自分も年寄りの部類に入ってしまっているのでしょう

が，気分はまだ20代です（言い過ぎです，ごめんなさい）．この雰囲気を大事にしたくて，偉い人にだけ講演をお願いするというスタイルを取りませんでした．

最後に，４人の方にだけ普段より長めの時間を用意して講演をしてもらいました．いずれも活躍が伝わってくる講演で，改めて本グループの質の高さを実感しました．今回の４人の講演者は私の一存で決めましたが，４人のご講演を聞いただけでも本グループの全体像が浮かび上がる，うまい人選になっていたのではないかと自画自賛しています．もちろん，講演を快諾して頂いた４人の講師の講演の質の高さが成功に導いたことは言うまでもありませんが．次回はどんな趣向で全体会議が企画されるか今から楽しみです．

2005年度第1回幹事会議事録　　事務局

日時：2005.6.16 12:00--13:50

場所：国立情報学研究所１２階会議室

[報告事項]

○ 教科書シリーズの進行状況（杉原，山下，室田，渡辺）

（仮題）アルゴリズムサイエンスシリーズ　全16巻　　A5版 約200ページ

○ 電子ジャーナル（徳山）

・ECCCの成功（ドイツの大学）を見習ってECCCのアルゴリズム版を作る？

・維持が大変（お金と人手）

・本屋を巻き込めば継続可能だが

-> 全体討論で議論

○ 成果報告書（堀山）

・印刷体のものを各研究代表者に送る

○ 確率シンポジウム（徳山）

・資金は基本的に折半

○ ニューズレター（宇野・牧野）

・７月出版を目安に準備

[検討事項]

○NHC国際会議に続いて，今年度も国際会議を開催するか？

・若手の育成を重視し，サマースクール（またはスプリングスクール）を実施

・前半スクール後半チュートリアル？

–> 全体討論で議論

○次回の全体会議の場所，担当者

・名古屋大，平田先生

・11／21，22予定

○林先生のコメント

・審査が厳しくなっている．

– きちんと評価ー＞反映　という傾向．

– 中間審査の結果で減額されたり，最終報告の結果で次期プロジェクトに反映されたりするようになってくる．

・この特定は情報基盤を支える重要なものである．

・現実的な解法，具体的な成果が求められる．

・領域の連携が重要：単なる集まりでは無い（連携することでどんな結果が得られたか？目標に対してどこまで到達したか？）

・「情報学」が終わるのでこの特定が情報系の代表格になる

・グランドチャレンジを期待する．

「新世代の計算限界」イベントカレンダー　＋　事務連絡

特定領域研究も2年目に入り，段々と盛り上がってきて事務局も嬉しい忙しさです．春学校，ミニプロジェクトなど新しい試みも始まります．皆様，これからもご協力の程よろしくお願いします．

★ 報告書の作成について皆様のご協力有難うございました．作成方法やフォーマットなどについてご意見をお持ちでしたら，伊藤，堀山までお寄せ下さい．

★ ミニ研究集会はどなたがどんな思いつきで企画されても結構ですから，どしどし行って下さい．総括班から費用のサポートもいたします．

全体会議 （予定） 11/21(月),22(火) 名古屋大学

列挙合宿 （宇野毅明・中野眞一・上原隆平）

3日間，泊り込みで列挙・数え上げを中心に組み合わせアルゴリズムに関する雑談をします．

9/27(火)13:00 – 29(木)11:30 群馬県伊香保町 群馬大学セミナーハウス

7/11(月)–15(金) ICALP, ポルトガル・リスボン
7/11(月)–15(金) IFORS, ハワイ （参加者: 伊藤大雄, 巳波）
7/18(月)–21(木) ランダムネスと計算に関わるワークショップ 仙台国際センター (参加者: 元木光雄)
7/19(火)–22(金) Combinatorial Pattern Matching 韓国済州島
7/25(月)–27(水) LAシンポジウム 福岡県宗像市
8/15(月)–17(水) WADS, カナダ・ウォータールー
8/16(火)–29(金) COCOON, 中国・昆明
8/29(月)–9/2(金) MFCS, ポーランド・グダニスス
10/1(土)–5(水) CP2005 スペイン・バルセロナ （参加者: 元木光雄）
10/3(月)–6(木) ESA, スペイン・イビザ
10/21(金)–10/22(土) 第17回RAMPシンポジウム 青森県弘前市 シティ弘前ホテル
10/23(日)–25(火) FOCS 2005 アメリカ・ピッツバーグ
12/7(水)–12/9(金) I-SPAN2005 アメリカ・ラスベガス
12/19(月)–21(水) ISAAC, 中国・海南島
1/22(日)–1/24(火) SODA2006 アメリカ・マイアミ

このニュースレターについて

ニュースレター各号は電子メールで配布する予定です．短い記事や連絡事項は全て掲載しますが，長い記事，イベントの詳細などはwebページに掲載する予定です．webページには詳細まで全てを載せた完全版を掲載して，目次，あるいは各記事の末尾のURLを参照すると，web版の同じ記事を参照できるようにいたします．

記事は，各回，1つの研究課題に担当をお願いする予定です．各研究課題で2000–4000字程度，研究に関わる記事を書いていただければと思います．通常，このようなニュースレターでは，研究成果を報告するのが一般的だと思われますが，この特定領域では「研究者の交流」に焦点を当てたいため，「研究の成果以外」の記事を面白く解説していただければと思います．例えば，最近参加した国際会議の情報を，どのようなものが流行っていたか，何が面白かったか，などの主観的な解説を交えて報告したり，最近考えている問題，あるいはオープン問題を，この辺までは解けるがここがうまくいかない，といった解説を交えて紹介する，という形です．

また，研究者間の交流を促進するため，各研究者の，国内外の会議への出席予定を集約して掲載していこうと考えています．研究者の交流には，顔をあわせる回数を増やすことが肝要です．他の研究者の参加予定がわかれば，会議への出席のモチベーションを高めることにもつながり，それがディスカッションや研究成果を生むきっかけにもなるでしょう．特定領域メンバーの皆さんには，自分のわかる範囲で，国内外の会議・研究会の情報と，自分の参加予定を教えていただければと思います．

この他，個人からの寄稿を募集いたします．100-1000字程度で，情報宣伝されたいことを自由な形式で書いて送っていただければ，掲載いたします．メールで配布する関係上，テキスト形式のものしか扱えませんが，そこはご了解お願いいたします．

次回は10月ごろを予定しています．

★ ニュースレター編集委員では，皆様からのご意見をお待ちしております．編集方針や内容の追加など編集全体にかかわることから細かいことまで，幅広いご意見をお願いいたします．

■■ 新世代の計算限界 ニュースレター ■■

編集委員長 宇野 毅明 uno@nii.jp（問合せ先）

副編集委員長 牧野 和久 makino@sflab.sys.es.osaka-u.ac.jp

特定領域研究

「新世代の計算限界」ニュースレター　　第 4 号　　2006/1/27

はじめに

このニュースレターは，特定領域・新世代の計算限界のメンバーの情報交換と交流を目的とした情報発信誌です．毎回，いくつかの研究関連の記事と，特定領域のスケジュール・活動報告と，各研究者の活動予定などをお送りいたします．今回は，名古屋大学高木直史先生の研究科紹介と，11月に行われた全体会議，幹事会の報告を行います．

1. 中心？隙間？それとも辺境？　　ー 高木 直史 (名古屋大学)

2. 第3回全体会議の報告　　ー 平田富夫(名古屋大学)

3. 2005年度第2回幹事会議事録　　ー 事務局

4. イベントカレンダー ＋ 事務連絡

5. このニュースレターについて

中心？隙間？それとも辺境？　　高木 直史 (名古屋大学)

■ 集積システム論

主要大学の中では少し遅れをとりましたが、名古屋大学でも2003年４月に情報系の大学院研究科として、情報科学研究科が設立されました。計算機数理科学専攻、情報システム学専攻、メディア科学専攻、複雑系科学専攻、社会システム情報学専攻の５つの専攻からなっています。本特定領域研究には、計算機数理科学専攻の平田先生、柳浦先生(昨年１０月に転入)も参加されています。(藤戸先生は豊橋技術科学大学に転出されました。)私と高木一義先生は情報システム学専攻の集積システム論講座(大講座：３研究室)に所属しています。

集積システム論というと、半導体回路工学等をイメージされるかもしれませんが、集積回路で構成されるシステムが対象であり、いわゆるシステムLSIや組込みシステムのハードウェア(アーキテクチャ)やソフトウェアに関する研究を行う学問と考えています。現在、年間100億個以上のマイクロプロセッサ(4ビット以上)が出荷されていますが、そのうち、パソコンやワークステーション等の汎用のコンピュータに用いられるのは2%程度であり、ほとんどが組込み用に使われています。実際、あらゆる家電製品にマイクロプロセッサが組み込まれており、一般家庭で40～50個はあるといわれています。また、自動車にも多く使われており、高級車では70～80個使われています。

以前は、集積回路を部品として汎用コンピュータを作るために、汎用機のアーキテクチャ、汎用機のOS、汎用機のソフトウェア、そして部品としてのIC設計の研究が行われていました。しかし、今は、コンピュータ(プロセッサ)は部品となり、メモリや種々の周辺回路とともにボード上、さらには、一つのLSI上に集積されています。

集積（組込み）システムのアーキテクチャ、組込み用プロセッサのアーキテクチャ、組込みOS、組込みソフトウェア、そしてシステムとしてのLSI設計の研究が必要です。

私は、集積システム論は、電気・情報分野の「中心」に位置すると思い（たく）、実際、産業界はシステムLSIや組込みソフトウェアの高度技術者を必要としているのですが、残念ながら、我国の大学では電気電子の分野と情報の分野の「隙間」になっています。企業では、半導体技術者等を社内再教育でこの分野に振り向けているのが現状です。

■ 集積システムの設計支援とハードウェアアルゴリズム

これまでは、本特定領域研究の皆様にはピンと来ない話だったかと思います。しかし、実は、集積システムの設計過程は、組合せ最適化問題の宝庫です。処理のどの部分をハードウェアで行いどの部分をソフトウェアで行うか等を決めるシステムレベルの設計から、LSIのレイアウトまで、最適化問題を解く作業の連続です。最適化の対象は、計算時間や面積に加え、消費電力が重要になっています。ちょっと意外かもしれませんが、よく現れる処理は、ソフトウェアで行うよりハードウェアで行った方が消費電力が少なくて済みます。製造手順の最適化もあります。少し前の話になりますが、IBMの岩野さんらが、プリントボードに多数のホールを開ける作業を、巡回セールスマン問題の解法を応用して効率化されたことを覚えておられる方もおられると思います。

本特定領域研究には、「ハードウェアアルゴリズムの評価に関する研究」という課題で参加させて頂いています。ハードウェアアルゴリズムの評価は、それの基づく回路の性能によって行います。そのためには、回路の安定したモデルが必要です。従来、組合せ回路モデル上での段数および素子数、さらには、配線領域も考慮したVLSIモデル上での面積が評価基準として用いられています。段数は計算時間の指標ですが、現実には、論理ゲートでの遅延よりも配線での遅延の方が大きくなっており、配線遅延を含めた計算時間を評価できる回路モデルと評価基準の確立が必要だと考えています。また、消費電力を評価するための回路モデルと評価基準も必要だと考えています。
近年、LSIの配線層数が増えてきており、さらに、先日、東北大学でLSIチップを貼り合わせた3次元LSIが開発されました。3次元のVLSIモデルも興味深い研究課題ではないかと思います。

我々の研究は、本特定領域研究では「辺境」に位置しますが、皆さんにとっても、いろいろ面白い課題があると思います。

第3回全体会議の報告　　平田富夫（名古屋大学）

昨年の11月21日、22日に開かれました第3回全体会議についてご報告いたします。

これまで科研の集会というと研究発表のみというスタイルが多かったと思いますが、前回6月の第2回全体会議では、メンバーのコラボレーションを促進することを主目的として各研究班を紹介するポスターセッションがもたれました。（そのコンセプトは前回の全体会議企画担当の浅野哲夫先生の記事（ニュースレター第3号）をご覧ください。）

第3回の全体会議もこのコラボレーション路線を引き継ぎました。今回はオープン問題を持ち寄り共同でチャレンジすることをメインにしましたが、この企画は、第2回全体会議の直後に浅野哲夫先生と岩間先生にご相談して決めたものです。皆さんがお持ちのオープン問題で全体会議に話題提供できるものを募集したところ5人の先生方が応じてくださいました。この場を借りてこの5人の先生方にお礼申し上げます。私の印象としては、だれもがすぐ理解でき、しかもアイデアが出せそうな問題で非常によい問題だったと思います。中には他のメンバーの結果と結びついて発展した話題もあったようです。このような試みは短期的な成果を求めるのが目的ではありませんが、これを機会にひとつでも成果に結びつくものが出てくれば今回の全体会議は大成功

といえます。

２日目の講演はSODA、FOCSで発表を予定しているメンバーを中心に、私と柳浦先生が興味をもっている話（は皆さんも興味があるだろうと勝手に考えて）で人選させてもらいました。内容はレベルが高く楽しめたのではないかと思います。ご講演いただいた５人の先生方にこの場を借りてお礼申し上げます。

場所は初日が野依記念学術交流館で、２日目がIB電子情報館大講義室でした。野依記念学術交流館は野依良治先生のノーベル賞受賞を記念して建てられた瀟洒な建物です。カンファレンスホール（２００席）と会議室８室（１室１０名～２０名、間仕切り撤去可）があり、オープン問題セッションの後のディスカッションにはうってつけでした。この会場は人気があり早くからの予約が必要ですが、今回はたまたま１日だけあいていたので使わせてもらいました。

６月に次回会議の日程を決めたにもかかわらず、私の不手際で会議の直前まで案内をだすことができませんでした。伊藤先生はじめ事務局の先生方にはご心配をおかけしました。幸い柳浦先生が１０月に名古屋大学に着任されてからは進捗著しく無事会議を終えることができました。ご協力いただいた皆様に感謝します。

2005年度第2回幹事会議事録　　事務局

日時: 2005.11.21, 16:00--17:30

場所: 名古屋大学　野依学術交流館　カンファレンスホール

[活動報告]

○ミニ研究集会

・組合せゲーム・パスル（9/12, 京大）

・複雑ネットワーク・ウェブグラフ（9/13, 関学）

・列挙アルゴリズム（9/27--29, 群馬大）

・Complexity（10/11, 東工大）

○ポスドク

・西村治道（10月～, 京大）

○招聘研究者

○国際会議渡航補助

・FOCS（河原林[東北大]）

○事務員

・宮本希（８月～）

○国際会議 ランダムネス [渡辺]

7/18--21, 東北大学

[進捗状況報告／討論]

○教科書シリーズ [杉原]

順調。脱稿2件

○ニュースレター [牧野・宇野]

・これまでに3回発行。4回目は来年の1月。

・年に2回程度の予定で進めたい。->了承 (必要ならば、号外を適宜。)

○電子ジャーナル [定兼]

・引き続き、検討を続ける

・協力が必要な場合は、後日に相談

○春学校、ワークショップ (2/27(月) ～ 3/3(金))

・オーガナイザ・プログラム:浅野孝夫

・ローカルアレンジ:西野・垂井

・2/27(月) ～ 3/1(水) 春学校

- 電通大図書館 AV教室 (301号室, 306号室)

- 講師は5名

・3/2(木) ～ 3/3(金) ワークショップ

- 調布クレストンホテル

・春学校 … 初学者の道案内を目指す (定員 90名)

(※ 参考: 春学校に参加させてみたい学生数 … 会場だけで 30名以上)

近隣の諸国にもアナウンスを流す

・春学校/ワークショップではregistration fee を徴収する (高額ではない)

○ミニプロジェクト

・ゲーム [伊藤]

－ミニ研究集会を開催

－今後、スクールみたいなのを開催したい

・Complexity [垂井]

－ミニ研究集会を開催、今後も開催予定

－学生にも声をかけたい

・ジオメトリ [加藤]

－３月後半、学生対象の mini school

－講師 加藤・浅野・徳山・(David Avis)

・列挙 [中野]

－ミニ研究集会を開催

○電子情報通信学会 特集号 [増山]

・来年６月に、和文論文誌、特定の解説論文の特集

○ICALP ワークショップ

・SATの厳密解法関係のミニワークショップの提案(渡辺先生)

－ヨーロッパの人々とも相談する必要あり

(後日、渡辺先生によって申請、採録された。)

○電子情報通信学会 英文論文誌 [和田]

・来年の８～１０月頃、〆切は２月頃

・基本は研究論文 (解説論文も ok かも)

・もう少し検討

○予算の使途

・国際会議発表のための海外渡航の補助

○次回の全体会議

・九州地区(山下、定兼)

・2006年、５月か６月頃

○電子情報通信学会 全国大会 企画 [山下]

・3月24日(金) ～ 27日(月) 国士舘大学

・若手(主に博士課程の学生)のためのシンポジウム

・参加費と旅費は、総括班から支援

○次回以降の春学校/ワークショップ

・来年度からは、時期を夏休みぐらいにしたい

・早急に内容の相談を始める必要がある

○EATCS記事募集 [牧野]

・特定内外で、記事があれば、牧野まで

○特定領域としての成果

・どんな集まりで、どんなアイデアが出て、どんな進展・研究があったか

どんなに細かいことでも良いので、事務局まで教えてほしい

○次の特定領域

・来年は、調査研究の申請をする

・そのために、今の特定領域で、領域として集まった成果を挙げる

「新世代の計算限界」イベントカレンダー　＋　事務連絡

成果報告書の執筆依頼

今年度の成果報告書を領域として作成する時期となりました．詳細は別途メール・ウェブで御連絡いたしますが，昨年度と同じ要領で，A01 から C11 の研究課題ごとに「研究活動報告」と「発表文献リスト」を御執筆いただけますようお願い申し上げます．なお，提出〆切は 3月31日(金) です．

http://keisan-genkai.lab2.kuis.kyoto-u.ac.jp/members/reports.html

旅費の補助

総括班予算より国際会議等の旅費の補助を行います。補助希望者は伊藤までお申し出ください。特に締め切りなどは設定しておりません。

・ジオメトリ合宿　(加藤直樹 浅野哲夫、徳山豪、David Avis)

2006年3月15日昼から17日まで

コミュニティ嵯峨野（京都府勤労者研修センター）（http://www.com-sagano.com/）

〒616-8372 京都市右京区嵯峨天龍寺広道町3-4

・COMP-NHC 学生シンポジウム（田中圭介）

2006年3月24日(金)～26 日(日)のいずれか一日、国士舘大学世田谷キャンパス(東京都世田谷区)

電子情報通信学会 2006 年総合大会 シンポジウム講演 (B) DS-1「COMP-NHC 学生シンポジウム」

（総合大会は2006年3月24(金)～27(月)）

3/27(月)-29(水) EWCG'06 (22nd European Symposium on Computational Geometry) Delphi, Greece
3/31(金)-4/2(日) Algebra and Combinatorics 2006 Manila, Philippines
4/24(月)-25(火) 第19回 回路とシステム軽井沢ワークショップ 軽井沢プリンスホテル西館
5/21(日)-23(火) STOC'06 Seattle, Washington, USA
6/5(月)-7(水) SoCG'06 Sedona, Arizona, USA
6/20(火)-22(木) The Second International Conference on Algorithmic Aspects in Information and Management 香港
6/22(木)-24(土) WG2006 (グラフアルゴリズムの会議です) ノルウェー, ベルゲン
6/25(日)-28(水) INFORMS International Hong Kong 2006 香港
7/3(月)-5(水) SIROCCO2006 Chester, United Kingdom
7/6(木)-8(土) SWAT 2006 リガ (ラトビア)
7/9(日)-16(日) ICALP 2006 ベネチア (イタリア)
7/30(日)-8/4(金) ISMP2006 Rio de Janeiro, Brazil
8/15(火)-18(金) COCOON 2006 台北（台湾）
8/22(火)-24(木) IFIP/TCS 2006 Santiago, Chile
9/11(月)-15(金) ALGO 2006 チューリッヒ (スイス)

このニュースレターについて

ニュースレター各号は電子メールで配布する予定です．短い記事や連絡事項は全て掲載しますが，長い記事，イベントの詳細などはwebページに掲載する予定です．webページには詳細まで全てを載せた完全版を掲載して，目次，あるいは各記事の末尾のURLを参照すると，web版の同じ記事を参照できるようにいたします．

記事は，各回，1つの研究課題に担当をお願いする予定です．各研究課題で2000-4000字程度，研究に関わる記事を書いていただければと思います．通常，このようなニュースレターでは，研究成果を報告するのが一般的だと思われますが，この特定領域では「研究者の交流」に焦点を当てたいため，「研究の成果以外」の記事を面白く解説していただければと思います．例えば，最近参加した国際会議の情報を，どのようなものが流行っていたか，何が面白かったか，などの主観的な解説を交えて報告したり，最近考えている問題，あるいはオープン問題を，この辺までは解けるがここがうまくいかない，といった解説を交えて紹介する，という形です．

また，研究者間の交流を促進するため，各研究者の，国内外の会議への出席予定を集約して掲載していこうと考えています．研究者の交流には，顔をあわせる回数を増やすことが肝要です．他の研究者の参加予定

がわかれば，会議への出席のモチベーションを高めることにもつながり，それがディスカッションや研究成果を生むきっかけにもなるでしょう．特定領域メンバーの皆さんには，自分のわかる範囲で，国内外の会議・研究会の情報と，自分の参加予定を教えていただければと思います．

この他，個人からの寄稿を募集いたします．100-1000字程度で，情報宣伝されたいことを自由な形式で書いて送っていただければ，掲載いたします．メールで配布する関係上，テキスト形式のものしか扱えませんが，そこはご了解お願いいたします．

次号は6月ごろを予定しています．

★ ニュースレター編集委員では，皆様からのご意見をお待ちしております．編集方針や内容の追加など編集全体にかかわることから細かいことまで，幅広いご意見をお願いいたします．

■■ 新世代の計算限界 ニュースレター ■■

編集委員長 宇野 毅明 uno@nii.jp（問合せ先）

副編集委員長 牧野 和久 makino@sflab.sys.es.osaka-u.ac.jp

平成17年度 第1回 全体会議

日時　平成 17 年 6 月 16 日 (木), 17 日 (金)

会場　国立情報学研究所 12 階会議室

プログラム

6 月 16 日 (木)

10:00 – 10:50　A01–A10 班の研究紹介

11:00 – 12:00　ポスターセッション (A01–A10 班)

12:00 – 14:00　幹事会

14:00 – 14:30　B01–B06 班の研究紹介

14:40 – 15:40　ポスターセッション (B01–B06 班)

16:00 – 16:55　C01–C11 班の研究紹介

17:05 – 18:00　ポスターセッション (C01–C11 班)

6 月 17 日 (金)

9:30 – 12:00　全体会議

13:30 – 14:15　時間枠つき配送計画問題に対するメタ戦略アルゴリズム
柳浦睦憲 (京都大学) 359

14:15 – 15:00　孤立したクリークの線形時間列挙
伊藤大雄 (京都大学) 364

15:30 – 16:15　Compact Encoding of Plane Triangulations with Efficient Query Support
中野眞一 (群馬大学) 369

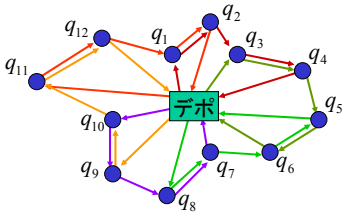
16:15 – 17:00　オンライン予測の理論と応用
瀧本英二 (東北大学) 373

時間枠つき配送計画問題に対するメタ戦略アルゴリズム

柳浦睦憲 （京都大学）
with
橋本英樹（京都大学） 茨木俊秀（関西学院大学）
今堀慎治（東京大学） 久保幹雄（東京海洋大学）
増田友泰（アクセンチュア） 野々部宏司（法政大学）
祖父江謙介（トヨタ） 宇野毅明（国立情報学研究所）

時間枠付配送計画問題

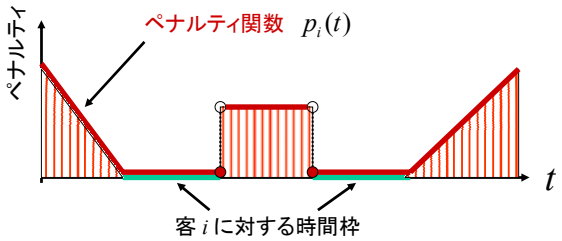
入力: 節点$V = \{0, 1, \ldots, n\}$ (0: デポ, $i \geq 1$: 客), 車両$M = \{1, \ldots, m\}$,
距離 d_{ij}, 移動時間 t_{ij}, 容量 Q_k, 重み q_i
出力: 総距離を最小にする車両ルート
制約: 容量制約 および 時間枠制約



容量制約
$q_1 + q_2 + q_3 + q_4 \leq Q_1$
$q_5 + q_6 + q_7 + q_8 \leq Q_2$
$q_9 + q_{10} + q_{11} + q_{12} \leq Q_3$

一般化時間枠

各客はサービスを受ける時刻に対する希望を提示する



$p_i(t)$: 非凸かつ不連続でもよい
（ただし区分線形関数のみ）

目的関数

$$cost(\sigma) = D(\sigma) + T(\sigma) + Q(\sigma)$$

σ	車両スケジュール
$D(\sigma)$	総距離
$T(\sigma)$	総時間ペナルティ
$Q(\sigma)$	総容量超過

時間枠制約および容量制約
⇩
ソフト制約

計算例

配送計画問題の基本モデルの問題例

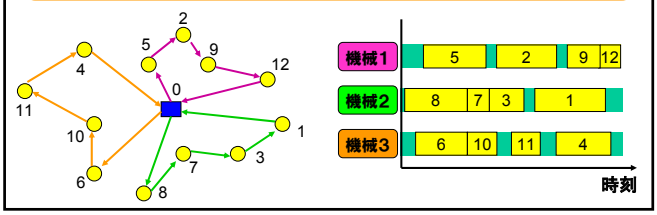
計算例1

時間枠つきの問題例

計算例2

スケジューリング

客	⇔	仕事
車両	⇔	機械
移動時間	⇔	処理時間とセットアップ時間
時間枠制約	⇔	準備時間や納期など
容量制約	⇔	資源制約



問題構造と探索空間

車両スケジュール:

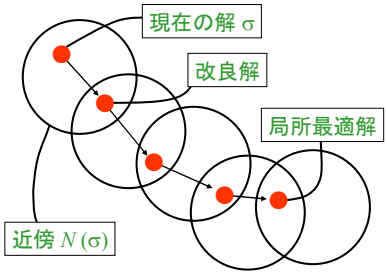
(a) 客の車両への割当
(b) 各車両における客の訪問順序
(c) 各客のサービス開始時刻

(a) と (b) ⟶ 局所探索法により探索

(c) ⟶ 動的計画法により最適に解く
((a)と(b)は固定という条件の下で)

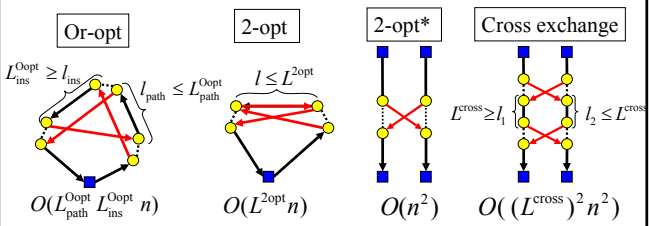
局所探索法

適当な初期解から始め、現在の解 σ の近傍 $N(\sigma)$ の中に σ よりもよい解 σ′があれば σ:= σ′と置き換える操作を反復



- 探索空間
- 解の評価法
- 近傍
- 初期解生成法

近傍操作



近傍内の解: 現在の解のパスを高々4つつなぎ合わせることで生成できる

最適サービス開始時刻決定問題

もともとの目的関数 $cost(\sigma) = D(\sigma) + T(\sigma) + Q(\sigma)$

問題（車両ルートは固定）
Optimal Start Time Problem (OSTP)

入力: 車両 k の客の訪問順序
$\sigma_k(0), \sigma_k(1), \ldots, \sigma_k(n_k), \sigma_k(n_k+1)$

出力: 車両 k の時間ペナルティを最小にするような、各客のサービス開始時刻

⟹ 動的計画法により厳密に最適化

OSTPの関連研究

時間ペナルティ関数が一般の場合

Ibaraki, Imahori, Kubo, Masuda, Uno & Yagiura, 2005

時間ペナルティ関数が凸の場合

- 関連研究:
  Garey, Tarjan & Wilfong 1988
  Powell & Solomon 1992
  Davis & Kanet 1993
  Taillard, Badeau, Gendreau, Guertin & Potvin 1997
  Tamaki, Komori & Abe 1999
  Ahuja & Orlin 2001
  Hochbaum & Queyranne 2003
- OSTP は線形計画問題になる
- isotonic median regression 問題を含む
- $O(n_k \log n_k)$ 時間のアルゴリズムあり

動的計画法

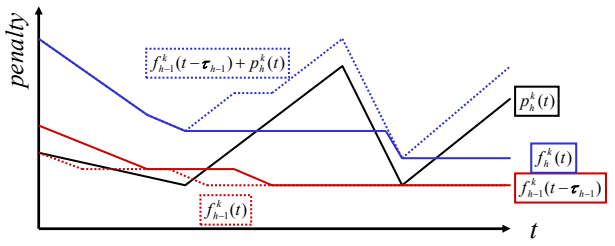
$f_h^k(t)$: 客 $\sigma_k(0), \sigma_k(1), \ldots, \sigma_k(h)$ が時刻 t 以前にサービスされるときのこれらの客の時間ペナルティの最小値

$$f_0^k(t) = \begin{cases} +\infty, & t \in (-\infty, e_0) \\ 0, & t \in [e_0, +\infty) \end{cases}$$

$$f_h^k(t) = \min_{t' \leq t} (f_{h-1}^k(t' - \tau_{h-1}) + p_h^k(t')), \quad 1 \leq h \leq n_k + 1$$

e_0: 車両のデポからの出発可能時刻
τ_h: h 番目の客から $h+1$ 番目の客への移動時間
$p_h^k(t)$: h 番目の客の時間ペナルティ関数

動的計画法の実行例



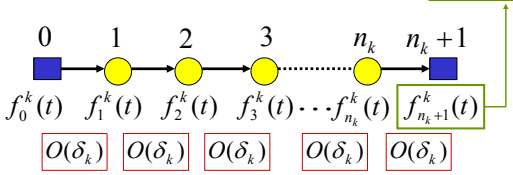
$$f_h^k(t)=\min_{t'\le t}(f_{h-1}^k(t'-\tau_{h-1})+p_h^k(t'))$$

動的計画法の計算時間

n_k: 車両 k のルート内の客数

δ_k: 車両 k のルート内の客の時間ペナルティ関数の線形区分数の合計 (通常 $\delta_k=O(n_k)$)

最適ペナルティ値決定



総計算時間: $O(n_k\delta_k)$

時間ペナルティの評価の高速化

アイデア
- 近傍内の解の評価に現在の解 σ の $f_h^k(t)$（計算済）を再利用
- 解が更新されたときには動的計画法(DP)を再計算

ペナルティ関数が一般の場合:
近傍内の解の評価: $O(\delta_k)$
解の移動の際のDPの再計算: $O(n_k\delta_k)$

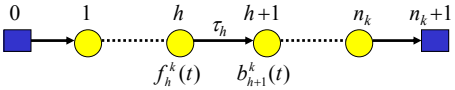
ペナルティ関数が凸の場合:
近傍内の解の評価: $O(\log \delta_k)$
解の移動の際のDPの再計算: $O(\delta_k \log \delta_k)$

平衡木を利用

時間ペナルティの高速計算

$b_h^k(t)$: 客 $\sigma_k(h), \sigma_k(h+1), \ldots, \sigma_k(n_k+1)$ が時刻 t 以降にサービスされるときのこれらの客の時間ペナルティの最小値

$f_h^k(t)$ と同様に計算できる



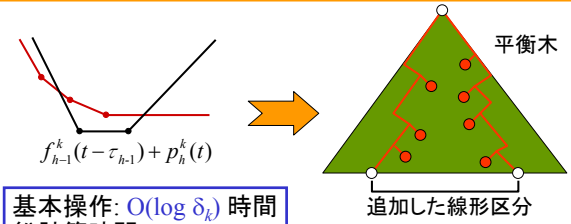
ルート k の最小ペナルティ: $\min_t\left(f_h^k(t)+b_{h+1}^k(t+\tau_h)\right)$

- ペナルティが一般の場合$O(\delta_k)$, 凸の場合$O(\log \delta_k)$時間
- 2-opt*には直接利用可．それ以外の場合は交換されるパス内の客の$f_h^k(t)$を効率よく再計算できるよう探索順序に工夫の必要あり．

DP: 時間ペナルティが凸の場合

$p_i(t)$: 全ての i に対して凸 $\Rightarrow f_h^k(t)$: 凸

$f_h^k(t)$ を平衡木で表現
- 葉節点 ↔ $f_h^k(t)$の線形区分のひとつ
- 根から葉へのパス
  ↔ 葉に対応する線形区分の傾きや切片などの情報



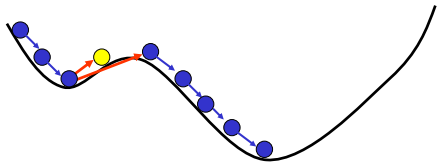
基本操作: $O(\log \delta_k)$ 時間
総計算時間: $O(\delta_k \log \delta_k)$

効率化のアイデア

- 近傍の制限
  - 近傍リスト: TSP や VRP に対し大きな効果
  - サービス開始時刻が近い客のペア
- 動的計画法の関数 $f_h^k(t)$ の区分数の削減
  - 関数 $f_h^k(t)$ の線形区分の中で対応するペナルティ値が非常に大きいものを削除

反復局所探索法 (ILS)

- 局所探索を多数反復
- 過去の探索で得られたよい解に少しのランダムな変形を加えたものを初期解



計算実験

問題例

- Gehring & Homberger のベンチマーク問題例
  （Solomonの問題例と同様の生成法．より大規模）
- 時間枠制約と容量制約: 絶対制約
- 客数: 200, 400, 600, 800, 1000
- 各サイズに対して60問（全部で300問）

計算環境と実験方法

- C 言語; PC（Pentium IV 2.8GHz）
- 絶対制約 → ペナルティ関数; 適応的重み調整
- 出力する解: 絶対制約を満たす解
- 車両数: 既知の最良値（± 1）

number of customers		best known	MB (2003)	GH (2002)	LC (2003)	our ILS
200	CNV	692	694	696	694	694
	CTD	169281	168537	179328	173061	170331
	time (min)		5.88	3.83	21.66	33.3
400	CNV	1386	1389	1392	1390	1384
	CTD	392444	390386	428489	408281	401285
	time (min)		12.49	12.95	43.32	66.6
600	CNV	2076	2082	2079	2088	2070
	CTD	799355	796172	890121	836261	827192
	time (min)		29.39	23.53	64.97	100
800	CNV	2754	2760	2765	2766	2750
	CTD	1429914	1535849	1361586	1475281	1426133
	time (min)		42.32	106.53	86.63	133.3
1000	CNV	3438	3446	3446	3451	3434
	CTD	2106125	2078110	2290367	2225366	2169452
	time (min)		440.82	361.2	108.29	166.6

CNV: cumulative number of vehicles
CTD: cumulative total distance

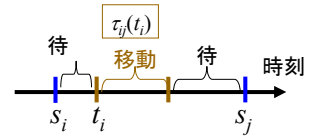
MB: Mester and Bräysy
GH: Gehring and Homberger
LC: Le Bouthillier and Crainic

より高い汎用性を目指して

- 時刻依存の移動時間および移動コスト
  - 朝夕のラッシュ
  - 生産ラインにおけるセットアップ
- 移動時間が可変，移動時間に応じたコスト
  - 有料道路の利用により移動時間を短縮
  - 特急仕事として高速処理

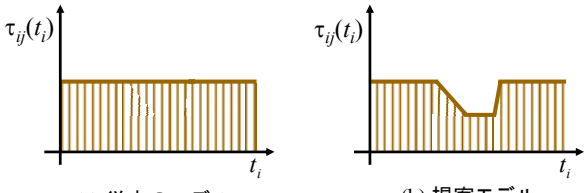
→ 一般の時間ペナルティをもつ問題に上のいずれかを追加した問題を考える

時刻依存の移動時間 $\tau_{ij}(t_i)$



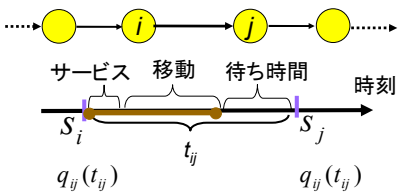
- 連続
- FIFO

$$t < t' \Rightarrow t + \tau_{ij}(t) < t' + \tau_{ij}(t')$$

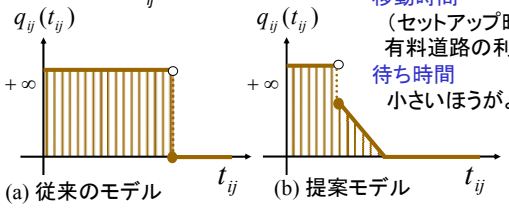


(a) 従来のモデル　(b) 提案モデル

移動時間コスト関数 $q_{ij}(t_{ij})$



サービス時間
（処理時間）
人手やコストをかけて短縮可能
移動時間
（セットアップ時間）
有料道路の利用など
待ち時間
小さいほうがよい場合



(a) 従来のモデル　(b) 提案モデル

計算の複雑さに関する結果

- 時刻依存の移動時間および移動コスト
  - 移動時間関数の総複雑度に対して線形時間のDP
  - 移動時間関数の複雑度が各客ペアでO(1)
    → 移動時間が定数の場合と同程度の計算時間
- 移動時間が可変，移動時間に応じたコスト
  - 移動時間コスト関数が一般
    → NP困難; 擬多項式時間のDP
  - 移動時間コスト関数が凸（時間ペナルティ関数は一般）→ 多項式時間のDP

まとめ

- 時間枠に対する要求を一般的なペナルティ関数として表現できる汎用的な問題の定式化
  → 時間ペナルティ最小化問題を解く必要性
  → 動的計画法の提案
- 高速化のさまざまな工夫
- Gehring & Homberger のベンチマーク問題例に対する良好な結果
- 移動時間に対する汎用的な定式化

今後の課題

- 異なるタイプの汎用化
- 配送ルートの探索能力の向上
- 大規模問題例への適用
- 時間枠の取り扱い →
  より実装しやすい単純なアルゴリズムで
  高速かつ実用的なものの開発
  cf. 提案手法はいずれも非常に複雑で実装困難

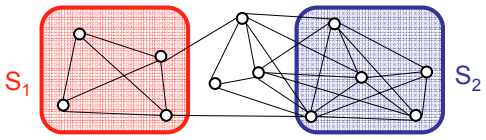


クリークと列挙

- 最大クリーク問題
  - 近似度 $\Omega(n^{1-\varepsilon})$ [Hastad 99]
- 極大クリークの列挙
  - O(nm)時間／個[Tsukiyama, et al. 77]
  - $O(\Delta^4)$時間／個[Uno03]（Δは最大次数）
  - しかし指数($O(3^{n/3})$)個存在[Moon, et al. 65]

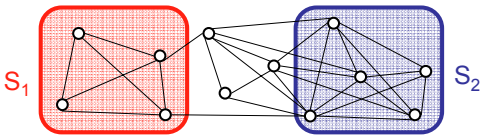
Why Cliques?

- Inside: Densely connected.
- Inside-Outside: Sparsely connected.



Isolated cliques

- Let $c>0$ be a constant. A clique $S \subseteq V$ with k vertices is an c-isolated clique if $|E(S)|<ck$. ($E(S)$={edges between S and V-S}.)
- 1-isolated cliques = isolated cliques.



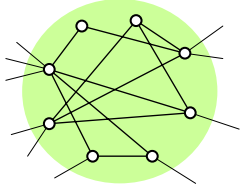
$|E(S_1)=2<4 \Rightarrow$ isolated clique

$|E(S_2)=9 \geqq 5 \Rightarrow$ non isolated clique

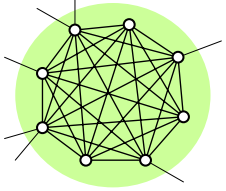
Related work

- Flake, Lawrence, Giles (2000)
  - Community $S \subset V$: $|E(v,S)|>|E(v,V-S)|$ $\forall v \in S$.

Community of Flake, et al.



Isolated clique

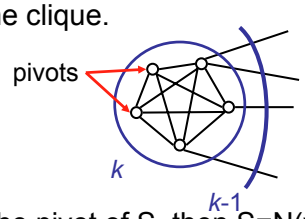


Preliminary Result

- Theorem 0.1. All isolated cliques can be enumerated in linear time.
- Corollary 1. The # of isolated cliques is $O(m)$ for any graph.

Observation for Proving Theorem 0.1

- Lemma 1. An isolated clique has a vertex (called a pivot) that has no outgoing edge from the clique.



- If v is the pivot of S, then S=N(v)∪{v}.

Strategy of enumeration

- Check each vertex whether or not it can be a pivot.
- Sort and renumber all vertices as $d(v_1) \leqq d(v_2) \leqq \ldots \leqq d(v_n)$.
- If $\exists j>i$, $v_j \in N(v_i)$ (adjacent vertices of v_i), v_i can be ignored (we can consider that the vertex having the minimum index in a isolated clique is the pivot): Test (a).

Observation 2

- Lemma 2. If S is an isolated clique and v is the pivot, then $\sum_{w \in S} d(w) < (d(v)+1)^2$. (1)
- Proof. Let k=|S|=d(v)+1. $\sum_{w \in S} d(w) < k(k-1)+k=k^2 = (d(v)+1)^2$. □

Observation 2

- Lemma 3. If v has the minimum indices in S=N(v)∪{v} and S satisfies (1), then $d(w)<2d(v)+1 \quad \forall w \in S$.
- Proof. Let k=|S|=d(v)+1. If $d(w) \geqq 2d(v)+1=2k-1$ for a $w \in S$, $\sum_{w \in S} d(w) \geqq (k-1)^2+2k-1=k^2 = (d(v)+1)^2$, contradiction. □

Strategy 2

- If v passes Test (a), we check whether S=N(v)∪{v} satisfies (1): Test (b). (This can be done in O(d(v)) time.)
- If N(v) passes this test, $d(w)<2d(v)+1=O(d(v)) \quad \forall w \in N(v)$ from Lemma 3.

Observation 3

- Lemma 4. If $S=\{v=w_1, \ldots, w_k\}$ is an isolated clique and v is the pivot of S ($d(w_1) \leqq \ldots \leqq d(w_k)$), then $S_i=\{w_1, \ldots, w_i\}$ has at most i-1 outgoing edges from S.
- Proof. Assume that $|E(S_i,V-S)| \geqq i$. Then $d(w_i) \geqq d(v)+1$, and hence $d(vj) \geqq d(v)+1$ for all j=i+1, ..., k. Therefore $\sum_{w \in S} d(w) = \sum_{w \in Si} d(w) + \sum_{v \in S-Si} d(w) \geqq i+(k-i)=k$, contradiction.

Strategy 3

- Assume that v passed Tests (a) and (b) (primal tests).
- Let $S=N(v)\cup\{v\}=\{v=w_1, w_2, ..., w_k\}$ $(d(w_1)\leqq d(w_2)\leqq\ldots\leqq d(w_k))$.
- Clique test: From i=1 to k,
  - check whether (1) w_i is adjacent to $w_1, ..., w_{i-1}$ (i.e., $S_i=\{w_1, ..., w_i\}$ is a clique) and
  - (2) S_i has at most i-1 outgoing edges from S.
  - If not, *v* is not a pivot and then skipped (finish checking v).

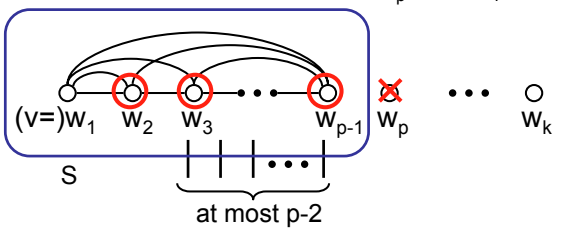
Running time

- Sorting vertices by their degrees: O(m).
- Primal tests: O(d(v)) for each $v\in V$, i.e., O(m).
- Clique test: Assume the test breaks at w_p. $d(w_1)+d(w_2)+\ldots+d(w_p)=O(w_p^2)\rightarrow O(m^2)$?

→ More precise estimation!

Running time (Cont.)

- Assume the test is done until w_p. $(k=d(v_1)+1)$



By v: $O(d(w_1)+d(w_2)+\ldots d(w_p))=O(pk)$

By other pivots: $O((p-1)d(w_{p-1}))=O(pk)$

} O(pk)

→ Amortize as $O(k)=d(w_i)$ for each vertex in S.

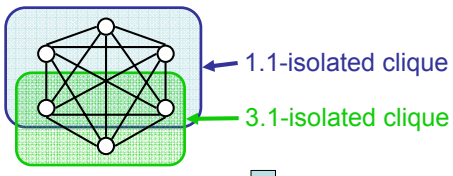
Running time (Cont.)

- Sorting vertices by their degrees: O(m).
- Primal tests: O(d(v)) for each $v\in V$, i.e., O(m).
- Clique test: O(d(v)) for each $v\in V$, i.e., O(m).

→ O(m). ··· Theorem 0.1 is proved.

Extension

- Theorem 0.1. All isolated cliques can be enumerated in linear time.
- For general c-isolated cliques?



- Maximal ones are important.

Results

- Theorem 1. All maximal *c*-isolated cliques of a graph with *n* vertices can be enumerated in $O(c^5 2^{2c} m)$ time.
- Corollary 1. For any constant *c*, all maximal *c*-isolated cliques can be enumerated in linear time.
- Corollary 2. For any $c=O(\log n)$, all maximal *c*-isolated cliques of a graph with n vertices can be enumerated in polynomial time.

Results (cont.)

- Theorem 2. Let c, x, and y are functions of n s.t. $c=xy$. There is a graph with m edges for which the # of maxmal c-isolated cliques is $\Omega((2x^y/c^2)m)$.

- Cor. 3. If $c=\omega(1)$, there is a graph with n vertices consisting of super-linear # of maximal c-isolated cliques.
- Cor. 4. If $c=\omega(\log n)$, there is a graph with n vertices consisting of super-polynomial # of maximal c-isolated cliques.

Results (cont.)

- Cor. 1. If $c=O(1)$, all maximal c-isolated cliques can be enumerated in linear time.
- Cor. 3. If $c=\omega(1)$, there is a graph consisting of super-linear # of maximal c-isolated cliques.

- $c=\Theta(1)$ is the tight bound for enumerating all maximal c-isolated cliques in linear time.

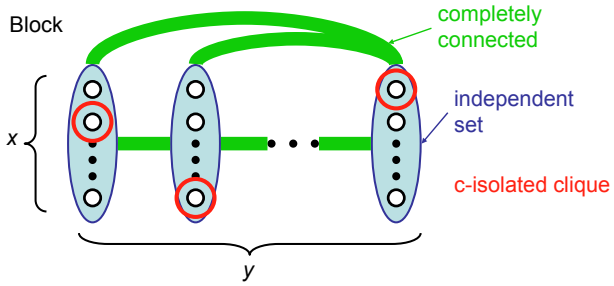
Results (cont.)

- Cor. 2. If $c=O(\log n)$, all maximal c-isolated cliques can be enumerated in polynomial time.
- Cor. 4. If $c=\omega(\log n)$, there is a graph consisting of super-polynomial # of maximal c-isolated cliques.

- $c=\Theta(\log n)$ is the tight bound for enumerating all maximal c-isolated cliques in polynomial time.

Proof of Theorem 2

- Theorem 2. Let c, x, and y are functions s.t. $c=xy$. There is a graph with m edges for which the # of maxmal c-isolated cliques is $\Omega((2x^y/c^2)m)$.



Proof of Corollaries 3 and 4

- If $c=\omega(1)$, then by letting x=2, y=c/2 $(2x^y/c^2)m$ becomes super-linear.
- If $c=\omega(\log n)$, then by letting x=c/log$n$, y=log$n$ $(2x^y/c^2)m$ is super-polynomial.

Other Results: Pseudo-Clieques

- Let $\alpha(k)$ and $\beta(k)$ are functions. Pseudo-Clique $PC(\alpha, \beta)$ is a vertex-proper-subset $S \subset V$ ($|S|=k$) s.t.
- $\mathrm{av}_{v\in S}\, d_{G(S)}(v) \geqq \alpha(k)$ and
- $\min_{v\in S}\, d_{G(S)}(v) \geqq \beta(k)$.

Results for PC

- Theorem 3. Suppose $f(k)=\Omega(1)$ and $0<\varepsilon<1$ is a constant.
  - There is a graph including super-poly. # of maximal isolated PC(k-f(k),k^{ε}).
  - There is a graph including super-poly. # of maximal isolated PC(k-k^{ε},k/f(k)).
- Proposition 1. All maximal isolated PC(α,c_1k) and PC(k-c_2,k^{ε}) are enumerated in poly. time for constant $c_1<1$ and $c_2 \geqq 1$.

Results for PC (Cont.)

- Theorem 4. There is a graph including super-poly. # of maximal isolated PC(k-$(\log k)^{1+\varepsilon}$,k/$(\log k)^{1+\varepsilon}$) for any $0<\varepsilon$.
- Theorem5. All maximal isolated PC(k-logk,k/logk) can be enumerated in poly. time.

Summary

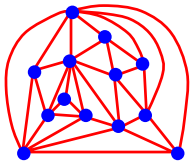
- Introduce f-isolated cliques with parameter function c.
- All c-isolated cliques can be enumerated in linear time for any constant c.
- $c=\Theta(1)$ is the tight bound of linear time enumeration.
- All c-isolated cliques can be enumerated in poly. time if c=O(logn).
- $c=\Theta(\log n)$ is the tight bound of poly. time enumeration.

新世代の計算限界　　全体会議　2005/06/17

Compact Encoding of Plane Triangulations
with Efficient Query Support

クエリを効率的にサポートする
極大平面グラフのコンパクトな符号化

山中克久　○中野眞一
群馬大学



m 辺

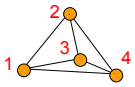


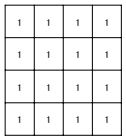
2m bit　＋少し

000011100110111001100111001010110110011001

超大規模なグラフを扱いたい

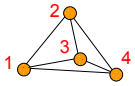
隣接行列　　n^2 bit

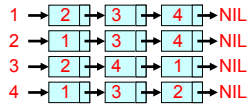




指定した
2点間に
辺ある？

隣接リスト　　2m log n　bit　＋(ポインタ)





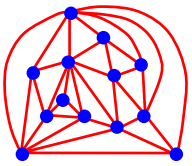
指定した
1点に
接続する
辺のリストは？

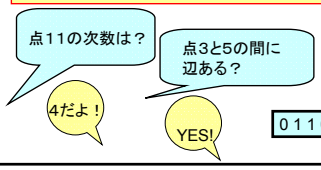
超大規模なグラフを扱いたい

- グラフスパナー
  （本質的でない辺を削除）
  (非可逆)

- 巧妙な符号化 (定数bit / 各辺)
  （＋クエリの定数時間サポート）

インターネットのグラフ
3Dモデル





高速化？　ページング減少？
高速クエリ

011001110010101101100110001

既知の結果その1

・もし、対象のグラフがt個あれば、
　平均の符号長は　log t bit 以上必要
・情報理論的な下限　= log t
　極大平面グラフの場合
　　1.08 m bit　[Tutte 62]
　木の場合　　2m – o(n) bit
・任意の列挙アルゴリズムを利用して符号化できる
　k番目のグラフを　kの2進数表記に符号化する
　ただし、符号化・復号化に指数時間かかる

既知の結果その2

クエリサポートなし

・一般の平面グラフ	4m bit	[Turan 84]
・一般の平面グラフ	3.58m bit	[Keeler他　95]
・極大平面グラフ	1.53m bit	[同上]
・極大平面グラフ	1.33m bit	[He他　99]
・極大平面グラフ	1.33m bit	[Poulalhon 03] ICALP 2003
	1.08m bit 下限	

グラフを符号化して送り、複合化して使用

既存の結果その3

クエリサポートあり

・木	2m +o(n)bit	[Jacobson 89] FOCS 89
・一般平面グラフ	2m+8n+o(n)bit	[Munro他97] FOCS 97
・一般平面グラフ	2m+2n+o(n)bit	[Chiang他01] SODA 01
・極大平面グラフ	2m+n+o(n)bit	[Chuang他]
一般平面グラフ	2m+5n+o(n)bit	ICALP 98
・極大平面グラフ	2m+o(n)bit	[中野 2005]

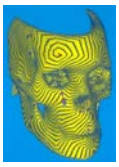
グラフを符号化して記憶し、複合化せずに使用

なぜ平面グラフ？



- 道路、鉄道、川等のネットワークは平面
- 交差点に点を追加すれば平面グラフ
- 何枚かの平面グラフの重ね合わせで一般のグラフに

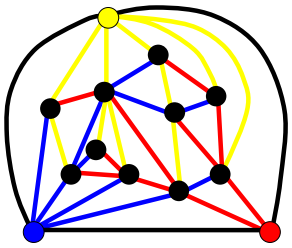
なぜ極大平面グラフ？

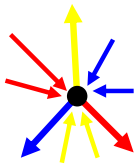


- ワイヤーフレームモデル
- 平面双対
- 扱いやすいから

アイディアその1

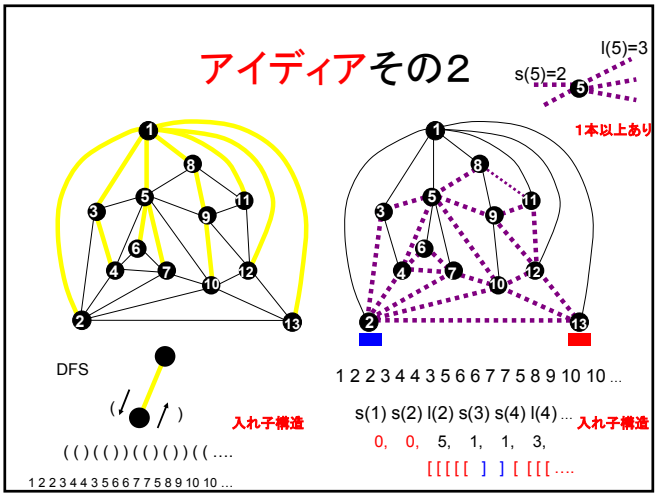
- リアライザ

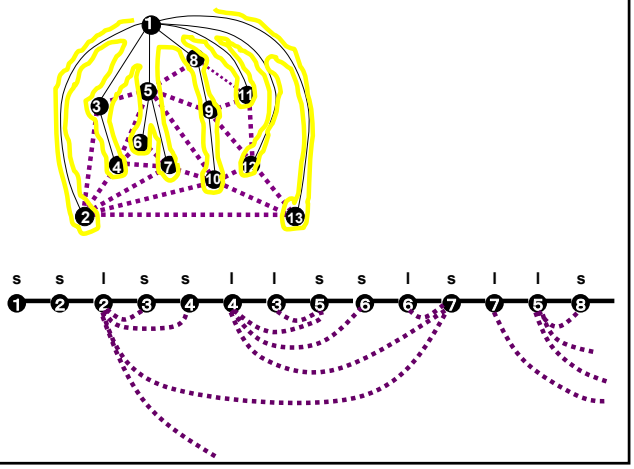




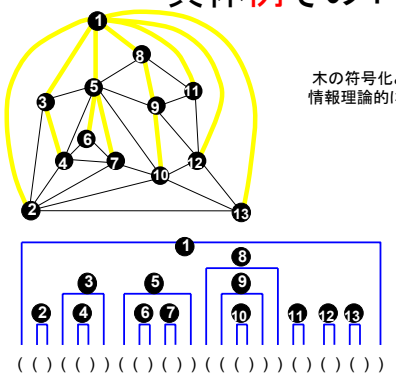
グラフ描画
フロアプラン

アイディアその2



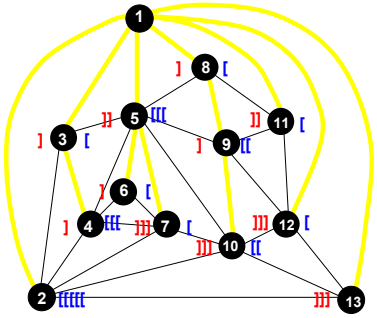


具体例その1

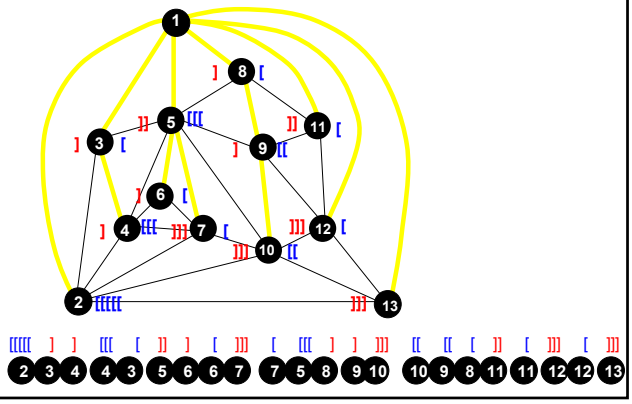


木の符号化としては
情報理論的に最適！

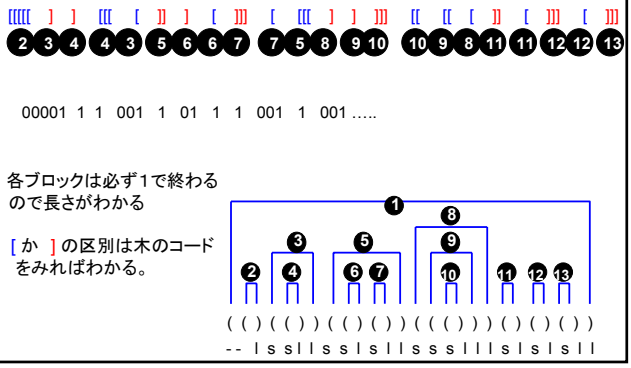
具体例その2



具体例その3



具体例その4



00001 1 1 001 1 01 1 1 001 1 001 .....

各ブロックは必ず1で終わるので長さがわかる

[か] の区別は木のコードをみればわかる。

bit 数の見積もり

- 各辺につき2bit 必要　　計2m bit

- 木の辺　　-----　(と)
- 木以外の辺　-----　[と]

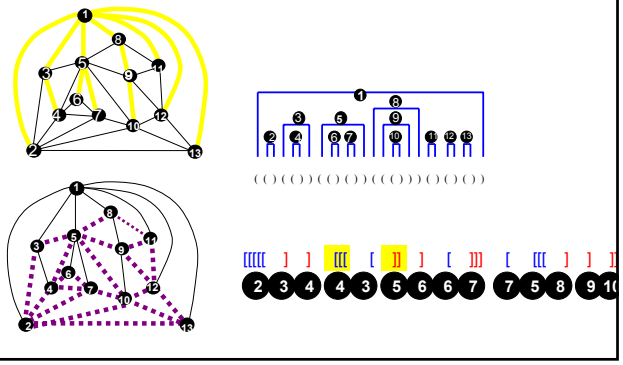
クエリのサポートその1

既知の結果（多段のテーブルを利用）
[Munro他 97 + Chiang他 01]

- bit列が与えられたとき、o(n) bitの補助テーブルを利用して rank(p), select(i) を 定数時間で計算できる。
- バランスされた括弧の列が与えられたとき、o(n) bit の補助テーブルを利用して findclose(p), findopen(p), enclose(p), wrapped(p) を定数時間で計算できる。

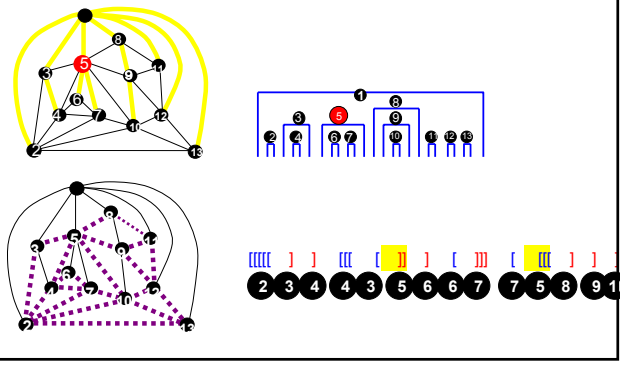
隣接クエリ

入力 2点　　出力 2点間に辺あり・なし



次数クエリ

入力 点v　　出力 vの次数



隣接点のリスト

- 隣接点のリストをO(d(v))時間で作成できる

略

まとめ

既知のベスト（クエリサポートつき）
極大平面グラフ　2m+n+o(n)bit　[Chuang他 ICALP98]

今回の結果
極大平面グラフ　2m+o(n)bit　[中野 05]

主なアイディア
リアライザの3本の木を
1本　＋　2本　とみなすこと

おしまいです

- 御静聴ありがとうございます。

- 質問・コメント・アドバイス等歓迎します。
- 応用？

中野眞一（群馬大学）

オンライン予測の理論と応用

東北大学大学院情報科学研究科
A01班　瀧本 英二

クイズ王に匹敵する問題

「タイガーウッズは寅年生まれである．○か×か？」



正解は

×

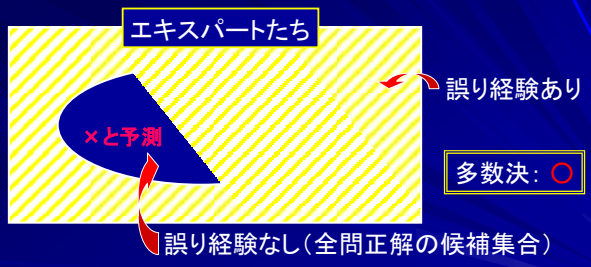
タイガーウッズはウサギ年生まれ

二分法（Halving Algorithm）

- クイズ王（エキスパート）N人のうち少なくとも1人は全問正解すると仮定
- 二分法：
  「これまで一度も間違えていないエキスパートたちの予測の多数決に従う」

誤り回数は高々$\lfloor \log_2 N \rfloor$

二分法の解析



- 間違えたとき，候補は半分以下
- 誤り回数が m ⇒ 候補数 $\leq N / 2^m$　$m \leq \lfloor \log_2 N \rfloor$
- 仮定より，　$1 \leq$ 候補数

二分法 ∈ 乗算型重み更新

- $v_i \in [0,1]$：エキスパート i の重み
- 初期重み $v_i = 1/N$
- $x_i \in \{-1,1\}$：エキスパート i の予測値
- 二分法の出力：重みつき多数決
  $\mathrm{sgn}(\sum_{i=1}^{N} v_i x_i \geq 0)$
- 重み更新
  $v_i \leftarrow v_i b_i$ ／ 規格化

ただし，
$b_i = 1$　・・・エキスパート i が正しかったとき
0　・・・エキスパート i が間違えたとき

重みつき平均アルゴリズム
—— 全問正解者がいない場合 ——

- 重み更新
  $v_i \leftarrow v_i b_i$ / 規格化
  ただし,
  $b_i = 1$ ・・・ エキスパート i が正しかったとき
  $\epsilon_0 \eta$ ・・・ エキスパート i が間違えたとき

$$\text{誤り回数} \le m^* + O\left(\sqrt{m^* \ln N} + \ln N\right)$$

m^* は最も成績の良かったエキスパートの誤り回数

パーセプトロン ∈ 加算型重み更新

- 学習目標 $v^* = (0, ..., 1, ..., 0)$ の線形分離関数（シングルトン）の学習
- パーセプトロンの出力：重みつき多数決
  $y' = \mathrm{sgn}(\sum_{i=1}^{N} v_i x_i \ge 0)$
- 重み更新
  $v_i \leftarrow v_i + \eta (y - y') x_i$
  ただし, y は真の値, η は学習定数
- 誤り回数 = $\Omega(N)$　cf. 二分法は $\lfloor \log N \rfloor$

パーセプトロン vs Winnow
加算型重み更新　　乗算型重み更新

- 学習目標が $v^* = (1, 0, 1, 0, 0, ..., 1)$ のとき
  ただし, $k = \sum_i v^*_i$
- パーセプトロン
  $v_i \leftarrow v_i + \eta (y - y') x_i$
  誤り回数 = $\Omega(kN)$
  カーネル手法と整合する
- Winnow
  $v_i \leftarrow v_i \exp(\eta (y - y') x_i)$ / 規格化
  誤り回数 = $O(k \log N)$　・・・ attribute efficient
  一般に, カーネル手法と整合しない

この問題と解析の特徴

- オンライン性
  - 予測と結果の提示が交互に繰り返される
- ユニバーサル性
  - エキスパートの予測や結果の系列に対して何の仮定もおかない
- 最悪値評価
  - アルゴリズムの性能を最悪の場合で評価する
- 相対評価
  - アルゴリズムの性能を，最適なエキスパートの成績を用いて相対的に評価する

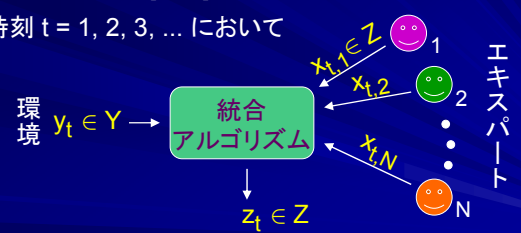
オンライン予測

- モデル化
  - エキスパート統合モデル
- 統合アルゴリズム
  - Winnow (1988)
  - Aggregating Algorithm (1990)
  - Weighted Majority, Weighted Averaging (1993,1994,1999)
  - GD, EG family (1994)
  - Potential-Based (2001)
  - Following Perturbed Leader (2003)
- 応用
  - 学習，符号化，統計的推定，投資，ゲーム理論，最適化，…

エキスパート統合モデル

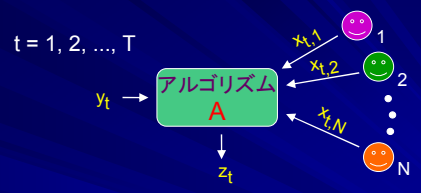
Y ・・・真の結果値の集合
Z ・・・予測値の集合
L: $Y \times Z \to [0,\infty]$ ・・・損失関数

各時刻 t = 1, 2, 3, ... において



アルゴリズムの損失：　$L(y_t, z_t)$
エキスパート i の損失：$L(y_t, x_{t,i})$

相対損失(regret)



- アルゴリズム A の累積損失: $\mathrm{Loss}_A^T = \sum_{t=1}^T L(y_t, z_t)$
- エキスパート i の累積損失: $\mathrm{Loss}_i^T = \sum_{t=1}^T L(y_t, x_{t,i})$
- アルゴリズム A の相対損失: $R_A^T = \mathrm{Loss}_A^T - \min_i \mathrm{Loss}_i^T$

目標: $R^T{}_A \to$ small

クイズ王に匹敵する問題

- Y = {0,1}
- Z = {0,1}
- L(y, z) = |y − z|

} に相当

$\mathrm{Loss}^T{}_A$ = アルゴリズム A の誤り回数
$\mathrm{Loss}^T{}_i$ = エキスパート i の誤り回数
m^* = $\min_i \mathrm{Loss}^T{}_i$

$$\exists A, \quad R_A^T \le 4\sqrt{m^* \ln N} + 2.5 \log_2 N$$

統合アルゴリズムの原理

Vovk の Aggregating Algorithm (AA)

- 各エキスパート i に対し，重み $v_{t,i}$ を保持
  $(v_{t,i} \ge 0, \Sigma_{1 \le i \le N} v_{t,i} = 1)$
- 予測の統合

$$\forall y \in Y, L(y, z_t) \le -c(\eta) \ln \sum_{i=1}^N v_{t,i} e^{-\eta L(y, x_{t,i})}$$

を満たす $z_t \in$ Z を出力
c(η): 問題 (Y, Z, L) に固有の値

- 重み更新

$$v_{t+1,i} = \frac{v_{t,i} e^{-\eta L(y_t, x_{t,i})}}{\text{規格化係数}}$$

AAの性能

- **定理**

任意のエキスパート，任意の環境の振る舞いに対し，
最適なエキスパートを i^* = argmin_i $\mathrm{Loss}^T{}_i$ とすると，

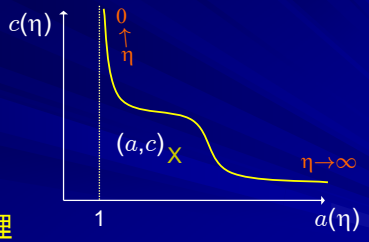
$$\mathrm{Loss}_{AA}^T \le c(\eta) \left(\eta \mathrm{Loss}_{i^*}^T + \ln \frac{1}{v_{1,i^*}} \right)$$

特に，初期重みが一様($v_{1,i}$ = 1/N)のとき，

$$\mathrm{Loss}_{AA}^T \le c(\eta) \left(\eta \mathrm{Loss}_{i^*}^T + \ln N \right)$$
$$\equiv a(\eta) \mathrm{Loss}_{i^*}^T + c(\eta) \ln N$$

AAの最適性

$$\mathrm{Loss}_{AA}^T \le a(\eta) \mathrm{Loss}_{i^*}^T + c(\eta) \ln N$$



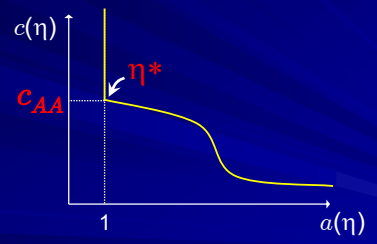
- **定理**

問題 (Y, Z, L) が“自然”ならば，
∀A, ∃エキスパート, ∃環境

$$\mathrm{Loss}_A^T > a \mathrm{Loss}_{i^*}^T + c \ln N$$

凸損失関数に対する性質

L(y,z) が z に関して下に凸のとき
（2次損失，相対エントロピー損失，Hellinger損失，．．．）



$$\mathrm{Loss}_{AA}^{T} \le \mathrm{Loss}_{i*}^{T} + c_{AA} \ln N$$

Weighted Averaging Algorithm (WAA)

- 簡便なアルゴリズム（AAの近似）
- Y = Z = [0,1]，L：凸損失関数と仮定
- 予測の統合

$$z_t = \sum_{i=1}^{N} v_{t,i} x_{t,i}$$

- 定理

$$\mathrm{Loss}_{WAA}^{T} \le \mathrm{Loss}_{i*}^{T} + c_{WAA} \ln N$$

$$(c_{AA} \le c_{WAA})$$

さまざまな凸損失関数と c_{AA}, c_{WAA}

$\mathrm{Loss}_{AA}^{T} \le \mathrm{Loss}_{i*}^{T} + c_{AA} \ln N$

$\mathrm{Loss}_{WAA}^{T} \le \mathrm{Loss}_{i*}^{T} + c_{WAA} \ln N$

損失関数	$L(y, z)$	c_{AA}	c_{WAA}
2次損失	$(y - z)^2$	1/2	2
相対エントロピー損失	$(1-y)\ln\frac{1-y}{1-z} + y \ln\frac{y}{z}$	1	1
Hellinger損失	$\frac{1}{2}((\sqrt{1-y} - \sqrt{1-z})^2 + (\sqrt{y} - \sqrt{z})^2)$	$1/\sqrt{2}$	1
絶対値損失	$\lvert y - z \rvert$	凸関数ではない	

ダイバージェンスを用いた導出

- KLダイバージェンス（相対エントロピー）
  確率ベクトル v, u に対し，
  $\mathrm{RE}(v \,\|\, u) = \sum_i v_i \ln (v_i / u_i)$

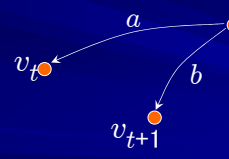
- 重み更新の導出
  $v_{t+1} = \mathrm{argmin}_v \left(\eta \sum_i v_i L(y_t, x_{t,i}) + \mathrm{RE}(v \,\|\, v_t)\right)$

$$= \frac{v_{t,i} e^{-\eta L(y_t, x_{t,i})}}{\text{規格化係数}}$$

上界の導出

- $v^* = (0, \ldots, 1, \ldots, 0) \in [0,1]^N$ （第 i^* 成分のみ1）

$$L(y_t, z_t) - L(y_t, x_{t,i^*}) \le c\,(\mathrm{RE}(v^* \,\|\, v_t) - \mathrm{RE}(v^* \,\|\, v_{t+1}))$$



v_t が v^* に“時刻 t における”相対損失分以上近づく

- t=1, ..., T で和を取ると，
  相対損失 $\le$ c $\mathrm{RE}(v^* \,\|\, v_1)$ = c ln N

オンライン予測の応用

オンラインアルゴリズムの統合

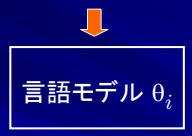
- オンライン問題を解くアルゴリズム $A_1, \ldots, A_N$
- 入力系列 $S = y_1, \ldots, y_T$

$\max_S \min_i A_i(S)$ の損失 $\leq \min_i \max_S A_i(S)$の損失

AA の損失 $\leq \min_i A_i$の損失 $+ c_{AA} O(\ln N)$

確率モデルの統合と情報圧縮

… so she was considering in her ___?



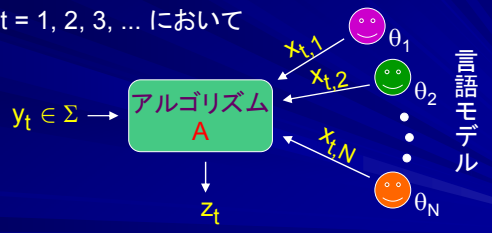
	Pr(· | context, θ_i)
mind	0.232
thought	0.183
own	0.129
office	0.073
:	:

確率モデルの統合モデル

$\Sigma = \{1, \ldots, K\}$: アルファベット

$y_1, y_2, \ldots, y_{t-1} \in \Sigma \longrightarrow \boxed{\theta_i} \longrightarrow x_{t,i}(\cdot) = \Pr(\cdot \mid y_1, \ldots, y_{t-1}, \theta_i)$

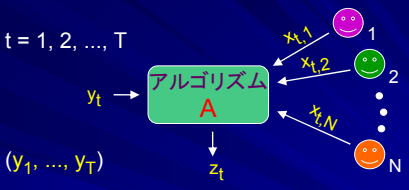
各時刻 t = 1, 2, 3, … において



アルゴリズムの尤度: $z_t(y_t) = \Pr(y_t \mid y_1, \ldots, y_{t-1}, A)$

モデル θ_i の尤度: $x_{t,i}(y_t) = \Pr(y_t \mid y_1, \ldots, y_{t-1}, \theta_i)$

ユニバーサル符号と冗長度



- Aの尤度: $P(S \mid A) = \prod_t P(y_t \mid y_{1..t-1}, A) = \prod_t z_t(y_t)$
- θ_i の尤度: $P(S \mid \theta_i) = \prod_t x_{t,i}(y_t)$
- A + ユニバーサル符号 ⇒ 符号長 $= -\log_2 P(S \mid A)$
  θ_i + ユニバーサル符号 ⇒ 符号長 $= -\log_2 P(S \mid \theta_i)$
- 冗長度 $= -\log_2 P(S \mid A) - \min_i (-\log_2 P(S \mid \theta_i))$

AAの適用とベイズ混合

以下の問題 (Y, Z, L) と等価

- $Y = \Sigma = \{1, \ldots, K\}$
- $Z = \{ z \in [0,1]^K : \Sigma$ 上の分布 $\}$
- $L(y, z) = -\ln z(y)$ ・・・ 対数損失
  ⇒ $\mathrm{Loss}^T_A = -\ln P(S \mid A)$ ・・・ 符号長
- AA の出力 = WAA の出力 = ベイズ混合

$$z_t(j) = \sum_{i=1}^N v_{t,i} x_{t,i}(j) = \sum_{i=1}^N \Pr(\theta_i \mid y_{1..t-1}) \Pr(j \mid y_{1..t-1}, \theta_i)$$

冗長度 = 相対損失 $= \mathrm{Loss}^T_A - \mathrm{Loss}^T_{i^*} \leq \ln N$

無限のエキスパートの統合

- $Y = \{0,1\}$
- エキスパート $\theta \in [0,1]$
  $x_{t,\theta}(1) = \Pr(1 \mid y_{1..t-1}, \theta) = \theta$
  $x_{t,\theta}(0) = \Pr(0 \mid y_{1..t-1}, \theta) = 1 - \theta$
- AAの出力 = KT-Estimator

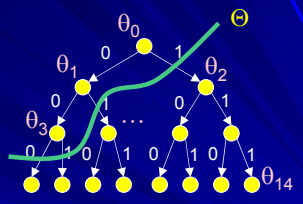
$$z_t(y) = \int v_{t,\theta} x_{t,\theta}(y) d\theta = \frac{\sum_{s=1}^{t-1} y_s + 1/2}{t}$$

- 相対損失 = O(log T)

Context Tree Weighting

各枝刈り Θ：モデル

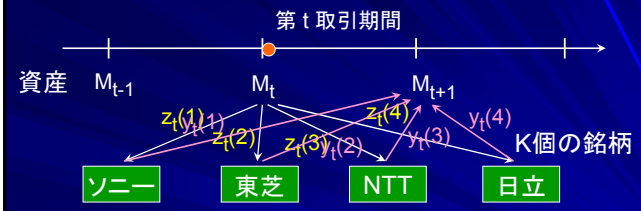
Pr(y | ･･･001, Θ) = θ_2
Pr(y | ･･･010, Θ) = θ_4



Nグラムモデル

符号長 = 最適な Θ の符号長 + O(Θ の葉の数)

ポートフォリオ

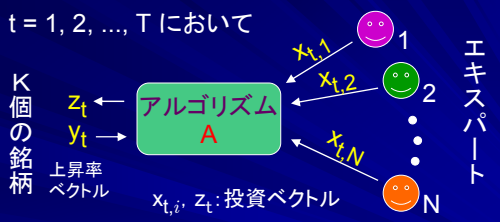


- 全額投資．銘柄 j の株を $M_t\, z_t(j)$ の金額で購入
  ($z_t(1) + \cdots + z_t(K) = 1$)
- 株をすべて売却．銘柄 j の株価の上昇率を $y_t(j)$ とする

新しい資産 $M_{t+1} = M_t \sum_j y_t(j)\, z_t(j) = M_t\, (y_t \cdot z_t)$

投資アドバイスの統合

各時刻 t = 1, 2, ..., T において



- Aの資産: $M_{T+1} = M_1 \prod_t z_t \cdot y_t$
- エキスパート i のアドバイスに従ったときの資産:
  $M_{T+1,i} = M_1 \prod_t x_{t,i} \cdot y_t$
- 競合比: $M_{T+1} / \max_i M_{T+1,i}$

AAの適用

以下の問題 (Y, Z, L) と等価

- $Y = [0, \infty]^K$
- $Z = \{ z \in [0,1]^K \mid z(1) + \cdots + z(K) = 1 \}$
- $L(y, z) = -\ln (y \cdot z)$ ･･･ ポートフォリオ損失
- $\mathrm{Loss}^T_A = -\ln M_{T+1}$
- AA の出力 = WAA の出力

$$z_t = \sum_{i=1}^{N} v_{t,i} x_{t,i}$$

競合比 = $e^{-\text{相対損失}} \geq 1 / N$

オンライン投資

- ポートフォリオ問題において，毎時刻全額投資するかわりに，定額（例えば1万円）投資
- 株価の上昇率に上限 $B > 0$ を仮定
  （相対損失を有限に抑えるため）

以下の問題 (Y, Z, L) と等価

- $Y = [0, B]^K$
- $Z = \{ z \in [0,1]^K \mid z(1) + \cdots + z(K) = 1 \}$
- $L(y, z) = y \cdot z$ ･･･内積損失

WAAの適用

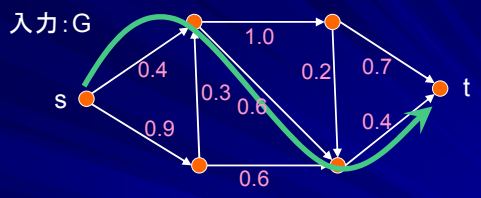
- 内積損失 $L(y, z) = y \cdot z$ は凸ではない
- 適当な η に対して

相対損失 = $O\left(\sqrt{2BL^* \ln N} + B \ln N\right)$

L^* = 最適なエキスパートの損失

Path Kernel 法

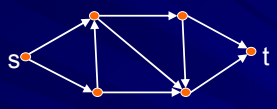
オンライン最短路問題



1. あるs-t 道 P を（確率的に）選ぶ．この確率を $z_t(P)$ とする．
2. 各辺の遅延時間 $d_t(e) \in [0,1]$ が明らかとなる．
   道Pに沿って s から t に到達する時間は $y_t(P) = \sum_{e \in P} d_t(e)$
3. 到達時間の期待値 $\sum_P y_t(P)\, z_t(P) = y_t \cdot z_t$

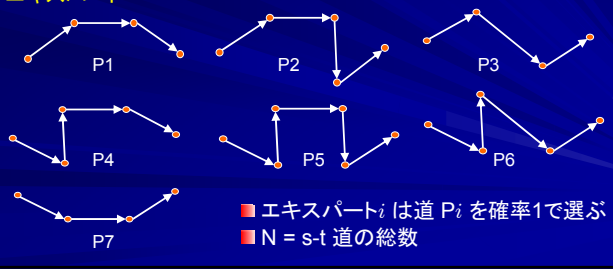
目標：$\sum_t y_t \cdot z_t - \min_P \sum_t y_t(P) \rightarrow$ 小

オンライン投資への還元



- $B = \max_P |P|$
- $Y = [0,B]^N$
- Z = s-t道上の分布の集合
- $L(y, z) = y \cdot z$

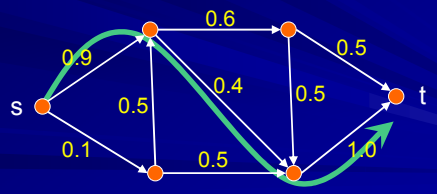
エキスパート



- エキスパートi は道 P_i を確率1で選ぶ
- N = s-t 道の総数

Path Kernel 法

- N（道の総数）は指数的になりうる
- すべての道 P に対し，重み $v_{t,P}$ を保持できない
- その代わり，各辺 e に対し，遷移確率 $a_t(e)$ を保持
- 関係式 $v_{t,P} = \prod_{e \in P} a_t(e)$ によって間接的に $v_{t,P}$ を表現



$v_{t,P} = 0.9 * 0.4 * 1.0 = 0.36$

重み更新の模倣

条件：

（更新前） $v_{t,P} = \prod_{e \in P} a_t(e)$

$$v_{t+1,P} = \frac{v_{t,P} e^{-\eta y_t(P)}}{\text{normalize}}$$

（更新後） $v_{t+1,P} = \prod_{e \in P} a_{t+1}(e)$

を満たすような辺上の重み更新

$a_t \rightarrow a_{t+1}$

を行う必要がある

重み更新の模倣

- 任意の P に対し，次の式を満たす a_{t+1} を求めればよい

$$v_{t+1,P} = \prod_{e \in P} a_{t+1}(e) = \frac{\prod_{e \in P} a_t(e) b_t(e)}{\sum_P \prod_{e \in P} a_t(e) b_t(e)}$$

ただし，$b_t(e) = \exp(-\eta\, d_t(e))$

道 P の損失 = 辺の損失の和
($L(y_t, x_{t,P}) = \sum_{e \in P} d_t(e)$)

Path Kernels

- 辺の重みベクトル: **a** = (a(e_1), ..., a(e_m))
- パスの重みベクトル: **v** = (v_{P1}, ..., v_{PN}),,

$$\forall P, v_P = \prod_{e \in P} a(e)$$

この関係を, **v** = Φ(**a**) と表す.

- 係数ベクトル : **b** = (b(e_1), ..., b(e_m))

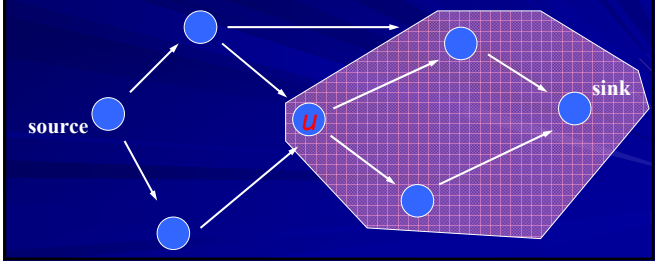
Path Kernel

$$K(a,b) = \Phi(a) \cdot \Phi(b) = \sum_{P} \prod_{e \in P} a(e)b(e)$$

normalization factor

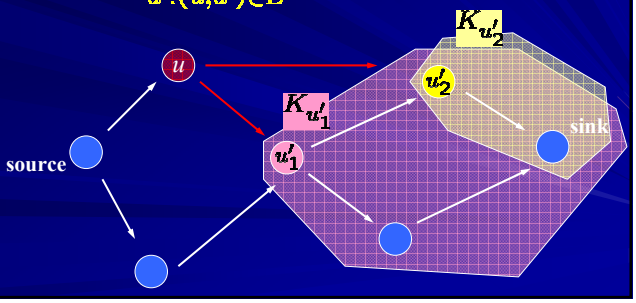
Path Kernel の計算

$$K_u = \sum_{P:\text{from } u} \prod_{e \in P} a(e)b(e)$$



Path Kernel の計算

- $K_{\text{sink}} = 1$
- $K_u = \sum_{u':(u,u') \in E} v(u,u')b(u,u')K_{u'}$

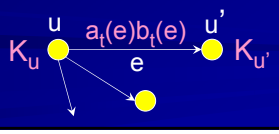


Weight Pushing Algorithm

- 目標 $\forall P, \prod_{e \in P} a_{t+1}(e) = \frac{\prod_{e \in P} a_t(e)b_t(e)}{K_{\text{source}}(a_t, b_t)}$
- 漸化式 $K_u = \sum_{u':(u,u') \in E} a_t(u,u')b_t(u,u')K_{u'}$

$$a_{t+1}(e) = \frac{a_t(e)b_t(e)K_{u'}}{K_u}$$

目標達成！



まとめ

- さまざまなオンライン最適化問題が，共通の統合スキーム（AA，WAA）を用いて解ける
- 一般の最適化問題への適用
  - 各時刻 t における損失が，それまでの履歴に依存する
  - オフラインで最適な解を求めるのが困難
- 構造的エキスパートの統合の可能性
  - 決定リストの効率の良いオンライン学習
- モデルのさらなる拡張
  - リスク情報を用いた統合

平成17年度 第2回 全体会議

日時　平成 17 年 11 月 21 日 (月), 22 日 (火)

会場　名古屋大学 野依記念学術交流館 / IB 電子情報館 中棟 IB 大講義室

プログラム

11 月 21 日 (月)

10:30 – 12:00　未解決問題セッション

Domain-Specific Image Segmentation and Shape Matching
浅野哲夫 (北陸先端科学技術大学院大学)

柔体を扱う計算幾何学
浅野哲夫 (北陸先端科学技術大学院大学)

線的施設配置問題
加藤直樹 (京都大学)

外面が四角形 (以上) である格子凸描画を求める線形時間アルゴリズムの開発
三浦一之 (福島大学)

幾何的巡回セールスマン問題の厳密アルゴリズムについて
岡本吉央 (豊橋技術科学大学)

文字列検索における時間と領域のトレードオフ
定兼邦彦 (九州大学)

12:00 – 13:30　幹事会

13:30 – 15:50　未解決問題に対するグループ討論

16:00 – 17:30　全体会議

11 月 22 日 (火)

10:15 – 11:00　透過的データ圧縮
定兼邦彦 (九州大学) 382

11:10 – 11:55　確率伝搬法の可能性について
渡辺治 (東京工業大学) 387

13:30 – 14:15　RNA 配列の比較アルゴリズム
浅井潔 (東京大学) 390

14:30 – 15:15　3 つの資源節点集合を持つ 4 点連結グラフを均等分割する問題について
石井利昌 (豊橋技術科学大学) 398

15:30 – 16:15　平面グラフ、曲面上のグラフ、マイナーに関して閉じているグラフに関する彩色問題
河原林健一 (東北大学) 408

16:30 – 17:30　未解決問題グループ討論の結果報告

透過的データ圧縮
Transparent Data Compression

K. Sadakane and R. Grossi: Squeezing Succinct Data Structures into Entropy Bounds, Proc. ACM-SIAM SODA 2006, to appear.

九州大学システム情報科学研究院
定兼　邦彦
2005年11月22日

背景

- データ圧縮の目的 (過去)
  - ディスク容量の節約
  - 通信コスト(料金，時間)の削減

保存用

- データ圧縮の目的 (現在)
  - アクセスの高速化 (CPU速度 > ディスク速度)
  - 連続的なアクセスに限られる
- ランダムアクセスができたらどうなるか

透過的データ圧縮

もし圧縮データの任意部分を高速に復元できれば

- データを圧縮したまま保存できる
  - ディスク容量の節約
  - 高速なアクセスが可能
- 圧縮されていることを意識しなくていい

本研究の結果

- 長さ n の文字列 S を圧縮 (アルファベットサイズσ)
- サイズ: LZ78 [Ziv, Lempel 78] と漸近的に同じ

$$nH_k + \mathrm{O}\left(\frac{n(\log\sigma + \log\log_\sigma n + k)}{\log_\sigma n}\right) \text{ bits}$$

(H_k: S の k 次経験的エントロピー)

- S の i 文字目からの連続する $\log_\sigma n$ 文字 ($\log n$ ビット) を定数時間で復元可能 ($decode(S,i)$)
  (計算モデル: word RAM (語長 $\log n$ ビット))
- このアクセス時間は未圧縮の場合と同じ

研究の動機

- Succinctデータ構造を更に圧縮したい
  - bit vector
  - 検索木
  - グラフ
  - 圧縮接尾辞木

Succinctデータ構造

- あるデータ集合 D を格納するデータ構造
- データ構造のサイズ: 情報理論的下限に近い
  - 情報理論的下限 $L = \log$ (D の場合の数)
- 高速な問合せが可能
  - 補助的なデータ構造 (索引) を使用
  - サイズ: 漸近的に無視できる (o(L) bits)

集合のSuccinctデータ構造

- 集合 $D \subset \{1,2,...,n\}$ を格納
- 問合せ (定数時間)
  - *member*(D,i): D 中に i が存在するか
  - *rank*(D,i): D 中の i 以下の要素の数
  - *select*(D,j): D 中で j 番目に小さい要素
- サイズ: $n + o(n)$ bits [J89] [M96]

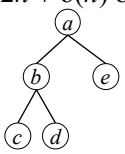
$$\begin{array}{cccc} & 1 & i & n \\ S: & 0100011 & 0001001000001 & \end{array}$$

$rank(D,i) = 3$

7

木のSuccinctデータ構造

- n 節点の順序木 T を格納
  - 通常のデータ構造は $O(n \log n)$ bits
- T は $\frac{1}{n+1}\binom{2n}{n} \approx 4^n$ 通り存在 (Catalan数)
  - 情報理論的下限 = $2n - \Theta(\log n)$ bits
- 問合せ(定数時間)
  - 長男，兄弟，親，深さ，preorder，子孫の数など
- サイズ: $2n + o(n)$ bits [MR01] [GRR04]



S ((( ) ( )) ( ))

木を括弧列 S で表現

8

問: Succinctデータ構造は それ以上圧縮できないか?

- 答: 場合によっては可能
- 例: 集合 $D \subset \{1,2,...,n\}$ の要素数が少ない場合
- 要素数が m の集合は $\binom{n}{m}$ 通り

$B(m,n) = \log\binom{n}{m} \approx m\log\frac{n}{m} + (n-m)\log\frac{n}{n-m}$ bitsで表現できるはず

- $B(m,n) + O(n \log\log n / \log n)$ bitsのデータ構造で*member*, *rank*, *select*を定数時間で返すものが存在 [RRR02]

FID (Fully Indexable Dictionary) と呼ばれる

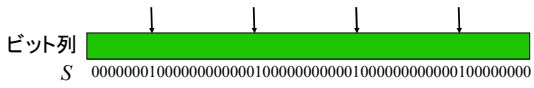
9

FIDを用いたポインタの圧縮

ある n ビットのデータ構造(ビット列)へのポインタ m個を格納する場合

- ポインタの値 i を $S[i] = 1$ で表現
- S をFIDで圧縮．ポインタは*select*で求まる
- $m = O(n/\log n)$ のとき，FIDのサイズは

$$\log\binom{n}{O(n/\log n)} = O\left(\frac{n}{\log n}\log\frac{n}{n/\log n}\right) + O\left(\frac{n\log\log n}{\log n}\right) = O\left(\frac{n\log\log n}{\log n}\right)$$



10

問: 木のSuccinctデータ構造は 圧縮できるか?

- FIDでは不可能
  - (と) が同数ある ⇒ $B(n,2n) = 2n$ bits 必要
  - $2n + O(n \log\log n/\log n)$ bits [GRR04]
- データ間の相関を考慮する必要がある
  - FIDでは 0 次のエントロピーまで圧縮

$$B(m,n) = m\log\frac{n}{m} + (n-m)\log\frac{n}{n-m} = nH_0$$

  - k 次のエントロピーまで圧縮したい

11

本研究の圧縮法の応用

- 集合 $D \subset \{1,2,...,n\}$ に対する*member*, *rank*, *select*を定数時間で返すデータ構造
- サイズ: $nH_k + O(n \log\log n/\log n)$ bits (k=O(log log n))
  - H_kは D を表す0,1列 S の k 次経験的エントロピー
- EID (Entropy-Bound Indexable Dictionary) と呼ぶ
- FID よりもさらに小さい

$$nH_k \le nH_{k-1} \le \cdots \le nH_0 \approx B(m,n)$$

12

EIDのデータ構造とアルゴリズム

- データ構造
  - D を表す0,1列 S を圧縮したもの nH_k+O(n log log n/log n) bits
    (任意の連続する log n ビットを定数時間で復元可)
  - FIDの補助データ構造 O(n log log n/log n) bits
- 問合せアルゴリズム
  - FIDとほぼ同じ ($S[i,i+\log n-1]$ へのメモリ参照を $decode(S,i)$に置き換える)
- どんな問合せの計算量も漸近的には同じ

13

木のSuccinctデータ構造の圧縮

- FIDでは不可能
  - $2n$ + O(n log log n/log n) bits [GRR04]
- EIDでは可能
  - 木を表現する括弧列 S の H_k まで圧縮可 (k=O(log log n))
  - $2nH_k$ + O(n log log n/log n) bits
  - 問合せの計算量は圧縮前と同じ
  - 構造が同じ部分木があると H_k は小さくなる
    (接尾辞木で特に有効)

14

EIDの圧縮サイズの限界

- S = 010101...010101 を圧縮する場合
  - FID: $nH_0 = n$ bits (+ O(n log log n/log n))
  - EID: nH_1 = O(log n) bits (+ O(n log log n/log n))
- エントロピーが小さいと第2項が無視できない
- *rank* を定数時間で返すデータ構造のサイズは
  Ω(n log log n/log n) bits [Miltersen 05]
  つまり第2項は最適

15

従来の圧縮法

16

従来の圧縮法

辞書式圧縮法

LZ77 [Ziv, Lempel 77]

LZ78 [Ziv, Lempel 78]

LZW[Welch 84]
compress

LZSS [Storer, Szymanski 82]
gzip

統計的圧縮法

PPM[Cleary, Witten 84]
PPMD [Howard 93]
PPM*[Cleary, Teahan, Witten 95]

block sorting
[Burrows, Wheeler 94]
高圧縮率、PPMより高速 (bzip2)

context tree weighting
[Willems, Shtarkov, Tjalkens 95]
PPMより高圧縮率

17

LZ77圧縮法

- 文字列を辞書へのポインタで置き換える
- 辞書 = すでに圧縮した文字列

....a compressed suffix tree consists of a compressed suffix array, a Pat tree and edge-length information.

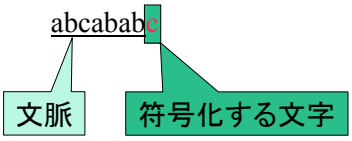
....a compressed suffix tree consists of [l=19, d=36] array, a Pat [l=4, d=51] and edge-length information.

圧縮率は文字列のエントロピーに収束

18

PPM

- 文字を1文字ずつ符号化
- 各文字の符号は文脈から決まる
  - 文脈:符号化する文字の直前の k 文字
- 圧縮サイズ: $nH_k = \sum_{s\in A^k} n_s \sum_{c\in A} p_c \log \frac{1}{p_c}$

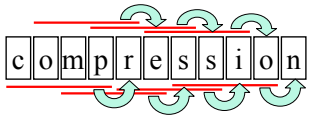


19

高次圧縮の問題点

- k 次のエントロピーの圧縮率を達成するには隣接する文字列の情報を用いて圧縮する必要がある
- 一部分を復元する場合も全体を復元ことになる

$k = 4$



20

従来の圧縮法との比較

	漸近的圧縮率	$\log n$ ビットの復号時間
LZ77 [ZL77]	nH_k	$O(n)$
LZ78 [ZL78]	nH_k	$O(n)$
PPM [CW84]	nH_k	$O(n)$
CTW [WST95]	nH_k	$O(n)$
Block Sorting [BW94]	nH_k	$O\left(\frac{\log^2 n}{\log\log n} + \log n \cdot \log\sigma\right)$ [GGV03]
本研究	nH_k	$O(1)$

21

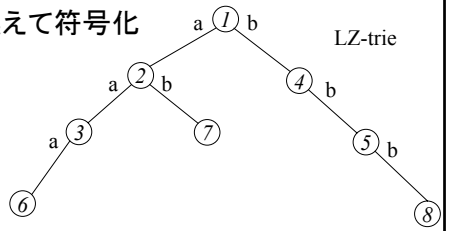
新圧縮法の概要

LZ78の改良+補助データ構造

22

LZ78 圧縮法

- 文字列を辞書中のフレーズに分割
- 数字に置き換えて符号化
- 辞書を更新



LZ-trie

S = aaabbbaaaabbbb
②③④⑤ ⑥ ⑦ ⑧

出力 ①a②a①b④b③a②b⑤b

23

LZ78の圧縮率 [Ziv, Lempel 78]

長さ n の文字列 S を分解したフレーズの数 c は

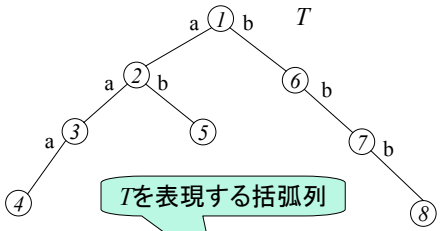
$$\sqrt{n} \le c \le \frac{n}{\log_\sigma n} \quad (\sigma: \text{アルファベットサイズ})$$

- 圧縮後のサイズ: $c(\log c + \log\sigma)$ bits
- S が定常エルゴード情報源 (エントロピー H) から生成されるなら $\frac{c\log c}{n} \to H \quad (n\to\infty)$
- S の k 次経験的エントロピーH_kに対し

$$c\log c \le nH_k + c\log\frac{n}{c} + \Theta(kc + c) \quad \text{[Kosaraju, Manjini 99]}$$

24

本研究のデータ構造



S = a a a b b b a a a a b b b b

R ② ③ ⑥ ⑦ ④ ⑤ ⑧

P 1 2 4 5 7 10 12

Tを表現する括弧列

フレーズの添字を格納
添字が T のpreorderと一致するように付け替える

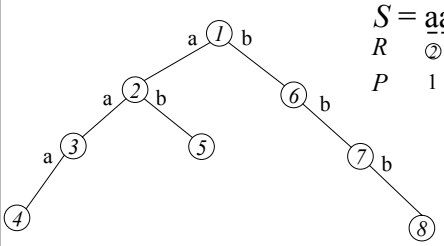
Tの枝ラベル

フレーズの開始位置を格納

*decode*アルゴリズム

$S[i,i+\log n-1]$ を復号する場合

1. $S[i]$ を含むフレーズ p を求める
2. p を表すLZ-trieのノード v を求める
3. v から根に向かうパス上のラベルを復号



S = a a a b b b a a a a b b b b

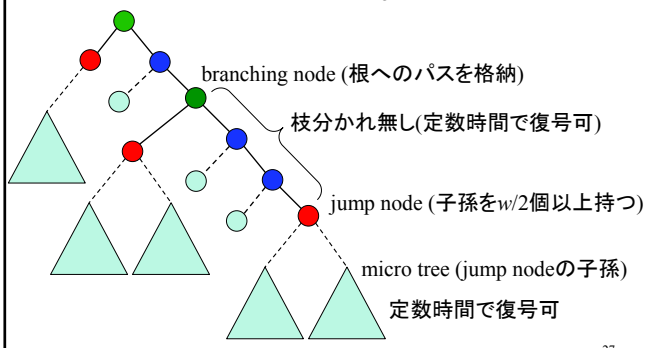
R ② ③ ⑥ ⑦ ④ ⑤ ⑧

P 1 2 4 5 7 10 12

26

Long phraseの復号

- Long phrase: 長さ $w = \frac{1}{2}\log_\sigma n$ 以上のフレーズ



27

Short phraseの復号

- Short phrase: 長さ $w = \frac{1}{2}\log_\sigma n$ 未満のフレーズ
- Sの長さ $\frac{1}{2}\log n$ の部分列はshort phraseを $O(\log n)$ 個含む可能性あり ⇒ 定数時間で復号できない
- $r > 1$ 個の連続するshort phraseをそのまま格納
  - 対応する R は格納しない
- データ構造のサイズは増加しない
  - R を格納する場合: $r \log c$ bits
  - そのまま格納する場合: $\frac{1}{2}\log n$ bits
  - $\frac{1}{2}\log n < r \log c$ $(\because \sqrt{n} \le c)$

28

まとめ

新圧縮法の提案

- 任意の文字列を高次エントロピー限界まで圧縮
- 部分列の定数時間復号 (未圧縮と同じ時間)

応用

- 既存の索引構造のサイズを改善
- 検索速度も同じ
- 個々の索引ごとに圧縮法を考える必要がない

課題

- 文字列の更新
- LZ77などの改良

29

Nov. 22, 2005

計算限界

確率伝播法とその可能性について[1]

渡辺 治 (東京工業大学)

本日の話題

1. 確率伝播法 (Belief Propagation Method)
2. メッセージ伝播アルゴリズムの特徴と可能性について
3. アルゴリズムの平均的解析のモデル (Planted Solution Model)

例題として：グラフの二分割問題 Graph Bisection Problem

[1]このファイルは発表時に使用したプレゼンテーション用ファイルをA4版に変更したものです．スタイル等が硬くて見にくい部分がありますがご勘弁下さい．

1．確率伝播法 (Belief Propagation Method) について

一言でいうと

確率変数 $X_1,\ldots,X_n$（各々の定義域を $A_1,\ldots A_n$ とする）により決まる系 G において，次のような周辺確率を求める方法である．

$$p(a) = \Pr_G[X_1=a] = \sum_{a_2\in A_2,\ \cdots\ a_n\in A_n} \Pr[X_1=a \wedge X_2=a_2 \wedge \cdots X_n=a_n].$$

ただし

確率変数間の依存関係が単純で，同時確率分布を分解して表わすことができる場合に限る $\Longrightarrow$ ベイジアン・ネットワーク

歴史

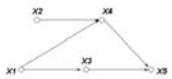
- AI の分野で Pearl が 1982 年に提唱したもの．
- 統計力学の研究者 MacKay らが LDPC 符号の復号法に使用して注目を集めた．それ以後，統計力学&情報理論を中心に研究が進んでいる．
- 最近では survey propagation なるものも登場している．

上記の周辺確率よりも，もっと一般的には次のような確率を求める（求めたい）ことが多い．

$$\Pr_G[X_1=a \mid X_n=b] = \frac{\sum_{a_2\in A_2,\ \cdots\ a_{n-1}\in A_{n-1}} \Pr[X_1=a \wedge X_2=a_2 \wedge \cdots X_n=b]}{\sum_{a_1\in A_1,\ a_2\in A_2,\ \cdots\ a_{n-1}\in A_{n-1}} \Pr[X_1=a_1 \wedge X_2=a_2 \wedge \cdots X_n=b]}$$

ベイジアン・ネットワーク：

同時確率分布の分解法を示した確率変数間の依存グラフ



$$p(a_1,a_2,a_3,a_4,a_5) = p(a_1)p(a_2)p(a_3|a_1)p(a_4|a_1,a_2)p(a_5|a_3,a_4)$$

ただし，たとえば次のように略記する：

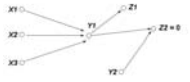
$$\Pr_G[X_2=a_2 \& X_4=a_4] = p(a_2,a_4)$$

注意！（矢印がない関係はすべて独立）

$$\begin{aligned} p(a_1,a_2,a_3,a_4,a_5) &= \underline{p(a_1)}p(a_2)\underline{p(a_3|a_1)}p(a_4|a_1,a_2)p(a_5|a_3,a_4) \\ &= p(a_2)p(a_1,a_3)p(a_4|a_1,a_2)p(a_5|a_3,a_4) \\ &= p(a_1,a_2,a_3,a_4)p(a_5|a_3,a_4) \\ &= p(a_1,a_2,a_3,a_4,a_5) \end{aligned}$$

BP の計算方法：

確率変数間のメッセージ伝播により各確率変数の belief を計算する．



毎ステップ，各頂点において，次のような計算を行う：

以下，頂点 Y_1 と，Y_1 の取りうる値 a に注目．

（準備）

- $\pi_{Y_1}(a) = \Sigma_{\boldsymbol{b}}\ \Pr[Y_1=a|\boldsymbol{X}=\boldsymbol{b}]\cdot(\pi_{X_1\to Y_1}(b_1)\cdot\pi_{X_2\to Y_1}(b_2)\cdot\pi_{X_3\to Y_1}(b_3))$.
- $\lambda_{Y_1}(a) = \lambda_{Z_1\to Y_1}(a)\cdot\lambda_{Z_2\to Y_1}(a)$.

（メッセージの計算）

親へ（例：$Y_1 \longrightarrow Z_1$）： $\pi_{Y_1,Z_1}(a) = \pi_{Y_1}(a)\cdot\lambda_{Z_2\to Y_1}(a)$.

子へ（例：$Y_1 \longrightarrow X_1$）： $\lambda_{Y_1\to X_1}(b) \approx \Pr[X_1=b]$ の一部

（Y_1 への X_1 以外の情報により得られる値）

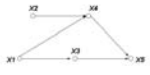
（現時点での $Y_1=a$ に対する belief の計算）

$\mathrm{Bel}_{Y_1}(a) = \alpha\cdot\lambda_{Y_1}(a)\pi_{Y_1}(a)$.

これまでにわかっていること：

定理．

1. 依存グラフに閉路がなければ正しく周辺確率を計算する．
2. その場合の計算時間は $\mathcal{O}(n)$（n は頂点数）である．



閉路あり



閉路なし

でも，経験的に... 閉路があっても大抵うまくいく場合がある！

1. LDPC 符号（Gallager 符号）の復号化
2. Turbo 符号の復号化
3. 画像修復，様々な制約充足問題

2．ＢＰ（メッセージ伝播法）の特徴と可能性

私の直感：

確率伝播法 $\iff$ 乱択局所探索アルゴリズム

補足

- 乱択局所探索アルゴリズムにもいろいろあり，その性質も大きく異なる．上記の対応は「貪欲型」に対するもの．(もっと正確には，決定にランダム性を入れて多少ソフト化したもの．)
- 単純に乱択化しても効率が悪くなってしまう場合がある．

  比ゆ： 5 回サイコロを投げた和が 15 の元で，すべて 3 が出る確率 P_0

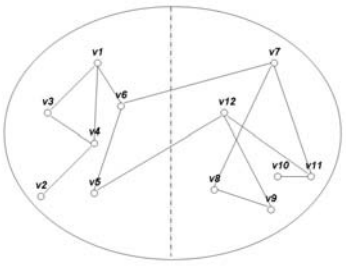
  $$\underset{\text{計算で求まる}}{P_0 = \cdots} \iff \underset{\text{多量のサンプルが必要}}{P_0 = \frac{\text{すべて3の組数}}{\text{和が15の組数}}}$$

- 「貪欲型」が有効な場合に使える？(収束性がよい場合)
- もちろん（？）最悪時はダメ．平均的によい $\Longrightarrow$ 平均時解析

3．平均時解析の例

例題： グラフの二分割問題 Graph Bisection Problem

Graph Bisection Problem
Input: An undirected graph $G=(V,E)$, where $|V|=2n$ for some n.
Task: Find an *equal size* partition V_0 and V_1 of V with min. # of cut edges.
Remark. Find one of them if there are several solutions.



知られていること：

- この問題はＮＰ-困難．
- 平均で多項式時間のアルゴリズムが知られている．
  その入力グラフのモデルとして planted solution model が導入された．
  - (Boppana, 1987): deterministic polynomial-time but not so simple
  - (Jerrum and Sorkin, 1998): randomized $O(n^2)$ time
  - (Condon and Karp, 2001): randomized $O(n+m)$ time
  - (F. McSherry, 1999, etc): simplified spectral method

ＢＰによるアルゴリズムの導出

確率変数
C_i $(1 \le i \le 2n)$: 頂点 v_i が V_0, V_1 のどちらに属するか？
E_{ij} $(1 \le i < j \le 2n)$: $E_{ij}=1 \Leftrightarrow v_i, v_j$ 間に辺が存在する．

計算の目標
与えられたグラフ G に対し，ＢＰを用いて次の周辺確率を求める．

$$p_i = \Pr[C_i = 1 \mid C_1 = 1 \wedge \bigwedge_{ij} E_{ij} = e_{ij}]$$

ただし，$e_{ij} = \begin{cases} 1, & G \text{は辺 } (v_i, v_j) \text{を持つ}, \\ 0, & G \text{は辺 } (v_i, v_j) \text{を持たない}. \end{cases}$

その $p_i > 0.5$ か否かで C_i を決める．

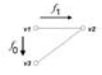
ベイジアン・ネットワーク



得られたアルゴリズム

非常に単純なメッセージ伝播アルゴリズム

program PseudoBP($G=(V,E)$, p, r);
  set all x_i to 0;
  repeat MAXSTEP times **do** {
    $x_1 \leftarrow +\infty$;
    for each $i \in V$,
      $x_i \leftarrow \sum_{j \in N(i)} f_1(x_j) + \sum_{j \notin N(i)} f_0(x_j)$;
    if all beliefs are stabilized **then break**;
  }
  output($x_1, ..., x_{2n}$); // Classification is (sign(x_1), ..., sign(x_{2n})).
end-program



補足：

1. 関数 f_0, f_1 の定義：

$$f_1(z) = \begin{cases} h_1 \cdot \theta_1, & \text{if } \theta_1 < z, \\ h_1 \cdot z, & \text{if } -\theta_1 \le z \le \theta_1, \\ h_1 \cdot (-\theta_1), & \text{if } z < -\theta_1; \end{cases} \quad f_0(z) = \begin{cases} -h_0 \cdot \theta_0, & \text{if } \theta_0 < z, \\ -h_0 \cdot z, & \text{if } -\theta_0 \le z \le \theta_0, \\ -h_0 \cdot (-\theta_0), & \text{if } z < -\theta_0, \end{cases}$$

ただし，

$$a_0 = \frac{1-p}{1-r},\ a_1 = \frac{p}{r},\ h_0 = \left|\frac{a_0-1}{a_0+1}\right|,\ h_1 = \left|\frac{a_1-1}{a_1+1}\right|,\ \theta_0 = \left|\frac{\ln a_0}{h_0}\right|,\ \theta_1 = \left|\frac{\ln a_1}{h_1}\right|.$$

2. 本当のＢＰではない！
   - $\Pr[C_i=1]$ と $\Pr[C_i=0]$ の比の対数を求めることにした．
   - メッセージの伝播で大きな簡単化を 1 つ行った．

実際動かしていると非常にうまく働く．何とか証明したい！

そこで

- アルゴリズムの平均的解析 $\Longrightarrow$ Planted Solution Model
- MAXSTEP $= 2 \Leftarrow$ それでも結構よく働く

平均時計算量のモデル

Planted Solution Model ＝ 入力グラフを生成する手法

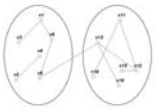
アルゴリズムの平均的解析のモデルとしてお勧め？

今回用いた Planted Solution Model

パラメータ n（頂点数 $2n$），$p, r, 0 < r < p < 1$ に対し，
次のようにグラフ $G = (V, E)$ を生成する．

1. $V_0 = \{1, ..., n\}$, $V_1 = \{n+1, ..., 2n\}$, and $V = V_0 \cup V_1$.
2. Put an edge (i, j) into E
   with probability p if $C_i = C_j$, and
   with probability r if $C_i \neq C_j$,

   where $C_i = 0 \iff i \in V_0$ and $C_i = 1 \iff i \in V_1$.



要するに

答えを作り，それを元に問題を（ランダムに）作成する方法．

重要な性質

定理． パラメータ n, p, r の something に

$$p - r = \Omega\left(\frac{1}{\sqrt{n}}\right)$$

という関係があるとき，埋め込んだ解 (planted solution) が，生成したグラフに対する Bisection Problem の唯一の解となる．

⇓

Planted Solution Model のもとでは，アルゴリズムの正当性は，生成したグラフに対し，埋め込んだ解が正しく見出せるか否かを調べればよい．

得られた結果

定理． Planted Solution Model のもとでアルゴリズムを実行させたとき，

$$\Pr[\text{ the algorithm yields the planted solution }] \geq 1 - 2n \cdot e^{-c_3 n \frac{(p-r)^4}{p^2}}.$$

系．

For any $\delta > 0$ and any p and r, $cp < r < p < 1$,
$p - r \geq c_2 n^{-1/2} \log(1/(\delta(p-r)))$
$\Rightarrow$ the algorithm answers correctly with probability $> 1 - \delta$.

これまでのアルゴリズムとの比較：

(Boppana, 1987)	$p - r = \Omega(n^{-1/2})$ (almost!?)
(Dyer and Frieze, 1989)	$p - r = \Omega(n^{-1/2})$ when p is large, e.g., $\Omega(1)$
(Jerrum and Sorkin, 1998)	$p - r = \Omega(n^{-1/6})$
(Condon and Karp, 2001)	$p - r = \Omega(n^{-1/2+\epsilon})$

その他にも...

- Most Likely Partition 問題（with Onsjoe）
- MAX-2SAT 問題に対する同様のアプローチ（with 山本）
- 固有値を求める手法にできないか？

未解決問題：本当のＢＰの妥当性？

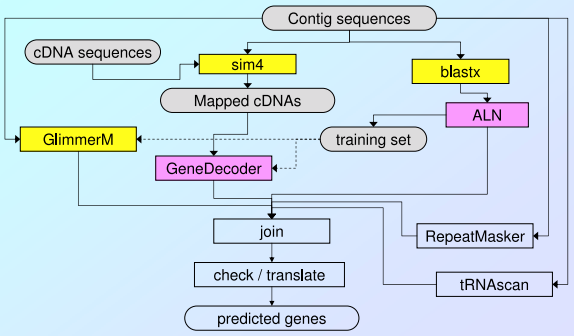
参考文献

R. McEliece, D. MacKay, and J.F. Cheng, Turbo decoding as an instance of Pearl's "Belief Propagation" algorithm, *IEEE J. on Selectead Areas in Communications*, 16(2):140–152, 1998.

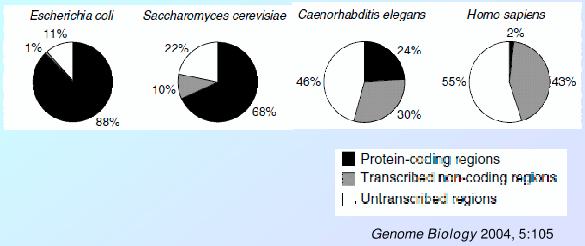
RNA配列の比較アルゴリズム

1. 東京大学大学院新領域創成科学研究科
2. 産業技術総合研究所生命情報科学研究センター
浅井　潔

麹菌
Aspergillus oryzae遺伝子発見パイプライン



転写産物(RNA)の大部分は非コード領域 !!

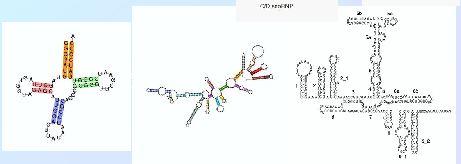


Genome Biology 2004, 5:105

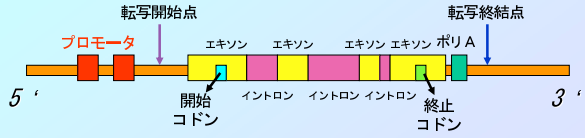
様々なタイプの機能性非コードRNAがある

機能性RNAもゲノム上にコードされている
miRNAの発見、RNAi（RNA干渉）の開発
ncRNAは、生体内のネットワークの重要な要素の一つ





遺伝子の構造（真核生物）



タンパク質コード遺伝子の発見法

- 既知転写産物との類似性
  - DB上の既知遺伝子（DNA）で相同性検索
  - DB上の既知タンパク質で相同性検索
  - cDNAをゲノムDNA配列に「貼り付ける」
- 比較ゲノム
  - 保存領域（synteny）は「重要」
- “ab initio” 遺伝子発見
  - 統計的な情報を用いた遺伝子の確率モデル

タンパク質コード遺伝子の発見法

- 既知転写産物との類似性
  - アラインメントによる配列の比較
    - 動的計画法（DP）
    - BLAST
- 比較ゲノム
- “ab initio” 遺伝子発見
  - 統計的な情報を用いた遺伝子の確率モデル

モデルによるゲノムDNAの「局所検索」

非コードRNA遺伝子の発見法

- 既知転写産物との類似性
  - アラインメントによる配列の比較
    - 動的計画法（DP）
    - BLAST？？？？
- 比較ゲノム
  - きわめて重要(QRNA, RNAz)
- “ab initio” 遺伝子発見
  - 統計的な情報を用いた遺伝子の確率モデル

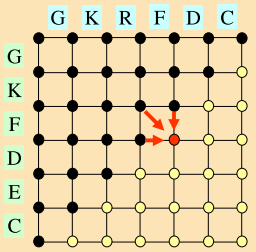
However, is it OK to define the “conserved region” by sequence similarities ?

モデルによるゲノムDNAの「局所検索」

RNA配列情報解析の課題

- ゲノム配列からの既知ncRNA発見
  - tRNAscan-SE, Snoscan, Infernal
- cDNA配列からのncRNA発見
  - クラスタリング、二次構造予測（xxxfold）
- 比較ゲノム保存領域からのncRNA発見
  - 保存領域抽出、ncRNA判定（QRNA, RNAz）
- 特定モチーフを持つncRNA発見
  - 二次構造モチーフと特定配列。標的予測

配列の比較：2次元DP



$$F(i, j) = \max \begin{cases} F(i-1, j-1) + s(x_i, y_j) \\ F(i, j-1) - d \\ F(i-1, j) - d \end{cases}$$

メモリ　$O(L^2)$

計算時間　$O(L^2)$

通常のアライメント法

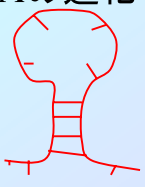
```
G T T A A C T G A G T A A C G
| x x | x | | | | | x | | |
G C A A G C T G A G T T A C G
```

	A	C	G	T
A	1.1	-2.7	-1.2	-2.8
C	-2.0	1.4	-2.1	-1.1
G	-1.1	-2.1	1.4	-2.1
T	-2.7	-1.2	-2.6	1.1

- 塩基配列の各位置が、進化の過程で、それぞれ独立に他の塩基への置換を起こすというモデルに基づいている。
- ClustalWなど

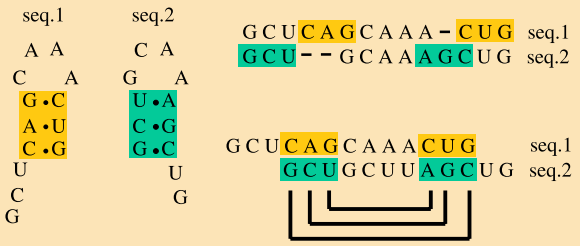
二次構造をもつRNAの進化

```
T T G T T C G A A A G A A C G
| | | x x | | | | | x x | |
T T G A C C G A A A G G T C G
```

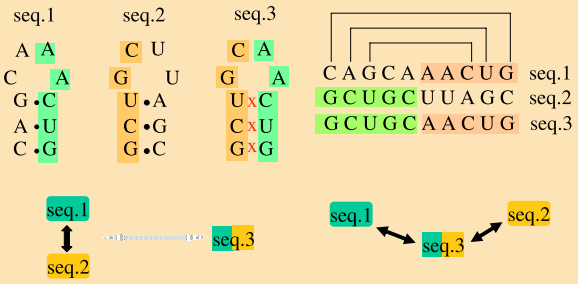


- 塩基対をつくる塩基ペアは、塩基対を保つような塩基置換の仕方（共置換）をする。
- →離れた2点での塩基の進化は独立でない。
- 配列の相同性が低くなってくると従来のアライメント法はうまくいかなくなってくる。

二次構造を考慮したアラインメント



二次構造を考慮したスコア



あらゆるRNA配列情報解析の基礎

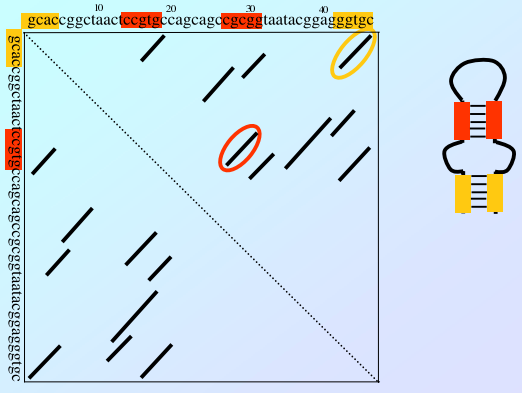
RNA配列の比較

- 配列の文字列としての類似性
  - ステム部分の塩基対類似性
  - 非塩基対部分の配列類似性
- RNAの二次構造の類似性
  - 二次構造が異なる　→ どう比較するのか？
  - 二次構造が分からない→ どう比較するのか？

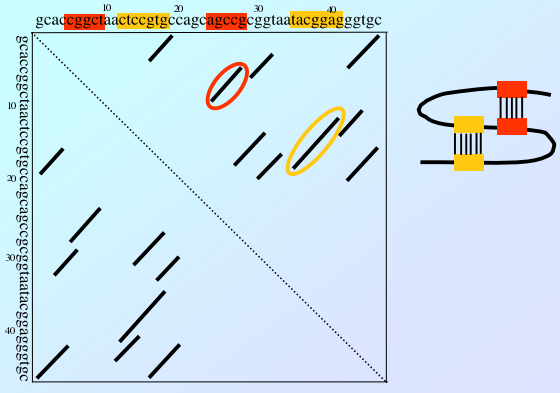
RNAの2次構造予測

- 自由エネルギー最小化（含：準最適構造）
  - Nussinov & Jacobson (“Nussinov Algorithm, 1980)
  - Mathews, Turner & Zuker (MFOLD, 2000)
- 配列比較解析
  - 相同RNA配列群が必要、結果が初期整列に依存
  - Chiu and Kolodziejczak (1991)
  - Eddy and Durbin (CM=プロファイルSCFG, 1994)

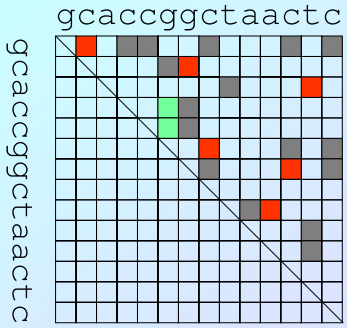
Secondary Structure Prediction of RNA



Secondary Structure Prediction of RNA

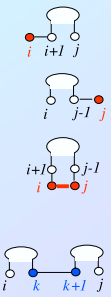


Secondary Structure Prediction of RNA



Nussinov アルゴリズム

- $M(i,j)$: maximum # of base pairs in $(x_i, \ldots x_j)$
  - $M(i,j) = M(i+1, j)$
  - $M(i,j) = M(i, j-1)$
  - $M(i,j) = M(i+1, j-1) + 1$
  - $M(i,j) = \max_k (M(i,k)+M(k+1,j))$



確率文脈自由文法(SCFG) による RNA二次構造予測

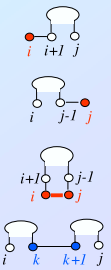
Σ = {a, c, g, u}, (x,y = alclglu)

S = xS $M(i,j) = M(i+1, j)$

S = Sx $M(i,j) = M(i, j-1)$

S = xSy $M(i,j) = M(i+1, j-1) + 1$

S = SS $M(i,j) = \max_k (M(i,k)+M(k+1,j))$



SCFGのCYK アルゴリズム

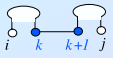
$\gamma(i,j)$: maxmum probability of $(xi, \ldots xj)$ is parsed by S

S = xS
S = Sx
S = xSy
S = SS

$$\gamma(i,j) = \max \begin{cases} \gamma(i+1,j) + \log p(x_i S); \\ \gamma(i,j-1) + \log p(S x_j); \\ \gamma(i+1,j-1) + \log p(x_i S x_j); \\ \max_{i<k<j} \{\gamma(i,k) + \gamma(k+1,j) - \log p(SS)\} \end{cases}$$

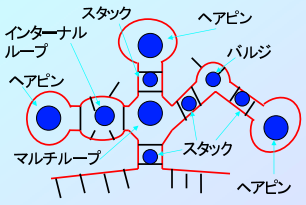
RNA二次構造予測の 計算複雑度

- $M(i,j) = \max_k (M(i,k)+M(k+1,j))$



  - メモリ: $M(i,j)$ for all position $i,j = L^2$
  - 計算時間: Iterate for all $i,j,k = L^3$

Turnerのエネルギーパラメーター



RNA配列比較の課題

- 2本配列の比較
  - 共通二次構造の推定とアラインメント
  - 局所アラインメント（検索）
- 配列群のマルチプルアラインメント
- 配列群の共通二次構造予測
- 二次構造付配列への構造アラインメント
  - 局所アラインメント（検索）
- 二次構造への構造アラインメント
  - 局所アラインメント（二次構造モチーフ検索）
- 配列クラスタリング
- 特定RNAのモデル
  - 局所アラインメント（特定RNA発見）
- 比較ゲノム保存領域からの機能性RNA発見

SCARNA

Marlet

PHMMTS

PSTAG

共通2次構造予測

- Sankoff (1985)
  - 2(N)本のRNAの折畳み。$O(L^{3N})$ time, $O(L^{2N})$space
- Gorodkin, Heyer & Stormo (FOLDALIGN, 1997)
  - 2本局所整列、分岐構造なし、塩基対の最大化、$O(L^4)$ time
  - 多重整列：　トーナメント法＋　Greedy アルゴリズム
- Mathews & Turner (Dynalign, 2002)
  - 自由エネルギー最小化＋配列比較解析
  - ステム間距離をM以下 $O(M^3 L^3)$ time
- Perriquet, Touzet & Dauchet (CARNAC, 2003)
  - 局所配列類似性　＋　エネルギー　＋　塩基対共変

2本のRNA配列からの共通二次構造の計算

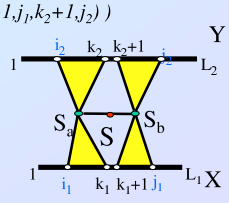
$\gamma(i_1,j_1,i_2,j_2)$: 4 次元のDP行列

(# of non-terminal is constant)

$$\gamma(i_1,j_1,i_2,j_2) = \max_{k_1,k_2} (\gamma(i_1,k_1,i_2,k_2) + \gamma(k_1+1,j_1,k_2+1,j_2))$$

メモリ：$O(L^4)$

計算時間：$O(L^6)$



長さの6乗の計算時間とは？

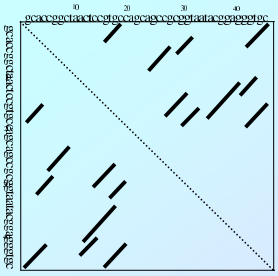
- 配列長が2倍になると64倍の計算時間
- 配列長が10倍になると100万倍！！
- 1分の100万倍は約2年
- Sankoffアルゴリズムでは、150塩基の2配列の共通二次構造の計算に10分以上かかります、、、

SCARNA

Stem Candidate Aligner for RNA

- For each nucleotide sequences,
  - Extract stem candidates of a fixed length
  - Decompose each stem candidates into two parts:
    - 5' and 3' stem component (left SC and right SC)
  - Sort all SCs as a sequence by their positions
- Pairwise alignment DP of SCSs
- Remove inconsistent stem matches
- Construct backbone of common secondary structure
- Alignment of remaining nucleotide

Stem Candidates

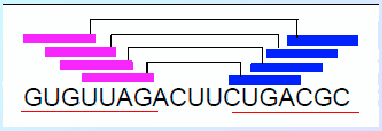


Base-pairing probabilities are calculated by McCaskill's algorithm.

Base pairs of low probabilities are not used

Stem fragments of a fixed length

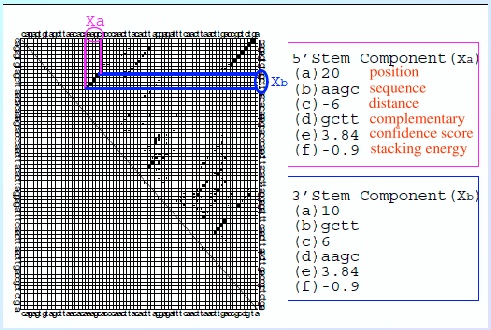
Stem candidates longer than the fixed length is treated as continuous stem fragments



SCARNA
Stem Candidate Aligner for RNA

- For each nucleotide sequences,
  - Extract stem candidates of a fixed length
  - Decompose each stem candidates into two parts:
    5' and 3' stem component (left SC and right SC)
  - Sort all SCs as a sequence by their positions
- Pairwise alignment DP of SCSs
- Remove inconsistent stem matches
- Construct backbone of common secondary structure
- Alignment of remaining nucleotide

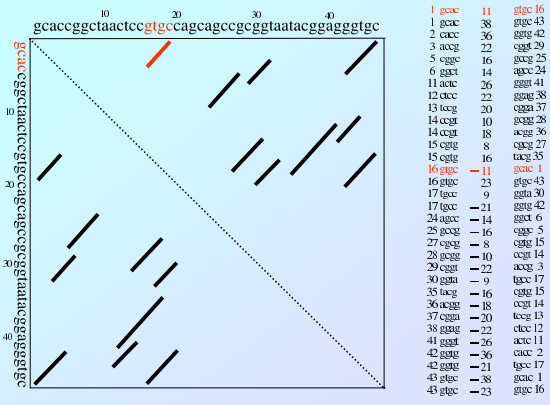
Decomposition of stem fragments into stem components



SCARNA
Stem Candidate Aligner for RNA

- For each nucleotide sequences,
  - Extract stem candidates of a fixed length
  - Decompose each stem candidates into two parts:
    5' and 3' stem component (left SC and right SC)
  - Sort all SCs as a sequence by their positions
- Pairwise alignment DP of SCSs
- Remove inconsistent stem matches
- Construct backbone of common secondary structure
- Alignment of remaining nucleotide

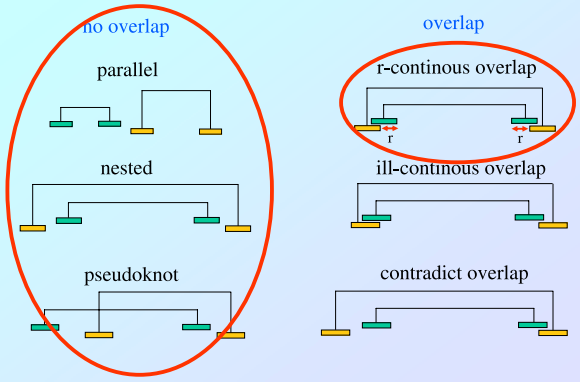
Stem Component Sequence (SCS)



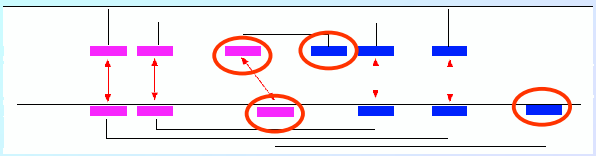
SCARNA
Stem Candidate Aligner for RNA

- For each nucleotide sequences,
  - Extract stem candidates of a fixed length
  - Decompose each stem candidates into two parts:
    5' and 3' stem component (left SC and right SC)
  - Sort all SCs as a sequence by their positions
- Pairwise alignment DP of SCSs
- Remove inconsistent stem matches
- Construct backbone of common secondary structure
- Alignment of remaining nucleotide

Relations of two stem fragments



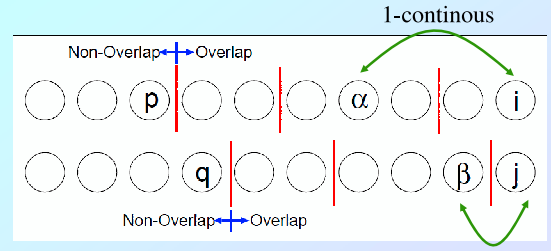
Left-right consistency of the SC match in SCS alignment



Left-right consistency of the SC match in SCS alignment

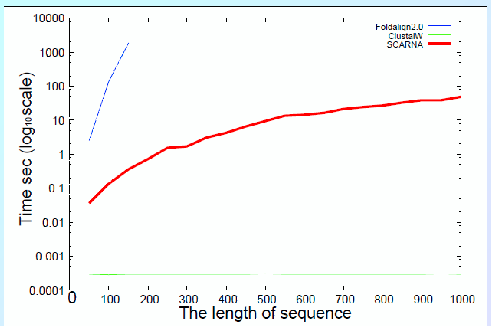


Dependencies in DP of SCSs

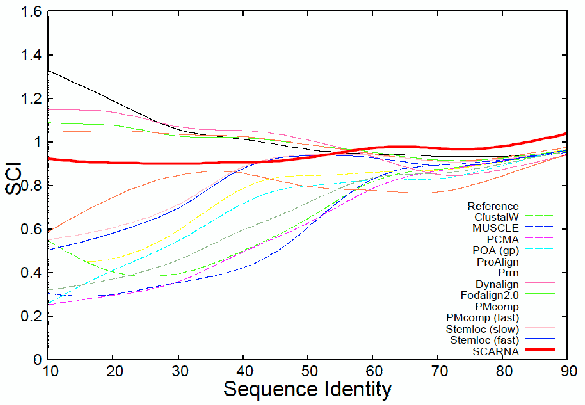


= SCs with same positions and different complementary partners

Computational Time



SCARNA



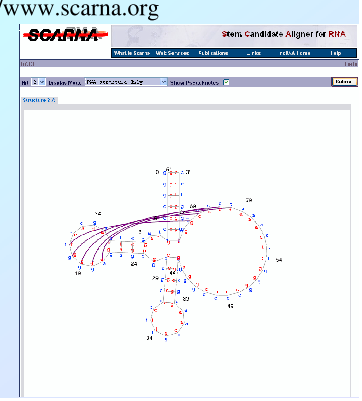
Scarna web server

http://www.scarna.org



Scarna web server

http://www.scarna.org



Acknowledgments

- "Functional RNA Project" of METI
- Grant-in-Aid for Scientific Research on Priority Area "Comparative Genomics"
- AIST, CBRC, BIRC
- JBIC
- The University of Tokyo

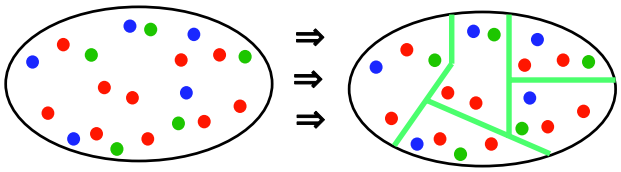
3つの資源節点集合を持つ４点連結グラフを均等分割する問題について

石井 利昌 (豊橋技術科学大学)
岩田 健吾 (マツダ)
永持 仁　(京都大学)

Background

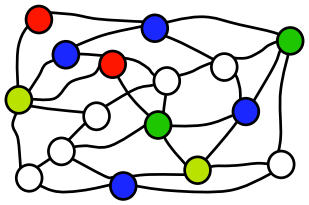
Districting Problem
- political constituencies
- school board boundaries
- sales or delivery regions

Criteria
- equity
- contiguousness



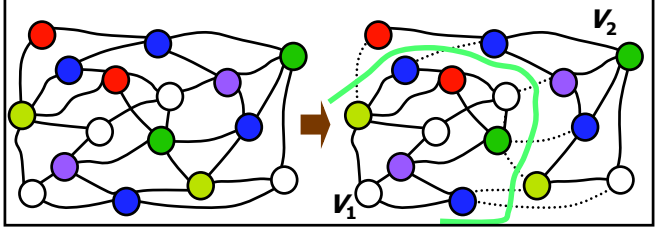
k-bipartition Problem

Input:
i) graph $G=(V, E)$.
ii) disjoint subsets $T_1, T_2, T_3, T_4, .., T_k \subseteq V$
(Resource sets)
($|T_i|$: even)



k-bipartition Problem

Output:
a partition $\{V_1, V_2\}$ of V → ***k*-bipartition**
s.t.
(1) $|T_i \cap V_1| = |T_i \cap V_2| = |T_i|/2$ for each i,
(2) Both of V_1 and V_2 induce connected graphs



Related Results

k : # of resource sets, $n=|V|$, $m=|E|$

·Testing whether a k-bipartition exists or not is NP-hard even if $k=1$ [Dyer, Frieze 85][Chleikova 99]

Related Results

k : # of resource sets, $n=|V|$, $m=|E|$

·Testing whether a k-bipartition exists or not is NP-hard even if $k=1$ [Dyer, Frieze 85][Chleikova 99]

·Sufficient condition for which a k-bipartition exists:
1-bipartition ・・・ 2-connectivity suffices.
$O(m)$ time [Suzuki et al.90][Wada, Kawaguchi94]
2-bipartition ・・・ 3-connectivity suffices.
$O(n^2 \log n)$ time [Nagamochi et al. 02]

Conjecture
Every $(k+1)$-connected graph admits a k-bipartition.

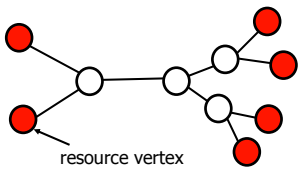
Our Recent Results

3-bipartition

(1) 5-vertex-connectivity does not suffice!
(2) 4-vertex-connectivity suffices if K4 is contained.
(3) For the edge version of k-bipartition (k=1,2,3), (k+1)-edge-connectivity suffices.

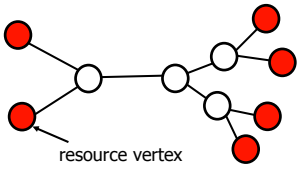
A 1-vertex-connected graph which has no 1-bipartition of V

k=1



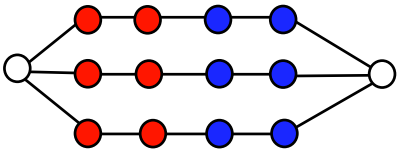
A 1-vertex-connected graph which has no 1-bipartition of V

k=1



A 2-vertex-connected graph which has no 2-bipartition of V

k=2



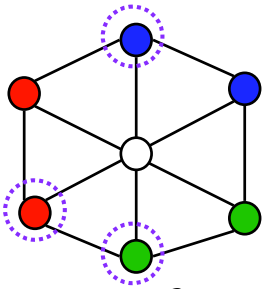
Our Results

3-bipartition

(1) 5-vertex-connectivity does not suffice!
(2) 4-vertex-connectivity suffices if K4 is contained.
(3) For the edge version of k-bipartition (k=1,2,3), (k+1)-edge-connectivity suffices.

3-bipartition

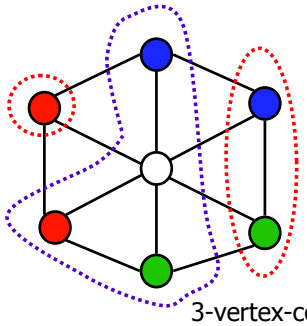
3-vertex-connectivity does not suffice.



3-vertex-connected graph

3-bipartition

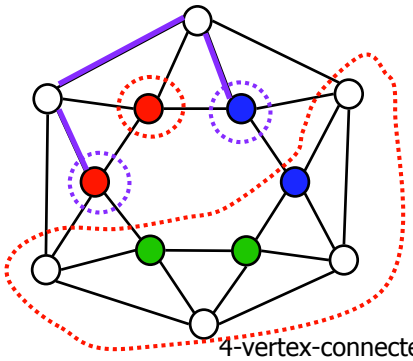
3-vertex-connectivity does not suffice.



3-vertex-connected graph

3-bipartition

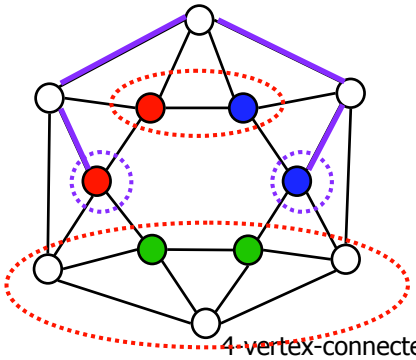
4-vertex-connectivity does not suffice.



4-vertex-connected graph

3-bipartition

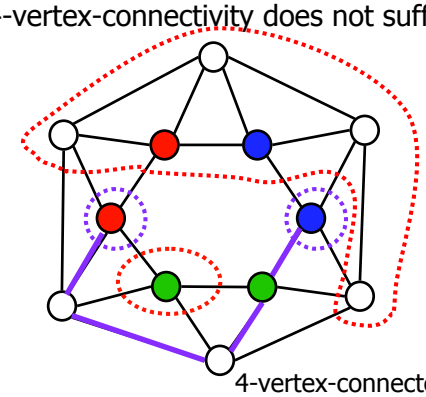
4-vertex-connectivity does not suffice.



4-vertex-connected graph

3-bipartition

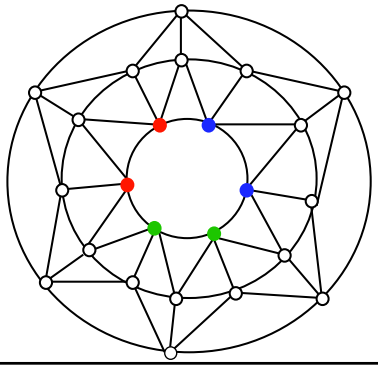
4-vertex-connectivity does not suffice.



4-vertex-connected graph

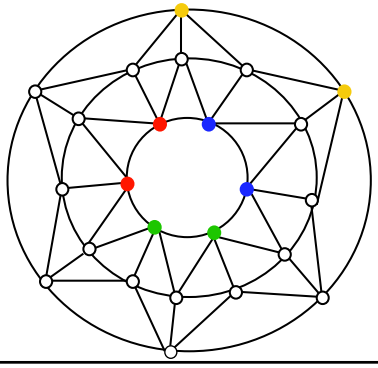
3-bipartition

5-vertex-connectivity does not suffice.



4-bipartition

5-vertex-connectivity does not suffice.



Our Results

3-bipartition

(1) 5-vertex-connectivity does not suffice!

(2) 4-vertex-connectivity suffices if K4 is contained.

(3) For the edge version of k-bipartition (k=1,2,3), (k+1)-edge-connectivity suffices.

Theorem

If G is a 4-vertex-connected graph and contains K4, then there exists a 3-bipartition, and moreover, a 3-bipartiton can be found in $O(n^3 \log n)$ time.

Algorithm for finding a 3-bipartition

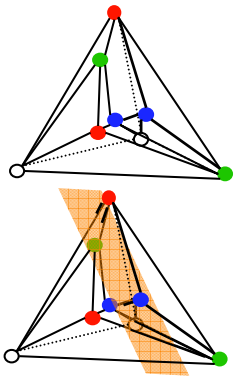
Reduction to a geometrical problem [Nagamochi et al. 02]

Phase 1

Find an embedding of G into the 3-dimensional space R^3 called **"convex-embedding"**.

Phase 2

Bisect V in R^3 into $\{V_1, V_2\}$ by a plane called **"ham-sandwich cut"**.

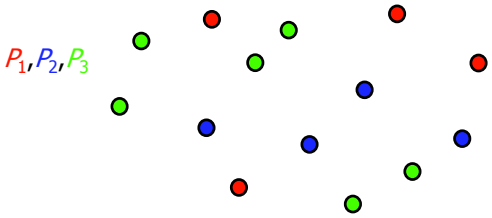


Ham-sandwich cut

$P_1, P_2, \ldots, P_k$: k subsets of points

Ham-sandwich cut with respect to $P_1, P_2, \ldots, P_k$

$\cdots$ hyperplane bisecting each P_i

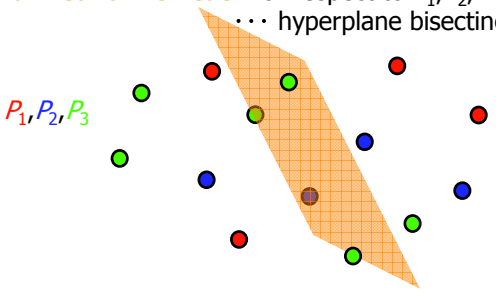


Ham-sandwich cut

$P_1, P_2, \ldots, P_k$: k subsets of points

Ham-sandwich cut with respect to $P_1, P_2, \ldots, P_k$

$\cdots$ hyperplane bisecting each P_i

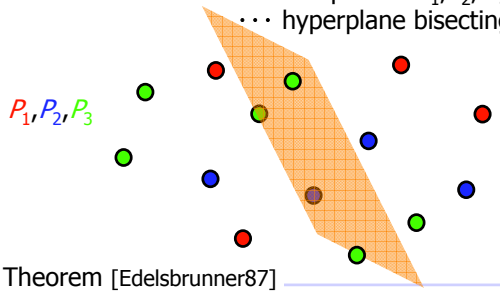


Ham-sandwich cut

$P_1, P_2, \ldots, P_k$: k subsets of points

Ham-sandwich cut with respect to $P_1, P_2, \ldots, P_k$

$\cdots$ hyperplane bisecting each P_i



Theorem [Edelsbrunner87]

In R^k, a ham-sandwich cut w.r.t. $P_1, \ldots, P_k$ always exists.

$O(n^{3/2})$ if k=3 (n : #points) [Chi-Yuan et al.94]

Algorithm for finding a 3-bipartition

Reduction to a geometrical problem [Nagamochi et al. 02]

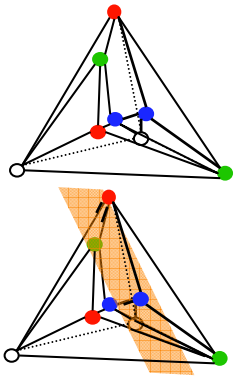
Phase 1

Find an embedding of G into the 3-dimensional space R^3 called **"convex-embedding"**.

Phase 2

Bisect V in R^3 into $\{V_1, V_2\}$ by a plane called **"ham-sandwich cut"**.

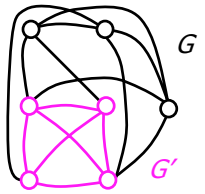
(1) $|T_i \cap V_1| = |T_i \cap V_2| = |T_i|/2$



Convex Embedding [Nagamochi et al.02]

$N_G(v)$: the set of neighbors of v.

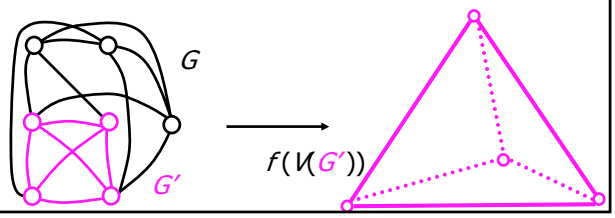
f: V R^k is a **convex embedding** of G with boundary G' into R^k,
if (i)
(ii)
(iii)



Convex Embedding [Nagamochi et al.02]

$N_G(v)$: the set of neighbors of v.

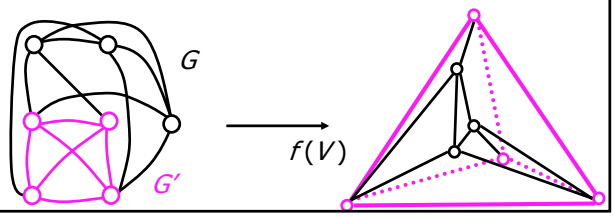
f: V R^k is a **convex embedding** of G with boundary G' into R^k,
if (i) the convex hull of $f(V(G'))$ is isomorphic to G',
(ii)
(iii)



Convex Embedding [Nagamochi et al.02]

$N_G(v)$: the set of neighbors of v.

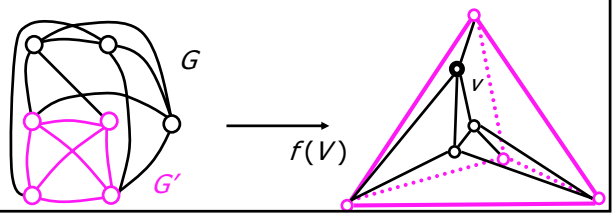
f: V R^k is a **convex embedding** of G with boundary G' into R^k,
if (i) the convex hull of $f(V(G'))$ is isomorphic to G',
(ii) For $\forall v \in V - V(G')$,
$f(v)$ is strictly included in the convex hull of $f(N_G(v))$.
(iii)



Convex Embedding [Nagamochi et al.02]

$N_G(v)$: the set of neighbors of v.

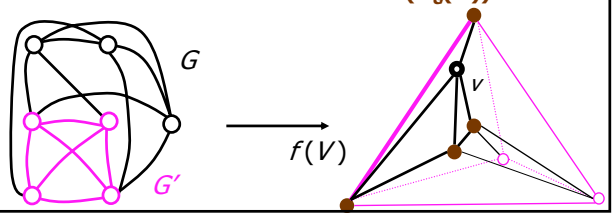
f: V R^k is a **convex embedding** of G with boundary G' into R^k,
if (i) the convex hull of $f(V(G'))$ is isomorphic to G',
(ii) For $\forall v \in V - V(G')$,
$f(v)$ is strictly included in the convex hull of $f(N_G(v))$.
(iii)



Convex Embedding [Nagamochi et al.02]

$N_G(v)$: the set of neighbors of v.

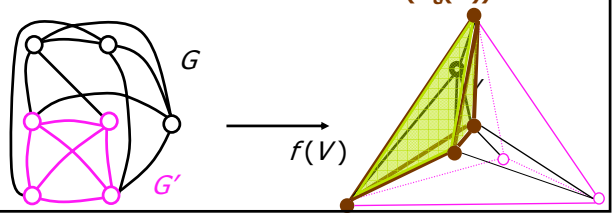
f: V R^k is a **convex embedding** of G with boundary G' into R^k,
if (i) the convex hull of $f(V(G'))$ is isomorphic to G',
(ii) For $\forall v \in V - V(G')$,
$f(v)$ is strictly included in the convex hull of $f(N_G(v))$.
(iii)



Convex Embedding [Nagamochi et al.02]

$N_G(v)$: the set of neighbors of v.

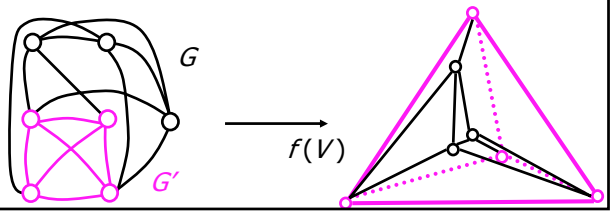
f: V R^k is a **convex embedding** of G with boundary G' into R^k,
if (i) the convex hull of $f(V(G'))$ is isomorphic to G',
(ii) For $\forall v \in V - V(G')$,
$f(v)$ is strictly included in the convex hull of $f(N_G(v))$.
(iii)



Convex Embedding [Nagamochi et al.02]

$N_G(v)$: the set of neighbors of v.

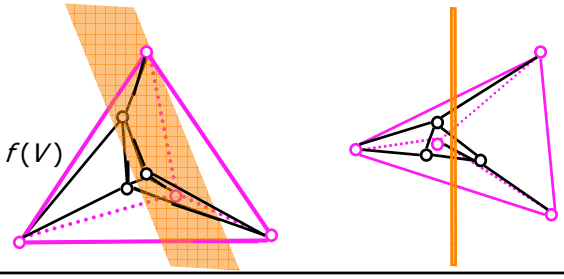
$f: V \to R^k$ is a **convex embedding** of G with boundary G' into R^k, if (i) the convex hull of $f(V(G'))$ is isomorphic to G'.
(ii) For $\forall v \in V - V(G')$, $f(v)$ is strictly included in the convex hull of $f(N_G(v))$.
(iii) Points of $\{f(v) \mid v \in V\}$ are in general position.



Convex Embedding

Lemma [Nagamochi et al.02]

$f: V \to R^k$: a convex embedding of G with boundary G' into R^k.
$\{V_1, V_2\}$: a parition of V obtained by separating $f(V)$ with **an arbitrary hyperplane**.
⇒ Both of V_1 and V_2 induce connected graphs.



Algorithm for finding a 3-bipartition

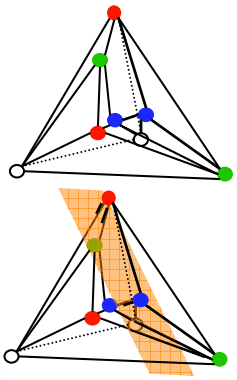
Reduction to a geometrical problem [Nagamochi et al. 02]

Phase 1
Find an embedding of G into the 3-dimensional space R^3 called **"convex-embedding"**.

Phase 2
Bisect V in R^3 into $\{V_1, V_2\}$ by a plane called **"ham-sandwich cut"**.

(1) $|T_i \cap V_1| = |T_i \cap V_2| = |T_i|/2$

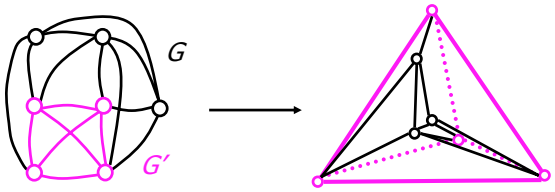
(2) V_1 and V_2 induce connected graphs



3-bipartition

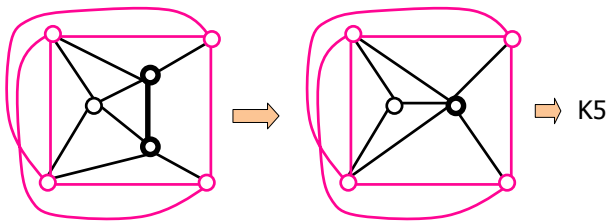
Theorem

G: a 4-connected graph which includes K4 (denoted by G').
⇒ G has a convex embedding into R^3 with boundary G'



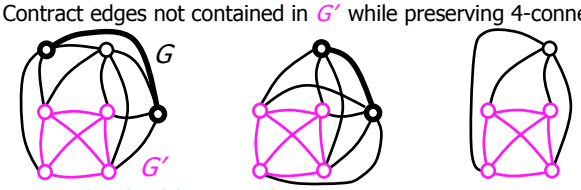
Key Lemma

Lemma Let G be a 4-vertex-connected graph G ($\neq$K5), and H be a subgraph of G with H=K4.
Then G has a contractible edge in $E(G)$-$E(H)$ in such a sense that its contraction preserves 4-vertex-connectivity.

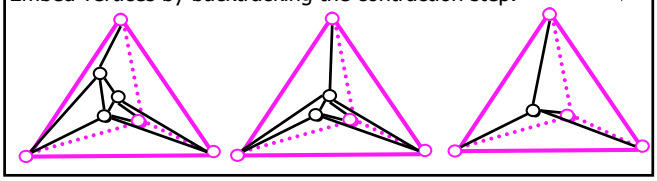


Algorithm for finding a convex embedding into R^3

Step 1 (contraction step)
Contract edges not contained in G' while preserving 4-connectivity



Step 2 (embedding step)
Embed vertices by backtracking the contraction step.



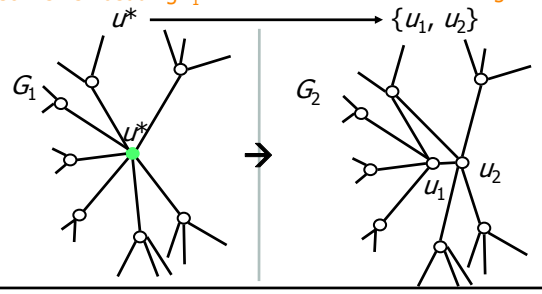
Embedding Step

Given:

G_1: graph obtained from G_2 by contracting u_1 and u_2 into u^* such that $(u_1,u_2) \in E$, $|N_G(u_i)| \geqq 4$

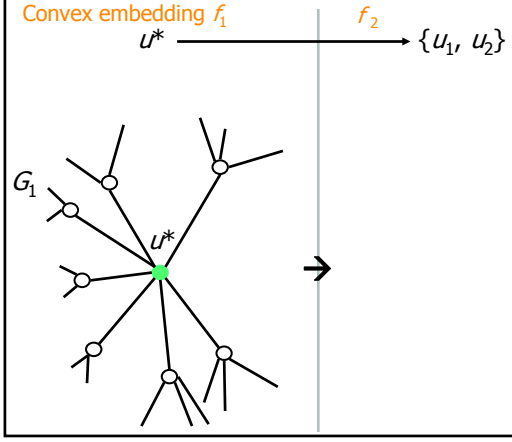
f_1: convex embedding of G_1

Convex embedding f_1 — Convex embedding of G_2



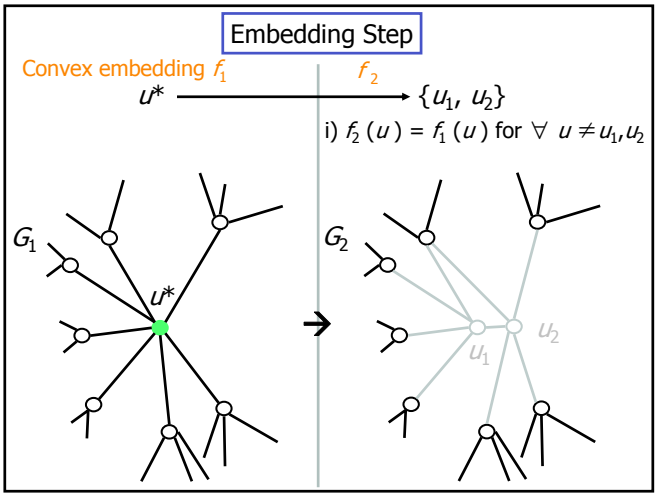
Embedding Step

Convex embedding f_1 f_2



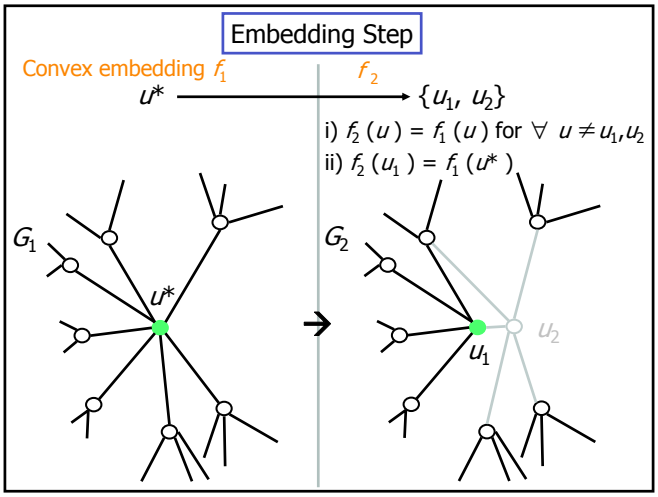
Embedding Step

Convex embedding f_1 f_2



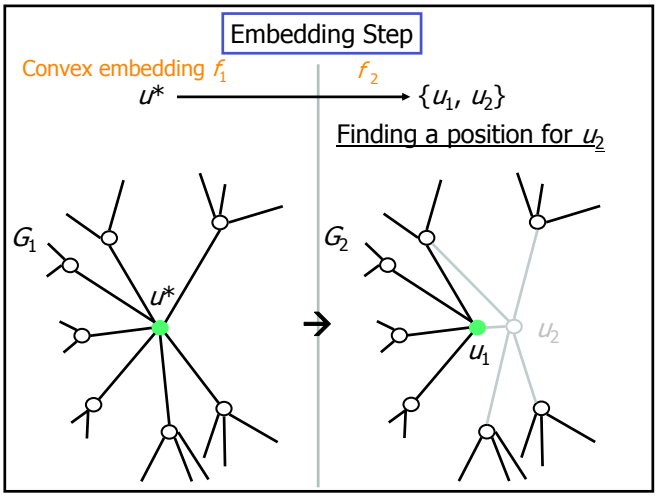
Embedding Step

Convex embedding f_1 f_2



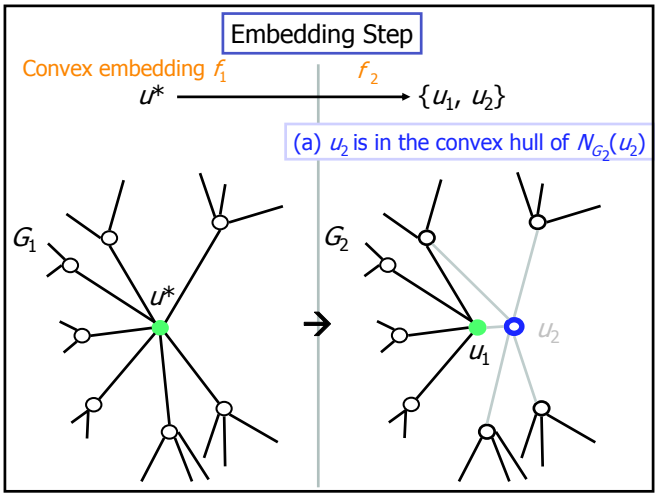
Embedding Step

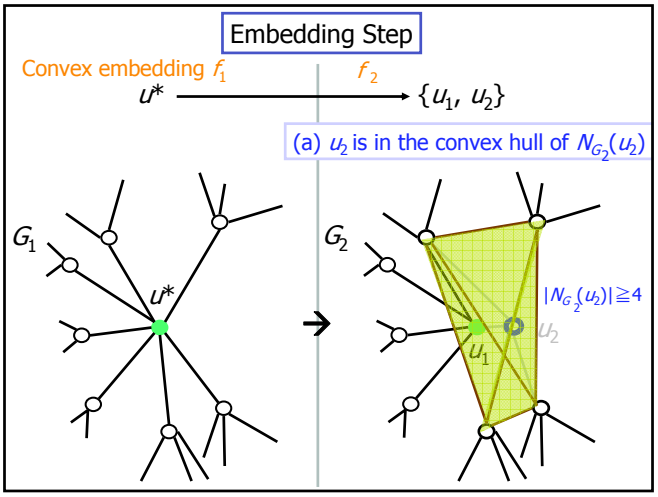
Convex embedding f_1 f_2

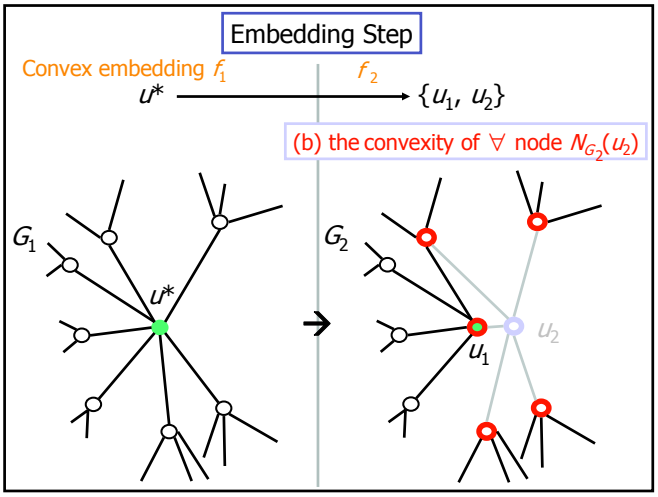


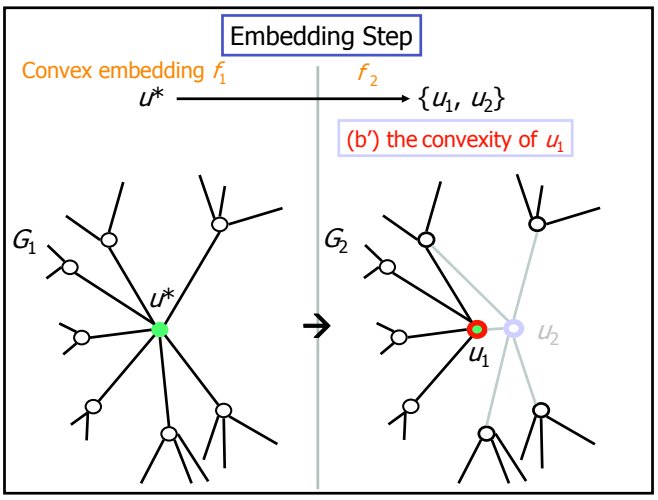
Embedding Step

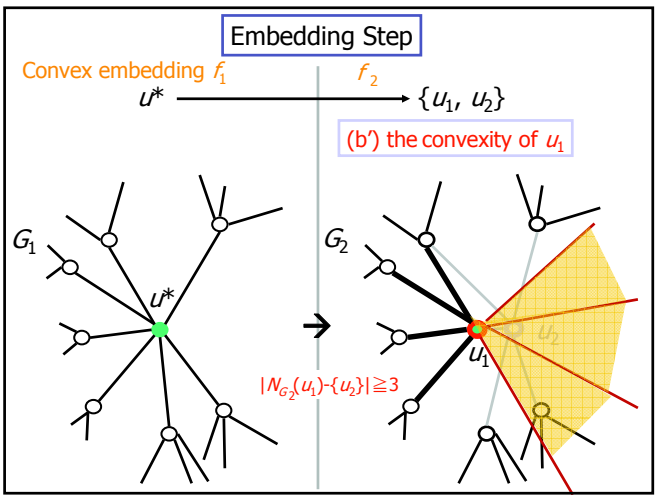
Convex embedding f_1 f_2

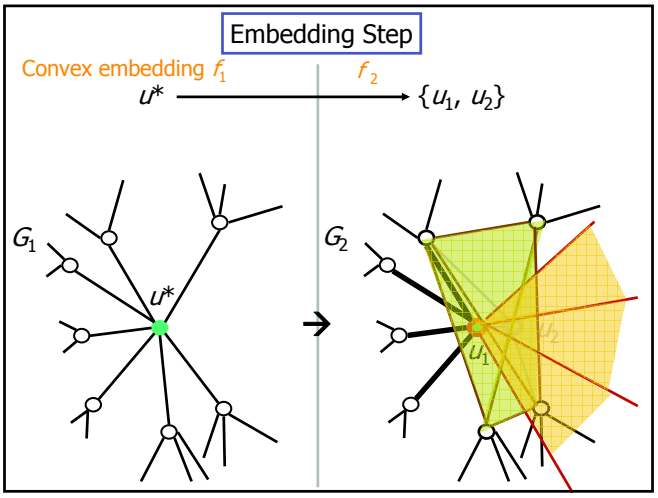


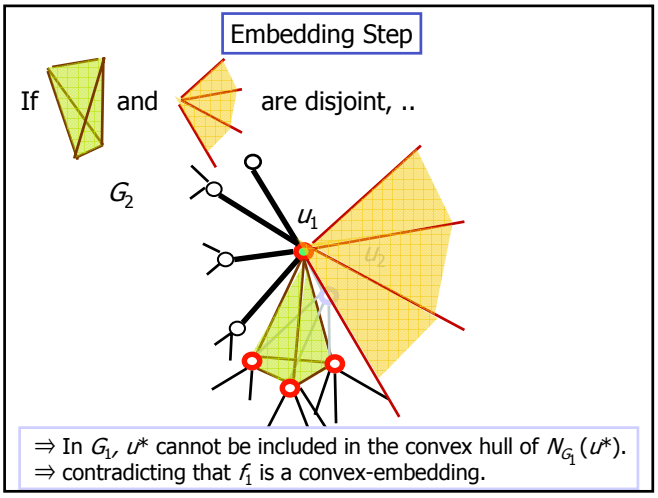

Embedding Step
Convex embedding f_1
f_2
u^*
$\{u_1, u_2\}$
(a) u_2 is in the convex hull of $N_{G_2}(u_2)$
G_1
G_2
u^*
u_1
u_2
$|N_{G_2}(u_2)| \geqq 4$


Embedding Step
Convex embedding f_1
f_2
u^*
$\{u_1, u_2\}$
(b) the convexity of $\forall$ node $N_{G_2}(u_2)$
G_1
G_2
u^*
u_1
u_2


Embedding Step
Convex embedding f_1
f_2
u^*
$\{u_1, u_2\}$
(b') the convexity of u_1
G_1
G_2
u^*
u_1
u_2


Embedding Step
Convex embedding f_1
f_2
u^*
$\{u_1, u_2\}$
(b') the convexity of u_1
G_1
G_2
u^*
u_1
u_2
$|N_{G_2}(u_1)-\{u_2\}| \geqq 3$


Embedding Step
Convex embedding f_1
f_2
u^*
$\{u_1, u_2\}$
G_1
G_2
u^*
u_1
u_2


Embedding Step
If
and
are disjoint, ..
G_2
u_1
u_2
⇒ In G_1, u^* cannot be included in the convex hull of $N_{G_1}(u^*)$.
⇒ contradicting that f_1 is a convex-embedding.

Our Results

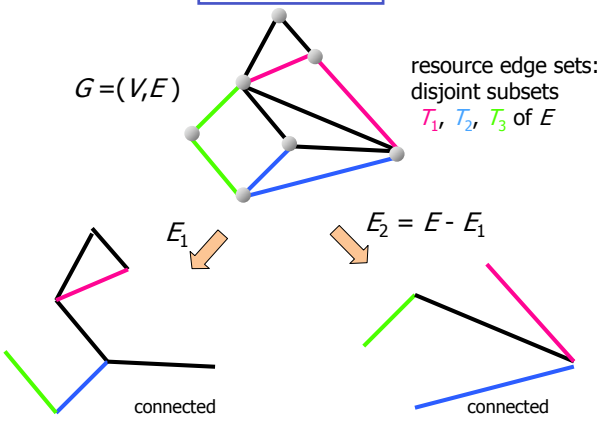
3-bipartition

(1) 5-vertex-connectivity does not suffice!

(2) 4-vertex-connectivity suffices if K4 is contained.

(3) For the edge version of k-bipartition (k=1,2,3), (k+1)-edge-connectivity suffices.

Edge-Version



Edge-Version

Input: a graph and subsets T_i of resource edge sets

Output: a bipartition $\{E_1, E_2\}$ of E

s.t. $|E_1 \cap T_i| = |E_2 \cap T_i|$

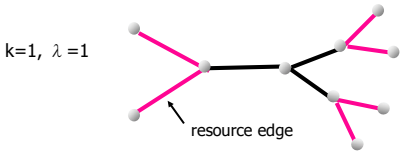
E_1 and E_2 induce connected graphs.

For the edge version of k-bipartition (k=1,2,3), (k+1)-edge-connectivity suffices.

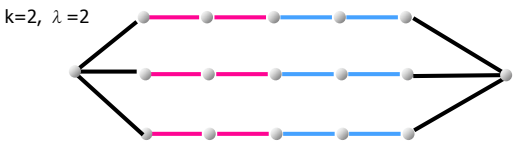
G --> Line graph $L(G)$

(k+1)-edge-connected --> (k+1)-vertex-connected & Kk+1

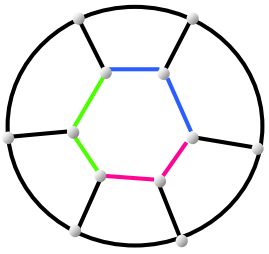
A 1-edge-connected graph which has no 1-bipartition of E



A 2-edge-connected graph which has no 2-bipartition of E



A 3-edge-connected graph which has no 3-bipartition of E



24 vertices
deg=5
κ =5

What we have done is ...

Every 4-vertex-connected graph G admits a 3-bipartition if G has a K_4

5-vertex-connecitivity does not suffice for 3-bipartition
5-vertex-connecitivity does not suffice for 4-bipartition
5-vertex-connecitivity does not suffice for 5-bipartition

The vertex version implies the edge version.

Every (k+1)-edge-connected graph G admits a k-bipartition of E (k=1,2,3).

Open Problems

·Sufficient condition for which a k-bipartition exists

Conjecture
Every (k+1)-vertex-connected graph with Kk+1 admits a k-bipartition.

the edge version

Conjecture
Every (k+1)-edge-connected graph admits a k-bipartition.

Open Problem

Define $f(k)$ be the smallest p such that every p-vertex-connected graph admits a k-bipartition.

$f(1)=2$, $f(2)=3$

For $k>5$, prove $f(k) \geqq k+1$.

$f(3) \geqq 6$, $f(4) \geqq 6$, $f(5) \geqq 6$

For $k>3$, bound $f(k)$ from above by k+constant.

$f(k) = O(\Sigma |T_i|)$

The same questions for the edge version.

Approximating graph coloring of minor-closed graphs

Joint Work with Erik Demaine, Mohammad Hajiaghayi, Bojan Mohar, Robin Thomas
Partially joint Work with Neil Robertson and Paul Seymour

Ken-ichi Kawarabayashi
Tohoku University
E-mail: k_keniti@dais.is.tohoku.ac.jp
http://www.dais.is.tohoku.ac.jp/~k_keniti

Contents (Mostly, FOCS paper)

- Motivation (FOCS paper)
- 2-approx. of the chromatic number of minor-closed graphs (FOCS paper)
- Tree-width, Grid-minor, RS-structure.
- Overview of Algorithm (Robertson-Seymour)
- Approx. the list-chromatic number of minor-closed graphs.
- Toward Structural Theorem

Why is it accepted in FOCS?

- It is building on math deep theory. (although NOT AT ALL practical.)
- Minor-closed graphs are natural. (a generalization of planar graphs.)
- It tells how to use RS' main structural theorem.
- It is a bit easier to access (than RS' papers)
- Nice approx. for graph coloring of minor-closed graphs.
- Lucky.

Motivation

Mathematical Motivation

1. Hadwiger's Conjecture. (A far generalization of 4CT)
2. Graph Minor Theory (Robertson-Seymour)

Algorithmic Motivation

1. Chromatic number is hard to compute.
   NP-complete even for deciding 3-colorability of Planar graphs.
2. Even hard to approx.
   NP-hard to approx. within constant factor.
3. NP-complete to decide the chromatic number of minor closed graphs. (Even for planar graphs)
   Can you approx. ?

Algorithmic Results

- Theorem (Demaine, Hajiaghayi, KK, FOCS2005) There exists a 2-approx. algorithm for the chromatic number in minor-closed graphs. (graphs with no K_k-minor)
- The best known result was $O(k \sqrt{\log k})$ approx.
- Proof uses the whole graph minor papers….
- Robertson-Seymour theory consists of 23 papers. Most of them are published in JCTB.

Why is it 2-approx ?

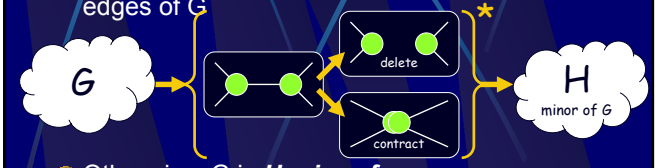
- The main theorem says that if G is Kk-minor-free graphs, then it can be decomposed into two graphs G_1,G_2 such that both G_1 and G_2 have tree-width at most f(k).
- If tree-width is bounded, one can compute the chromatic number in the linear time.
- It remains to give an algorithm for the main theorem…

Proof depends on

- Robertson-Seymour theorem.
- It gives a structural theorem for minor-closed graphs.
- Once we have this structure, the rest of proof is not so hard (but not trivial.)
- The main challenge is how to obtain RS-structure.
- It depends on the whole graph minor papers.

Minors

- A graph G ***has a minor H*** if H can be formed by removing and contracting edges of G



- Otherwise, G is ***H-minor-free***
- For example, planar graphs are both $K_{3,3}$-minor-free and K_5-minor-free

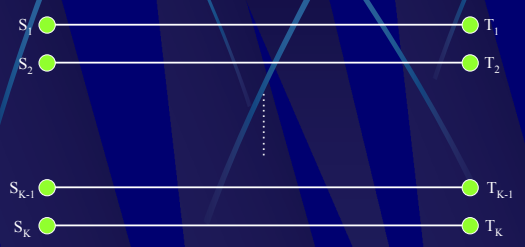
Graph Minor Theory [Robertson & Seymour 1984–2004]

- Seminal series of ≥ 20 papers
- Powerful results on excluded minors:
  - Every **minor-closed** graph property (preserved when taking minors) has a finite set of **excluded minors** [Wagner's Conjecture]
  - Every minor-closed graph property can be decided in polynomial time
  - For fixed graph H, graphs minor-excluding H have a special structure: drawings on bounded-genus surfaces + "extra features"

Highlights of Graph Minor Theory

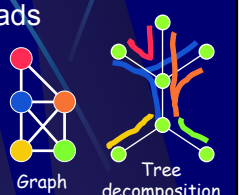
- Theorem(The disjoint paths problem) For fixed k, there is a polynomial time algorithm for deciding the disjoint paths problem.
- Minor testing can be done.
- Tree-width and grid-minors are discovered.
- Many mathematical and algorithmic applications.

The disjoint paths problems



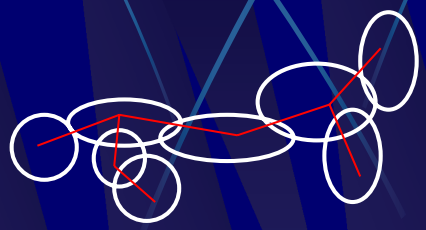
Treewidth [GM2—Robertson & Seymour 1986]

- ***Treewidth*** of a graph is the smallest possible width of a **tree decomposition**
- ***Tree decomposition*** spreads out each vertex as a connected subtree of a common tree, such that adjacent vertices have overlapping subtrees
  - ***Width*** = maximum overlap − 1



- Treewidth 1 ≡ tree; 2 ≡ series-parallel; ...

Tree-Decomposition



Tree-Decomposition of Graph

A tree-decomposition of a graph G is (T,W), where T is a tree and W=(W_t : t ⊂V(T)) satisfies

- $\bigcup_{t \subset V(T)} W_t = V(G)$
- If t' ⊂ T[t,t"], then $W_t \cap W_{t"} \subset W_{t'}$
- uv ⊂ E(G) for some t ⊂ V(t) s.t. u, v ⊂ W_t.

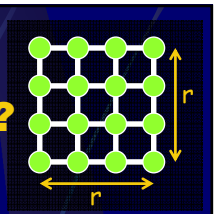
The width is max(|W_t|-1 : t ⊂ V(T)).
The tree-width of G is a minimum width.

- Tree-width at most 1 < = > G is a forest.
- Tree-width at most 2 < = > G is series parallel.
- Tree-width at most 3 < = > G has no minor isomorphic to K_5, Octahedron, 5-prism, V_8.
- Tree-width of the complete graph of order n is n-1.
- Tree-width is minor-monotone.
- The (k × k)-grid minor has the tree-width k.

Tree-Width

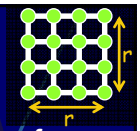
- Discovered by Robertson-Seymour.
- NP-hard to determine tree-width.
- A linear time to decide whether tree-width is k or not for fixed k.
- Many NP-hard problems can be solved in polynomial time if a given graph has small tree-width. (even linear)
- It is useful for structural results.
- It is a key for the proof of RS.
- It is closely related to grid.

Grid Minors Why important ?



- **r × r grid**:
  - r^2 vertices, 2 r (r − 1) edges
  - Treewidth ~ r
- r × r grid is the **canonical** planar graph of treewidth Θ(r): every planar graph of treewidth w has an Ω(w) × Ω(w) grid minor [Robertson, Seymour, Thomas 1994]
  - So any planar graph of large treewidth has an r × r grid minor **certifying** large treewidth
  - What about nonplanar graphs?

Grid Minors Why important ?



- For any fixed graph H, every H-minor-free graph of treewidth ≥ w(r) has an r × r grid minor [GM5—Robertson & Seymour 1986]
  - Re-proved & strengthened [Robertson, Seymour, Thomas 1994; Reed 1997; Diestel, Jensen, Gorbunov, Thomassen 1999]
  - Best bound of these: $w(r) = 2^{0^{5^{|V(H)|^3 r}}}$ [Robertson, Seymour, Thomas 1994]
  - New optimal bound: w(r) = Θ(r) [Demaine,Hajiaghayi KK 2005]
    - Grids certify large treewidth in H-minor-free graph

Huge Grid is important

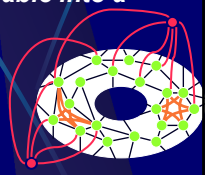
- Routing problem
- The disjoint paths problem and its generalization.
- Actually, Robertson-Seymour use this idea.

Structure of H-minor-free Graphs [GM16—Robertson & Seymour 2003] Main result of RS

- Every H-minor-free graph can be written as O(1)-**clique sums** of graphs
- Each summand is a graph that can be O(1)-**almost-embedded** into a bounded-genus surface
- O(1) constants depend only on |V(H)|

Almost-Embeddable Graphs

- A graph is ***O(1)-almost-embeddable into a bounded-genus surface*** if it is
  - A bounded-genus graph
  - + a bounded number of **vortices**:
    - ***Vortex*** = Replace a face in the bounded-genus graph by a graph of bounded **pathwidth**
    - The interiors of the replaced faces are disjoint
  - + a bounded number of **apices**:
    - ***Apex*** = extra vertex with any incident edges



What do we need ?

- Crosscaps
- Handles
- Genus
- Vortex
- Apex (easy)

But

- There cannot be so many crossings that are far apart.
- The genus addition process stops quite soon.

Otherwise, we would get a desired minor, a contradiction.

We know that

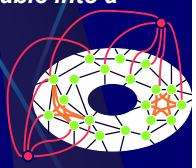
- Any long jump must be contained in the handle. This tells how to detect a handle.
- Any crossings and crosscaps are contained in small area. This tells how we can find a crosscap and a vortex.
- If there is no crosscap in the small area, then it is either vortex or planar graph.
- There cannot be many non-planar small areas that are far apart. This tells us that there are bounded number of vortices.

In summary

1. Stating with huge grid H.
2. As long as there is a long jump, we shall detect handles.
3. Otherwise the graph is embedded into a surface such that all the non-planar graphs are in small areas.
4. We shall look at each small area, and detect either vortex or crosscap.
5. There are only finitely many vortices and crosscaps. So the process stops.

Almost-Embeddable Graphs

- A graph is ***O(1)-almost-embeddable into a bounded-genus surface*** if it is
  - A bounded-genus graph
  - + a bounded number of **vortices**:
    - ***Vortex*** = Replace a face in the bounded-genus graph by a graph of bounded **pathwidth**
    - The interiors of the replaced faces are disjoint
  - + a bounded number of **apices**:
    - ***Apex*** = extra vertex with any incident edges



Approx. list coloring

- Theorem[Mohar and KK]

There is an O(k)-approx. for graphs without Kk-minor, I.e., minor-closed graphs.

Actually, it is "almost" O(√logk)-approx.

It is approximating within O(√logk)c + O(k), where c is optimal.

The best know appox. was O(k √ logk) approx.

Open: O(1) ? (Maybe NP-hard.)

Algorithm for List-coloring

- Theorem[KK & BM]

There is an $O(n^3)$ algorithm for the following:

Input : A graph G, vertex set Z with |Z| <= 4k, precoloring of Z and each vertex in G has 16k-colors available in each list.

Output : Determine either

- G has a K_k-minor, or
- Precoloring of Z can be extended to the whole graph G, or
- G has a subgraph H such that H has no K_k-minor and has a vertex set Z' with |Z'| <=4k such that some precoloring of Z' cannot be extended to H.

Algorithm for List Coloring

- Corollary:

There is an $O(n^3)$ algorithm for deciding the following:

(1) G has a K_k-minor

(2) G has a 16k-list-coloring

(3) G has a subgraph H such that H has no K_k-minor and no 12k-list-coloring.

It is easy to list-color by O(k √ logk) colors

NHC Spring School and Workshop on Discrete Algorithms

Feb. 27th – Mar. 3rd, 2006

University of Electro-Communications / Chofu Creston Hotel

Spring School

Feb. 27th (Mon.)

09:00 – 12:30 Data-Driven Computing
Bernard Chazelle (Princeton University) 415

12:30 – 14:00 Lunch

14:00 – 17:30 Sensor Networks: A Digital Bridge to the Physical World
Leonidas J. Guibas (Stanford University) 423

Feb. 28th (Tue.)

09:00 – 12:30 Games in Networks: Routing, Network Design and Potential Games
Eva Tardos (Cornell University) 456

12:30 – 14:00 Lunch

14:00 – 17:30 Polynomial Time Algorithms for Market Equilibria
Vijay V. Vazirani (Georgia Institute of Technology) 473

Workshop

Mar. 1st (Wed.)

09:00 – 12:30 Random Sampling Techniques and Approximation of MAX-CSP
Marek Karpinski (University of Bonn) 509

12:30 – 14:00 Lunch

14:00 – 17:30 Discussion

Mar. 2nd (Thur.)

09:30 – 10:30 Games in Networks, Equilibria, and Inefficiency
Eva Tardos (Cornell University)

10:30 – 11:00 Break

11:00 – 12:00 Approximation Schemes for Metric Clustering and Partitioning
Marek Karpinski (University of Bonn) 511

12:00 – 13:30 Lunch

13:30 – 14:30 Discrete Optimization and VLSI-Design
Bernhard Korte (University of Bonn)

14:30 – 15:00 Break

15:00 – 16:00 Approximation Algorithms for Facility Location
Jens Vygen (University of Bonn) 519

16:00 – 16:30 Break

16:30 – 17:30 Algorithms for a Networked World
Magnus M. Halldorsson (University of Iceland) 529

Mar. 3rd (Fri.)

09:30 – 10:30 Algorithms for String Manipulation and Related Problems
D. T. Lee (Academia Sinica) 530

10:30 – 11:00 Break

11:00 – 12:00 Dynamic Data Structures in Computational Geometry
Timothy M. Chan (University of Waterloo) 553

12:00 – 13:30 Lunch

13:30 – 14:30 Geometric Networks: Integer Linear Programming and Combinatorial Algorithms
Alexander Wolff (University of Karlsruhe) 564

14:30 – 15:00 Break

15:00 – 16:00 Geometric Embeddings and Graph Expansion
James R. Lee (UC Berkeley) 572

16:00 – 16:30 Break

16:30 – 17:30 Distance Trisector and Voronoi Diagram with Neurtal Zone
Takeshi Tokuyama (Tohoku University) 575

Copyright © Bernard Chazelle | Princeton, January 2006 | home | To appear in "Math Horizons," 2006 | AAAS '06 slides

Could Your iPod Be Holding the Greatest Mystery in Modern Science?

by Bernard Chazelle

Tuturologists are an amiable bunch, so it is a puzzle why the future has been so cruel to them. From flying cars and self-cleaning houses to that bugaboo of workaholics—the leisure society—the soothsayer's trail is littered with the carcasses of pet predictions turned roadkill.

Gordon Moore need not worry. The co-founder of Intel tried his hand at crystal gazing once—and struck gold. His celebrated "law" makes the outlandish prediction that every 18 months, like clockwork, white-clad technicians will huddle in a silicon wafer clean room and cram twice as many transistors onto a microchip.

Moore's Law has ruled the roost for the last 40 years. All the oohs and aahs you hear about the digital revolution are nothing but the squeals humans emit when tickled pink by Moore's Law. From the nice (medical imaging, e-commerce, whole-genome sequencing) to the vital (Xbox, IM, iPod), its rule has been a veritable ticklefest. Moore's Law has been the sizzling cauldron in which savvy cooks have whipped up a dazzling variety of tasty dishes. Without it, the Information Superhighway would be a back alley to Snoozeville; the coolest thing about a computer would still be the blinking lights.

Moore's law has had a good run but, alas, its days are numbered. By mid-

century, a repeal is all but certain. With the heady days of the Incredible Shrinking Chip receding in the past, expect the revolution to grind to a halt; expect pioneers to give way to tinkerers. Bye-bye ticklefest, hello slumber party.

No tears please. Perched atop their towering achievements, computer scientists (the cooks, remember?) will bask in the soothing certainty that their glorious science died at its peak. With a tinge of sadness but not a little pride, they'll chime in unison "There is nothing new to be discovered in computer science now."

If you think you've seen this movie before, you have. A few short years before Einstein turned our world upside down, the great Lord Kelvin bloviated this gem for the ages: "There is nothing new to be discovered in physics now." Not his lordship's finest hour.

Moore's Law has fueled computer science's sizzle and sparkle, but it may have obscured its uncanny resemblance to pre-Einstein physics: healthy and plump—and ripe for a revolution. Computing promises to be the most disruptive scientific paradigm since quantum mechanics. Unfortunately, it is the proverbial riddle wrapped in a mystery inside an enigma. The stakes are high, for our inability to "get" what computing is all about may well play iceberg to the Titanic of modern science.

Brilliant foresight or latest tripe from the Kelvin school of prophecy?

Computing is the meeting point of three Big Ideas: universality; duality; self-reference. To this triad, the modern view adds the concept of tractability and the revolutionary algorithmic paradigm. Here's how it works:

Universality Few would mistake your iPod for an IBM Blue Gene/L—the world's fastest computer. Yet, fundamentally, the two are the same. Why is that? At the heart of your iPod is a written document made of two parts: "*program, data*". The data section stores the songs as long sequences of 0s and 1s. The program section explains in words (again, 0s and 1s) how to read the data and turn it into sound. Add to this mix a smattering of hardware, the *control,* to read the program and follow its instructions, and voilà: you've got yourself an iPod. The beauty of the scheme is that the control need not know a thing about music. In fact, simply by downloading

the appropriate program/data document, you can turn your iPod into an earthquake simulator, a word processor, a web browser, or a paperweight. Your dainty little MP3 player is a *universal* computer.

Separating *control* (the hardware) from *program* (the software) was the major insight of Alan Turing—well, besides this little codebreaking thing he did in Bletchley Park that helped win World War II. The separation was the key to universality. No one had seen anything quite like it before. At least not since the Chinese philosopher opined: "Give a man a fish and you feed him for a day. Teach a man to fish and you feed him for a lifetime." In Confucius's hands, the specialized view of fishing = river + fisherman finds itself replaced by a universal one: fishing = river + fishing manual + you. There you have it, computing = data + program + control. The control part of your iPod is a marvel of electronics, but the shocker is that it need not be so: universal computers can be built with control boxes vastly simpler than a cuckoo clock. For all purposes, computing = data + program.

Duality Consider the iPod document "*Print this, Let 'em eat cake*". Push the start button and watch the words "*Let 'em eat cake*" flash across the screen. Note how the program part of the document, *Print this*, is interpreted as a command—printing is what it wants and printing is what it gets. Contrast this with the data part, *Let 'em eat cake*, which is treated as plain text: no one's eating anything (to Marie-Antoinette's later chagrin). Strings of 0s and 1s are interpreted in one of two ways: as form (data) or as content (program). Tapping into the comic, artistic, and academic potential of this duality, great minds went to work: Abbott and Costello ("Who's on First?"), Magritte ("Ceci n'est pas une pipe"), and Saussure ("signified vs. signifier"). Staring at the sublime will, of course, send the deeper thinkers among us rushing for the classics—such as Homer Simpson's immortal quip: "Oh Marge, cartoons don't have any deep meaning; they're just stupid drawings that give you a cheap laugh."

Self-Reference Write the iPod document "*Print this twice, Print this twice*" and press the start button. The screen lights up with the words: "*Print this twice, Print this twice*". Lo and behold, the thing prints itself! Just like a computer virus (remember, I did *not* teach you this). The magic word is "twice." For example, the iPod document "*Print this, Print this*" prints this: "*Print this*"—more Dr. Seuss than self-replication.

The "Big Ideas" were the air that the Gang of Four, Princeton branch,

breathed all day—that would be Alonzo Church, Alan Turing, Kurt Gödel, and John von Neumann. Mother Nature, of course, figured it all out a few billion years earlier. Reformat your genome by lining up the two strands of DNA one after the other, so it looks like a regular program-data iPod document (billions of letters long though):

"*ACAAGAT...GCCATTG, TGTTCTA...CGGTAAC*".

The base pairings (A,T) and (C,G) ensure that the two strands spell the same word with different letters. So, we lose no genomic information if we translate the "data" part and rewrite the whole document as the duplicated text

"*ACAAGAT...GCCATTG, ACAAGAT...GCCATTG*".

This is the biological analog of "*Print this twice, Print this twice*". Life's but a walking shadow, Macbeth warned us. Not quite. Life's but a self-printing iPod! Offended souls will bang on preachily about there being more to human life than the blind pursuit of self-replication—though Hollywood's typical fare would seem to refute that. Existential angst aside, *duality* is the option we have to interpret the word *ACAAGAT...GCCATTG* either as genes (the "form" encoding our genome) or as proteins (the "content" mediating the DNA replication). *Self-reference* is the duplication embodied in the base pairings. Viewed through the computing lens, life = duality + self-reference.

In the 1953 *Nature* article that unveiled to the world the structure of DNA, Watson and Crick signed off with this lovely understatement: *"It has not escaped our notice that the specific pairing we have postulated immediately suggests a possible copying mechanism for the genetic material."* Duality and self-reference embedded in molecules: what sweet music to Turing's ears this must have been! Alas, our war hero was a little distracted at the time, busy as he was enjoying the rewards that the British authorities had lavished upon him for saving millions of lives during World War II—generous rewards like a court conviction for homosexuality with a sentence of forced estrogen injections. Almost one year to the day of Watson and Crick's triumph, Alan Turing went home, injected cyanide into an apple, ate it, and died. His mother preferred to believe it was an accident.

Tractability The genesis of this fourth Big Idea was the ho-hum observation that checking the validity of a math proof tends to be much easier than finding the proof in the first place. But is it really? Amazingly, no one knows.

Welcome to the most important open question in all of computer science!

Ever wondered if your iPod's 5000-tune library is rich enough to let you compile a playlist of a thousand songs, no two which have ever been played back-to-back on MTV? Let's hope not, because not even an IBM Blue Gene/L could do the job in less time than has passed since dinosaurs were last seen roaming the earth. To find such a playlist (proof-finding) seems hopelessly hard, even on a computer, but to test whether a tentative playlist fits the bill (proof-checking) is a cinch: simply match all possible pairs against MTV's complete playlist, which is readily accessible on the web.

The twin reality of hard proof-finding and easy proof-checking is hardly an MTV-induced aberration. Computer scientists have catalogued over 1000 problems just like it. Of course, courtesy of Murphy's Law, these "Jurassic-1K" include all of the questions humanity is desperate to answer—in artificial intelligence, computational biology, resource allocation, rational drug design, etc.

OK, so life is tough. But since when has that observation qualified as a Big Idea?

Since 1970, roughly. Just as Einstein rebuilt Newtonian mechanics around the constancy of the speed of light, Cook, Edmonds, Karp, and Levin set out to rebuild computing around the notion of *tractability*. A problem is tractable if it can be solved in time growing polynomially in the input size, which is a fancy way of saying 'reasonably fast.' None of the Jurassic-1K appear to be tractable. At least those in the know believe they are not—of course, not so long ago, those in the know believed the earth was flat. Sadly, the great promise of computing seems to lie with problems afflicted with exponentialitis: the dreaded ailment that places even small-size problems beyond the reach of any computer.

This much we know: it's genetic. If a single one of the Jurassic-1K is tractable then, wonder of wonders, all of them are. These tough puzzles are nothing but different translations of the same Shakespeare play. Heady

stuff! The day your playlist question can be answered in a few hours will be the day public-key cryptography dies, bringing down with it all of e-commerce. That day will see biology conquer its highest peak, protein folding, and mathematicians contemplate early retirement. Indeed, the day the Jurassic-1K are shown to be tractable (P=NP in computer parlance), proof-finding will be revealed to be no more difficult than proof-checking. Andrew Wiles, the conqueror of Fermat's Last Theorem, will be found to deserve no more credit than his referees. (Note that this says nothing about *understanding* the proof.) To be P or not to be P, that is NP's question. It is likely that P=NP would do for science what the discovery of the wheel did for land transportation. Little wonder no one believes it.

To discover the wheel is always nice, but to roll logs in the mud has its charms, too. Likewise, the intractability of proof-finding would have its benefits. When you purchase a book from Amazon, the assurance that your transaction is secure is predicated on more than your endearing naiveté. For one thing, it relies critically on the intractability of factoring a number into primes.

Just as modern physics shattered the platonic view of a reality amenable to noninvasive observation, tractability clobbers classical notions of knowledge, trust, persuasion, and belief. No less. For a taste of it, consider the great *zero-knowledge* (ZK) paradox: two mutually distrusting parties can convince each other that each one holds a particular piece of information without revealing a thing about it. Picture two filthy-rich businessmen stuck in an elevator. Their immediate goal is (what else?) finding out who's the wealthier. ZK dialogues provide them with the means to do so while revealing zero information about their own worth (material worth, that is—the other kind is already in full view).

Here is a ZK question for the State Department: can a signatory to the Nuclear Non-Proliferation Treaty demonstrate compliance without revealing any information whatsoever about its nuclear facilities? Just as game theory influenced the thinking of cold war strategists, don't be surprised to see ZK theory become the rage in international relations circles.

Tractability reaches far beyond the racetrack where computing competes for speed. It literally forces us to think differently. The agent of change is the ubiquitous *algorithm*.

The Algorithmic Revolution An algorithm is an iPod program with a human face. If a computer could wash your hair, its program would look like "0110001100100110..." but the algorithm behind it might read: "*Rinse, lather, repeat.*" (Don't try this at home if you're a computer scientist.) An algorithm is a list of instructions that tells the computer what to do. It may loop around and entertain alternatives, as in "*Rinse, lather, repeat if unhappy, dry, go to office, answer question: why didn't you rinse the shampoo off your hair?*" An algorithm is, in essence, a work of literature.

The library's bottom shelves might stack the one-line zingers—algorithmic miniatures that loop through a trivial algebraic calculation to produce *fractals* (pictures of dazzling beauty and infinite intricacy) or print the transcendentally mysterious digits of π. Algorithmic zingers can do everything. For the rest, we have the sonnets on the middle shelves. With names like FFT, RSA, LLL, AKS, they are short and crisp, and tend to pack more ingenuity per square inch than anything else in the computing world. The top shelves hold the lush, richly textured, multilayered novels.

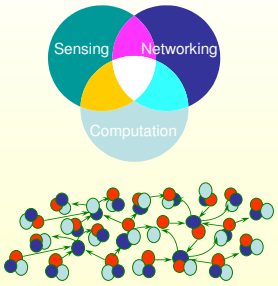
Give it to them, algorithmic zingers know how to make a scientist swoon. No one who's ever tried to compute the digits of π by hand can remain unmoved by the sight of its decimal expansion flooding a computer screen like lava flowing down a volcano. And that's not even the awesome part. For that, one must turn to the infamous Brazilian butterfly whose evil wing flaps cause typhoons in China. Zingers embody the potential of a local action to unleash colossal forces on a global scale: complexity emerging out of triviality. Cellular automata, chaos theory, dynamical systems, and all that.

For a glimpse of the fiction genre on the top shelves, check out *PCP*. Suppose that, after popping the genius pill, you wake up one bright morning with a complete proof of the Riemann hypothesis in your head (that's the "Notorious B.I.G." of math rap: the biggest open problem in the field). Few number theorists are likely to listen to your story. That is, until you offer them the *PCP deal*. You'll write down your proof in an agreed-upon format, and then let a "verifier" pick 10 lines at random. On the basis of these 10 lines alone, the verifier will decide whether your proof is correct. The shocker: beyond any reasonable doubt, she will be right! (Randomness plays a key role, but the chance of erring is less than that of the proverbial monkey typing all of Hamlet flawlessly.)

The mind reels. If your proof is fine, then it will pass any test the verifier can throw at it. But, based on only 10 lines, how can she know that you've proven the Riemann hypothesis and not a baby cousin like 2+2=4? If your proof is bogus, the intuition does not help much either. Presumably, the agreed-upon format is designed to smear any bug all across the proof. But how will the verifier be sure that you didn't play fast and loose with the formatting rules? So many ways to cheat; so little evidence to check. The PCP algorithm upends basic notions of evidence and persuasion, and accomplishes what is usually philosophy's prerogative: to turn the comprehended into the incomprehensible. Somewhere, Wittgenstein must be smiling.

Moore's Law has put computing on the map. Algorithms will now unleash its true potential. Physics, astronomy, and chemistry are all sciences of *formulae*. Chaos theory moved the algorithmic zinger to centerstage. The quantitative sciences of the 21st century (eg, genomics, neurobiology) will complete the dethronement of the *formula* by placing the *algorithm* at the core of their modus operandi. Algorithmic thinking is likely to cause the most disruptive paradigm shift in the sciences since quantum mechanics. And yes, you may trust the future to be kind to this prediction.

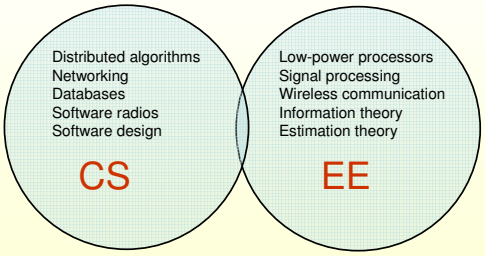
Sensor Networks: A Digital Bridge to the Physical World



Leonidas Guibas
Computer Science Dept.
Stanford University

NHC Spring School and
Workshop on Discrete Algorithms

Introduction

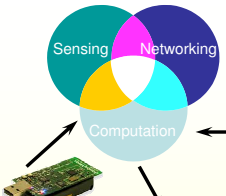


Many good algorithmic and theoretical questions!

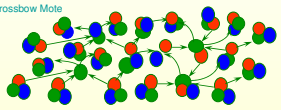
Lecture Outline

- **Part 1:** Introduction to Wireless Sensor Networks
  - Distributed monitoring applications; Sensor network hardware; Research issues in sensor networks; Naming and routing; Sensor tasking and control.
- **Part 2:** Structure Discovery and Information Brokerage
  - Morphological analysis (boundaries, holes, bridges); Landmarks and local coordinates; Information diffusion; Hierarchical hashing.
- **Part 3:** Lightweight Spatio-Temporal Reasoning
  - Configuration spaces; Collaboration groups; Identity management; Occupancy tracking; Conclusion

Smart Sensors and Sensor Networks





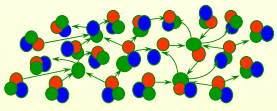


Untethered micro sensors will go anywhere and measure anything -- traffic flow, water level, number of people walking by, temperature. This is developing into something like a nervous system for the earth. -- **Horst Stormer in *Business Week, 8/23-30, 1999.***

- **Environmental sensing**
  - Traffic, habitats, pollution, hazards, security
- **Industrial sensing**
  - Machine monitoring and diagnostics (IC fab)
  - Power/telecom grid monitoring
- **Human-centered computing**
  - Smart, human-aware spaces and environments

Wireless Sensor Networks

- Distributed systems consisting of small, untethered, low-power nodes capable of sensing, processing, and wireless communication

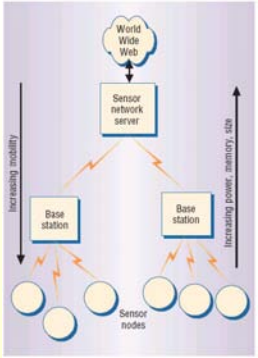




Sensoria Node

Monitoring the World

- Monitoring the environment and other spaces
- Monitoring objects
- Monitoring interactions between objects, or between objects and their environment



Petrel Nesting Behavior at Great Duck Island





7

Wireless Sensor Network Deployment

- Advantages:
  - sensors can be close to signal sources, yielding high SNR
  - phenomena can be monitored that are widely distributed across space and time
    - a `macroscope' [Culler]
  - a distributed architecture provides for scalable, robust and self-repairing systems
  - significant installation savings on cabling, etc. are possible

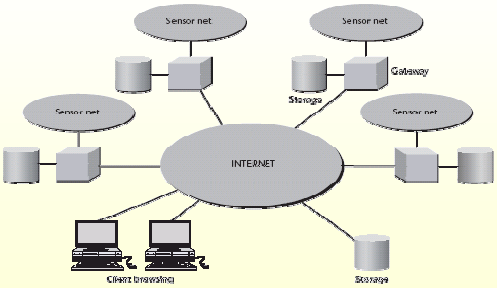
British Columbia winery with networked temperature sensors



Other data collection and monitoring: temperature in data centers (HP), oil tanker vibrations (BP/Intel), soil contaminants, etc.

8

Integration with Current Networks



Access to unfiltered information, highly localized in time and space.
Plans for next generation Internet all include edge sensor networks.

9

More Demanding Sensor Network Applications

- Beyond simple data collection and aggregation
  - dynamic, mobile foci of activity (tracking mobile objects)
  - Amidst clutter of irrelevant data
  - distributed attention: focus and context
  - acting on the world (closing the loop)
- Network must adapt to highly dynamic foci of activity
- Sensing is driven by user queries
- Sensing and communication tasks must be planned and allocated
- Resources must be apportioned between detection, tracking, etc.





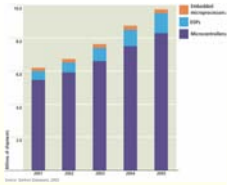
10

Sensor Network Hardware

11

Wireless Sensor Trends

- Of 9.6 billion µP's shipped in 2005, 98% were embedded processors!



- Riding on Moore's law, smart sensors get:

More powerful



Sensoria WINSNG 2.0
CPU: 300 MIPS
1.1 GFLOP FPU
32MB Flash
32MB RAM
Sensors: external

Easy to use



HP iPAQ w/802.11
CPU: 240 MIPS
32MB Flash
64MB RAM
Both integrated and off-board sensors

Inexpensive & simple



Crossbow Mica2dot mote
4 MIPS CPU (integer only)
8KB Flash
512B RAM
Sensors: on board stack (accel, light , microphone)

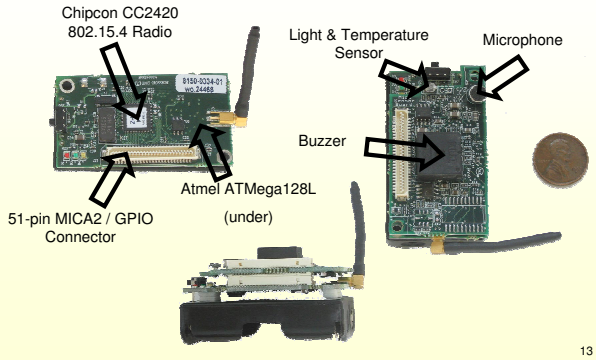
Supercheap & tiny



Smart dust (in progress)
CPU, Memory: TBD (LESS)
Sensors: integrated

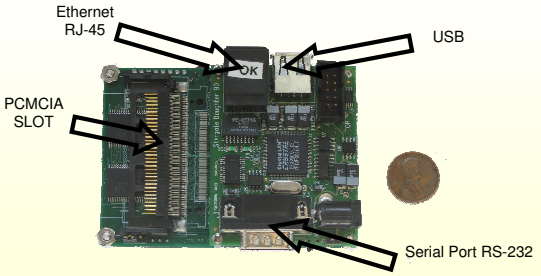
12

Currently Popular: Crossbow Motes



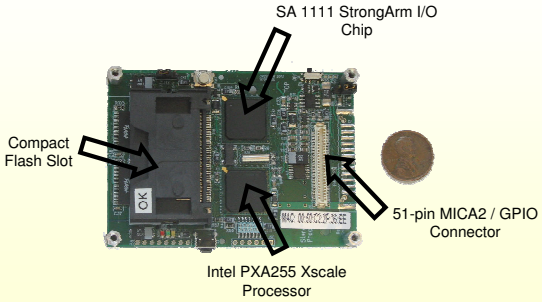
13

Crossbow Stargate - Top View



14

Crossbow Stargate - Bottom View



15

Specifications

MicaZ Mote

- TinyOS
- 16 Mhz Atmel ATMega128L
- 128 kB Program FLASH
- 512 kB Serial FLASH
- Current Draw
  - 8 mA – Active Mode
  - <15 uA – Sleep Mode
- Chipcon CC2420 802.15.4 Radio
  - 250 kbps
  - 26 Channels – 2.4 Ghz
  - Current Draw – 15 mA

Stargate

- Embedded Linux OS
- 400 Mhz Intel Xscale
- 64 MB SDRAM
- 32 MB FLASH
- Many different interfaces
  - RS-232, Ethernet, USB,…

www.xbow.com
http://computer.howstuffworks.com/mote4.htm

16

Power Breakdown …

	Active	Idle	Sleep
CPU	5 mA	2 mA	5 µA
Radio	7 mA (TX)	4.5 mA (RX)	5 µA
EE-Prom	3 mA	0	0
LED's	4 mA	0	0
Photo Diode	200 µA	0	0
Temperature	200 µA	0	0

Rene motes data, Jason Hill

Computation/communication ratio per byte:

- Rene motes:
  - Comm: (7mA*3V/10e3)*8=16.8µJ per 8 bit
  - Comp: 5mA*3V/4e6=3.8 nJ per instruction
  - Ratio: 4,400 instructions/hop
- Sensoria nodes:
  - Comm: (100mW/56e3)*32=58µJ per 32 bit
  - Comp: 750mW/1.1e9=0.7nJ per instruction
  - Ratio: 82,000 instructions/hop



Panasonic CR2354
560 mAh

This means

– Lithium Battery runs for 35 hours at peak load and years at minimum load, a three orders of magnitude difference!

17

Architectural Challenges

18

Sensor Network Challenges

- Power management
  - communication 1000s of times more expensive than computation
  - load balancing across nodes
  - coordinated sleeping/awake schedules
  - correlated sensor data
- In-network processing
  - data aggregation
  - overcounting of evidence
- Difficult calibration
  - localization
  - time-synchronization
- Constant variability
  - networking
  - sensing



[Picture from CACM June 2004]

Dense Sampling: Multi-Hop RF Advantage

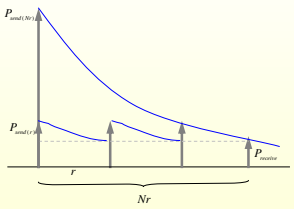
RF power attenuation near ground:

$$P_{receive} \propto \frac{P_{send}}{r^{\alpha}}, \quad \alpha : 3-5$$

Or equivalently, $P_{send} \propto r^{\alpha} P_{receive}$

Power advantage:

$$\frac{P_{send(Nr)}}{N \cdot P_{send(r)}} = \frac{(Nr)^{\alpha} P_{receive}}{N \cdot r^{\alpha} P_{receive}} = N^{\alpha-1}$$



Oversimplified: fixed overheads, delay, etc.

Dense Sampling: Detection and SNR Advantage

Sensors have a finite sensing range. A denser sensor field improves the odds of detecting a target within the range. Once inside the range, further increasing sensor density by *N* improves the SNR by 10log*N* db (in 2D). Consider the acoustic sensing case:

Acoustic power received at distance *r*: $P_{receive} \propto \frac{P_{source}}{r^2}$

Signal-noise ratio (SNR):

$$SNR_r = 10\log P_{receive} - 10\log P_{noise} = 10\log P_{source} - 10\log P_{noise} - 20\log r$$

Increasing the sensor density by a factor of *N* gives a SNR advantage of:

$$SNR_{\frac{r}{\sqrt{N}}} - SNR_r = 20\log\frac{r}{\frac{r}{\sqrt{N}}} = 10\log N$$

Collaborative Estimation

- Structuring communication is very important:

  In a setting where each node wishes to communicate some data to another node at random, interference hinders scaling:

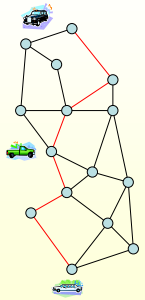
  the per node throughput scales as $\frac{1}{\sqrt{N}}$ (Gupta & Kumar '99)

  Effectively each node is using all of its energy to route messages for other nodes.

  In a sensor network, however, because data from nearby sensors are highly correlated, more intelligent information dissemination strategies are possible.

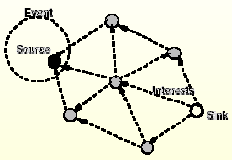
Networking Sensor Networks

- Network support for a small number of collaborative tasks.
- Data-centric, (as opposed to a node-centric) view of the world.
- Monitoring processes may migrate from node to node, as the phenomena of interest move or evolve.
- Communication flow and structure is dictated by the geography of signal landscapes and the overall network task.



`Semantic' Routing and Networking

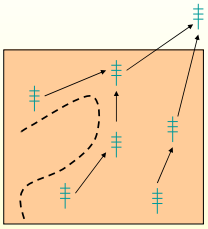
- We want to address spatial locations or information, not individual nodes
- Content and address in a message get intermixed – unlike classical networks
- In a distributed setting, how do we help information providers and information consumers find each other?



Directed diffusion
Geo-routing

In-Network Processing

- Information aggregation can happen on the way to a destination and provide substantial energy savings
- Need to balance quality of paths with quality of information collected
- But aggregation makes data lineage harder to ascertain
- Can we have "application-independent" paradigms of information aggregation?

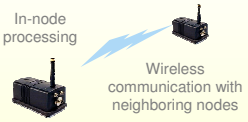


Temperature aggregation

25

Power-Aware Sensing, Computing, and Communication

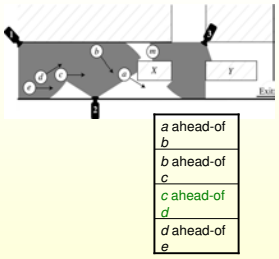
- Variable power systems
- Let most sensors sleep most of the time; use paging channels
- Exploit correlation in readings between nearby sensors
- Load-balance, to avoid depleting critical nodes



26

Sensor Tasking and Control

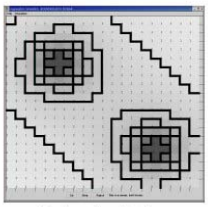
- Decide which sensors should sense and communicate, according to the high-level task – a non-trivial algorithmic problem
- Direct sensing of relations relevant to the task – do not estimate full world state



27

Enable Data-Base Like Operations

- Data only available right after sensing operation
- Dense data streams must be sampled, or otherwise summarized
- Must deal with distributed information storage – "where is the data?"
- Large flash memory availability can make in-network storage possible

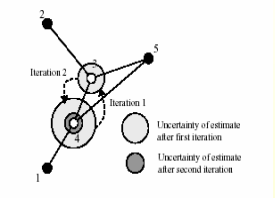


Field isolines

28

Self-Configuration for Ad-Hoc Deployment

- Network size makes it impossible to configure each node individually
- Environmental changes may require frequent re-calibration
- Network must recover after node failures



Iterative localization

29

Structure Discovery

- A sensor network is a novel type of computing device -- a sensor computer
- One of its first tasks is to discover its own structure and establish
  - information highways
  - sensor collaboration groups
- as well as adapt to its signal landscape

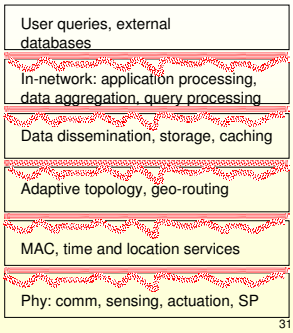


30

New System Architectures

- Resource constraints require close coupling between the networking application layers
- Can we define *application-independent* programming abstractions for sensor networks?

A sensor net stack?



31

Various Issues

- Integration of sensors with widely different modalities
  - High data-rate sensors (cameras, laser scanners)
- Sensor mobility
- Actuation



Distributed robotics

32

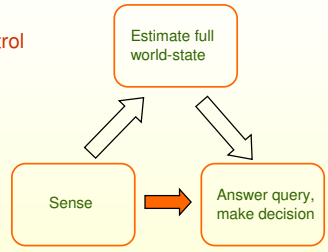
What Defines Sensor Networks?

- Multi-hop communication
  - Many nodes act as routers
  - Multiple paths exist and must be considered
- Bandwidth limitations
  - Volume of data sensed exceeds to capacity of the network to transport
- Power limitations
  - (At least some) nodes operate untethered and energy conservation must be considered in all of sensing, processing, and communication
- A cooperative system
  - All nodes serve one, or a small number of tasks

33

Sensor Network Research

- power awareness
- sensor tasking and control
- formation of sensor collaboration groups
- in-network, distributed processing
- node management, service establishment, software layers
- coping with noise and uncertainty in the environment



A key algorithmic problem is how to sense and aggregate only the portions of the world-state relevant to the task at hand, in a lightweight, energy-efficient manner.

34

Naming and Routing in Sensor Networks

35

Routing in Sensor Networks

- Point-to-point routing protocols in communication networks obtain route information between pairs of nodes wishing to communicate. Such protocols can be
  - proactive: the protocol maintains routing tables at each node that are updated as changes in the network topology are detected
  - reactive: the protocol constructs paths on demand only
- Because of the high rate of topology changes, reactive protocols are much more appropriate for sensor networks
- Several such protocols have already been developed for ad hoc mobile communication networks. Examples are:
  - Ad hoc on demand distance vector routing (AODV)
  - Dynamic source routing (DSR)
    - both, however, may flood the network to discover paths

36

Geographic Routing

- In sensor networks, naming and routing is frequently based on a node's attributes and sensed data, rather that on some pre-assigned network address.
- Geographic routing uses a node's location to name the node and discover paths to that node
- We assume that
  - nodes know their geographic location
  - nodes know their 1-hop neighbors
  - routing destinations are specified geographically (a point, a region)
  - each packet can hold a small amount ($O(1)$) of additional routing info to record where it has been on the network
  - most of the time we will model the connectivity graph of the nodes as a unit distance graph

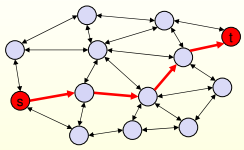
37

Routing Desiderata

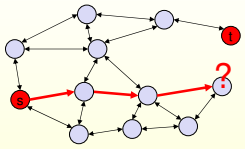
- Guaranteed delivery
- Path quality
- Energy awareness
- Robustness to low-level link volatility

38

Greedy Methods



In a greedy method, each node forwards a packet to its best neighbor



Greedy methods can get stuck at "dead-ends"

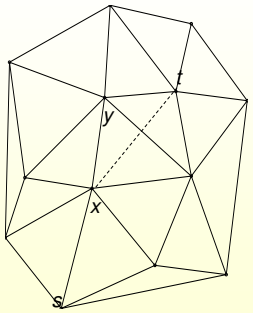
Note that no flooding is involved for route discovery

39

Greedy Unicast Geographic Routing

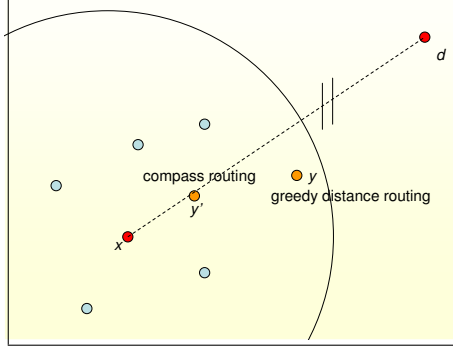
To go from source *s* to destination *t*, at each intermediate node *x* advance to the neighbor *y* that makes most progress towards *t*.

- greedy distance routing (GPSR)
- compass routing



40

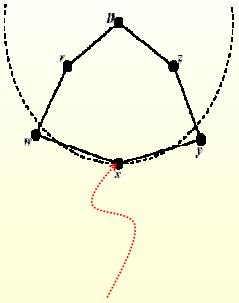
Neighbor Choice



41

Greedy Protocols Can Get Stuck

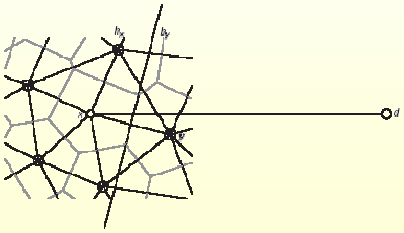
- The intermediate node *x* can be a local optimum towards the destination
- In general, local optima will arise if the node graph contains "holes" – areas with no sensor nodes
- To prove that such situations cannot happen we need to assume special properties about the connectivity graph *G*



42

Delaunay Triangulations (DT)

- In a Delaunay triangulation (dual to the Voronoi diagram of the nodes), packets cannot get stuck
- However, unless the nodes are spaced very closely, it is unlikely that the UDG will contain all DT edges



43

Measures of Path Quality

- First and foremost, a protocol should guarantee packed delivery, whenever such delivery is possible
- Second, the quality of the path produced should be good when compared to the optimal path available. Different path costs can be used:

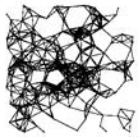
$$c(\pi) = \sum_{e \in \pi} l^d(e), \qquad d = 0,1,2,3,4,...$$

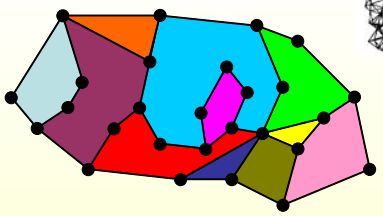
d = 0, hop length
d = 1, normal path length
d = 2, 3, 4 ..., energy costs

- These can be made roughly equivalent by assuming a constant node density or a minimum node spacing
  - This can be attained by a node clustering process

44

Planarizations

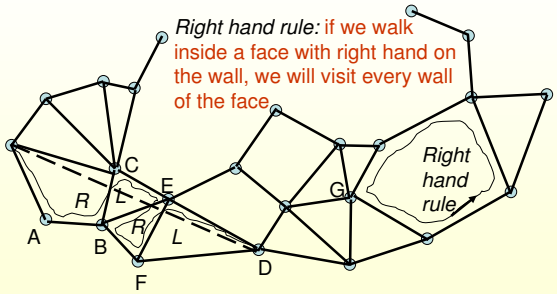




A planar straight-line graph has no crossing edges. It subdivides the plane into regions called faces.

45

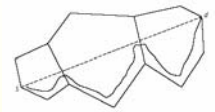
Traversing Planar Graphs: Perimeter Routing

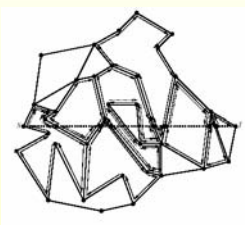


46

Routing in Planar Graphs

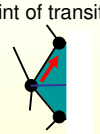
- To guarantee packet delivery, *it may be advantageous to disable some connections*, so as to make the routing graph planar
- On a planar graph, perimeter routing guarantees delivery
- Another variant is other face routing
- The quality of paths can be bad, however

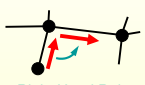




Perimeter/Face Routing Properties

- All necessary information is stored in the message
  - Source and destination positions are given
  - Point of transition to next face needs to be chosen



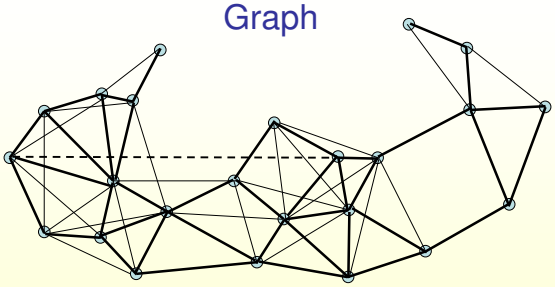


"Right Hand Rule"

- Completely local:
  - Knowledge about direct neighbors' positions sufficient
  - Faces are implicit, only local neighbor ordering around each node is needed

48

Planarizing the Communication Graph



We must delete just enough edges to make the graph planar

We must do so in as local a manner as possible

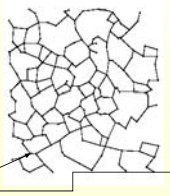
49

Planarization via Geometric Graphs

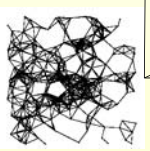
- defined by local rules?
- distributed construction?
- path quality (spanning property)? $\frac{|\pi^*|}{|st|}$

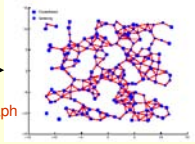


Gabriel Graph



Restricted Delaunay Graph (RDG)

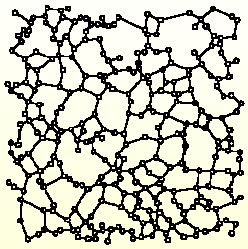


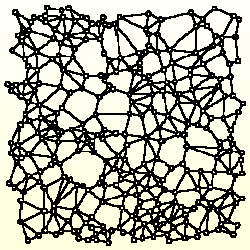


Relative Neighborhood Graph (RNG)

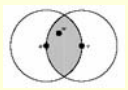
50

Larger RNG and GB Examples

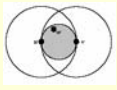




Relative Neighborhood Graph



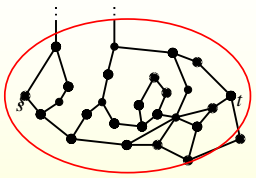
Gabriel Graph



51

Adaptive Algorithms

- We want the quality of paths we discover to be nearly optimal
- Alternatively, we want to discover optimal paths without searching the whole connectivity graph G
- If the optimal path between s and t has length L, then every node in that path is within an ellipse with foci s and t defined by L. This ellipse limits the part of G to be searched.
- If L is not known, it can be guessed, approximately

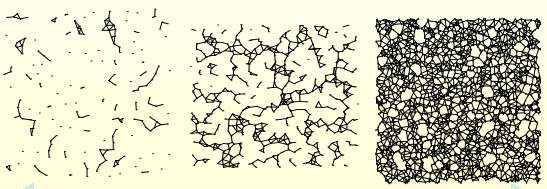


In general, finding a path of length L requires $O(L^2)$ work.

52

Average Path Quality

- Not interesting when graph not dense enough
- Not interesting when graph is too dense
- Critical density range ("percolation theory")
  - Shortest path is significantly longer than Euclidean distance



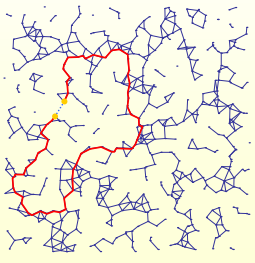
too sparse — critical density — too dense

53

Critical Density: Shortest Path vs. Euclidean Distance

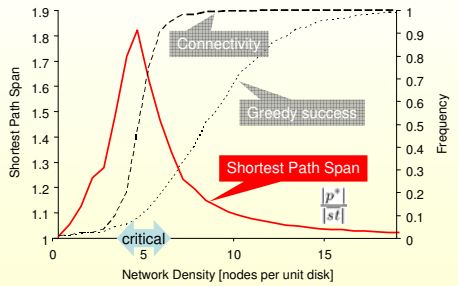
- Shortest path is significantly longer than Euclidean distance

$\frac{|\pi^*|}{|st|}$



54

Randomly Generated Graphs: Critical Density Range



55

Combining Greedy and Planarization Strategies: Greedy Perimeter Stateless Routing (GPSR)

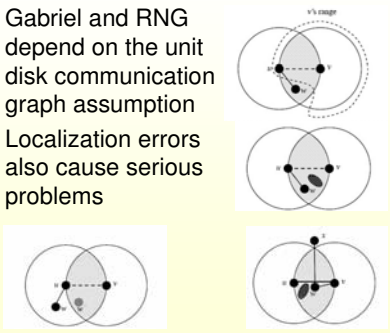
[Bose and Morin 1999,
Karp and Kung, Mobicom 2000]:
Planarize the connectivity graph *G*

- Use greedy distance protocol on the full graph *G*
- If stuck, switch to perimeter protocol on a planarization of *G*, until a node closer to the destination than the stuck node is encountered

56

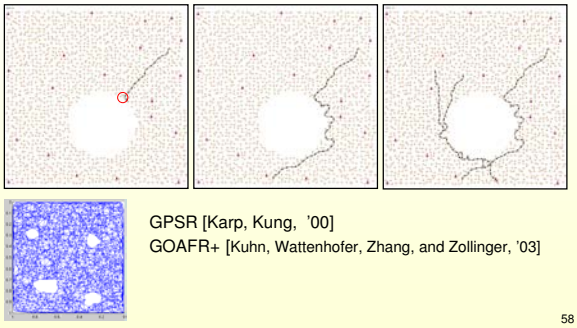
Planarization Process Is Not Robust

- Gabriel and RNG depend on the unit disk communication graph assumption
- Localization errors also cause serious problems



57

Greedy Protocols May Overload Critical Nodes



GPSR [Karp, Kung, '00]
GOAFR+ [Kuhn, Wattenhofer, Zhang, and Zollinger, '03]

58

Main Point

- Knowledge of the nodes' locations enables many powerful mechanisms for message transport and route discovery that avoid expensive flooding operations yet require no routing tables or other high-maintenance data structures.

59

Sensor Tasking and Control

60

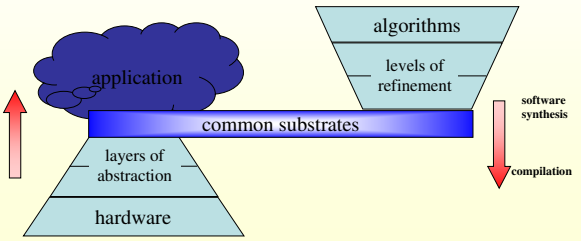
Programming Sensornets: Where the Two Sides Meet

Platform View

Spend more time designing system/component-level abstractions

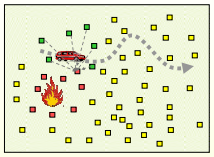
Information Processing View

Spend more time designing application-level abstractions



61

Collaborative Processing in Sensor Networks

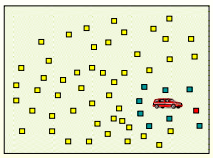


- What information is critical for the high-level tasks?
- What is the cost of accessing the information?
- Which nodes should participate in sensing, processing, or communication?
- How should the information be migrated?
- What is routing or querying in this context?

The information processing needs largely determine the roles of nodes, as well as the required support by other layers of a sensor network

62

Collaborative Processing
Group Formation in Sensor Networks

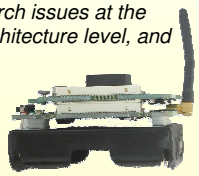


- Information needs and resource constraints define who should participate in the processing groups
- Group membership (e.g. location) defines the behavior of a node
- Challenges
  - Dynamic collaboration among nodes
  - Global property from local execution
  - Competing events/tasks
  - Real-time constraints/adaptation

63

Summary

- *Ubiquitous networked sensors provide a dense spatial and temporal sensing of the physical world*
- *They potentially provide low-latency access to information that is highly localized in time and space, and thus provide a way to sense and act on the physical world beyond what has been possible up to now*
- *Sensor networks raise many research issues at the physical node level, the system architecture level, and the algorithm deployment level*



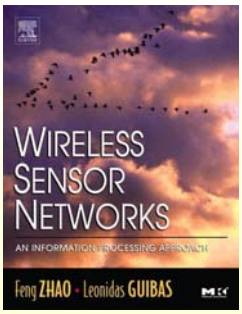
64

A Relevant Text

Wireless Sensor Networks: An Information Processing Approach

Feng Zhao and Leonidas Guibas

Morgan-Kaufmann 2004

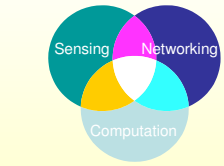


65

The End

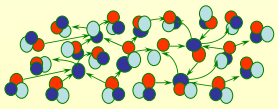
66

Structure Discovery and Information Brokerage in Sensor Networks



Leonidas Guibas
Computer Science Dept.
Stanford University





Structure Discovery

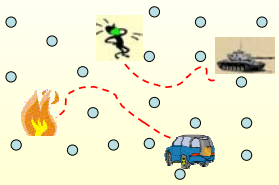
- A sensor network is a novel type of computing device -- a sensor computer
- One of its first tasks is to discover its own structure and establish
  - information highways
  - sensor collaboration groups
- as well as adapt to its signal landscape



[From D. Estrin]

Information Brokerage

- Information providers (sources, producers) and information seekers (sinks, consumers) need ways to find out about and rendez-vous with each other
- Challenges:
  - Neither knows where the other is
  - Highly dynamic environment
  - Limited computation and communication resources



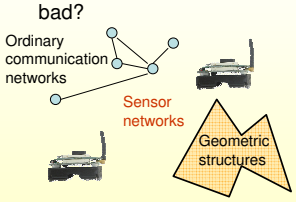
Talk Outline

- Naming and Routing
  - Landmarks and local coordinates
  - Hierarchical landmarks
- Sensor Layout Analysis
  - Boundary/hole detection
- Information Dissemination and Aggregation
  - Sweep
- Information Brokerage
  - Hierarchical geographic hashing
  - Double rulings
  - Information gradients

A Dilemma: Which Structure?

- Nodes are embedded in a physical space. Should we adopt the naming and routing structures already available in the host space?
- Or should we invent a space that better reflects the true network topology, and use that instead?

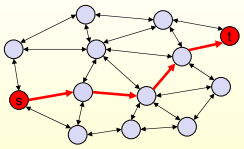
- What if our sampling is bad?



- What if the network is volatile?

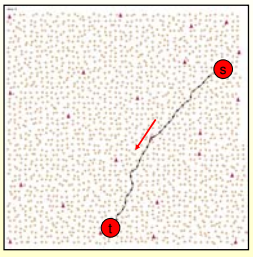
Greedy Geographic Routing

Assume known node positions

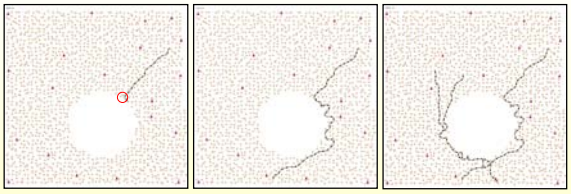


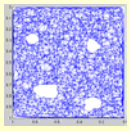
In a greedy manner, each node forwards a packet to its best neighbor

Note that there is little global state, yet no flooding is involved for route discovery



Such Greedy Protocols Get Stuck, May Overload Critical Nodes





GPSR [Karp, Kung, '00]
GOAFR+ [Kuhn, Wattenhofer, Zhang, and Zollinger, '03]

These require building a planar subgraph of the connectivity graph – not a robust process

Global Embedding Challenges



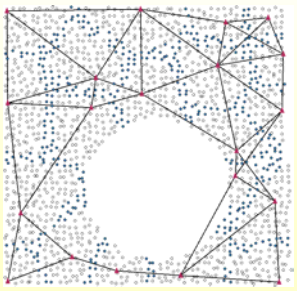
- Routing on geographic coordinates
  - Only works in 2-D space
  - Planarization is tricky (CLDP, etc.)
  - Sensitive to location inaccuracy
- Routing on virtual coordinates
  - Requires a global embedding of the link connectivity graph in the plane
  - Forcing a 2-D layout on a 3-D deployment may ignore much of the actual connectivity

Naming an Routing Based on Connectivity Information Only

- A two-tier approach utilizing combinatorial Delaunay complexes and local coordinates (GLIDER)
- A hierarchical approach using the Discrete Center Hierarchy (DCH)

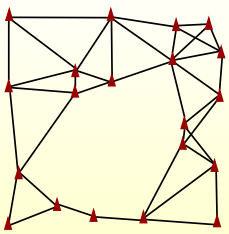
I. Using Landmarks and Local Coordinates: GLIDER

- Given a communication graph on sensor nodes with distances defined by hop counts
- Perform structure discovery:
  - Select a set of landmarks
  - Construct the Landmark Voronoi Complex (LVC)
  - Extract the Combinatorial Delaunay Triangulation (CDT) graph on landmarks



G is connected ⇔ CDT D(L) connected

- D(L) is compact – topology capture has complexity dependent on the number of large-scale features in the environment
- D(L) is stable – low- level link volatility unlikely to affect the combinatorial complex



D(L) is a global network atlas that can be known to all landmarks, or even all nodes

Local Routing with Global Guidance

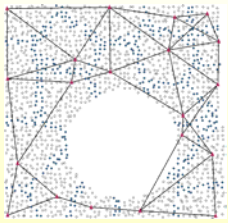
- Global Guidance

  the D(L) encodes global connectivity information that is accessible to every node for proactive route planning on tiles.
- Local Routing

  high-level routes on tiles are realized as actual paths in the network by using local reactive protocols.

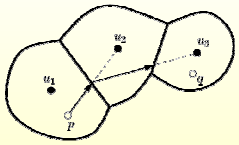
Information Stored at Each Node

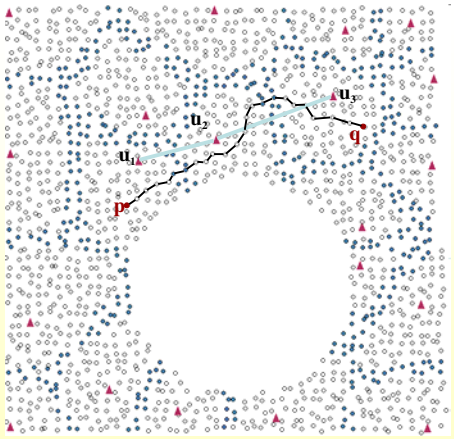
- The parents on the shortest paths to its home landmark, and its neighbor landmarks
- A bit to record if the node is on the boundary of a tile
- Its **coordinates** and those of its neighbors for intra-tile greedy routing
- Landmark nodes store the atlas D(L)



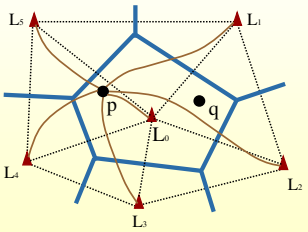
GLIDER -- Routing

- Routing
  - Global route plan
  - Local route
    - inter-tile
    - intra-tile





The Last Mile: Local Coordinates and Greedy Routing



Reference landmarks: $L_0,\ldots L_k$

$T(p) = L_0$

Let $s = \text{mean}(pL_0^2,\ldots, pL_k^2)$

Local virtual coordinates:

$c(p) = (pL_0^2 - s,\ldots, pL_k^2 - s)$

(centered metric)

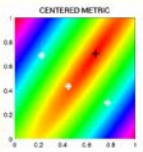
Distance function:

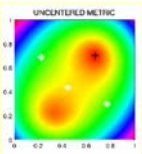
$d(p, q) = |c(p) - c(q)|^2$

Greedy strategy: to reach q, do gradient descent on the function d(p, q)

Local Landmark Coordinates – No Local Minima

- Theorem: In the continuous Euclidean plane, gradient descent on the function d(p, q) always converges to the destination q, provided that there are at least three non-collinear landmarks.
- In the discrete case, we empirically observe that landmark gradient descending does not get stuck on networks with reasonable density (each node has on average six neighbors or more).



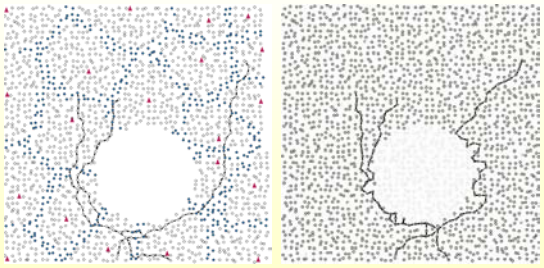


Centered vs. Uncentered Metrics

movie1.mpeg

movie2.mpeg

Simulations – Path Length and Load Balancing

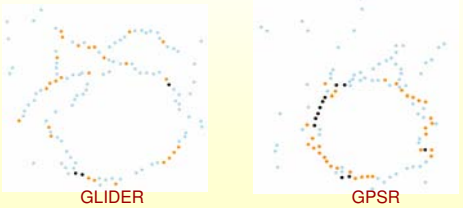


GLIDER GPSR

Each node on average has six one-hop neighbors

Simulations – Hot Spot Comparison

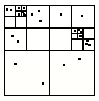
Randomly pick 45 source and destination pairs, each separated by more than 30 hops.



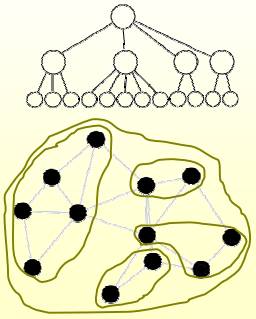
GLIDER GPSR

Blue (6-8 transit paths), orange (9-11 transit paths), black (>11 transit paths)

II. Naming and Routing via Hierarchical Decompositions of Graphs



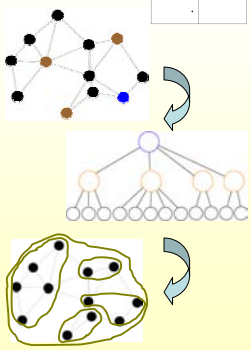
- Generalize quadtrees
- No node geographic coordinates assumed
- Required properties:
  - Clusters in level i of the decomposition have diameter at most $\alpha \cdot 2^i$, where α is a constant
  - Each cluster in level i+1 contains a small (constant) number of clusters in level i



Examples of HDs

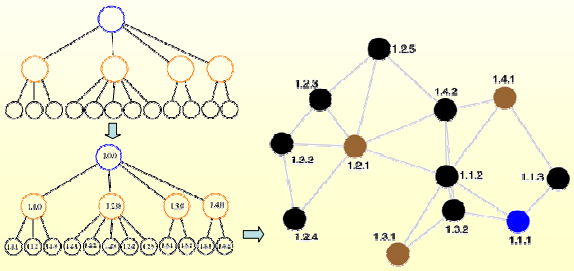


- A quad-tree induces a HD when the sensor field is dense and node coordinates are available.
- Discrete Center Hierarchy:
  - A hierarchical sampling of the nodes so that:
    - Nodes in level *i* are at least 2^i hops apart
    - Each node in level *i* is within 2^{i+1} hops from some node in level *i*+1



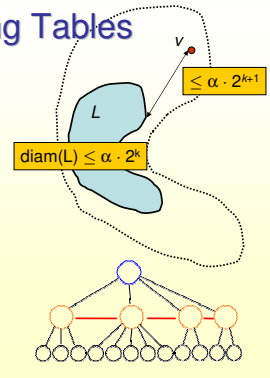
Addressing Scheme

- A HD yields an IP-type addressing scheme for nodes
- Clusters are also assigned addresses



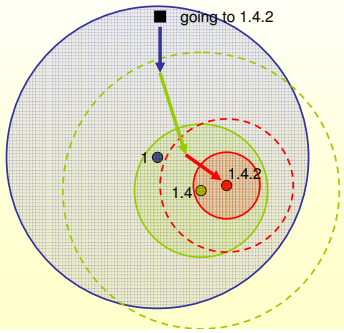
Neighboring Clusters and Local Routing Tables

- Def: A cluster *L* at level *k* is a neighboring cluster of a node *v* if $\text{dist}(v, L) \leq \alpha \cdot 2^{k+1}$
- A routing table is stored at each node, providing hop distances to all its neighboring clusters
- Under mild assumptions, each node has $O(\log n)$ neighboring clusters



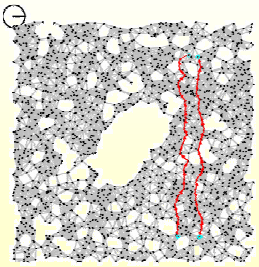
Getting to Your Destination

- Head in the direction of the cluster with the longest prefix that agrees with your destination address
- Use local routing tables to make the best local decision



Routing Scheme

- Routing quality:
  - By proof:
    - Efficient: $|path(u,v)| \leq 4 \cdot |d_{uv}|$
  - By simulation:
    - Balanced: Nodes high up in the hierarchy do not get overloaded
    - Robust: the failure of any given link does not affect many paths



Experimental Results

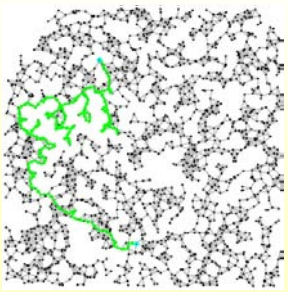
degree 6.21

Routing quality (2000 nodes)

Avg. deg.	Qual. of HD avg	Qual. of HD std	Qual. of GPSR avg	Qual. of GPSR std
6.21	1.08	0.18	4.91	6.79
6.80	1.06	0.11	4.04	7.41
7.39	1.05	0.09	3.25	7.02
7.93	1.09	0.16	2.04	3.10
8.53	1.07	0.12	1.59	2.22
8.94	1.07	0.10	1.51	2.42
9.82	1.07	0.10	1.35	1.62
10.2	1.06	0.09	1.31	1.80
10.8	1.05	0.09	1.44	2.90
12.0	1.06	0.11	1.15	1.30

Paths generated are near optimal

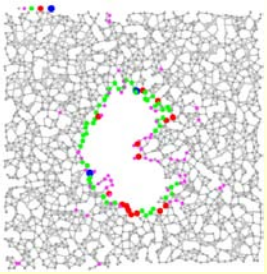
$$\text{Quality} = \frac{\text{HD path length}}{\text{Shortest path length}}$$



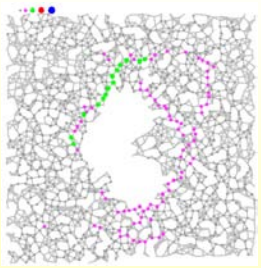
HD path – GPSR path

Hot Spots

2000 nodes, perturbed grid
100 random paths
max load = 32



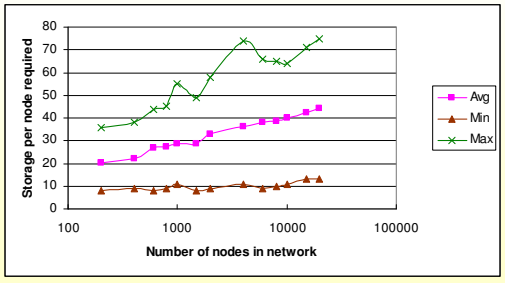
GPSR



HD

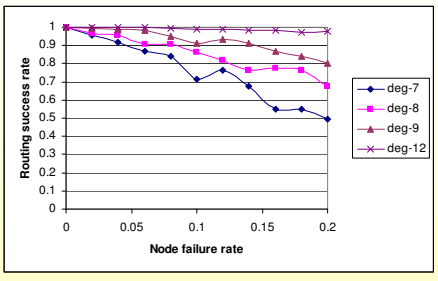
HD does not hug holes as much as GPSR

Routing Scalability



Storage used grows slowly
Network initialization cost ~ storage used

Routing Robustness



Routing performance degrades gracefully as node failure rate increases

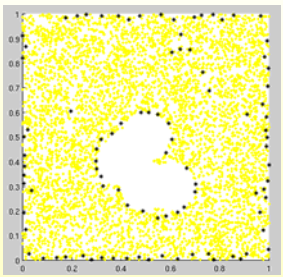
HD Names and Routes Summary

- HD effectively discovers the intrinsic geometry of the network
- Provides a hierarchy-based scheme with provable approximation quality on the routing paths
- Node/link failures affect mostly the low levels of the hierarchy

Sensor Layout Analysis

- Boundary/hole detection
- Robust planarization of the communication graph

Boundary Detection



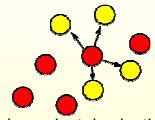
Information Dissemination and Aggregation

- Most sensor network applications need a robust and efficient implementation of certain basic data operations
- In such a data operations library one needs to include:
  - data dissemination (code images, parameter settings, etc.)
  - in-network data aggregation

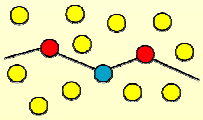
Related Work

Data Dissemination

- Epidemic approaches
  - Trickle/Deluge

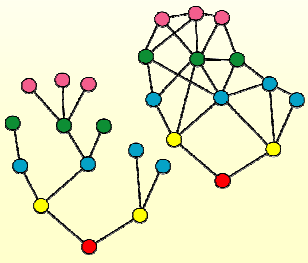


- Independent dominating sets



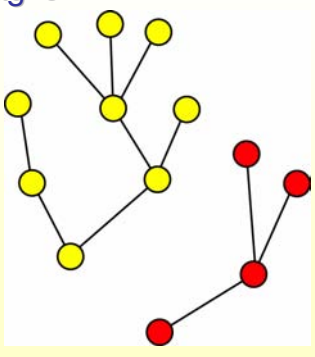
Data Aggregation

- Tree-based approaches
  - TAG/DAG
- Synopsis diffusion



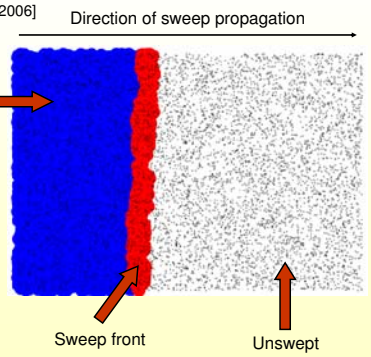
Tree-Based Approaches Are Fragile

- Single links are relied upon
- Long interval between establishment and use



Sweeps over a Sensor Network

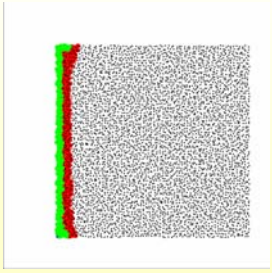
[Skraba, Fang, Nguyen, G. 2006]



- Unswept nodes
- Nodes in sweep
- Swept nodes

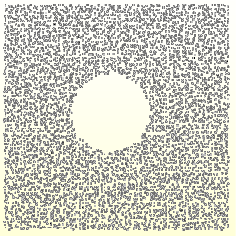
Global Picture

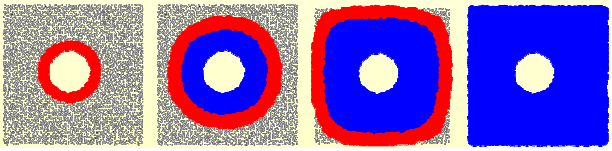
- Nodes are invited to join in the sweep by already active neighbors
- Nodes remove themselves from the sweep after they and all their neighbors have been processed
- A select subset of the nodes always holds the state of the sweep
- Active band moves across the network as nodes join and remove themselves
- Locality of advancing tests allows for parallelism



Sweep Requirements

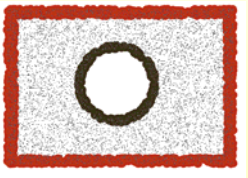
- Cover all nodes in a network, each exactly once
- Use a small active band
- Robust to link volatility
- Local, asynchronous control

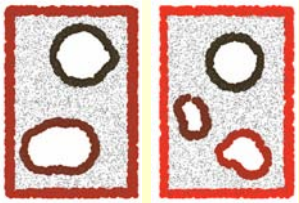




Preprocessing

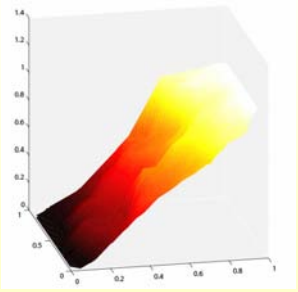
- Structure discovery
  - Some global information needs to be extracted from the network
- Boundary detection
  - source and sink for the sweep
- Auxiliary info for sweep control





Potential Field for Wavefront Diffusion

- Part of preprocessing
- Potential field
  - Sense of direction
  - Ordering
- Stable
- Used for many sweeps

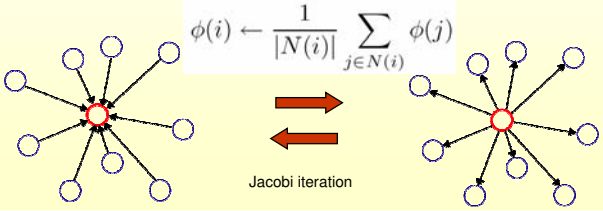


Potential Field Construction

- Fix potential values at certain boundary nodes
- Regular nodes iteratively average over neighbors' values



$$\phi(i) \leftarrow \frac{1}{|N(i)|} \sum_{j \in N(i)} \phi(j)$$



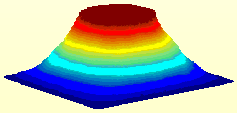
Intuition (Cont. Domain)

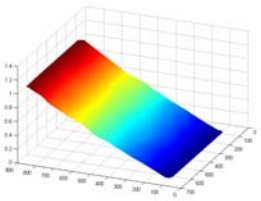
- Laplace's equation with Dirichlet boundary conditions

$$\nabla^2\phi(i) = 0$$

$$\phi(\text{source}) = 1 \qquad \phi(\text{sink}) = 0$$

- Solving discretized version on communication graph
- Smoothing



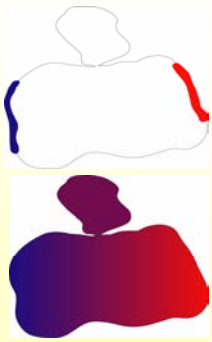


Properties

- Linear system
- Static case: Convergence guaranteed
  - Convergence can be slow (but done only once)
- Direct solution
- No strict maxima or minima at regular nodes
  - Harmonic functions
- Any non-plateau regular node has a strictly monotone path to a maximum or minimum

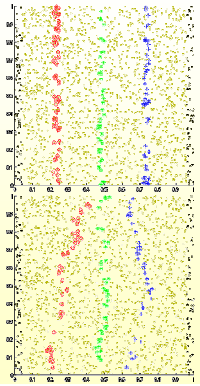
Plateaus

- All neighbors have same value
- Do not occur in continuous case
- Not strict extrema
- Cons:
  - Potential field provides no information
- Pros:
  - Easy to detect
  - Can also be addressed by building another potential within the pleateau
  - Boundary nodes can also be detected



Sweep Algorithm

- Begin *Unswept*
- Receive invitation
  - Enter *Sweep* and send data to inviter (aggregator)
- Possibly issue new invitations
- If all upstream neighbors have left the sweep
  - Forward data to downstream neighbor
- Leave *Sweep*



Simulations

- Stability of the potential field
- Robustness of the sweep
- 500 nodes
- Varying degrees of connectivity

- TOSSIM implementation
  - 20x20 grid
  - Different radio models
  - Robust to link failures/collisions



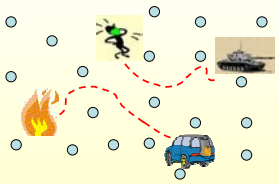
Conclusions

- Class of global operations on a WSN
- Still uses a transient local tree
  - But the tree is local and is used soon after it is built

- Two-part solution
  - Potential field
    - Captures link connectivity and global structure
    - Relatively stable
  - Sweep
    - Uses the potential field for local control
    - Robust
    - Easily extendible

Information Brokerage

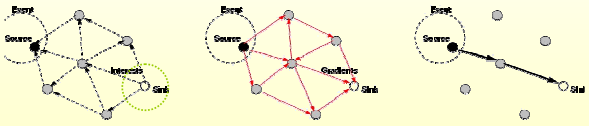
- Information providers (sources, producers) and information seekers (sinks, consumers) need ways to find out about and rendez-vous with each other
- Challenges:
  - Neither knows where the other is
  - Highly dynamic environment
  - Limited computation and communication resources



Current Approaches: Directed Diffusion

[Intanagonwiwat, Govindan, Estrin '00]

- Data-centric storage: data is named by attributes

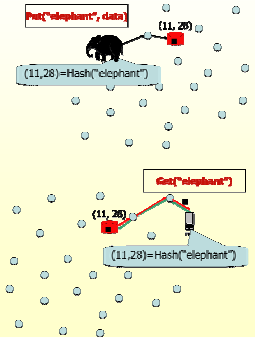


(a) Interest propagation (b) Initial gradients set up (c) Data delivery along reinforced path

Current Approaches: Geographic Hash Tables (GHT)

[Ratnasamy, Karp, Shenker, Estrin, Govindan, Yin, Yu '03]

- Event data is stored, by name, at home nodes; home nodes are selected by the named attributes, via a hash function
- Queries also go to the home nodes to retrieve the data (instead of to the nodes that detected the events)
- Routing usually done using a geographic routing protocol (GPSR)

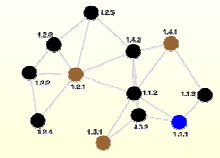


Information Brokerage Issues

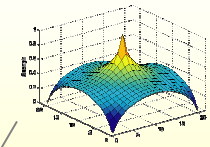
- Find a good balance between cost of information replication (storage size) and cost of information discovery (query time)
- Load balance
- Robustness
- Information brokerage is intimately coupled with
  - how network nodes are named
    - do we have coordinates?
  - how routing is done in the network

Distance-Sensitive Information Brokerage:
if producer and consumer are at a distance d, the query cost should be O(d)

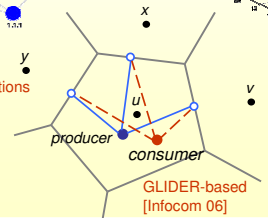
Approaches to Efficient Information Brokerage



Hierarchical Decompositions of Graphs



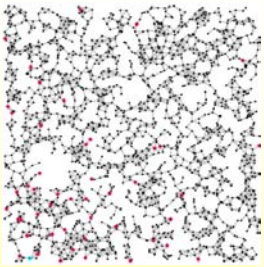
Information Gradients



GLIDER-based [Infocom 06]

Information Diffusion

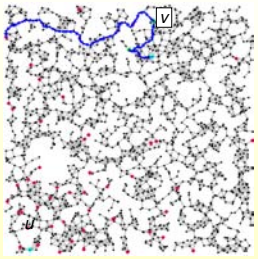
- Hash function: Generates a random valid address in a given cluster for any information type
  $\mu: \Sigma \times HD \rightarrow S$
- A producer hashes its information to all of its neighboring clusters
  - O(log n) hashes
  - Total path length to all hashes is O(D), where D is the diameter of the sensor field



A **producer** hashes its information to many nearby nodes and to few far away nodes.

Information Retrieval

- Consumer *v* looking for a particular information examines hash locations of that information in larger and larger clusters containing *v*
- Thm: The length of retrieval path from *v* is at most $4 \cdot d_{uv}$ where *u* is the producer (unknown to *v*)



Brokerage Costs

Size	# Info. servers		Query time	
	avg	std	avg	std
200	9.95	0.21	1.08	0.66
400	15.9	0.26	0.89	0.67
600	25.4	1.02	0.77	0.57
1000	31.5	4.00	0.83	0.57
2000	47.0	7.47	0.73	0.47
4000	61.2	11.3	0.73	0.42
6000	69.5	13.6	0.79	0.46
8000	79.0	16.5	0.77	0.39
10000	84.3	15.6	0.76	0.39

Storage cost grows slowly
Cost of query is distance sensitive

$$\text{Query time} = \frac{\text{Path length from consumer to hash location}}{\text{Shortest path length to producer}}$$

HD Brokerage Summary

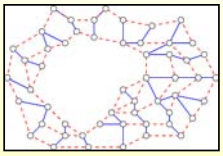
- HD effectively discovers the intrinsic geometry of the network
- Provides a hierarchy-based scheme with provable approximation quality on the routing paths
- Node/link failures affect mostly the low levels of the hierarchy
- Enables distance sensitive information brokerage

Resource Discovery Using Local Double Rulings

Associate with each node two connected `1-d' structures, call them roads – the red and blue

- All red roads together cover the network in a load-balanced fashion
- All blue roads together cover the network in a load-balanced fashion
- For any pair of nodes A and B, the red road from A has to intersect the blue road from B

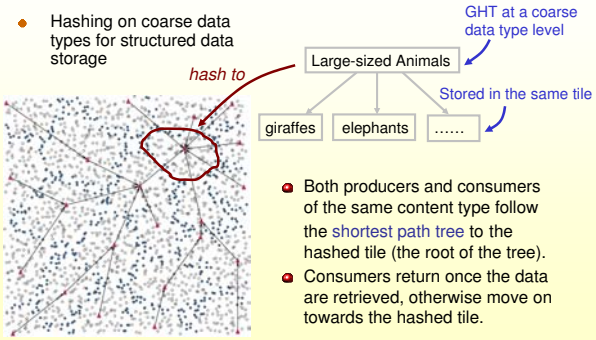
A double ruling derived via a Morse function ≡ distance to boundary



Information providers and seekers can meet by following blue and red roads respectively

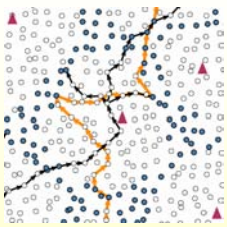
GLIDE-based Brokerage: At the CDT Level – Do Content-Based GHT

- Hashing on coarse data types for structured data storage



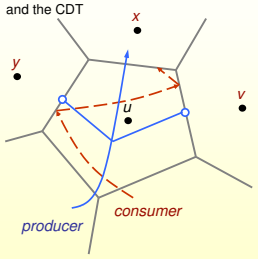
- Both producers and consumers of the same content type follow the shortest path tree to the hashed tile (the root of the tree).
- Consumers return once the data are retrieved, otherwise move on towards the hashed tile.

Within Each Tile – Double-Ruling Scheme for Transit Tiles



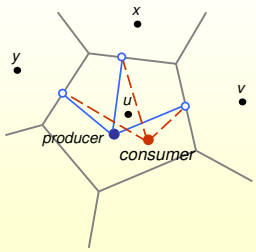
An example by simulation

Guides *v, x, y* are landmarks selected according to a set of rules based on hashing and the CDT



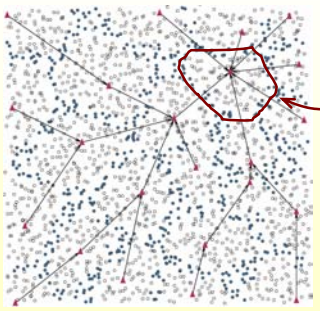
- Routes formed by following shortest paths to guides
- The two sets of curves always meet

Double-Ruling Scheme in Hashed Tile



- Producers and consumers are guaranteed to meet by following the two sets of curves.
- The consumers may not need to reach the hashed tile to fetch the data as the data are available at some transit tiles.

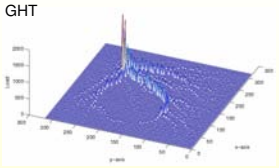
Reducing Producer Cost – *En Route* Data Aggregation



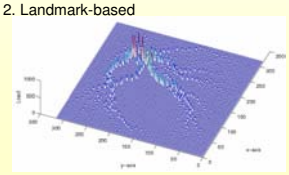
- Producers of the same content type share the shortest path tree (on CDT) rooted at the hashed tile.
- Data of the same type can be aggregated
  - Inside the tile if two producers share one
  - Inside the tile of their common ancestors

Locality Awareness Comparison with GHT by Simulations – Transmission Cost by Individual Node

1. GHT



2. Landmark-based



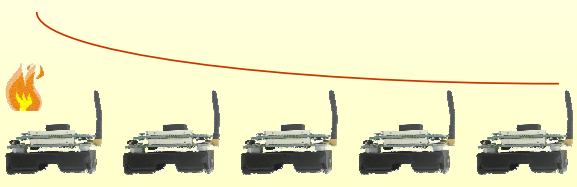
- Scenario: one producer; all nodes query for the producer data; one big hole in the network connectivity graph.
- Note the y-scale in figure 1 is twice of that in figure 2.
- The total load is much lower than using GHT.
- The load is also more balanced than using GHT.

GLIDER Brokerage Summary

- Distance-sensitive information brokerage is possible with very modest data replication
- Information discovery is closely coupled with the network node naming and routing
- In some ways, geometric methods and tools can be effectively used even when the connectivity graph is all we got

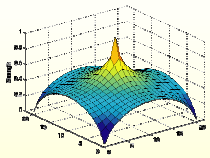
Information Potentials

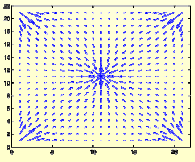
- Natural phenomena typically generate continuous fields (temperature, pressure ...)
- But it can be advantageous to also invent artificial potentials that diffuse information about event detections



Information Diffusion

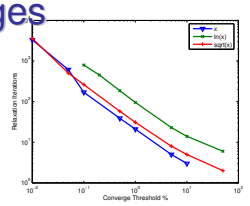
- Information sources can diffuse a quantity that we can think of as information strength via Laplace's equation (Dirichlet boundary c.)
- $\nabla^2 \Phi(x) = 0$
- $\Phi(u) = \frac{1}{d(u)} \Sigma_{v \in N(u)} \Phi(v)$
- Information seekers can ascend the gradient of this potential to find a source
- A harmonic function Φ has no local maxima or minima – its gradient can guide a packet, or a vehicle, to its maximum
- Usually smooth Φ by computing a square root, or logarithm

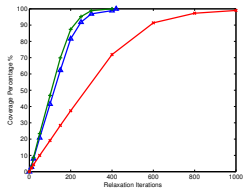




Diffusion Challenges

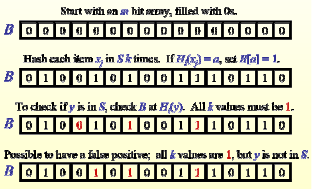
- Diffusion can be slow to converge
- What if there are multiple sources with the same type of information?
- What if there are many different types of sources?
- What about discretization effects?





Dealing with Many Potential Sources: Bloom Filters for Membership Testing

- Given a set $S = \{x_1, x_2, x_3, \ldots x_n\}$ on a universe U, want to answer queries of the form: Is $y \in S$?
- Example: a set of detection attributes
- Bloom filter provides an answer in
  - "Constant" time (time to hash).
  - Small amount of space.
  - But with some probability of being wrong.



Dealing with Many Potential Sources: Network Coding to Save Storage

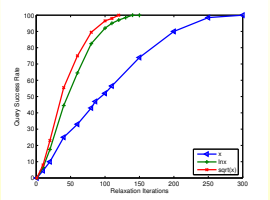
- Each node can compute a random linear combination of all the potentials it hears

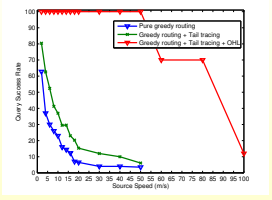
$$\sum_i \lambda_i \Phi_i$$



- If there are L active potential sources, then a neighborhood of size k around a node provides $\Omega(k^2)$ equations relating the local potential values
- But in a neighborhood of size k, the $O(k)$ boundary values determine all the interior values for each potential (harmonic function property)
- So we have enough equations to recover the unknown potentials if $k > L$ (k^2 constraints vs. kL unknowns)

Diffusion Brokerage Performance





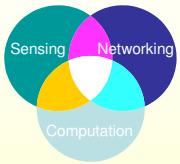
Information Diffusion Summary

- Diffused information potentials can guide both virtual and physical information seekers to the appropriate sources
- Multiple sources can be handled by having their potentials co-mingled and then decoded as necessary
- Sources may move and the potentials adapt in a smooth manner

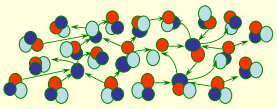
Conclusions

- Structure discovery and information brokerage are fundamental problems for WSNs
- With light preprocessing we can extract certain global quantities that can significantly help with local decisions
- These quantities reflect an understanding of the geometry or topology of the sensor filed and do not require localization
- The same quantities are also robust to local volatility in the network connectivity
- Such approaches integrate very well with current `narrow waist' sensor net protocols, such as SP (Berkeley)

Lightweight Spatio-Temporal Reasoning in Sensor Networks



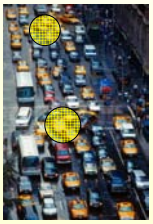
Leonidas Guibas
Computer Science Dept.
Stanford University



More Demanding Sensor Network Applications

- Beyond simple data collection and aggregation
  - dynamic, mobile foci of activity (tracking mobile objects)
  - Amidst clutter of irrelevant data
  - distributed attention: focus and context
  - acting on the world (closing the loop)
- Network must adapt to highly dynamic foci of activity
- Sensing is driven by user queries
- Sensing and communication tasks must be planned and allocated
- Resources must be apportioned between detection, tracking, etc.





Five Quick Vignettes on Lightweight Spatiotemporal Reasoning

1. Tracking Wide-Area Phenomena
2. Counting Moving Objects
3. Distributed Identity Management
4. Tracking Spatial Occupancy

Sensor selection

Sensor collaboration groups

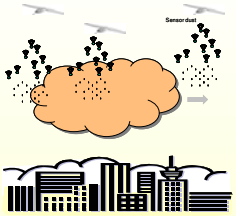
Network structure discovery

Lightweight information integration

Uncertainty and multiple hypotheses

V1. Large-Area Phenomena

- A chemical plume blows over a city after a factory leak.
- Networked sensors are air-dropped to track its extent and motion.
- The sensors organize themselves as appropriate, in order to perform this task.



Tracking a Large Shadow

We track a half-plane shadow across a field with light sensors.

A projector is used to throw a moving shadow onto a wall.

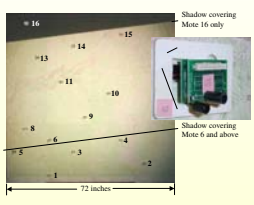
Sensor nodes are Berkeley/Cossbow motes with a radio and a light detector



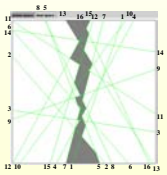
shadow

[Liu, Cheung, G., Zhao, WSNA '02]

Using Geometric Duality Points ↔ Lines

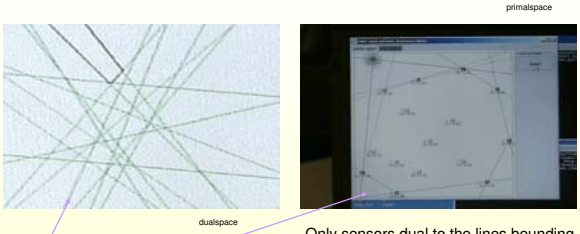


In a dual configuration space, the sensors become lines and the edge of the shadow a moving point, crossing cells in the arrangement of the lines.



Shaded cells indicate the trajectory of the shadow edge.

Selective Sensor Activation



Dual view

Primal view

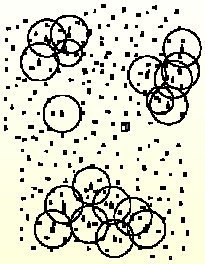
Only sensors dual to the lines bounding the current cell can be crossed next.

Thus, of all the sensors in the field, only four on the average need be active at once.

Some Lessons and Issues

- An appropriately chosen *configuration space* can transform a wide-area phenomenon into a localized one.
- Only a small fraction of the nodes in the field need be active at any one time.
- Most message traffic is along the shadow boundary: *the physical phenomenon dictates the communication paths*.

V2. Target Counting



[Fang, Zhao, G., MobiHoc'03]

Problem Spec:

- A sensor network with multiple targets present. Targets can be stationary or moving;
- Each sensor can detect the local superimposed amplitude of target signals (e.g., acoustic) at any instant of time;

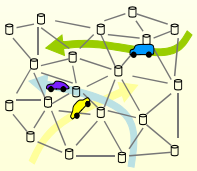
Objective:

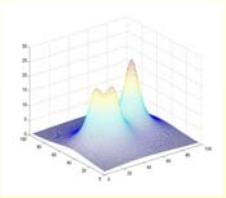
To determine the number of targets and their approximate locations in the field, forming an initial count and re-computing the count when targets move, enter, or leave the field.

Acoustic Signal Field Landscape

Goal: count and track the significant signal peaks in the field

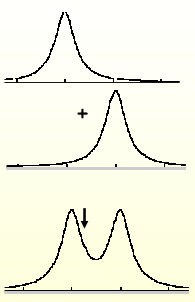
1. Signal attenuation rate, and the spacing and communication range of sensors have big impact on "signal resolution"
2. Number of detected peaks may not equal number of targets due to sampling artifacts and/or noise.

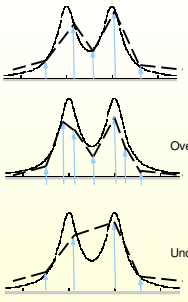




Combinatorial Signal Processing and Computational Topology

Scattered Amplitude Sampling

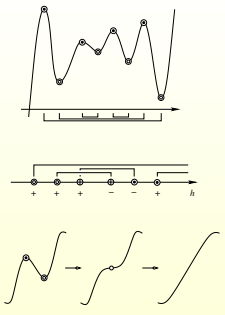




In 1-D, the number of peaks in sampled landscape cannot exceed the number of peaks in the true landscape. However, this is possible in 2-D.

Peak Landscape Simplification

- Some signal peaks may be noise
- Usually such peaks are near other critical points of the landscape
- Topological ideas, such as persistent homology can be used to simplify the landscape by canceling saddles with maxima, etc., removing noise

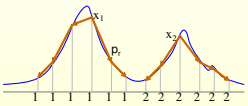


Downhill Flooding Protocol (DFP)

A sensor node is qualified as a **leader**, if its reading is higher than that of all its one hop neighbors.

Local *leader election* is conducted by sensors exchanging information with their neighbors via one hop broadcast.

p_r = received signal power at each node

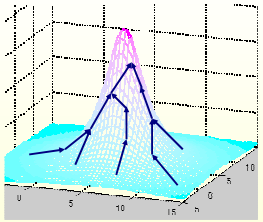


x_1 and x_2 are elected leaders, other nodes join one of the groups formed by the leaders: each node joins the highest leader it can reach by a monotone ascending path

1. Only sensors with myPr > threshhold will participate
2. Each sensor emits a packet in each protocol period, broadcasting its reading Pr and its ID
3. Sensors pass on or drop a packet P from their neighbors, according to the following rule:

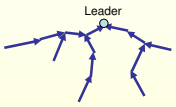
```
If (Pr recorded in the packet > myPr &
      Pr of the sensor relaying this
      packet > myPr)
   broadcast(P);
else
   drop(P);
```

Sensor Cluster Trees



For each node,

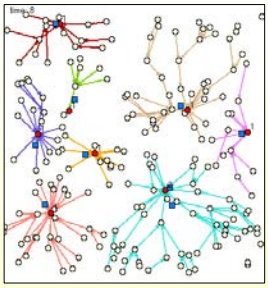
parent = the neighboring node with maximum Pr (received signal power)



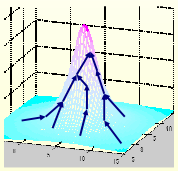
Bird's eye view of the cluster tree structure. Each node follows a strictly upwards path to the highest peak it can reach.

We call such groups of sensors aggregates, as they collaboratively perform a task.

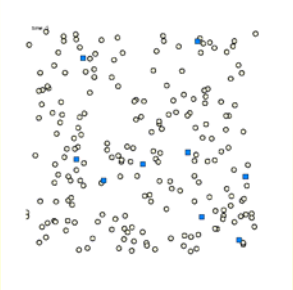
2-D View of a Sensor Field with Cluster Trees Formed Using DFP

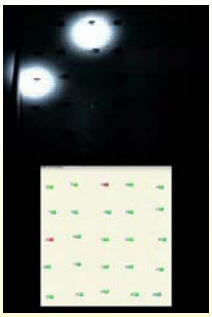


- Different colors mark different sensor clusters formed
- Each cluster has one leader



Target Counting Demo





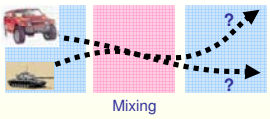
Simulation with 9 moving targets (above); Implementation on motes sensors (right)

jliebman

Some Lessons and Issues

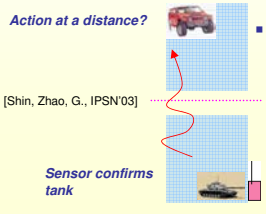
- Sensors naturally form *collaboration groups*. Target localization and counting can be performed in-network.
- These sensor collaboration groups must be maintained as the physical phenomena of interest change over time.
- Aggregates may be easier to sense than individual objects
- Equivalently, physical phenomena are translated into networking behaviors.
- Can such behaviors be programmed without naming the nodes individually?

V3. Distributed Identity Management



Mixing

- Multi-target Tracking (MTT)
  - Basic application of sensor networks
  - Data association problem → *Target mixing*

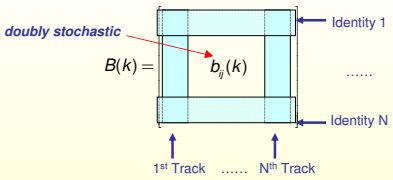


- Multi-target Identity Management
  - Represent and manage additional quantity called target identity
  - Simplified version
    - Position estimates are given
    - Fixed number of targets assumed

Approach A: Belief Matrix

The belief matrix $B(k)$ is the main quantity that the algorithm maintains

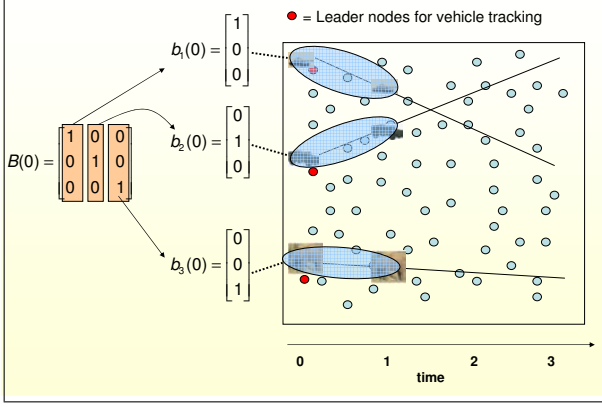
→ Which ID goes with which track, with what probability?



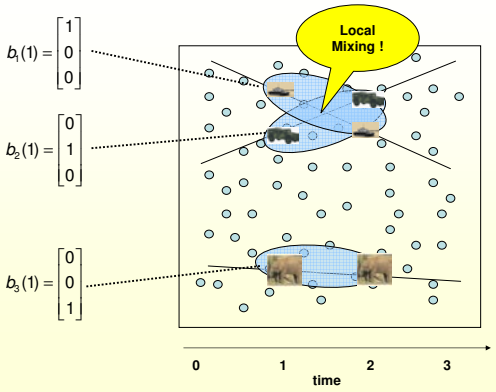
where $b_{ij}(k) = p(\mathrm{ID}(x_j(k)) = i)$ and $\vec{b}_i(k)$ is ID belief vector on i_{th} track.

Q: How to update $B(k)$, given $X(k+1)$?

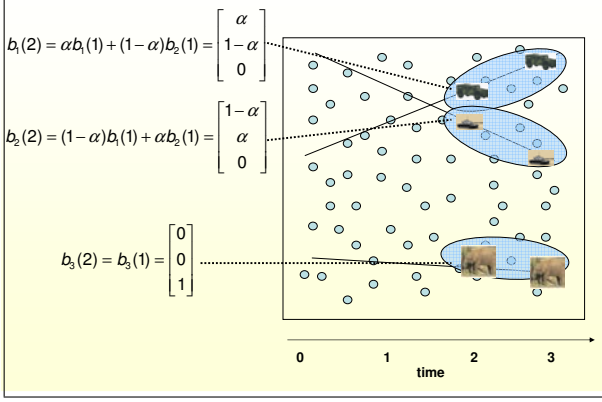
Distributed Management of B(k), I



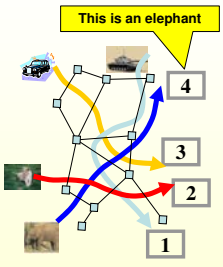
Distributed Management of B(k), II



Distributed Management of B(k), III



Incorporating Local Evidence



$$B = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0.1737 & 0.0947 & 0.3447 & 0.3869 \\ 0.3527 & 0.6473 & 0 & 0 \\ 0.3201 & 0.1744 & 0.3043 & 0.2011 \\ 0.1535 & 0.0836 & 0.3509 & 0.4120 \end{bmatrix}$$

$$B = \begin{bmatrix} 0.1737 & 0.0947 & 0.3447 & 0 \\ 0.3527 & 0.6473 & 0 & 0 \\ 0.3201 & 0.1744 & 0.3043 & 0 \\ 0.1535 & 0.0836 & 0.3509 & 1 \end{bmatrix}$$

Not doubly-stochastic → inconsistent!

Renormalization, Given Local Evidence

1. Ideal solution: Bayesian normalization,
   given the priors, all the mixing events in history
   and all the sensor evidence.
   Exact solution in this framework. (Bayesian posterior)
   Used as a reference - Desirable properties of the solution.

2. Realistic solution: Sinkhorn Iteration (repeatedly normalize rows and columns)
   [Sinkhorn 1964,1967; Sinkhorn and Knopp 1967]

What Do We Want?

- The belief matrix represents a probability distribution. The matrix *A* represents our *a priori* belief, but violates sum constraints.
- We would like to find the sum-constrained (feasible) matrix *B* that is the *closest distribution* to *A* (which is infeasible).
- Use Kullback-Leibler distance (measure of distance between distributions):

$$KL(B:A) = \sum_{j=1}^{n} \sum_{i=1}^{m} b_{ij} \log \frac{b_{ij}}{a_{ij}}$$

Sinkhorn Scaling and the Kullback-Leibler Distance

$$KL(B:A) = \sum_{j=1}^{n} \sum_{i=1}^{m} b_{ij} \log \frac{b_{ij}}{a_{ij}}$$

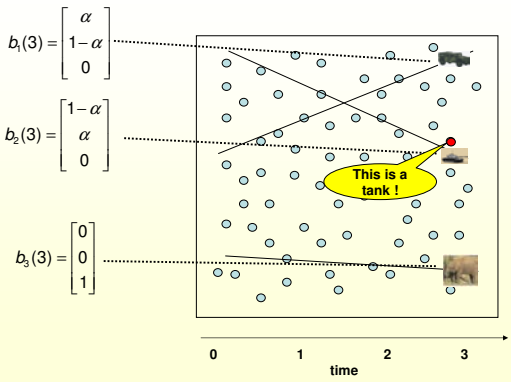
Theorem: Given a prior matrix $A \in \mathbb{R}^{m \times n}$, the matrix *B* that satisfies the row and column sum constraints, and minimizes the KL-distance from the prior matrix *A* is **always** the solution of the Sinkhorn scaling process.

[Balakrishnan, Hwang,Tomlin '04]

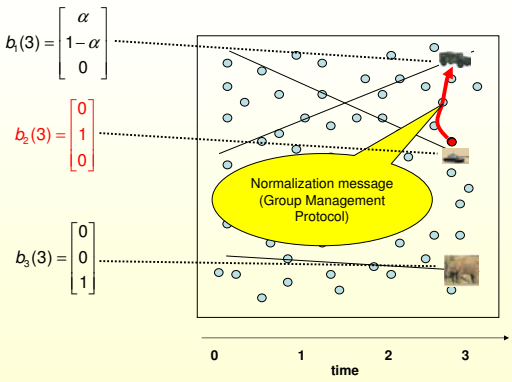
Solve by interior point methods:

$$\begin{aligned} \text{minimize} \quad & \textstyle\sum_{i=1}^{m} \sum_{j=1}^{n} b_{ij} \log \frac{b_{ij}}{a_{ij}} \\ \text{subject to} \quad & \textstyle\sum_{j=1}^{n} b_{ij} = r_i \; \forall i = 1 \cdots m \\ & \textstyle\sum_{i=1}^{m} b_{ij} = c_j \; \forall j = 1 \cdots n \\ & b_{ij} \geq 0 \; \forall i = 1 \cdots m; \; j = 1 \cdots n \end{aligned}$$

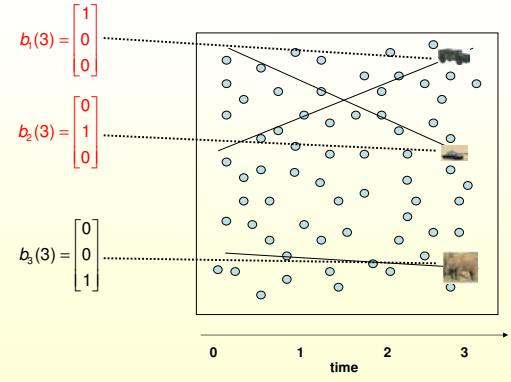
Distributed Management of B(k), IV



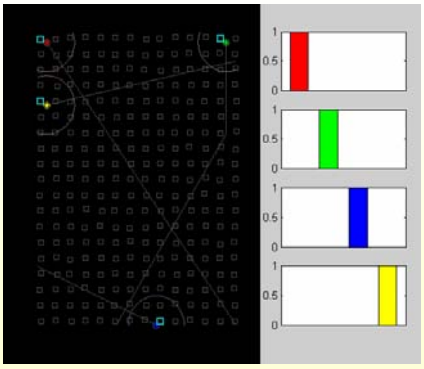
Distributed Management of B(k), V



Distributed Management of B(k), VI



Target Mixing Video



Particles filters are used to keep track about multiple hypotheses about the location of each vehicle

Distributed Implementation of Tracking and Normalization

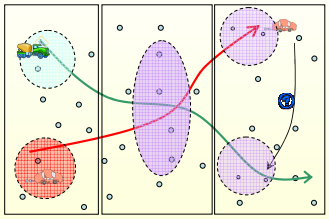
Q: Which nodes store and/or compute what information?

-- When do we track in joint space?

-- How to distribute B(k)?

-- How to implement the probabilistic normalization?

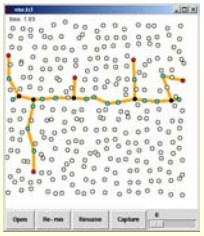
-- What is required at the communication/network layer to make the above happen?



ST marginal MT joint ST marginal

Managing Sensor Groups

- We have distributed columns of B(k) to leader nodes tracking targets.
- When a leader initiates a normalization based on local evidence, it has to know where are the other leaders that have non-zero mass on the evidence ID.
- Group Management Protocol: Maintains the group membership based on the ID probability mass.
- Communication needs to be minimized.



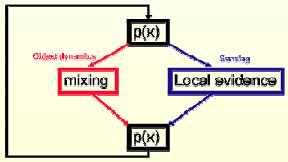
RoamHBA protocol
[Fang, Liu, G., Zhao, IPSN'04]

Approach B: Information Matrix

- Keep unnormalized beliefs by simply adding log-likelihoods after each local evidence event
- No communication necessary, except when mixing events occur or queries are made

$$L = \begin{bmatrix} l_{11} & \cdots & l_{1j} & \cdots & l_{1N} \\ l_{21} & \cdots & l_{2j} & \cdots & l_{2N} \\ & & \vdots & & \\ l_{N1} & \cdots & l_{Nj} & \cdots & l_{NN} \end{bmatrix}$$

$$l_{ij} = \sum_t \log(p(Z^t = (k,j) | x_j = i), k \in \{1, \cdots, N\}$$



[Shin, Lee, Thrun, G. '05 and Schumitch, Thrun, Bradski, Olukotun '05]

Some Lessons and Issues

- Collaboration groups need not always be physically clustered.
- Different attributes of a phenomenon can be tracked at different rates (target location, identity).
- A change of information representation can have a deep impact on cost trade-offs.
- How do information providers and information seekers locate each other?

V4. Image Sensor Networks

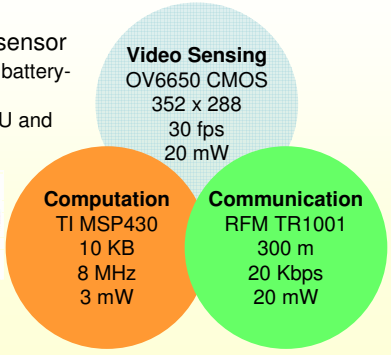
- CMOS technology enables the production of small, low-cost and low-power integrated image sensors
- Cameras (still or video) and other image sensors are becoming cheaper, smaller, and nearly ubiquitous
- However, truly distributed networked systems of image sensors are still not here



Wireless Camera Node

- CMOS image sensor
  - Small, cheap, battery-powered
  - Integrated CPU and radio



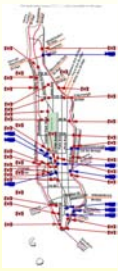


Current Multi-Imager Networks

- Data is transported over a wired network to a central location
- Human operators look at the data

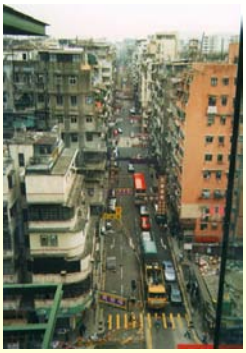


- This approach cannot scale:
  - vast amounts of data to move
  - wiring is expensive
  - automatic ways to filter the data are needed



Distributed Imager Challenges

- Imagers are high data rate sensors; therefore data must be compressed and summarized
  - compression must take into account shared data
  - goal of compression need not be reconstruction
- Vision algorithms can be expensive to run on weak capability, low power devices
- Visibility is non-local and discontinuous (occlusions, etc)
- Issues of privacy, etc.



Collaborative, Task-Driven Image Sensing

- Large numbers of simple, inexpensive cameras collaborate over a wireless network to accomplish a task
- Data is compressed locally and aggregated within the network
- Cameras are only tasked as the situation demands
- The system can be expanded incrementally to large numbers of nodes



The goal is to estimate certain high-level, global attributes of the environment.

The Initial Effort

- Use a camera network to obtain information about space occupancy by people.
- Useful for aggregate tracking, counting, etc.
- Crowd density implies multiple occlusions – no one camera by itself can do this.
- No image reconstruction --just high-level distributed spatial reasoning.



Packard 013

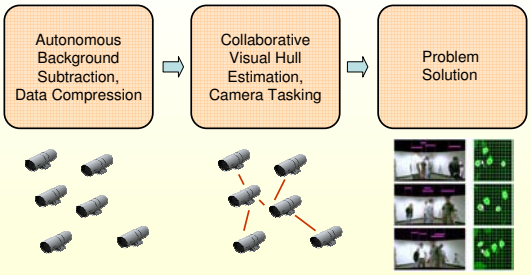


The Experimental Setup

- Web cameras:
  - 16 firewire webcams with 49 degree FOV
  - Placed around a 22 x 19 foot room
- Linux computers
  - A PC is connected to 2 webcams
  - A separate process is running for each webcam to simulate an individual camera node
  - All processes can communicate with each other over the network

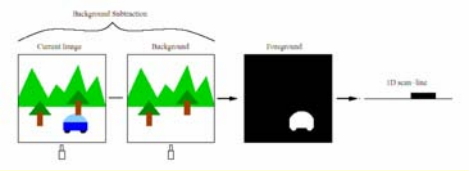


System Architecture

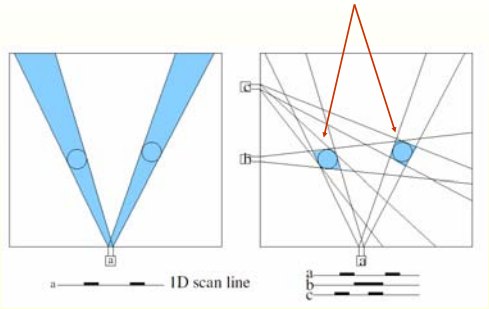


Local Processing

- Perform background subtraction
- Collapse to a single scan-line
- 640x480 RGB image → 640 bit scan-line (which can be further compressed)

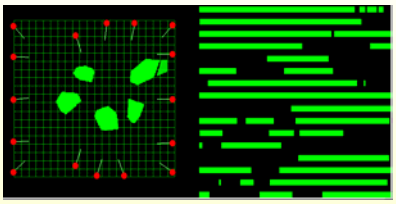


Occupancy Representation: The 2-D Visual Hull



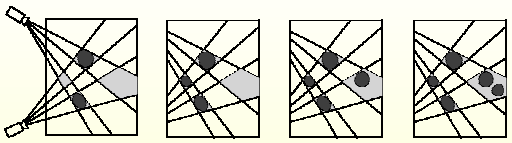
A Visual Hull Example

Top view of room with 5 people



Scanlines from 16 cameras

The Visual Hull Overestimates Occupancy

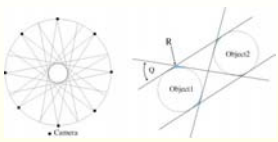


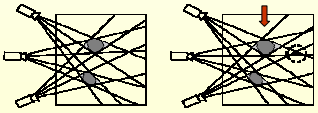
Visual hull regions surround each object.

Visual hull regions may also be empty; we call these the phantom regions

Pruning the Visual Hull

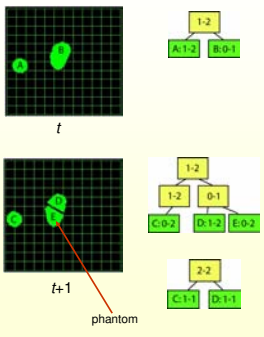
- Using more cameras reduces the overestimation – but it can never be fully eliminated
- Motion can allow the pruning of phantom regions



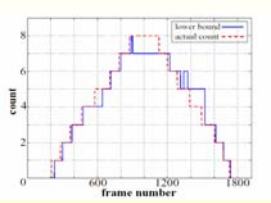


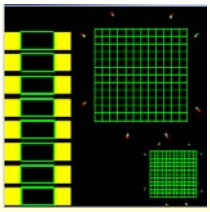
An Application: Counting People

- Given occupancy, bound the number of objects in each polygon of the visual hull
- The bounds over time can be used to constrain the count, using a tree data structure.



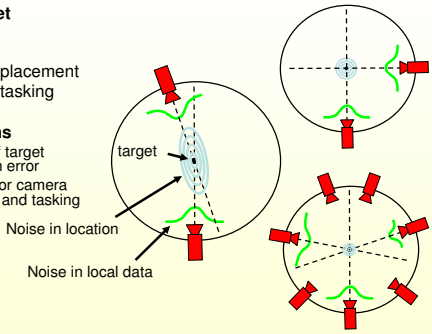
A Counting Example





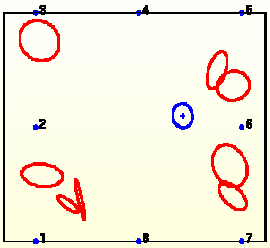
Localization – Where?

- Global: **Target localization**
- Best camera placement
- Best camera tasking
- **Contributions**
  - Analysis of target localization error
  - Solutions for camera placement and tasking

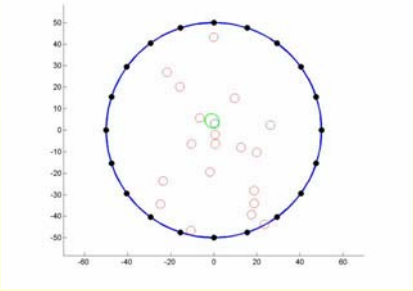


Localization w. Occlusions

- Suppose *M* moving objects in a room
- Given priors on these objects
- And camera positions
- We are interested in localizing one of them (blue prior)
- Which *k* cameras are best for localization?



Algorithm Animation



Scaling to Large Camera Networks

- Few foci of activity
- Episodic events of interest
- Camera control (aiming, panning, zooming)
- Camera selection (how many, which ones)

•Analysis
•Simulation
•Real Experiments



Some Lessons and Issues

- A surprising amount of spatial information can be captured by cameras sharing very few bits.
- Small subsets of cameras, when appropriately tasked, can provide accurate estimates.
- The system can perform counting without tracking, thus raising no privacy issues.
- Alternatively, low-res video cameras for occupancy can be combined with a few high-res still cameras that can be commanded to snap a few high-detail photos, capturing the essentials of a scene.

Five Quick Vignettes on Lightweight Spatiotemporal Reasoning

1. Tracking Wide-Area Phenomena
2. Counting Moving Objects
3. Distributed Identity Management
4. Tracking Spatial Occupancy

Sensor selection

Sensor collaboration groups

Network structure discovery

Lightweight information integration

Uncertainty and multiple hypotheses

Conclusions

- Ubiquitous networked sensors provide a dense spatial and temporal sampling of the physical world
- They allow low-latency access to information that is highly localized in time and space, and thus provide a way to sense and act on the physical world beyond what has been possible up to now
- Sensor networks raise many research issues at the physical node level, the system architecture level, and the algorithm deployment level
- A combination of global and local methods promise to provide robust tools for network structure discovery, understanding the global aspects of sensor layouts and signal landscapes

Acknowledgements

Stanford Students: Qing Fang, Jie Gao, Ali Ozer Ercan, Jaewon Shin, Feng Xie, Danny Yang

Stanford Postdocs: Vin de Silva

External Collaborators: Patrick Cheung, Julia Liu (PARC), Jie Liu, Feng Zhao (Microsoft), Hector Gonzales-Banos (Honda), Li Zhang (HP Labs), John Hershberger (Mentor Graphics)

Funding Sponsors: NSF, DARPA, ONR, Stanford NRC, Honda, Xerox

The End

Another kind of sensor network exhibiting lightweight spatiotemporal reasoning



Games in Networks:
Routing, Network Design, Potential Games, and Equilibria and Inefficiency

Éva Tardos
Cornell University

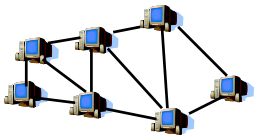
Part I

- what is a game?
- Pure and randomized equilibria
- Load balancing and routing as games

Why care about Games?

Users with a multitude of diverse economic interests sharing a Network (Internet)
- browsers
- routers
- servers

Selfishness:
Parties deviate from their protocol if it is in their interest



Model Resulting Issues as

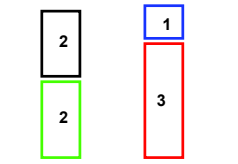
Games on Networks

A simple game: load balancing

Each job wants to be on a lightly loaded machine.

With coordination we can arrange them to minimize load

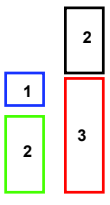
Example: load of 4



A simple game: load balancing

Each job wants to be on a lightly loaded machine.

- Without coordination?
- Stable arrangement:
No job has incentive to switch
- Example: some have load of 5



Games: setup

- A set of players (in example: jobs)
- for each player, a set of strategies
(which machine to choose)

Game: each player picks a strategy

For each strategy profile (a strategy for each player) → a payoff to each player
(load on selected machine)

Nash Equilibrium: stable strategy profile:
where no player can improve payoff by changing strategy

Games: setup

Deterministic (pure) or randomized (mixed) strategies?

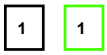
Pure: each player selects a strategy.
simple, natural, but stable solution may not exists

Mixed: each player chooses a probability distribution of strategies.
- equilibrium exists (Nash),
- but pure strategies often make more sense

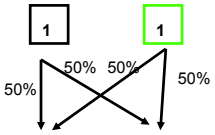
7

Pure versus Mixed strategies in load balancing

- Pure strategy: load of 1



- A mixed equilibrium
  Expected load of 3/2 for both jobs



Machine 1 Machine 2

8

Quality of Outcome: Goal's of the Game

Personal objective for player i:
min load L_i or expected load $E(L_i)$

Overall objective?

- **Social Welfare:** $\sum_i L_i$ or expected value $E(\sum_i L_i)$
- Makespan: $\max_i L_i$ or max expected value $\max_i E(L_i)$ or expected makespan $E(\max_i L_i)$

9

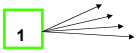
Example: simple load balancing

n identical jobs and n machines



All pure equilibria: load of 1 (also optimum)

A mixed equilibrium: prob 1/n each machine



expected load: $E(L_i) = 1+(n-1)\frac{1}{n} < 2$ for each i

$E(\max_i L_i)$: balls and bins: log n/log log n

10

Results on load balancing:

Theorem for $E(\max_i L_i)$:
- w/uniform speeds, p.o.a ≤ log m/log log m
- w/general speeds, worst-case p.o.a. is Θ (log m/log log log m)

11

Results on load balancing:

Theorem for $E(\max_i L_i)$:
- w/uniform speeds, p.o.a ≤ log m/log log m
- w/general speeds, worst-case p.o.a. is Θ (log m/log log log m)

Proof idea: balls and bins is worst case??

Requence of results by
[Koutsoupias/Papadimitriou 99],
[Mavronicolas/Spirakis 01],
[Koutsoupias/Mavronicolas/Spirakis 02],
[Czumaj/Vöcking 02]

12

Today:

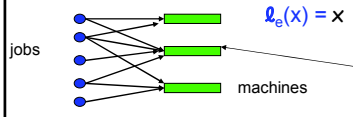
focus on pure equilibria

Does a pure equilibria exists?
Does a high quality equilibria exists?
Are all equilibria high quality?

some of the results extend to sum/max of $E(L_i)$

load balancing and routing

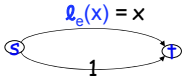
Load balancing:



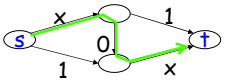
Delay as a function of load:

x unit of load → causes delay $\ell_e(x)$

Routing network:



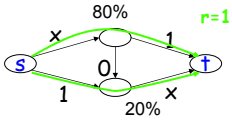
Allow more complex networks



Atomic vs. Non-atomic Game

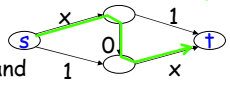
Non-atomic game:

- Users control an infinitesimally small amount of flow
- equilibrium: all flow path carrying flow are minimum total delay



Atomic Game:

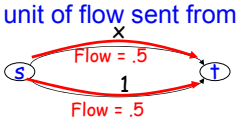
- Each user controls a unit of flow, and
- selects a single path or machine



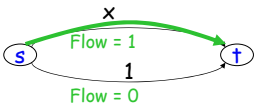
Both congestion games: cost on edge e depends on the congestion (number of users)

Example of nonatomic flow on two links

- One unit of flow sent from s to t



Traffic on lower edge is envious.



An envy free solution:

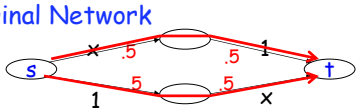
No-one is better off

Infinite number of players

- will make analysis cleaner by continuous math

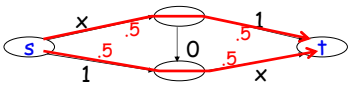
Braess's Paradox

Original Network



Cost of Nash flow = 1.5

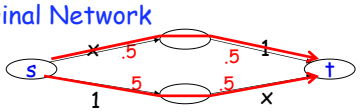
Added edge:



Effect?

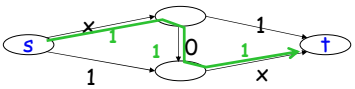
Braess's Paradox

Original Network



Cost of Nash flow = 1.5

Added edge:

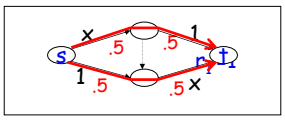


Cost of Nash flow = 2

All the flow has increased delay!

Model of Routing Game

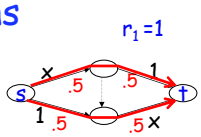
- A directed graph $G = (V,E)$
- source-sink pairs s_i, t_i for $i=1,..,k$
- rate $r_i \geq 0$ of traffic between s_i and t_i for each $i=1,..,k$



- Load-balancing jobs wanted min load
- Here want minimum delay:
  delay adds along path
  edge-delay is a function $\ell_e(\cdot)$ of the load on the edge e

Delay Functions

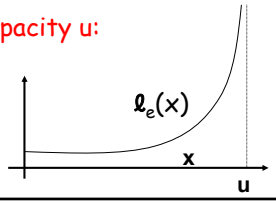
Assume $\ell_e(x)$ continuous and monotone increasing in load x on edge



No capacity of edges for now

Example to model capacity u:

$\ell_e(x) = a/(u-x)$



Goal's of the Game

Personal objective: minimize

$\ell_P(\mathbf{f})$ = sum of latencies of edges along P (wrt. flow **f**)

No need for mixed strategies

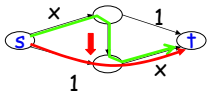
Overall objective:

C(f) = total latency of a flow **f**: $= \Sigma_P f_P \cdot \ell_P(\mathbf{f})$

=social welfare

Routing Game??

Flow represents
- cars on highways
- packets on the Internet



individual packets or small → continuous model

User goal: Find a path selfishly minimizing user delay

≈ true for cars,
packets?: users do not choose paths on the Internet: routers do!

With delay as primary metric → router protocols choose shortest path!

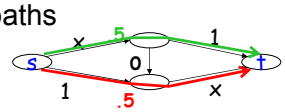
Connecting Nash and Opt

- Min-latency flow
  - for one s-t pair for simplicity
- minimize $C(f) = \Sigma_e f_e \cdot \ell_e(f_e)$
- subject to: f is an s-t flow
- carrying r units
- By summing over edges rather than paths where f_e = amount of flow on edge e

Characterizing the Optimal Flow

- Optimality condition: all flow travels along minimum-gradient paths

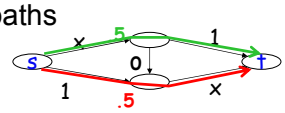
gradient is:
$(x\,\ell(x))'$
$= \ell(x) + x\,\ell'(x)$



Characterizing the Optimal Flow

- Optimality condition: all flow travels along minimum-gradient paths

gradient is:
$(x\,\ell(x))'$
$= \ell(x)+x\,\ell'(x)$



Recall: flow f is at Nash equilibrium iff all flow travels along minimum-latency paths

Nash ↔ Min-Cost

Corolary 1: min cost is "Nash" with delay
$\ell(x)+x\,\ell'(x)$

Corollary 2: Nash is "min cost" with cost
$\Phi(f) = \Sigma_e \int_0^{f_e} \ell_e(x)\,dx$

Why?
gradient of:
$(\int_0^{f_e} \ell_e(x)\,dx)' = \ell(x)$

Using function Φ

- Nash is the solution minimizing Φ

Theorem (Beckmann'56)

- In a network latency functions $\ell_e(x)$ that are monotone increasing and continuous,
- a deterministic Nash equilibrium exists, and is essentially unique

Using function Φ (con't)

- Nash is the solution minimizing value of Φ
- Hence,

$\Phi(\text{Nash}) \le \Phi(\text{OPT})$.

Suppose that we also know for any solution
$\Phi \le \text{cost} \le A\ \Phi$

→ $\text{cost(Nash)} \le A\ \Phi(\text{Nash}) \le A\ \Phi(\text{OPT}) \le A\ \text{cost(OPT)}$.
→ There exists a good Nash!

Example: $\Phi \le \text{cost} \le A\ \Phi$

Example: $\ell_e(x) = x$ then
- total delay is $x \cdot \ell_e(x) = x^2$
- potential is $\int \ell_e(\xi)\,d\xi = x^2/2$

More generally: linear delay $\ell_e(x) = a_e x + b_e$
- delay on edge $x \cdot \ell_e(x) = a_e x^2 + b_e x$
- potential on edge: $\int \ell_e(\xi)\,d\xi = a_e x^2/2 + b_e x$
- ratio at most 2

Degree d polynomials:
- ratio at most d+1

Sharper results for non-atomic games

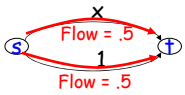
Theorem 1 (Roughgarden-Tardos'00)

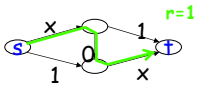
- In a network with linear latency functions
  - i.e., of the form $\ell_e(x) = a_e x + b_e$
- the cost of a Nash flow is at most 4/3 times that of the minimum-latency flow

Sharper results for non-atomic games

Theorem 1 (Roughgarden-Tardos'00)

- In a network with linear latency functions – i.e., of the form $\ell_e(x)=a_e x+b_e$
- the cost of a Nash flow is at most 4/3 times that of the minimum-latency flow

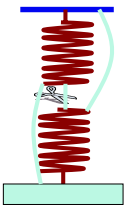




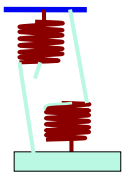
Nash cost 1 optimum 3/4

Nash cost 2 optimum 1.5

Braess paradox in springs (aside)



Cutting middle string



makes the weight rise

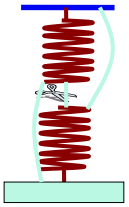
and decreases power flow along springs

Flow=power; delay=distance

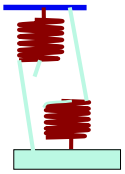
Bounds for spring paradox

Theorem 1' (Roughgarden-Tardos'00)

In a network with springs and strings cutting some strings can increase the height by at most a factor of 4/3.

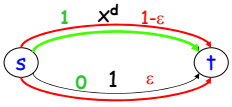


Cutting middle string



General Latency Functions

- Question: what about more general edge latency functions?
- Bad Example: (r = 1, d large)

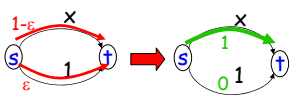


A Nash flow can cost arbitrarily more than the optimal (min-cost) flow

Sharper results for non-atomic games

Theorem 2 (Roughgarden'02):

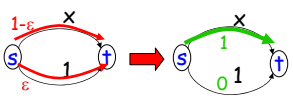
- In any network with any class of convex continuous latency functions
- the worst price of anarchy is always on two edge network



Sharper results for non-atomic games

Theorem 2 (Roughgarden'02):

- In any network with any class of convex continuous latency functions
- the worst price of anarchy is always on two edge network

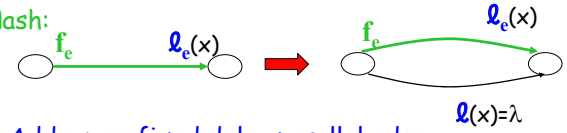


Corollary:
price of anarchy for degree d polynomials is $O(d/\log d)$.

Another Proof idea

Modify the network

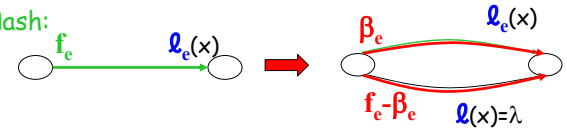
Nash:



- Add a new fixed delay parallel edge
  - fixed cost set $\lambda = \ell_e(f_e)$
- Nash not effected
- Optimum can only improve

Modified Network

Nash:



- fixed cost set $\lambda = \ell_e(f_e)$

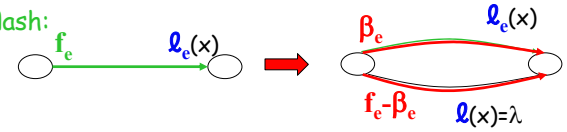
- Optimum on modified network

splits flow so that marginal costs are equalized

- and common marginal cost is $\lambda = \ell_e(f_e)$

Proof of better bound

Nash:



- Theorem 2: the worst price of anarchy is always two edge network

- Proof: Prize of anarchy on G is median of ratios for the edges

More results for non-atomic games

Theorem 3 (Roughgarden-Tardos'00):

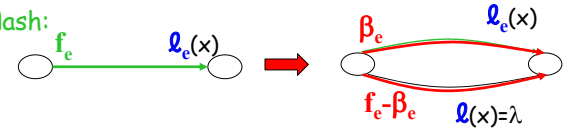
- In any network with continuous, nondecreasing latency functions

cost of Nash with rates r_i for all i	$\leq$	cost of opt with rates $2r_i$ for all i

Proof …

Proof of bicriteria bound

Nash:



common marginal cost on two edges in opt is $\lambda = \ell_e(f_e)$

- Proof: Opt may cost very little, but marginal cost is as high as latency in Nash
- → Augmenting to double rate costs at least as much as Nash

More results for non-atomic games

Theorem 3 (Roughgarden-Tardos'00):

- In any network with continuous, nondecreasing latency functions

cost of Nash with rates r_i for all i	$\leq$	cost of opt with rates $2r_i$ for all i

Morale for the Internet: build for double flow rate

Morale for IP versus ATM?

Corollary: with M/M/1 delay fns: $\ell(x)=1/(u-x)$, where u=capacity

Nash w/cap. $2u \le$ opt w/cap. u

Doubling capacity is more effective than optimized routing (IP versus ATM)

Part II

- Discrete potential games:
- network design
- price of anarchy stability

Continuous Potential Games

Continuous potential game: there is a function $\Phi(f)$ so that Nash equilibria are exactly the local minima of Φ

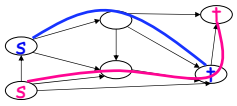
also known as Walrasian equilibrium Φ convex then Nash equilibrium are the minima. For example

$$\Phi(f) = \Sigma_e \int_0^{f_e} \ell_e(x)\,dx$$

Discrete Analog

Atomic Game

- Each user controls one unit of flow, and
- selects a single path



Theorem Change in potential is same as function change perceived by one user

[Rosenthal'73, Monderer Shapley'96,]

$\Phi(f) = \Sigma_e (\ell_e(1)+\ldots+\ell_e(f_e)) = \Sigma_e \Phi_e$

Even though moving player ignores all other users

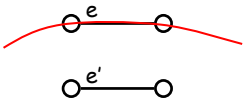
Potential: Tracking Happiness

Theorem Change in potential is same as function change perceived by one user

[Rosenthal'73, Monderer Shapley'96,]

$\Phi(f) = \Sigma_e (\ell_e(1)+\ldots+\ell_e(f_e)) = \Sigma_e \Phi_e$

Reason?



Potential before move:

$\ell_e(1)+\ldots \ell_e(f_e-1) + \ell_e(f_e)$

$+ \quad \ell_{e'}(1)+\ldots+\ell_{e'}(f_{e'})$

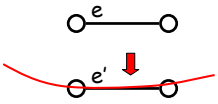
Potential: Tracking Happiness

Theorem Change in potential is same as function change perceived by one user

[Rosenthal'73, Monderer Shapley'96,]

$\Phi(f) = \Sigma_e (\ell_e(1)+\ldots+\ell_e(f_e)) = \Sigma_e \Phi_e$

Reason?



Potential after move:

$\ell_e(1)+\ldots \ell_e(f_e-1) + \ell_e(f_e)$

$+ \quad \ell_{e'}(1)+\ldots+\ell_{e'}(f_{e'}) + \ell_{e'}(f_{e'}+1)$

Change in Φ is $-\ell_e(f_e) + \ell_{e'}(f_{e'}+1)$

same as change for player

What are Potential Games

Discrete potential game: there is a function $\Phi(f)$ so that change in potential is same as function change perceived by one user

Theorem [Monderer Shapley'96] Discrete potential games if and only if congestion game (cost of using an element depends on the number of users).

Proof of "if" direction $\Phi(f) = \Sigma_e (\ell_e(1)+\ldots+\ell_e(f_e))$

Corollary: Nash equilibria are local min. of $\Phi(f)$

49

Why care about

Best Nash/Opt ratio?

Papadimitriou-Koutsoupias '99

Nash = outcome of selfish behavior

$\Rightarrow$worst Nash/Opt ratio: Price of Anarchy

Non-atomic game: Nash is unique...

Atomic Nash not unique!

50

Best Nash is good quality...

$$\text{Price of Stability} = \frac{\text{cost of best selfish outcome}}{\text{"socially optimum" cost}}$$

$$\text{Price of Anarchy} = \frac{\text{cost of worst selfish outcome}}{\text{"socially optimum" cost}}$$

Potential argument $\Rightarrow$ Low price of stability

But do we care?

51

Atomic Game: Routing with Delay

Theorems 1&2 true for the Nash minimizing the potential function, assuming all players carry the same amount of flow

Worst case on 2 edge network

52

Atomic Game: Price of Anarchy?

Theorem: Can be bounded for some classes of delay functions

e.g., polynomials of degree at most d at most exponential in d.

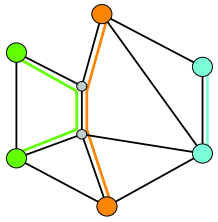
Suri-Toth-Zhou SPAA'04 + Awerbuch-Azar-Epstein STOC'05+ Christodoulou-Koutsoupias STOC'05

53

Network Design as Potential Game

Given: $G = (V,E)$,
costs $c_e(x)$ for all $e \in E$,
k terminal sets (colors)

Have a player for each color.



54

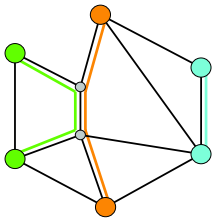
Network Design as Potential Game

Given: $G = (V,E)$,
costs $c_e(x)$ for all $e \in E$,
k terminal sets (colors)

Have a player for each color.

Each player wants to build a network in which his nodes are connected.

Player strategy: select a tree connecting his set.

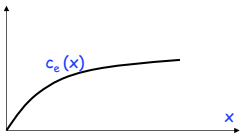


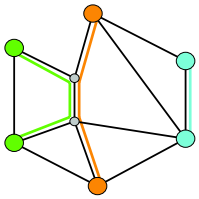
Costs in Connection Game

Players pay for their trees, want to minimize payments.

What is the cost of the edges?
$c_e(x)$ is cost of edge e for x users.

Assume economy of scale for costs:



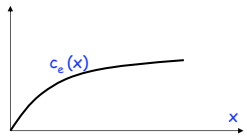


Costs in Connection Game

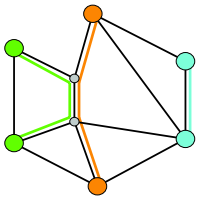
Players pay for their trees, want to minimize payments.

What is the cost of the edges?
$c_e(x)$ is cost of edge e for x users.

Assume economy of scale for costs:



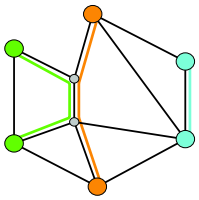
How do players share the cost of an edge?



A Connection Game

How do players share the cost of an edge?

Natural choice is fair sharing, or Shapley cost sharing:



A Connection Game

How do players share the cost of an edge?

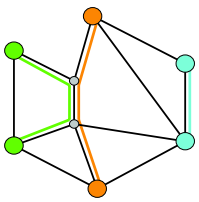
Natural choice is fair sharing, or Shapley cost sharing:

Players using e pay for it evenly:

$$c_i(P) = \sum c_e(k_e)/k_e$$

where k_e number of users on edge e

[Herzog, Shenker, Estrin'97]



A Connection Game

How do players share the cost of an edge?

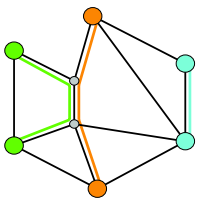
Natural choice is fair sharing, or Shapley cost sharing:

Players using e pay for it evenly:

$$c_i(P) = \sum c_e(k_e)/k_e$$

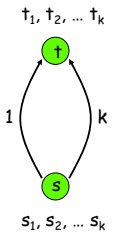
where k_e number of users on edge e

[Herzog, Shenker, Estrin'97]

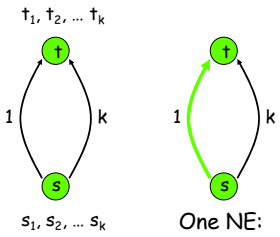


This is congestion game: $\ell_e(x) = c_e(x)/x$
with decreasing "latency"

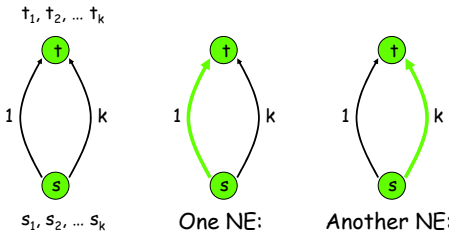
A Simple Example



A Simple Example



A Simple Example



Maybe Best Nash is good?

We know price of anarchy is bad.

Game is a potential game so maybe Price of Stability is better.

$$\text{Price of Stability} = \frac{\text{cost of best selfish outcome}}{\text{"socially optimum" cost}}$$

Do we care?

Nash as Stable Design

Need to Find a Nash equilibrium

- Stable design: as no user finds it in their interest to deviate

Need to find a "good" Nash

- Best Nash/Opt ratio? = Price of Stability [ADKTWR 2004]

Design with a constraint for stability

Results for Network Design

Theorem [Anshelevich, Dasgupta, Kleinberg, Tardos, Wexler, Roughgarden FOCS'04]
Price of Stability is at most $O(\log k)$ for k players

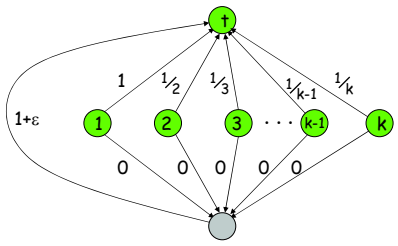
proof:

- edge cost c_e with $k_e > 0$ users
- edge potential with $k_e > 0$ users

$$\Phi_e = c_e \cdot (1+1/2+1/3+\ldots+1/k)$$

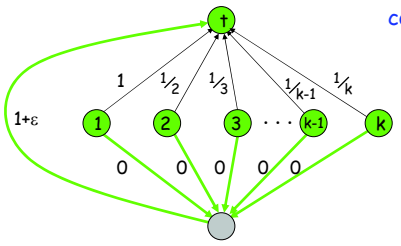
$\rightarrow$ Ratio at most $H_k = O(\log k)$

Example: Bound is Tight



67

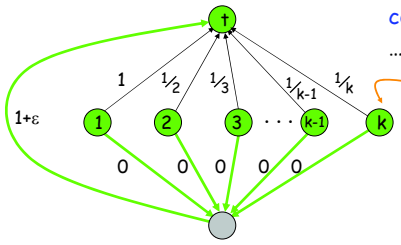
Example: Bound is Tight



cost(OPT) = 1+ ε

68

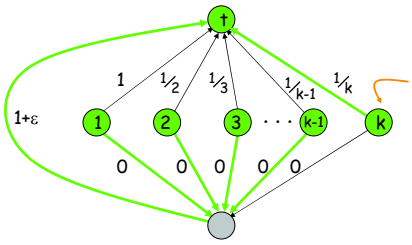
Example: Bound is Tight



cost(OPT) = 1+ ε
...but not a NE:
player k
pays (1+ ε)/k,
could pay 1/k

69

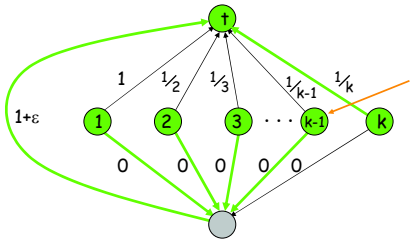
Example: Bound is Tight



so player k
would deviate

70

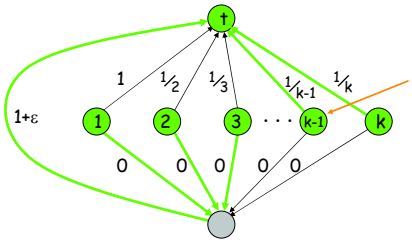
Example: Bound is Tight



now player k-1
pays (1+ ε)/(k-1),
could pay 1/(k-1)

71

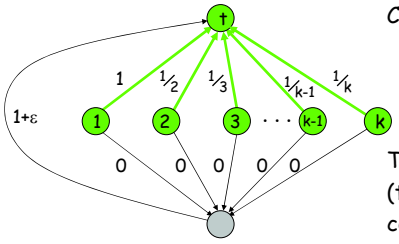
Example: Bound is Tight



so player k-1
deviates too

72

Example: Bound is Tight



Continuing this process, all players defect.

This is a NE! (the only Nash)

cost = $1 + \frac{1}{2} + \ldots + \frac{1}{k}$

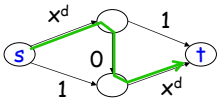
Price of Stability is $H_k = \Theta(\log k)$!

Congestion games

Routing with delay:

- cost increasing with congestion

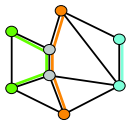
  e.g., $c_e(x) = x \cdot \ell_e(x) = x^{d+1}$



Network Design Game:

- cost decreasing with congestion

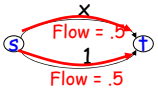
  e.g., $\ell_e(x) = c(x)_e/x$



Contrast with Routing Games

Routing games

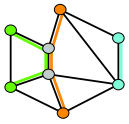
- $c_e(x)$ increasing
- Traffic maybe non-atomic OK? to split traffic
- Nash is unique
- Price of Stability grows with steepness of c:
  - worst case on 2 links
  - bicriteria bound



Design with Fair Sharing

- $c_e(x)$ decreasing
- Choice atomic

  need to select single path
- Many equilibria
- Price of Stability bounded by ≅ log n



Part III

Is Nash a reasonable concept?

Is the price of anarchy always small?
and what can be do when its too big (mechanism design)

Examples:

- Network design and
- Resource allocation

Why stable solutions?

Plan: analyze the quality of Nash equilibrium.
But will players find an equilibrium?

- Can a stable solution be found in poly. time?
- Does natural game play lead to an equilibrium?
- We are assuming non-cooperative players, what if there is cooperation?

Why stable solutions?

Plan: analyze the quality of Nash equilibrium.
But will players find an equilibrium?

- Can a stable solution be found in poly. time?
- Does natural game play lead to an equilibrium?
- We are assuming non-cooperative players, what if there is cooperation?

Answer 1: A clean solution concept and exists ([Nash 1952] if game finite)

Does life lead to clan solutions?

Why stable solutions?

- Finding an equilibrium?

Nonatomic games: we'll see that equilibrium can be found via convex optimization [Beckmann'56]

Atomic game: finding an equilibrium is polynomial local search (PLS) complete [Fabrikant, Papadimitriou, Talwar STOC'04]

79

Why stable solutions?

- Does natural game play lead to equilibrium?

we'll see that natural "best response play" leads to equilibrium if players change one at-a-time

See also:

Fischer¥Räcke¥Vöcking'06, Blum¥Even-Dar¥Ligett'06 also if players simultaneously play natural learning strategies

80

Why stable solutions?

- We are assuming non-cooperative players

Cooperation? No great models,
see some partial results on Thursday.

81

How to Design "Nice" Games?
(Mechanism Design)

Traditional Mechanism Design (VCG):

- use payments to induce all players to tell us his utility for connection
- Select a network to maximize social welfare (minimize cost)

82

How to Design "Nice" Games?
(Mechanism Design)

Traditional Mechanism Design (VCG):

- use payments to induce all players to tell us his utility for connection
- Select a network to maximize social welfare (minimize cost)

Cost lot of money; lots of information to share

83

How to Design "Nice" Games?
(Mechanism Design)

Traditional Mechanism Design (VCG):

- use payments to induce all players to tell us his utility for connection
- Select a network to maximize social welfare (minimize cost)

Cost lot of money; lots of information to share

Here:

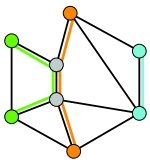
- design a simple/natural Nash game where users select their own graphs and
- analyze the Prize of Anarchy

84

Network Design Mechanism

How should multiple players on a single edge split costs?

We used fair sharing …
[Herzog, Shenker, Estrin'97]



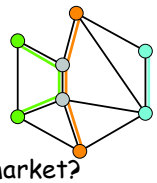
$c_i(P) = \sum c_e(k_e)/k_e$
where k_e number of users on edge e

which makes network design a potential game

Network Design Game Revisited

How should multiple players on a single edge split costs?

We used fair sharing …
[Herzog, Shenker, Estrin'97]



Another approach: Why not free market?
players can also agree on shares? …any division of cost agreed upon by players is OK.

Near-Optimal Network Design with Selfish Agents
STOC '03 Anshelevich, Dasgupta, Tardos, Wexler.

Network Design without Fairness

Results [Anshelevich, Dasgupta, Tardos, Wexler STOC'03]

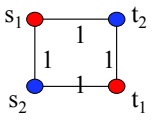
Good news: Price of Stability 1 when all users want to connect to a common source
(as compared to log n for fair sharing)

But: with different source-sink pairs
- Nash may not exists (free riding problem)
- and may be VERY bad when it exists

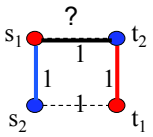
Partial good news: ∃ low cost Approximate Nash

No Deterministic Nash: Free Riding problem

Network Design
[ADTW STOC'03]



Users bid contribution on individual edges.
- Single source game: Price of Anarchy = 1
- Multi source: no Nash

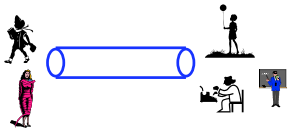


Mechanism Design

Example: Network design.

Results can be used to answer question:
Should one promote "fair sharing" or "free market"?

Another Example: Bandwidth Allocation



Many Users with diverse utilities for bandwidth.

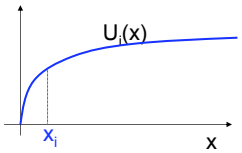
How should we share a given B bandwidth?

Bandwidth Sharing Game

Assumption:

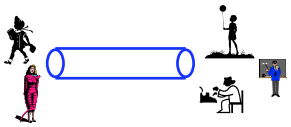
Users have a utility function $U_i(x)$ for receiving x bandwidth.

Assume elastic users (concave utility functions)



91

A Mechanism:



Many Users with diverse utilities for bandwidth.

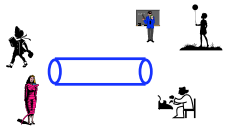
How should we share a given B bandwidth?

Kelly: proportional sharing

- Players offer money w_i for bandwidth.
- Bandwidth allocated proportional to payments:
  - effective price $p = (\Sigma_i w_i)/B$
  - player allocation $x_i = w_i / p$

92

A Mechanism:



Many Users with diverse utilities for bandwidth.

How should we share a given B bandwidth?

Kelly: proportional sharing

- Players offer money w_i for bandwidth.
- allocation proportional:
  - unit price $p = (\Sigma_i w_i)/B$
  - player i gets $x_i = w_i / p$

Thm: If players are price-takers (do not anticipate the effect of their bid on the price)

→ Selfish play results in optimal allocation

93

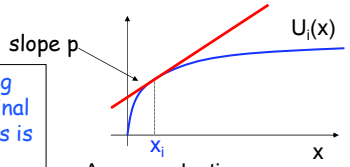
Price Taking Users

Given price p:

how much bandwidth does user i want?

Answer: keeps asking for more until marginal increase in happiness is at least p:

$U_i'(x)=p$



Assume elastic users (concave utility functions)

94

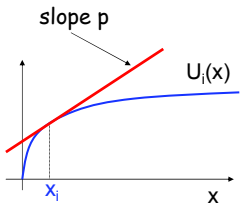
Price Taking Users: Kelly Mechanism Optimal

Equilibrium at price p:

each user i wants x_i such that $U_i'(x_i)=p$

Total bandwidth used up at price p

→ result optimal division of bandwidth

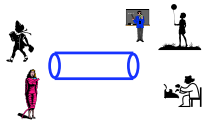


Assume elastic users (concave utility functions)

Price taking users standard assumption if many players

95

Kelly Proportional Sharing:



Players offer money w_i for bandwidth.

Bandwidth allocated proportional to payments

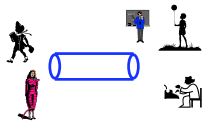
Johari-Tsitsikis, 2004:

what if players do anticipate their effect on the price?

Theorem: Price of Anarchy at most $\frac{3}{4}$ on any networks, and any number of users

96

Kelly Proportional Sharing:



Players offer money w_i for bandwidth.

Bandwidth allocated proportional to payments

Theorem [Johari-Tsitsikis, 2004] Price of Anarchy at most $\frac{3}{4}$ on any networks, and any number of users

Why not optimal? big users "shade" their price. User choice

$$U_i'(x_i)(1-x_i)=p$$

assuming total bandwidth is 1

Worst case: one large user and many small users

97

Summary

We talked about many issues

Price of Anarchy/Stability/Coalitions in the context of some Network Games:

- routing, load balancing, network design, bandwidth sharing

- Designing games (mechanism design)
  - network design

98

Algorithmic Game Theory

- The main ingredients:
  - Lack of central control like distributed computing
  - Selfish participants game theory
- Common in many settings e.g., Internet

Most results so far:

- Price of anarchy/stability in many games, including many I did not mention
- e.g. Facility location (another potential game) [Vetta FOCS'02] and [Devanur-Garg-Khandekar-Pandit-Saberi'04]:

99

Some Open Directions:

- Other natural network games with low lost of anarchy
- Design games with low cost of anarchy
- Better understand dynamics of natural game play
- Dynamics of forming coalitions

100

Polynomial Time Algorithms For Market Equilibria

Vijay V. Vazirani

Markets

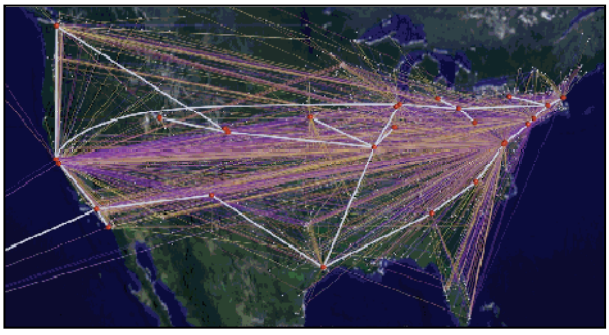


Stock Markets





Internet



- Revolution in definition of markets

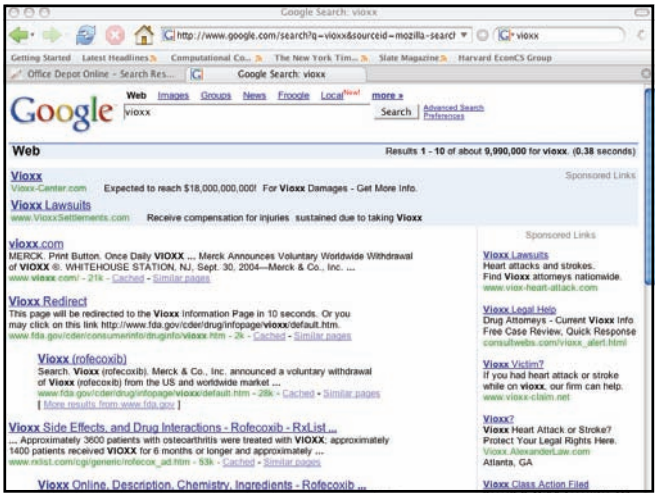
- Revolution in definition of markets
- New markets defined by
  - Google
  - Amazon
  - Yahoo!
  - Ebay

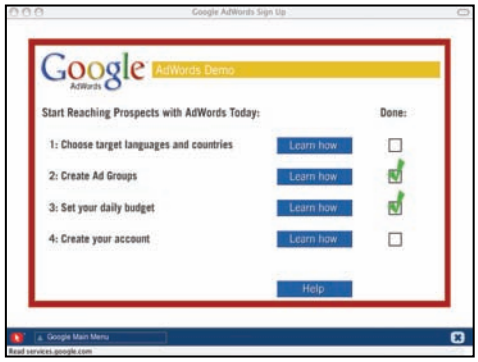
- Revolution in definition of markets
- Massive computational power available

- Revolution in definition of markets
- Massive computational power available
- Important to find good models and algorithms for these markets

Adwords Market

- Created by search engine companies
  - Google
  - Yahoo!
  - MSN
- Multi-billion dollar market
- Totally revolutionized advertising, especially by small companies.





How will this market evolve??

- The study of market equilibria has occupied center stage within Mathematical Economics for over a century.

- The study of market equilibria has occupied center stage within Mathematical Economics for over a century.

- This talk: Historical perspective
  & key notions from this theory.

2). Algorithmic Game Theory

- Combinatorial algorithms for traditional market models

3). New Market Models

- Resource Allocation Model of Kelly, 1997

3). New Market Models

- Resource Allocation Model of Kelly, 1997

- For mathematically modeling TCP congestion control

- Highly successful theory

A Capitalistic Economy

Depends crucially on
pricing mechanisms to ensure:

- Stability
- Efficiency
- Fairness

Adam Smith



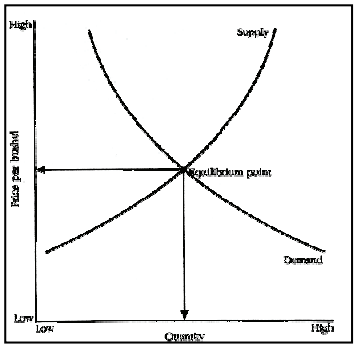
- *The Wealth of Nations*
  2 volumes, 1776.

Adam Smith



- *The Wealth of Nations*
  2 volumes, 1776.
- 'invisible hand' of
  the market

Supply-demand curves



Leon Walras, 1874



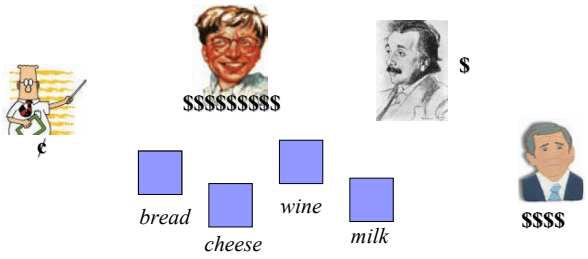
- Pioneered general
  equilibrium theory

Irving Fisher, 1891



- First fundamental
  market model

Fisher's Model, 1891



- People want to maximize happiness – assume linear utilities.

Find prices s.t. market clears

Fisher's Model

- n buyers, with specified money, $m(i)$ for buyer i
- k goods (unit amount of each good)
- Linear utilities: u_{ij} is utility derived by i on obtaining one unit of j
- Total utility of i,

$$u_i = \sum_j u_{ij} x_{ij}$$

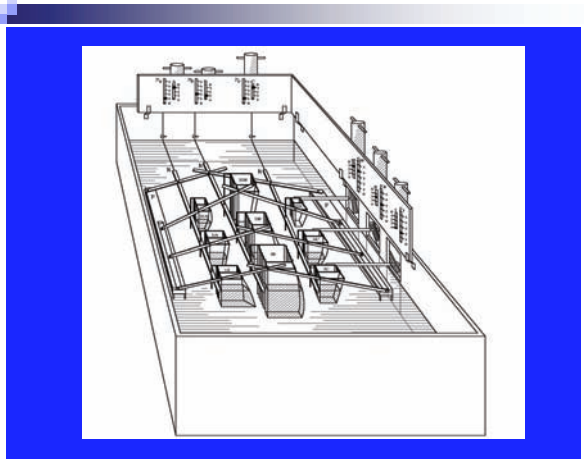
$$x_{ij} \in [0,1]$$

Fisher's Model

- n buyers, with specified money, $m(i)$
- k goods (each unit amount, w.l.o.g.)
- Linear utilities: u_{ij} is utility derived by i on obtaining one unit of j
- Total utility of i,

$$u_i = \sum_j u_{ij} x_{ij}$$

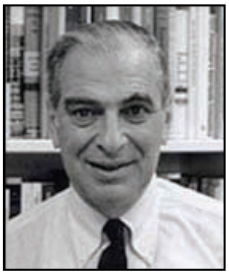
- Find prices s.t. market clears, i.e., all goods sold, all money spent.



Arrow-Debreu Model, 1954 Exchange Economy

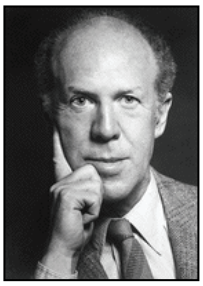
- Second fundamental market model
- Celebrated theorem in Mathematical Economics

Kenneth Arrow



- Nobel Prize, 1972

Gerard Debreu



- Nobel Prize, 1983

Arrow-Debreu Model

- n agents, k goods

Arrow-Debreu Model

- n agents, k goods
- Each agent has: initial endowment of goods, & a utility function

Arrow-Debreu Model

- n agents, k goods
- Each agent has: initial endowment of goods, & a utility function
- Find market clearing prices, i.e., prices s.t. if
  - Each agent sells all her goods
  - Buys optimal bundle using this money
  - No surplus or deficiency of any good

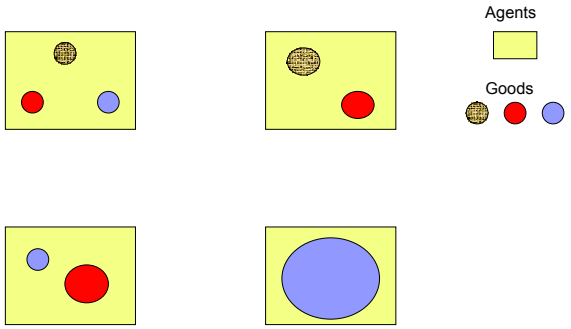
Utility function of agent i

- $u_i : R^k \rightarrow R$
- Continuous, monotonic and strictly concave
- For any given prices and money m, there is a unique utility maximizing bundle for agent i.

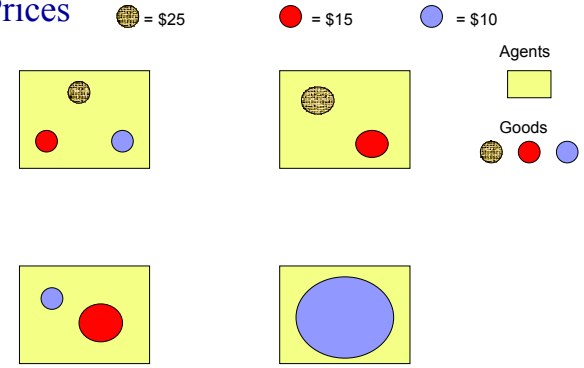
Arrow-Debreu Model



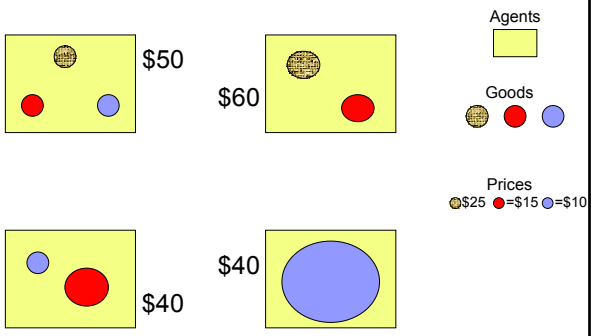
Initial endowment of goods



Prices

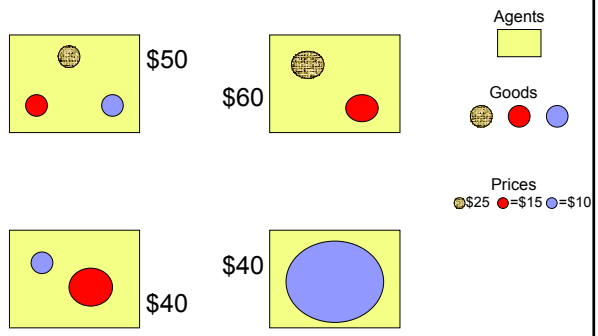


Incomes

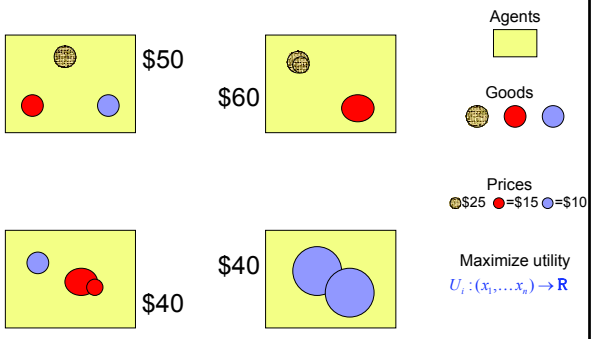


Maximize utility

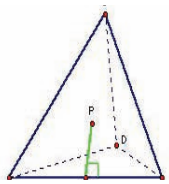
$U_i : (x_1, x_2, \ldots x_n) \to \mathrm{R}$



Find prices s.t. market clears



- Observe: If p is market clearing prices, then so is any scaling of p
- Assume w.l.o.g. that sum of prices of k goods is 1.
- Δ_k : k-1 dimensional unit simplex



Arrow-Debreu Theorem

- For continuous, monotonic, strictly concave utility functions, market clearing prices exist.

Proof

- Uses Kakutani's Fixed Point Theorem.
  - Deep theorem in topology

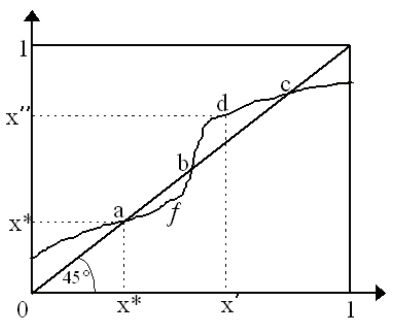
Proof

- Uses Kakutani's Fixed Point Theorem.
  - Deep theorem in topology
- Will illustrate main idea via Brouwer's Fixed Point Theorem (buggy proof!!)

Brouwer's Fixed Point Theorem

- Let $S \subseteq R^n$ be a non-empty, compact, convex set
- Continuous function $f : S \to S$
- Then $\exists x \in S : f(x) = x$

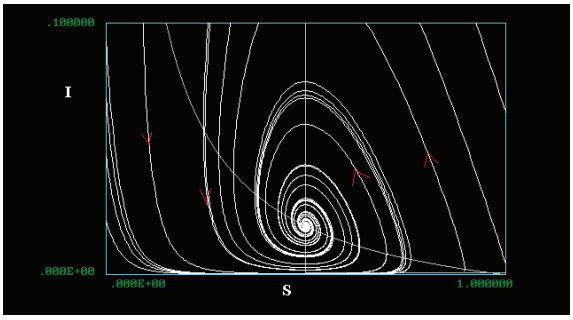
Brouwer's Fixed Point Theorem



Idea of proof

- Will define continuous function $f : \Delta_k \to \Delta_k$
- If p is not market clearing, $f(p)$ tries to 'correct' this.
- Therefore fixed points of f must be equilibrium prices.

Use Brouwer's Theorem



When is *p* an equilibrium price?

- *s(j):* total supply of good *j*.
- *B(i):* unique optimal bundle which agent *i* wants to buy after selling her initial endowment at prices *p*.
- *d(j):* total demand of good *j*.

When is *p* an equilibrium price?

- *s(j):* total supply of good *j*.
- *B(i):* unique optimal bundle which agent *i* wants to buy after selling her initial endowment at prices *p*.
- *d(j):* total demand of good *j*.
- For each good *j*: *s(j) = d(j)*.

What if *p* *is* not an equilibrium price?

- *s(j) < d(j)* => ↑ *p(j)*
- *s(j) > d(j)* => ↓ *p(j)*
- Also ensure $\underline{p} \in \Delta_k$

- Let $f(p) = p'$
- *S(j) < d(j)* => $p'(j) = \frac{p(j) + [d(j) - s(j)]}{N}$
- *S(j) > d(j)* => $p'(j) = \frac{p(j)}{N}$
- *N* is s.t. $\sum_j p'(j) = 1$

$\forall i : u_i$ is a cts. fn.

=> $\forall i : B(i)$ is a cts. fn. of $\underline{p}$

=> $\forall j : d(j)$ is a cts. fn. of $\underline{p}$

=> *f* is a cts. fn. of $\underline{p}$

$\forall i : u_i$ is a cts. fn.

=> $\forall i : B(i)$ is a cts. fn. of p

=> $\forall j : d(j)$ is a cts. fn. of p

=> f is a cts. fn. of p

By Brouwer's Theorem, equilibrium prices exist.

$\forall i : u_i$ is a cts. fn.

=> $\forall i : B(i)$ is a cts. fn. of p

=> $\forall j : d(j)$ is a cts. fn. of p

=> f is a cts. fn. of p

By Brouwer's Theorem, equilibrium prices exist.

q.e.d.!

Kakutani's Fixed Point Theorem

- $S \subseteq R^n$ convex, compact set
- $f : S \to 2^S$ non-empty, convex, upper hemi-continuous correspondence

$\Rightarrow \exists x \in S$ s.t. $x \in f(x)$

Fisher reduces to Arrow-Debreu

- Fisher: n buyers, k goods
- AD: $n+1$ agents
  - first n have money, utility for goods
  - last agent has all goods, utility for money only.

Combinatorial Algorithms for Market Equilibria

Vijay V. Vazirani

- Arrow-Debreu Theorem: Equilibria exist.

- Arrow-Debreu Theorem: Equilibria exist.
- Do markets operate at equilibria?

- Arrow-Debreu Theorem: Equilibria exist.
- Do markets operate at equilibria?
- Can equilibria be computed efficiently?

Arrow-Debreu is highly non-constructive

Arrow-Debreu is highly non-constructive

- "Invisible hand" of the market: Adam Smith
- Scarf, 1973: approximate fixed point algs.
- Convex programs:
  - Fisher: Eisenberg & Gale, 1957
  - Arrow-Debreu: Newman and Primak, 1992

- Used for deciding tax policies, price of new products etc.
- New markets on the Internet

Algorithmic Game Theory

- Use powerful techniques from modern algorithmic theory and notions from game theory to address issues raised by Internet.
- Combinatorial algorithms for finding market equilibria.

Two Fundamental Models

- Fisher's model
- Arrow-Debreu model,
  also known as exchange model

Combinatorial Algorithms

- Primal-dual schema based algorithms
  - Devanur, Papadimitriou, Saberi & V., 2002
    Combinatorial algorithm for Fisher's model
- Auction-based algorithms
  - Garg & Kapoor, 2004
    Approximation algorithms.

Approximation

- Find prices s.t. all goods clear
- Each buyer get goods providing
  at least $(1-\varepsilon)\times$optimal utility.

Primal-Dual Schema

- Highly successful algorithm design technique from exact and approximation algorithms

Exact Algorithms for Cornerstone Problems in P:

- Matching (general graph)
- Network flow
- Shortest paths
- Minimum spanning tree
- Minimum branching

Approximation Algorithms

set cover	facility location
Steiner tree	*k*-median
Steiner network	multicut
k-MST	feedback vertex set
scheduling . . .	

Main new idea

- Previous: problems captured via linear programs
- DPSV algorithm: problem captured via a nonlinear convex program

Fisher's Model

- *n* buyers, with specified money, *m(i)* for buyer *i*
- *k* goods (unit amount of each good)
- Linear utilities: u_{ij} is utility derived by *i* on obtaining one unit of *j*
- Total utility of *i*,

$$u_i = \sum_j u_{ij} x_{ij}$$

$$x_{ij} \in [0,1]$$

Fisher's Model

- *n* buyers, with specified money, *m(i)*
- *k* goods (each unit amount, w.l.o.g.)
- Linear utilities: u_{ij} is utility derived by *i* on obtaining one unit of *j*
- Total utility of *i*,

$$u_i = \sum_j u_{ij} x_{ij}$$

- Find prices s.t. market clears

Eisenberg-Gale Program, 1959

$$\max \sum_i m(i) \log u(i)$$

s.t.

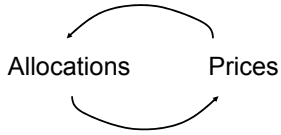
$$\forall i : u(i) = \sum_j u_{ij} x_{ij}$$

$$\forall j : \sum_i x_{ij} \le 1$$

$$\forall ij : x_{ij} \ge 0$$

DPSV Algorithm

- "primal" variables: allocations of goods
- "dual" variables: prices
- algorithm: primal & dual improvements



Market Equilibrium

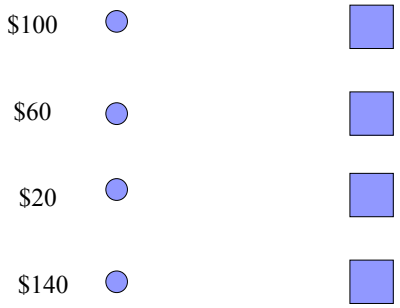
- Buyer i's optimization program:

$$\begin{aligned} \text{maximize} \quad & \sum_j u_{ij} x_{ij} \\ \text{subject to} \quad & \sum_j p_j x_{ij} \le m_i \end{aligned}$$

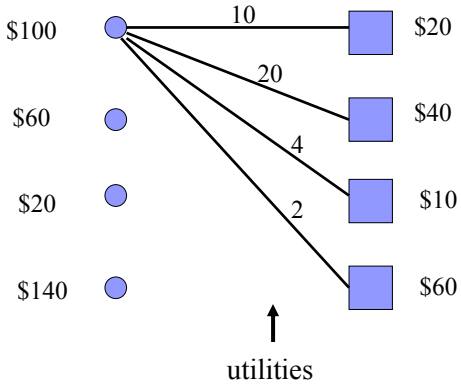
- Global Constraint:

$$\sum_i x_{ij} = 1 \qquad \forall j$$

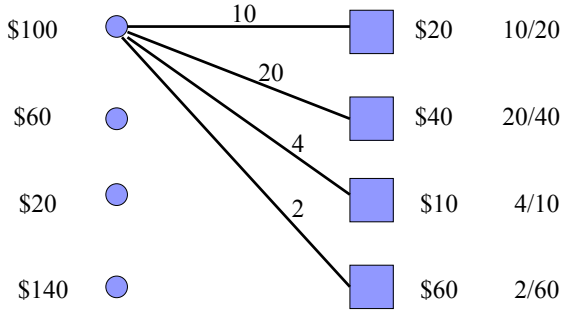
People Goods



Prices and utilities



Bang per buck

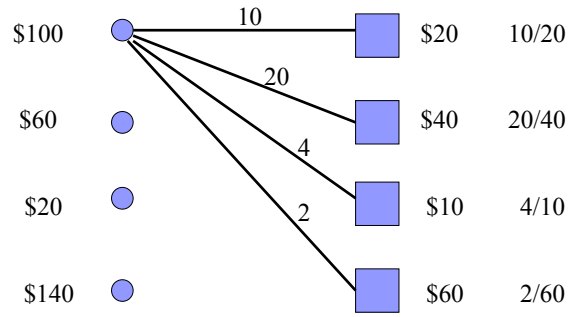


Bang per buck

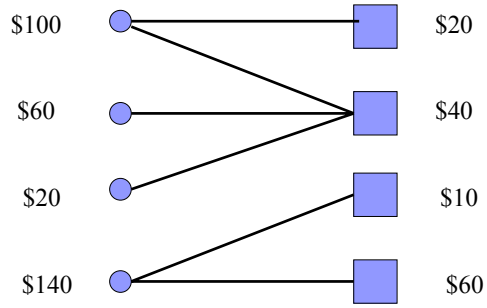
- Utility of $1 worth of goods
- Buyers will only buy goods providing maximum bang per buck

$$\max_j \frac{u_{ij}}{p_j}$$

Equality subgraph



Equality subgraph



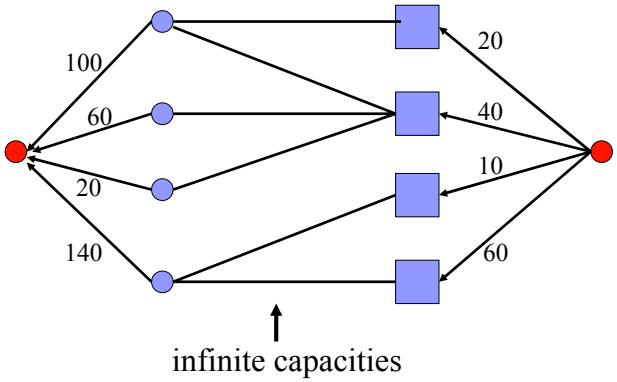
Most desirable goods for each buyer

- Any goods sold in equality subgraph make agents happiest
- How do we maximize sales in equality subgraph?

- Any goods sold in equality subgraph make agents happiest
- How do we maximize sales in equality subgraph?

Use max-flow!

Max flow



infinite capacities

Idea of Algorithm

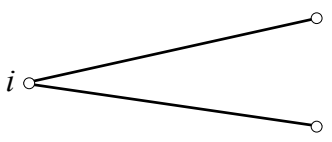
- Invariant: source edges form min-cut (agents have surplus)
- Iterations: gradually raise prices, decrease surplus
- Terminate: when surplus = 0, i.e., sink edges also form a min-cut

Ensuring Invariant initially

- Set each price to $1/n$
- Assume buyers' money integral

How to raise prices?

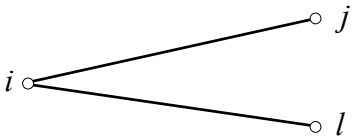
- Ensure equality edges retained



$$\frac{u_{ij}}{p_j} = \frac{u_{il}}{p_l}$$

How to raise prices?

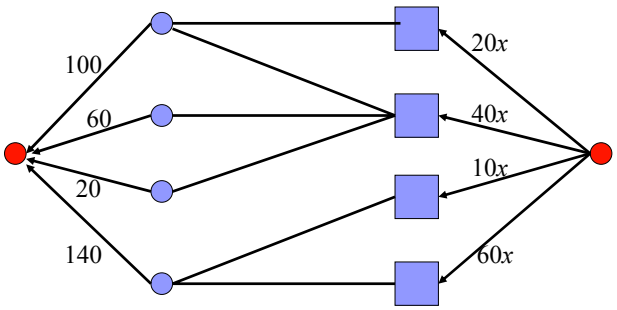
- Ensure equality edges retained



$$\frac{u_{ij}}{p_j} = \frac{u_{il}}{p_l}$$

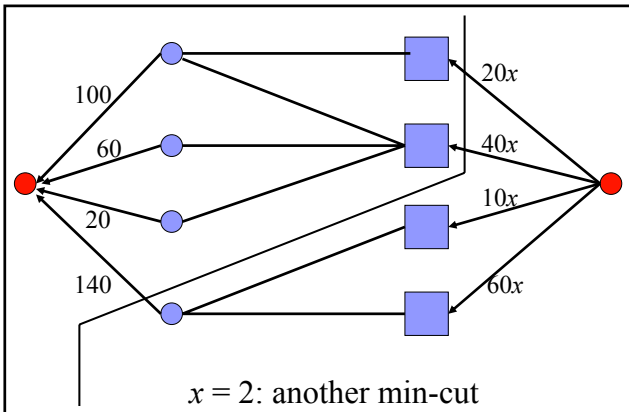
- Raise prices proportionately

$$\frac{p_j}{p_l} = \frac{u_{ij}}{u_{il}}$$



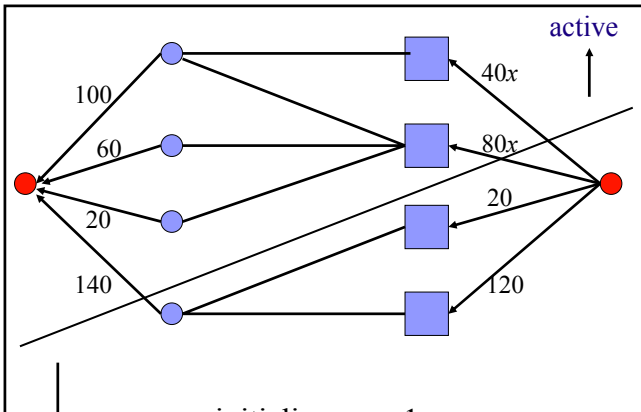
initialize: $x = 1$

$x \uparrow$



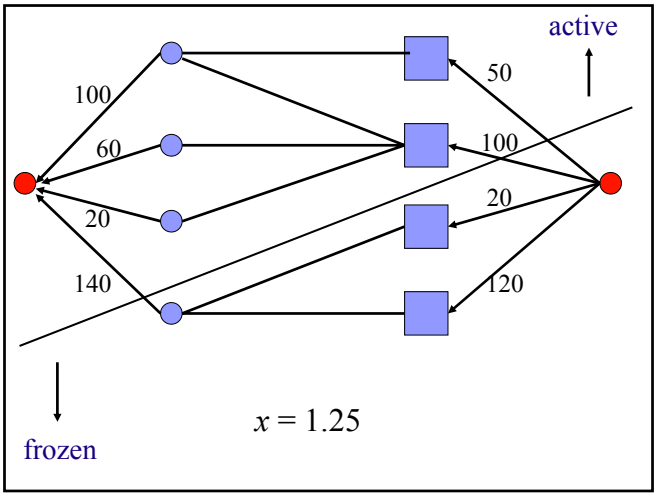
$x = 2$: another min-cut

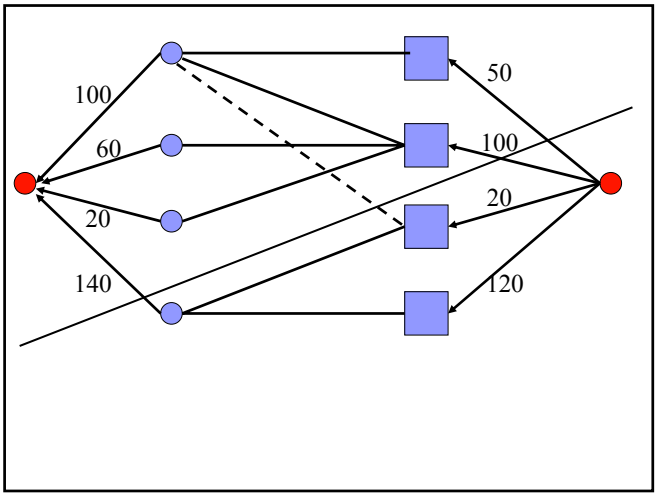
$x>2$: Invariant violated

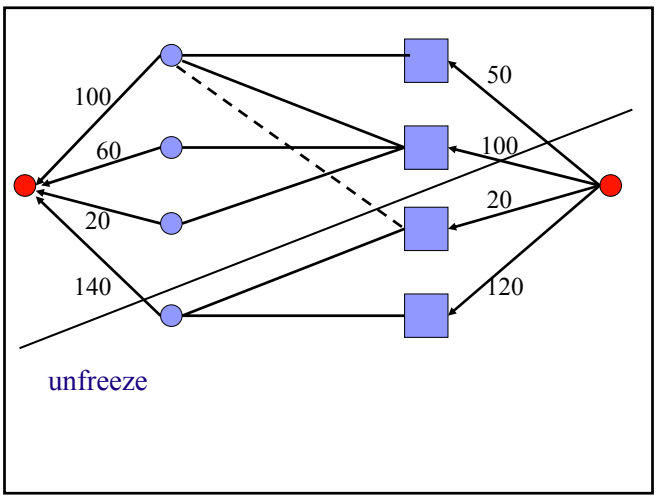


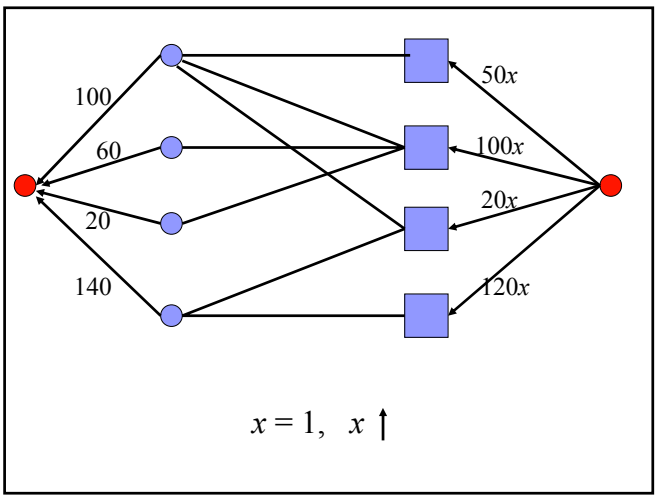
reinitialize: $x = 1$

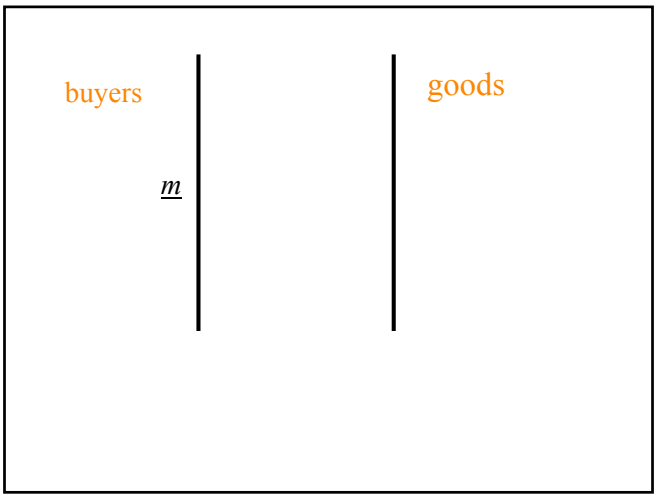
frozen

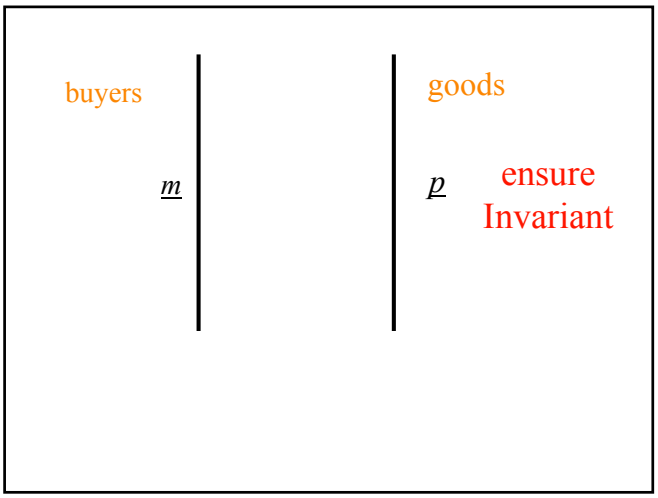

active
100
60
20
140
50
100
20
120
$x = 1.25$
frozen

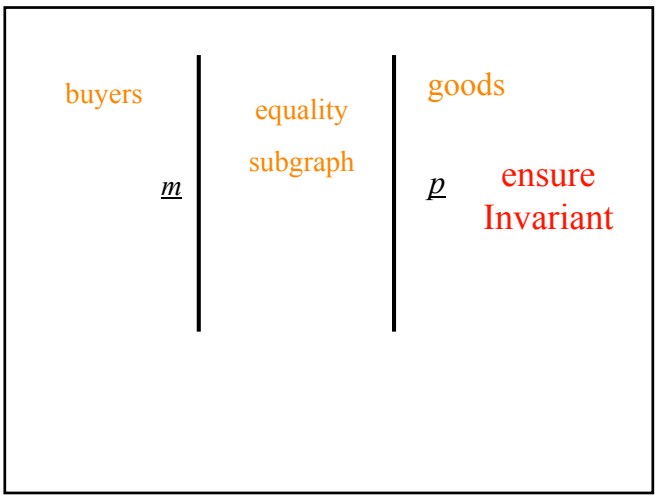

100
60
20
140
50
100
20
120

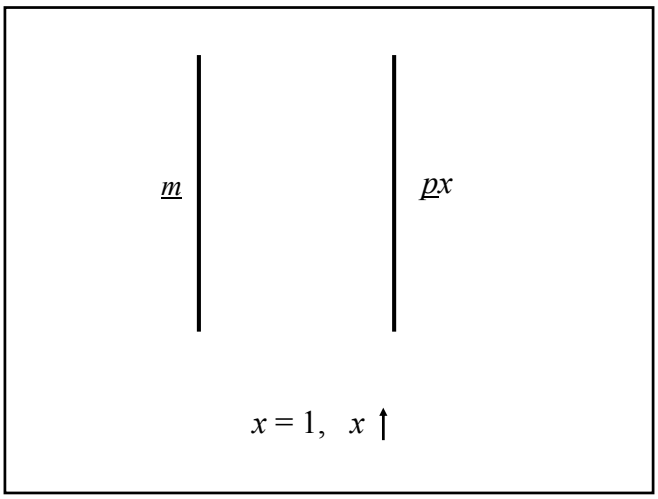

100
60
20
140
50
100
20
120
unfreeze

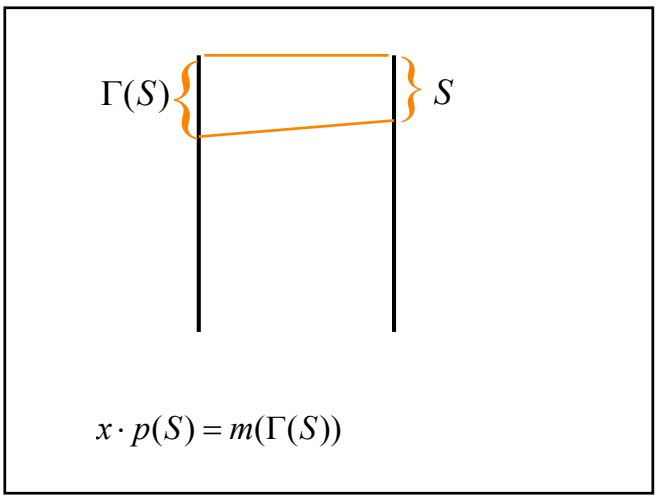

100
60
20
140
50x
100x
20x
120x
$x = 1, \quad x \uparrow$

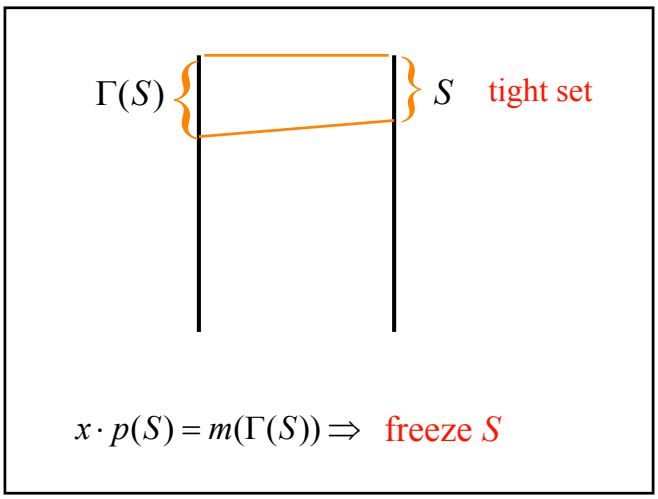

buyers
goods
m

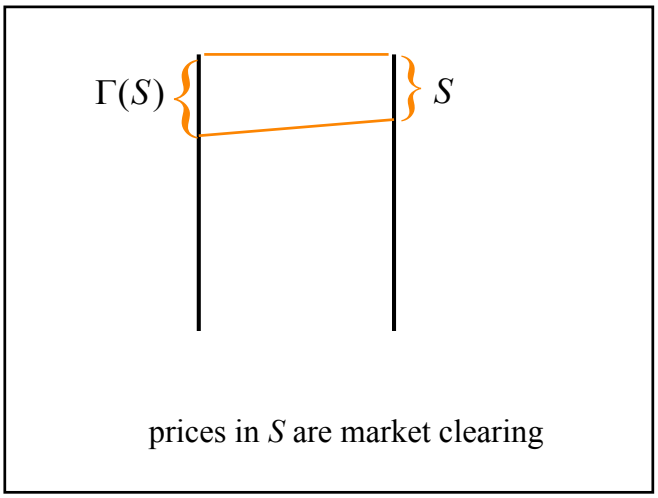

buyers
goods
m
p
ensure
Invariant

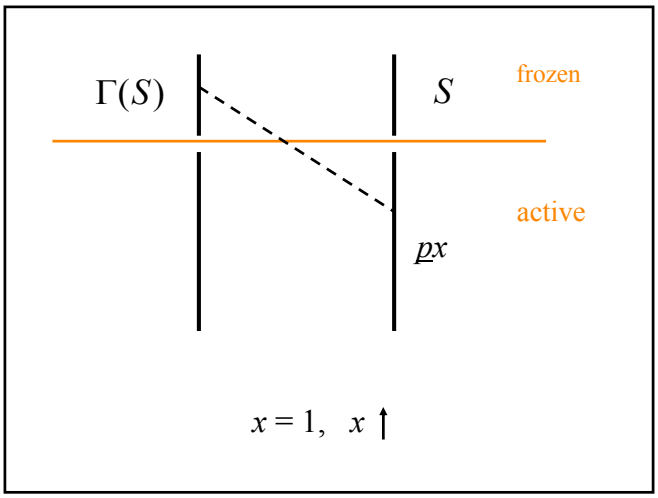

buyers
equality
subgraph
goods
m
p
ensure
Invariant

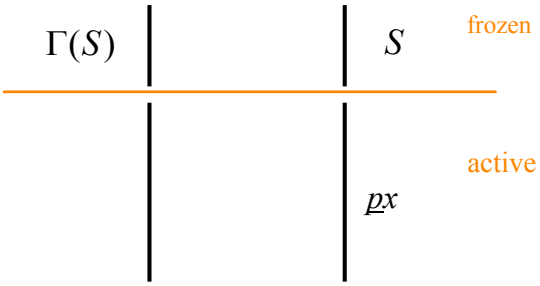

m
px
$x = 1, \quad x \uparrow$


$\Gamma(S)$
S
$x \cdot p(S) = m(\Gamma(S))$

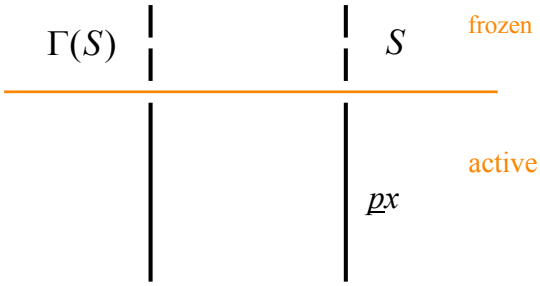

$\Gamma(S)$
S
tight set
$x \cdot p(S) = m(\Gamma(S)) \Rightarrow$ freeze S


$\Gamma(S)$
S
prices in S are market clearing

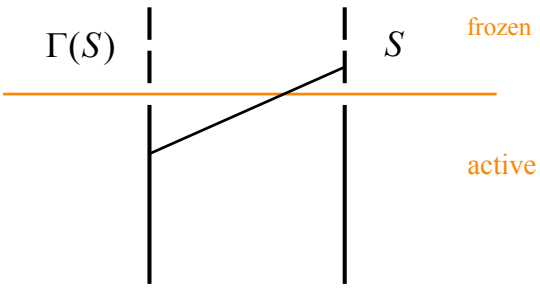

$\Gamma(S)$
S
frozen
active
px
$x = 1, \quad x \uparrow$



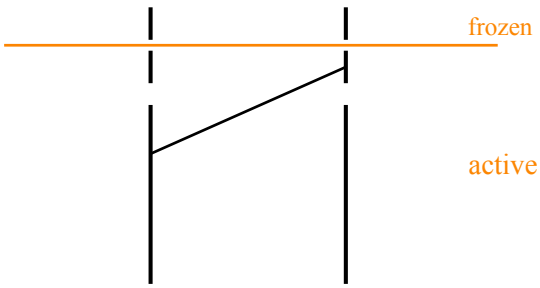
$x = 1, \quad x \uparrow$



$x = 1, \quad x \uparrow$



new edge enters equality subgraph



unfreeze component

- All goods frozen => terminate

  (market clears)

- All goods frozen => terminate

  (market clears)

- When does a new set go tight?

  •Solve as parametric cut problem

Termination

- Prices in S^* have denominators $\leq \Delta = nU^n$,
- Terminates in $Mn^2\Delta^2$ max-flows.

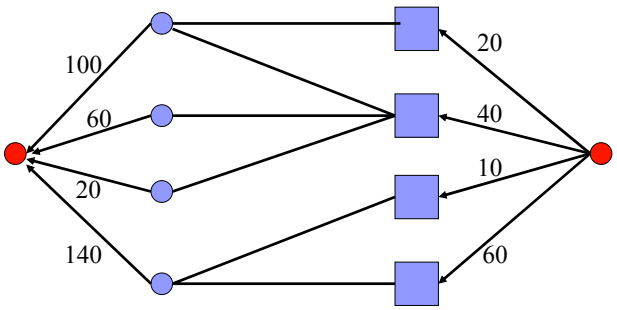
Polynomial time?

- Problem: very little price increase between freezings

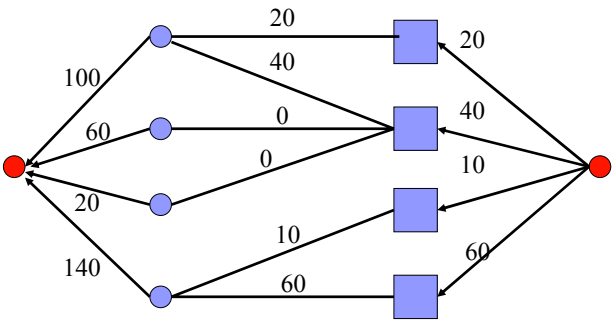
Polynomial time?

- Problem: very little price increase between freezings
- Solution: work with buyers having large surplus

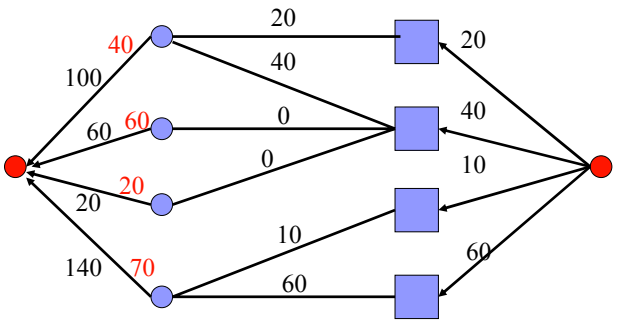
Max flow

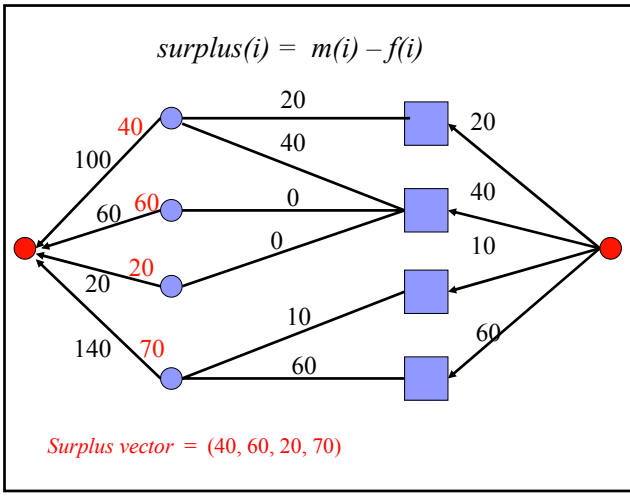


Max flow



surplus(i) = m(i) – f(i)



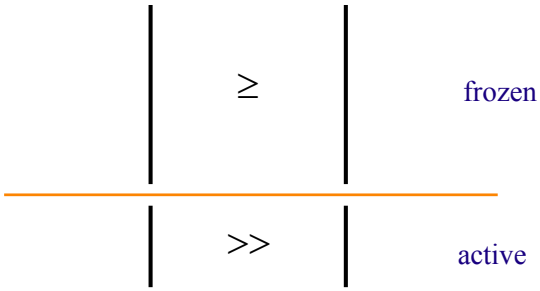


Balanced flow

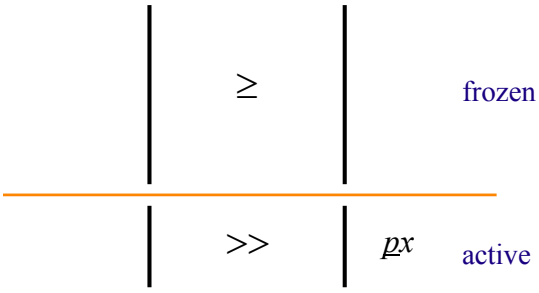
- A max-flow that minimizes l_2 norm of surplus vector
  - tries to make surpluses as equal as possible

Algorithm

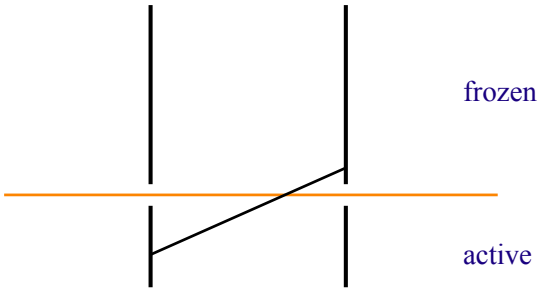
- Compute balanced flow



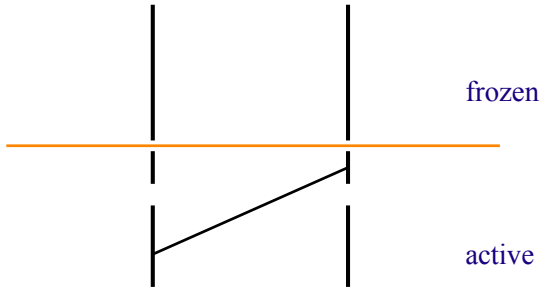
Active subgraph: Buyers with maximum surplus



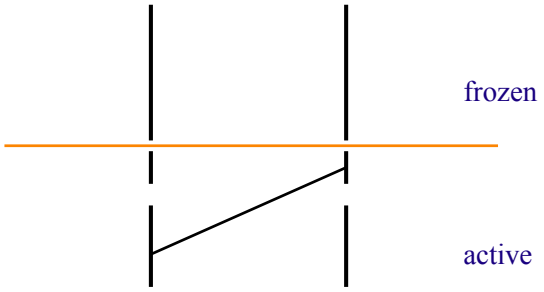
$x = 1, \quad x \uparrow$



new edge enters equality subgraph



Unfreeze buyers having residual path to active subgraph



Unfreeze buyers having residual path to active subgraph

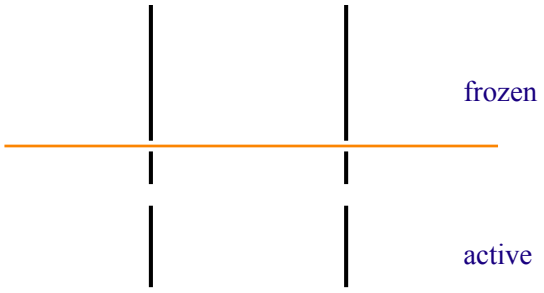
Do they have large surplus?

f: balanced flow

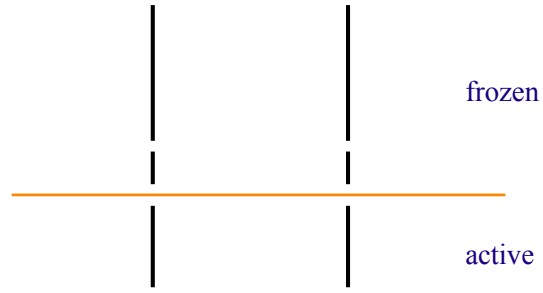
R(f): residual graph

Theorem: If *R(f)* has a path from *i* to *j* then

surplus(i) > *surplus(j)*



New set tight



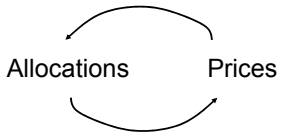
New set tight: freeze

Theorem: After each freezing, l_2 norm of surplus vector drops by $(1 - 1/n^2)$ factor.

- Two reasons:
  - total surplus decreases
  - flow becomes more balanced

Idea of Algorithm

- algorithm: primal & dual improvements



- measure of progress: l_2-norm of surplus vector

Polynomial time

Theorem: $O(n^2(n \log U + \log Mn^2))$

max-flow computations suffice.

Weak gross substitutability

- Increasing price of one good cannot decrease demand for another good.

Weak gross substitutability

- Increasing price of one good cannot decrease demand for another good.

=> never need to decrease prices (dual variables).

Weak gross substitutability

- Increasing price of one good cannot decrease demand for another good.

=> never need to decrease prices (dual variables).

- Almost all primal-dual algs work this way.

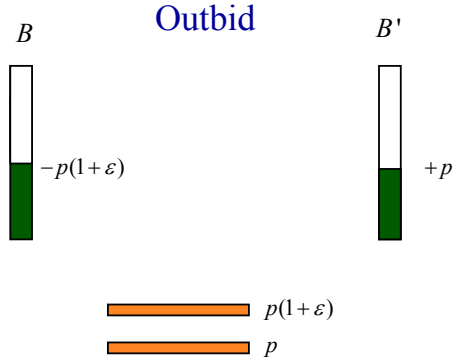
Arrow-Debreu Model

- Approximate equilibrium algorithms:
  - Jain, Mahdian & Saberi, 2003: Use DPSV as black box.
  - Devanur & V., 2003: More efficient, by opening DPSV.

Garg & Kapoor, 2004
Auction-based algorithm

- Start with very low prices
- Keep increasing price of good that is in demand
- B has excess money. Favorite good: g
  Currently at price p and owned by B'
- B outbids B'

Outbid



Auction-based algorithm

- Go in rounds: $B_1, B_2, \ldots B_n$
- In each round, total surplus decreases by $(1+\varepsilon)$ factor
- Hence $\log_{(1+\varepsilon)} M$ iterations suffice,
  M= *total money*

Arrow-Debreu Model

- Start with all prices 1
- Allocate money to agents (initial endowment)
- Perform outbid and update agents' money

Arrow-Debreu Model

- Start with all prices 1
- Allocate money to agents (initial endowment)
- Perform outbid and update agents' money
- Any good with price >1 is fully sold

Arrow-Debreu Model

- Start with all prices 1
- Allocate money to agents (initial endowment)
- Perform outbid and update agents' money
- Any good with price >1 is fully sold

$$\frac{\max price}{\min price} \leq \frac{\max u_{ij}}{\min u_{ij}}$$

- Eventually every good will have price >1

- Garg, Kapoor & V., 2004:

Auction-based algorithms for
additively separable concave utilities
satisfying weak gross substitutability

- Kapoor, Mehta & V., 2005:

Auction-based algorithm for
a (restricted) production model

Q: Distributed algorithm for equilibria?

- Appropriate model?
- Primal-dual schema operates via
local improvements

New Market Models

Resource Allocation Markets

Vijay V. Vazirani

Fisher's Model

- n buyers, with specified money, $m(i)$ for buyer i
- k goods (unit amount of each good)
- Linear utilities: u_{ij} is utility derived by i on obtaining one unit of j
- Total utility of i,

$$u_i = \sum_j u_{ij} x_{ij}$$

$$x_{ij} \in [0,1]$$

Fisher's Model

- n buyers, with specified money, $m(i)$
- k goods (each unit amount, w.l.o.g.)
- Linear utilities: u_{ij} is utility derived by i on obtaining one unit of j
- Total utility of i,

$$u_i = \sum_j u_{ij} x_{ij}$$

- Find prices s.t. market clears

Eisenberg-Gale Program, 1959

$$\max \sum_i m(i) \log u(i)$$

$$s.t.$$

$$\forall i : u(i) = \sum_j u_{ij} x_{ij}$$

$$\forall j : \sum_i x_{ij} \leq 1$$

$$\forall ij : x_{ij} \geq 0$$

Via KKT Conditions can establish:

- Optimal solution gives equilibrium allocations
- Lagrange variables give prices of goods

Eisenberg-Gale program helps establish:

- Equilibrium exists (under mild conditions)
- Equilibrium utilities and prices are unique

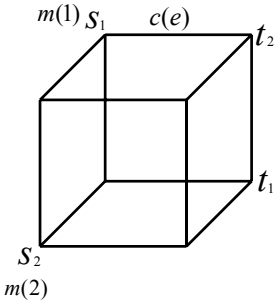
Eisenberg-Gale program helps establish:

- Equilibrium exists (under mild conditions)
- Equilibrium utilities and prices are unique
- Rational!!

Kelly's resource allocation model, 1997

Mathematical framework for understanding TCP congestion control

Kelly's model



Given:

network $G = (V,E)$

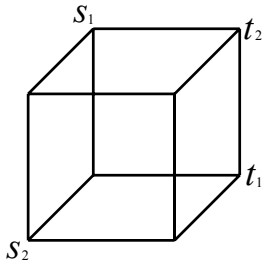
(directed or undirected)

capacities on edges

source-sink pairs (agents)

m(i): money/unit time agent *i* is willing to pay

Kelly's model



Network determines:

f(i): flow rate of agent *i*

Assume utility $u(i) = m(i) \log f(i)$

Total utility is additive

Convex Program for Kelly's Model

$$\max \sum_i m(i) \log f(i)$$

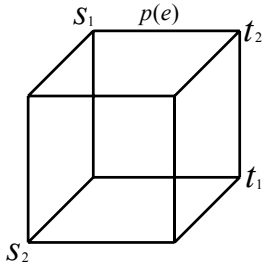
s.t.

$$\forall i : f(i) = \sum_p f_i^p$$

$$\forall e : flow(e) \le c(e)$$

$$\forall i, p : f_i^p \ge 0$$

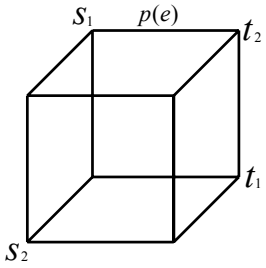
Kelly's model



Lagrange variables:

p(e): price/unit flow

Kelly's model



Optimum flow and edge prices are in equilibrium:

1). $p(e)>0$ only if e is saturated

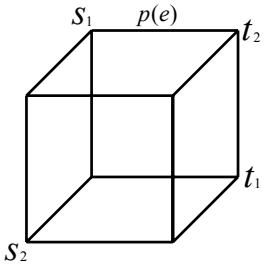
2) flows go on cheapest paths

3) money of each agent is fully used

Let rate(i) = cost of cheapest path for i

$m(i) = f(i)$ rate(i)

Kelly's model



Optimum flow and edge prices are in equilibrium:

1). $p(e)>0$ only if e is saturated

2) flows go on cheapest paths

3) money of each agent is fully used

Let rate(i) = cost of cheapest path for i

$f(i)$'s and rate(i)'s are unique!

TCP Congestion Control

- $f(i)$: source rate
- $p(e)$: prob. of packet loss (in TCP Reno)
  queueing delay (in TCP Vegas)

TCP Congestion Control

- $f(i)$: source rate
- $p(e)$: prob. of packet loss (in TCP Reno)
  queueing delay (in TCP Vegas)

Kelly: Equilibrium flows are proportionally fair: only way of increasing an agent's flow by 5% is to decrease other agents' flow by at least 5%

TCP Congestion Control

- $f(i)$: source rate
- $p(e)$: prob. of packet loss (in TCP Reno)
  queueing delay (in TCP Vegas)
- Low, Doyle, Paganini: continuous time algs. for computing equilibria (not poly time).

TCP Congestion Control

- $f(i)$: source rate
- $p(e)$: prob. of packet loss (in TCP Reno)
  queueing delay (in TCP Vegas)
- Low, Doyle, Paganini: continuous time algs. for computing equilibria (not poly time).
- AIMD + RED converges to equilibrium primal-dual (source-link) alg.

TCP Congestion Control

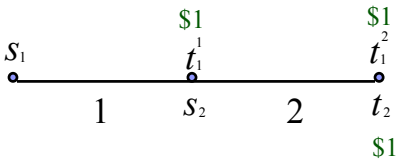
- *f(i):* source rate
- *p(e):* prob. of packet loss (in TCP Reno)
  queueing delay (in TCP Vegas)
- Low, Doyle, Paganini: continuous time algs. for computing equilibria (not poly time).
- FAST: for high speed networks with large bandwidth

Combinatorial Algorithms

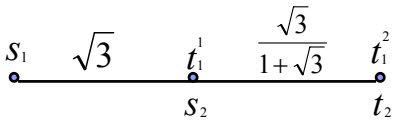
- Devanur, Papadimitriou, Saberi & V., 2002: for Fisher's linear utilities case
- Kelly & V., 2002: Kelly's model is a generalization of Fisher's model.

Find comb. poly time algs!

Irrational for 2 sources & 3 sinks

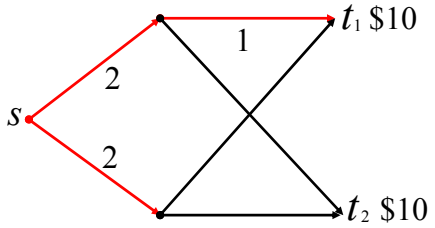


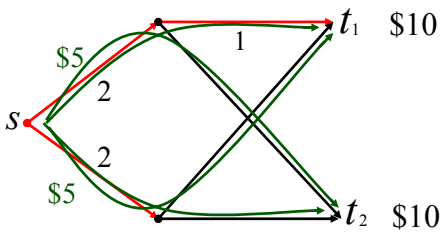
Irrational for 2 sources & 3 sinks

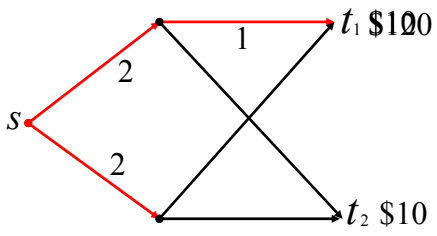


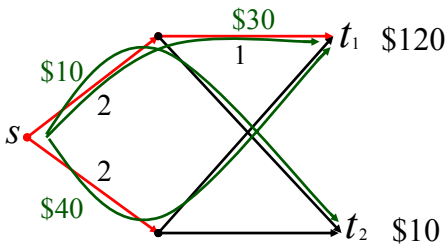
Equilibrium prices

- 1 source & multiple sinks
- 2 source-sink pairs



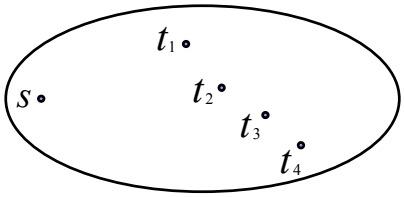




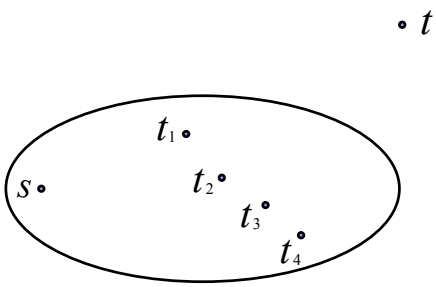


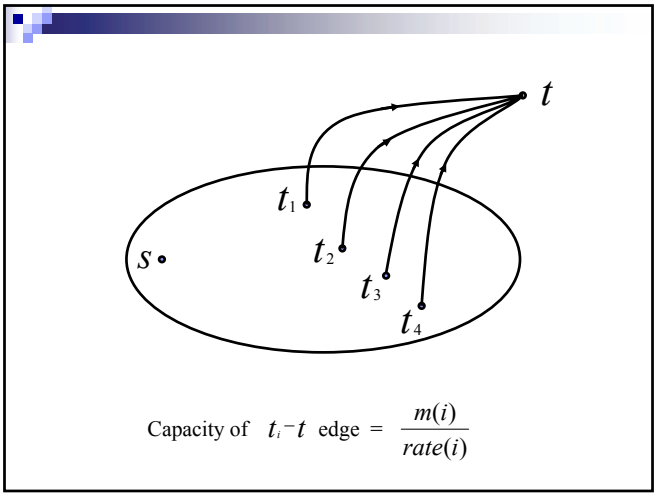
Jain & V., 2005: strongly poly alg

- Primal-dual algorithm
  - Usual: linear programs & LP-duality
  - This: convex programs & KKT conditions
- Ascending price auction
  - Buyers: sinks (fixed budgets, maximize flow)
  - Sellers: edges (maximize price)

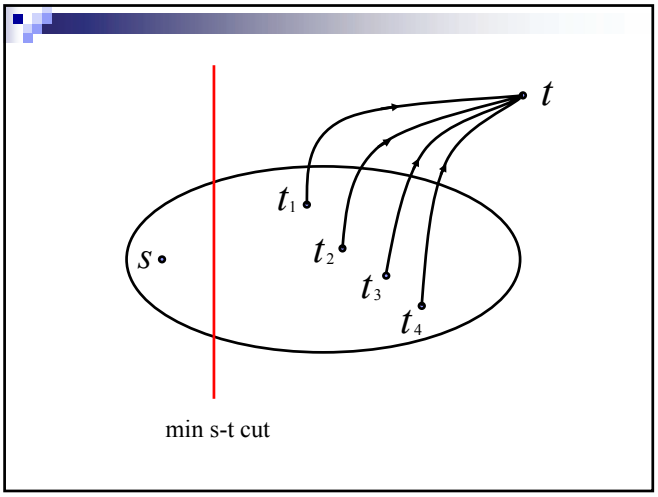


rate(i): cost of cheapest s – t_i path

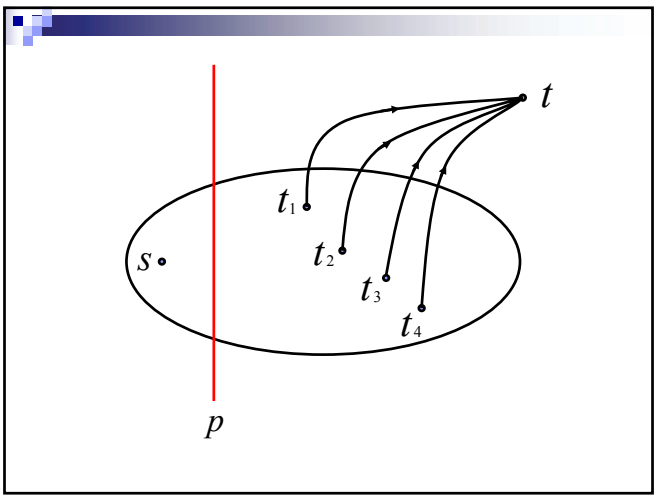


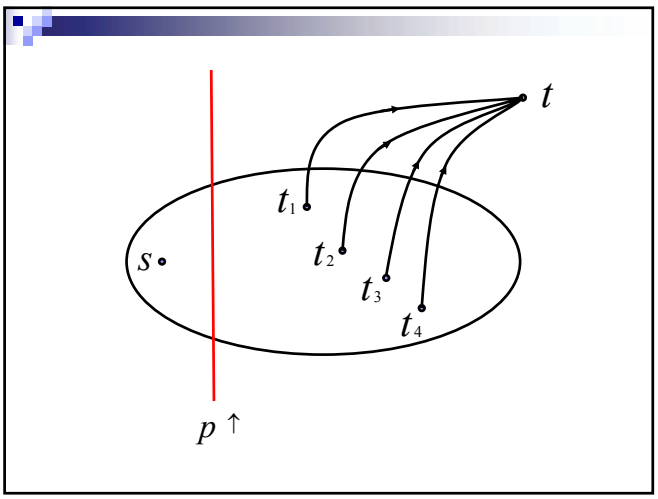


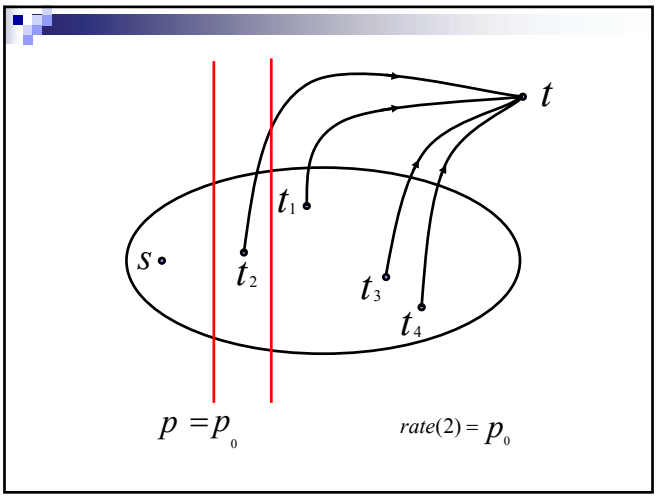
Capacity of $t_i - t$ edge = $\dfrac{m(i)}{rate(i)}$

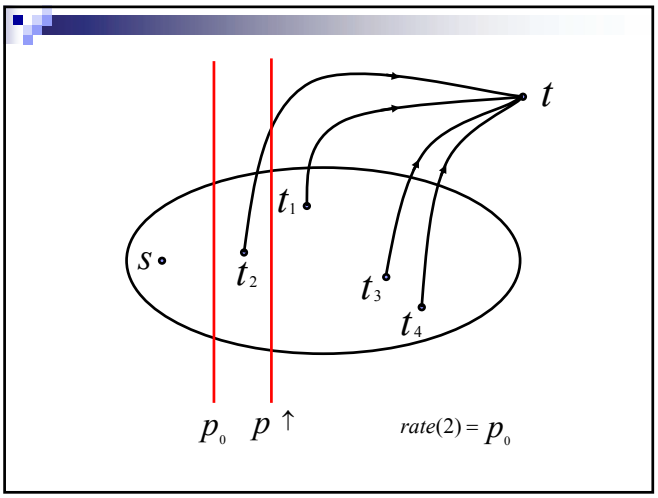


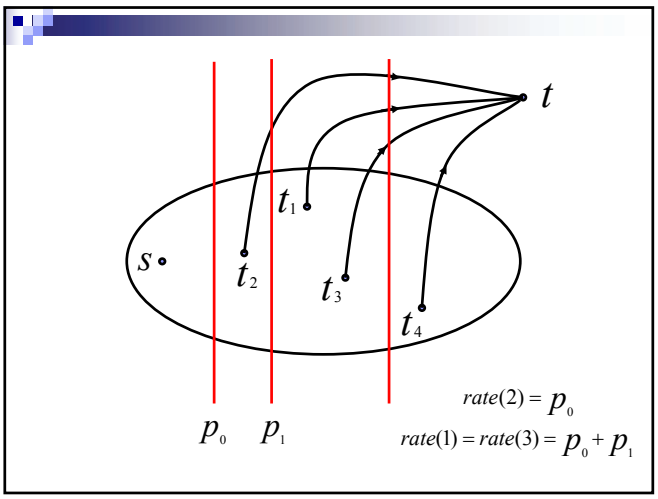
min s-t cut

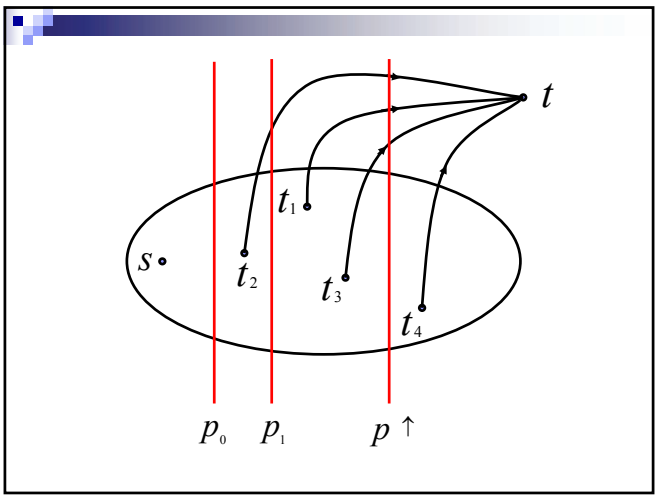


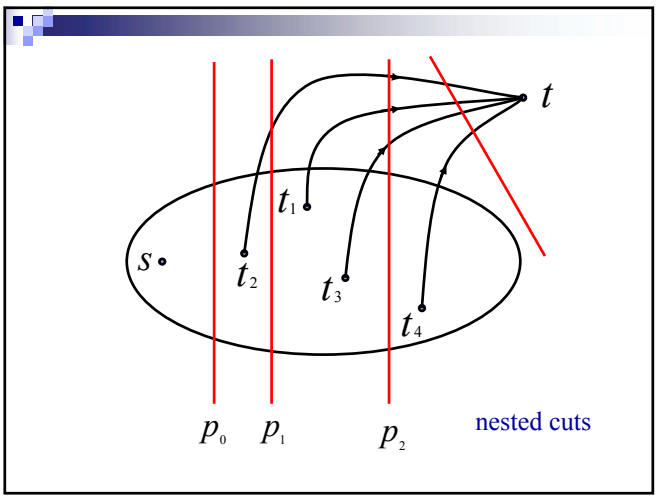


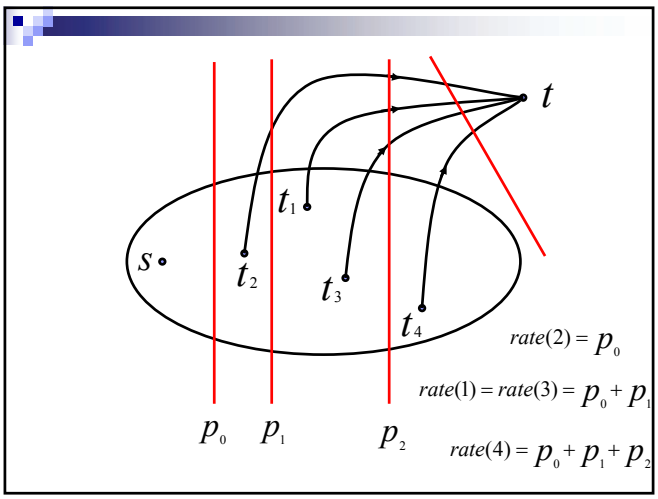




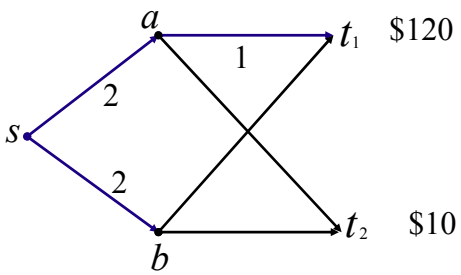


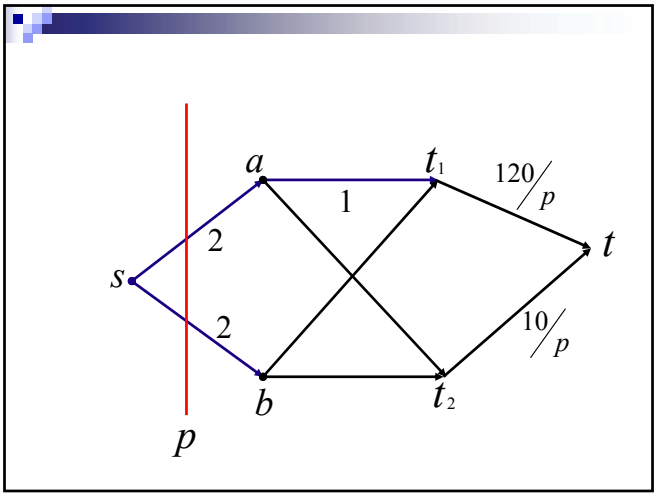


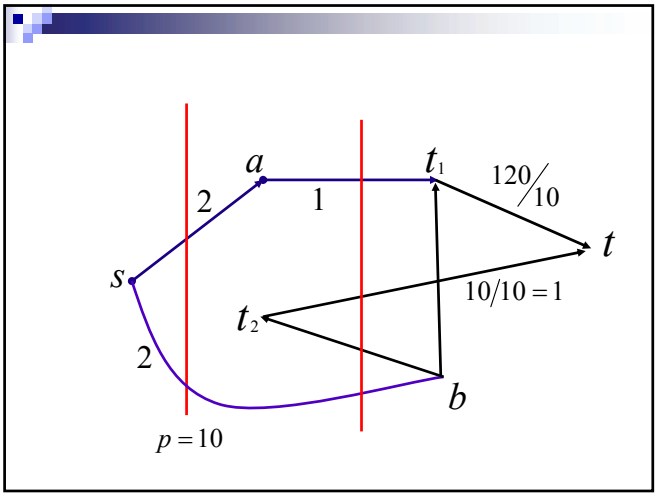


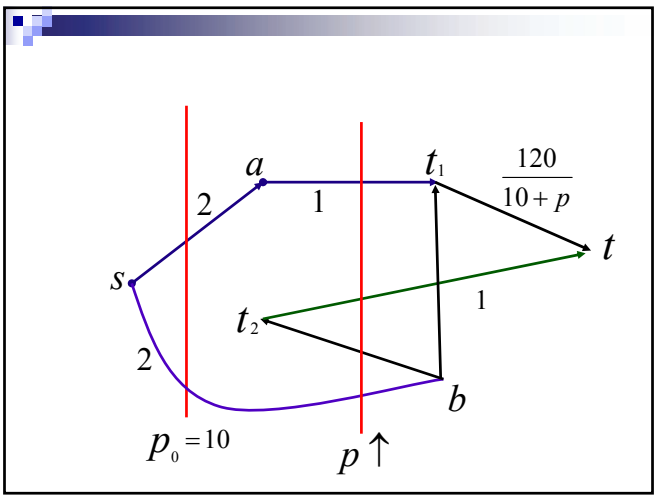


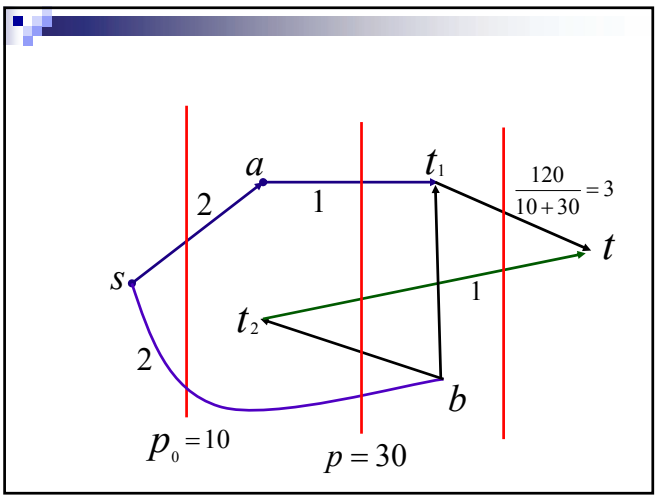
- Find s-t max flow
- Flow and prices will:
  - Saturate all red cuts
  - Use up sinks' money
  - Send flow on cheapest paths

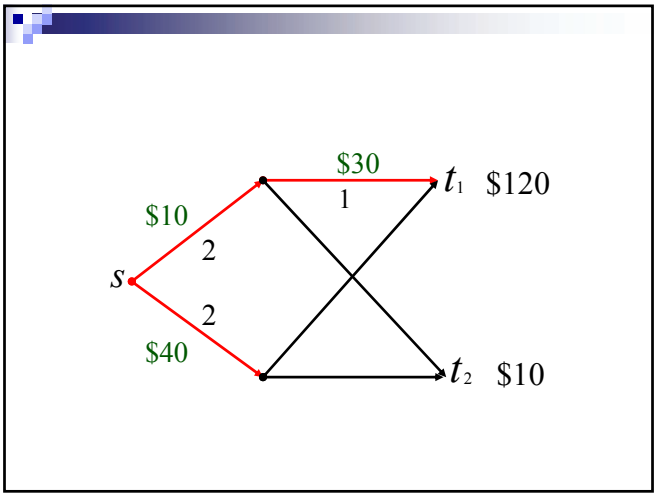


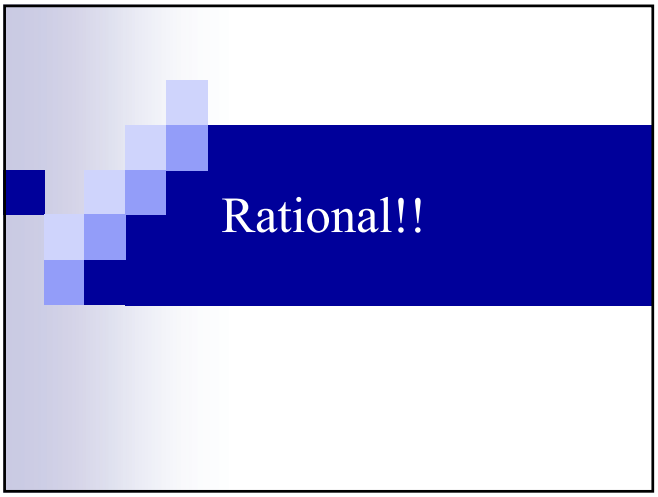

a
t_1
120/p
1
2
s
t
2
10/p
b
t_2
p


a
t_1
120/10
2
1
s
t
10/10 = 1
t_2
2
b
p = 10


a
t_1
120/(10+p)
2
1
s
t
1
t_2
2
b
$p_0 = 10$
p


a
t_1
120/(10+30) = 3
2
1
s
t
1
t_2
2
b
$p_0 = 10$
p = 30


$30
t_1 $120
1
$10
2
s
2
$40
t_2 $10


Rational!!

Max-flow min-cut theorem

Other resource allocation markets

- 2 source-sink pairs (directed/undirected)
- Branchings rooted at sources (agents)
- Spanning trees
- Network coding

Eisenberg-Gale-Type Convex Program

$$\max \sum_i m(i) \log u(i)$$

s.t. packing constraints

Eisenberg-Gale Market

- A market whose equilibrium is captured as an optimal solution to an Eisenberg-Gale-type program

- Megiddo, 1974: Let T = set of sinks (agents)
- For $S \subseteq T$ define $v(S)$ to be the max-flow possible from s to sinks in S.
- Then v is a submodular function, i.e., for

$$A \subseteq B \subseteq T,$$
$$t \notin A,$$
$$v(B+t) - v(B) \leq v(A+t) - v(A)$$

Simpler convex program for single-source market

$$\max \sum_i m(i) \log f(i)$$
$$s.t.$$
$$\forall S \subseteq T : \sum_{i \in S} f(i) \leq v(S)$$
$$\forall i : f(i) \geq 0$$

Submodular Utility Allocation Market

- Any market which has simpler program and v is submodular

Submodular Utility Allocation Market

- Any market which has simpler program and v is submodular
- Theorem: Strongly polynomial algorithm for SUA markets.

Submodular Utility Allocation Market

- Any market which has simpler program and v is submodular
- Theorem: Strongly polynomial algorithm for SUA markets.
- Corollary: Rational!!

- Theorem: Following markets are SUA:
  - 2 source-sink pairs, undirected (Hu, 1963)
  - spanning tree (Nash-William & Tutte, 1961)
  - 2 sources branching (Edmonds, 1967 + JV, 2005)
- 3 sources branching: irrational

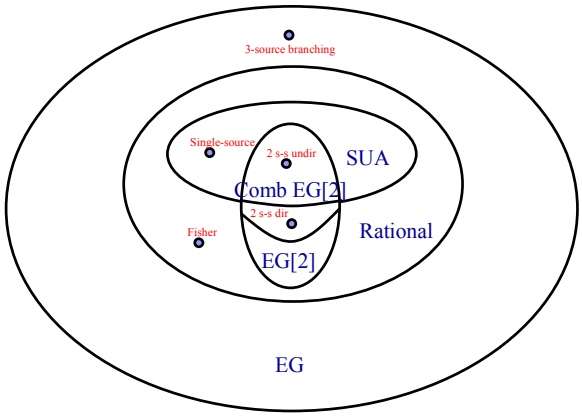
- Theorem: Following markets are SUA:
  - 2 source-sink pairs, undirected (Hu, 1963)
  - spanning tree (Nash-William & Tutte, 1961)
  - 2 sources branching (Edmonds, 1967 + JV, 2005)
- 3 sources branching: irrational
- Open (no max-min thoerems):
  - 2 source-sink pairs, directed
  - 2 sources, network coding

- Theorem: Following markets are SUA:
  - 2 source-sink pairs, undirected (Hu, 1963)
  - spanning tree (Nash-William & Tutte, 1961)
  - 2 sources branching (Edmonds, 1967 + JV)
- 3 sources branching: irrational
- Open (no max-min thoerems):
  - 2 source-sink pairs, directed
  - 2 sources, network coding

Chakrabarty, Devanur & V., 2006

- EG[2]: Eisenberg-Gale markets with 2 agents
- Theorem: EG[2] markets are rational.

- EG[2]: Eisenberg-Gale markets with 2 agents
- Theorem: EG[2] markets are rational.
- Combinatorial EG[2] markets: polytope of feasible utilities can be described via combinatorial LP.
- Theorem: Strongly poly alg for Comb EG[2].



Other properties:

- Efficiency
- Fairness (max-min + min-max fair)
- Competition monotonicity

Open issues

- Strongly poly algs for approximating
  - nonlinear convex programs
  - equilibria
- Insights into congestion control protocols?

Random Sampling Techniques and Approximation of CSP Problems

Marek Karpinski
University of Bonn

(NHC Spring School Lectures, Tokyo, March 1, 2006)

Abstract. We present some recent results and new *sampling* techniques for *absolute* and *relative* approximation of general *Constraint Satisfaction Problems* (CSP). The methods used are threefold and based on: Smooth or Linearized Integer Programs, combinatorial arguments, and special linear algebraic techniques. In particular we apply those techniques to construct *polynomial time approximation schemes (PTASs)* for certain instances of both *MAX*- and *MIN-CSP* including dense and subdense instances and general *metric* and *quasimetric* instances of those problems. In that context we study the generic sample complexity for approximating arbitrary CSP instances and try to establish tight upper bounds for their underlying core-sample sizes. We go also beyond CSP optimization problems and design first PTASs for general *metric* and *quasimetric* size-constraint Partitioning Problems.

Selected References

[1] N. Alon, W. F. de la Vega, R. Kannan and M. Karpinski, *Random Sampling and Approximation of MAX-CSPs*, J. Computer and System Sciences 67 (2003), 212-243.

[2] S. Arora, D. Karger and M. Karpinski, *Polynomial Time Approximation Schemes for Dense Instances of NP-Hard Problems*, J. Computer and System Sciences 58 (1999), 193-210.

[3] W. F. de la Vega, R. Kannan, M. Karpinski and S. Vempala, *Tensor Decomposition and Approximation Schemes for Constraint Satisfaction Problems*, Proc. 27th ACM STOC (2005), 747-754.

[4] W. F. de la Vega and M. Karpinski, *Approximation Complexity of Nondense Instances of MAX-CUT*, in preparation, 2006.

[5] W. F. de la Vega, M. Karpinski and C. Kenyon, *Approximation Schemes for Metric Bisection and Partitioning*, Proc. 15th ACM-SIAM SODA (2004), 506-515.

[6] W. F. de la Vega, M. Karpinski, C. Kenyon and Y. Rabani, *Approximation Schemes for Clustering Problems*, Proc. 35th ACM STOC (2003), 50-58.

[7] M. Karpinski, *Polynomial Time Approximation Schemes for Some Dense Instances of NP-Hard Problems*, Algorithmica 30 (2001), 386-397.

□

APPROXIMATION SCHEMES FOR METRIC BISECTION AND PARTITIONING

MAREK KARPINSKI
UNIVERSITY OF BONN

APPROXIMATING METRIC BISECTION AND RELATED PARTITIONING PROBLEMS

MAREK KARPINSKI
UNIVERSITY OF BONN

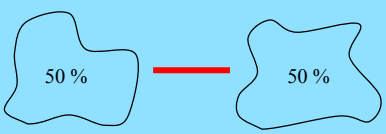
(JOINT WORK WITH W.F. DE LA VEGA AND CLAIRE KENYON)

MOTIVATED BY
"BALANCED" METRIC
AND QUASIMETRIC
CLUSTERING
AND
PARTITIONING
PROBLEMS

MOTIVATED BY
"BALANCED" METRIC
AND QUASIMETRIC
CLUSTERING
AND
PARTITIONING
PROBLEMS

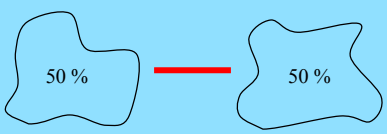
(MINIMIZING HAMILTONIANS)

MIN-BISECTION
OF
GRAPHS,
METRIC SPACES,
SET SYSTEMS, ...



´MIN-CONNECTIVITY´

MIN-BISECTION
OF
GRAPHS,
METRIC SPACES, √
SET SYSTEMS, ...



´MIN-CONNECTIVITY´

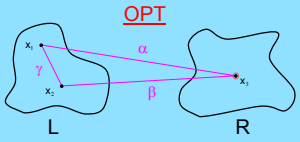
"DENSITY"

⇓

METRIC SITUATIONS:
PARTITIONING
OF
FINITE METRIC SPACES (X,d).

4

METRIC PARTITIONING PROPERTY:



$$W = \sum_{V\times V} d(x,y),$$
$$W_A = \sum_{A\times A} d(x,y).$$

$$Av\_\alpha \geq \frac{1}{2}\cdot Av\_\gamma \Rightarrow \boxed{W_L + W_R \leq 4\cdot OPT}$$

WE HAVE: $W = W_L + W_R + 2\cdot OPT$.
SO, $OPT \geq W/6$.

5

⇓

RED. TO ABSOLUTE (ADD.)
APPROX. TO WITHIN $\varepsilon\cdot W$
FOR EVERY $\varepsilon > 0$.

DENSE METHOD.

6

THE PROBLEM:
COMPUTING MIN/MAX BISECTION
OF A GIVEN METRIC SPACE (V,d).

THE PROBLEM
KNOWN TO BE NP-HARD EVEN
WHEN RESTRICTED
TO (1,2)-METRIC.

7

METRIC SPACE (V,d)
EQUICUT:
PARTITIONING *) (V_1,V_2) OF V
WITH $|V_1| = |V_2|$.

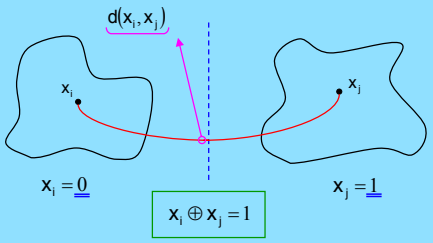
MINIMIZING/
MAXIMIZING

$$\sum_{\{v,w\}\ \text{CUT BY}\ (V_1,V_2)} d(v,w)$$

8

⇓ *)

$$\mathcal{S} = \{ x_i \oplus x_j = 1 \mid \{i,j\} \in E \}$$



9

MIN-CSP

$\oplus$

GLOBAL CONSTRAINT:

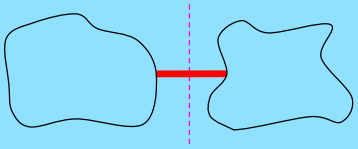
*) $\sum_{i=1}^{n} x_i = n/2$

• MIN-BISECTION

10

GIVEN A FINITE METRIC SPACE (V,d).

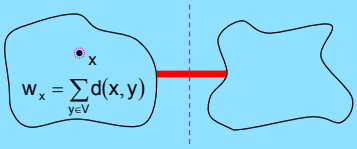
HOW LARGE A VALUE OF AN ARBITRARY EQUICUT ?



11

GIVEN A FINITE METRIC SPACE (V,d).

HOW LARGE A VALUE OF AN ARBITRARY EQUICUT ?



$W = \sum_{x \in V} w_x$

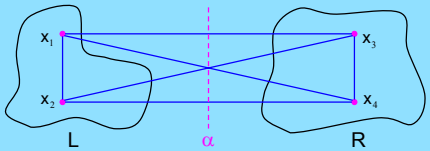
11

$W_L = \sum_{L \times L} d(x,y)$,

$W_R = \sum_{R \times R} d(x,y)$.

12

MIN-BISECTION$((V,d)) \geq W/6$.



$\alpha = d(x_1,x_3) + d(x_1,x_4) + d(x_2,x_3) + d(x_2,x_4)$

$\Downarrow$ (Δ)

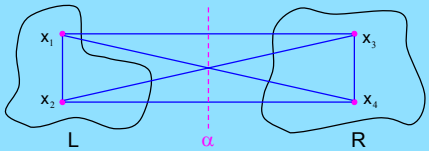
$d(x_1,x_2) + d(x_3,x_4) \leq \alpha$

$W_L + W_R \leq 4$ OPT

$W \leq 6$ OPT

13

MIN-BISECTION$((V,d)) \geq W/6$.



$\alpha = d(x_1,x_3) + d(x_1,x_4) + d(x_2,x_3) + d(x_2,x_4)$

$\Downarrow$ (Δ)

$\beta = d(x_1,x_2) + d(x_3,x_4) \leq \alpha$

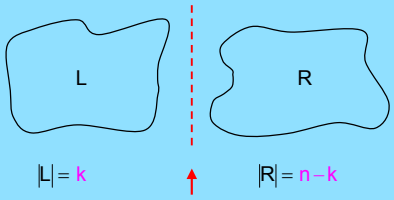
$W_L + W_R \leq 4$ OPT

$W \leq 6$ OPT

$E[\beta] = \frac{4(W_L + W_R)}{n^2}$

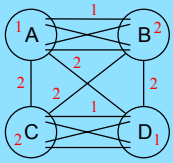
13

MIN-(k, n−k)-PART $((V,d)) \geq \dfrac{W}{2\left(1+\frac{k}{n-k}+\frac{n-k}{k}\right)}$



14

FIRST TRY
(BIASED SAMPLING):
PUTTING $v \in V$ ARBITRARILY
IF $d(v,L) \approx d(v,R)$.

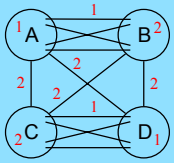


$|A| = |B| = |C| = |D| = n$

$OPT = 6n^2$

15

FIRST TRY ON HOW NOT TO TRY.
(BIASED SAMPLING):
PUTTING $v \in V$ ARBITRARILY
IF $d(v,L) \approx d(v,R)$.

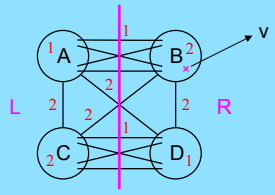


$|A| = |B| = |C| = |D| = n$

$OPT = 6n^2$

15

FIRST TRY ON HOW NOT TO TRY.
(BIASED SAMPLING):
PUTTING $v \in V$ ARBITRARILY
IF $d(v,L) \approx d(v,R)$.



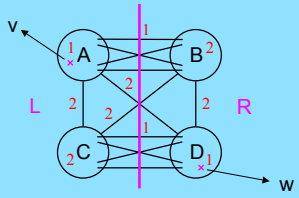
$d(v,L) = 3n$,
$d(v,R) = \underline{4n-2}$ √

$|A| = |B| = |C| = |D| = n$

$OPT = 6n^2$

15

FIRST TRY ON HOW NOT TO TRY.
(BIASED SAMPLING):
PUTTING $v \in V$ ARBITRARILY
IF $d(v,L) \approx d(v,R)$.



$d(v,L) = 3n-1 \approx 3n = d(v,R)$

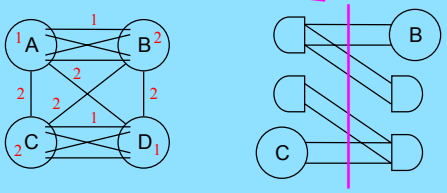
$d(w,R) = 3n-1 \approx 3n = d(w,L)$

$|A| = |B| = |C| = |D| = n$

$OPT = 6n^2$

15

FIRST TRY ON HOW NOT TO TRY.
(BIASED SAMPLING):
PUTTING $v \in V$ ARBITRARILY
IF $d(v,L) \approx d(v,R)$.



$|A| = |B| = |C| = |D| = n$

$OPT = 6n^2$

VALUE $= \underbrace{6n^2 + \frac{1}{2}n^2}$

15

IS
METRIC BISECTION
HARD TO APPROX. ?

16

A PTAS FOR GENERAL METRIC BISECTION:

(VIA LINEARIZED QUADRATIC PROGRAMS)

$$P_{(V,d)} = \frac{1}{2}\sum_{i\neq j} w_{ij}\left(x_i\overbrace{(1-x_j)}+x_j\overbrace{(1-x_i)}\right),$$

$$\sum_i x_i = n/2$$

17

A PTAS FOR GENERAL METRIC BISECTION:

(VIA LINEARIZED QUADRATIC PROGRAMS)

$$P_{(V,d)} = \frac{1}{2}\sum_{i\neq j} w_{ij}\left(x_i\overbrace{(1-x_j)}+x_j\overbrace{(1-x_i)}\right),$$

([AKK95], [FK00]) $\quad \sum_i x_i = n/2$

17

A PTAS FOR GENERAL METRIC BISECTION:

(VIA LINEARIZED QUADRATIC PROGRAMS)

$$P_{(V,d)} = \frac{1}{2}\sum_{i\neq j} w_{ij}\left(x_i\overbrace{(1-x_j)}+x_j\overbrace{(1-x_i)}\right),$$

([AKK95], [FK00]) $\quad \sum_i x_i = n/2$

(SMOOTH, BUT UNBOUND. WEIGHT PR.)

17

A PTAS FOR GENERAL METRIC BISECTION:

(VIA LINEARIZED QUADRATIC PROGRAMS) $\quad r_i = \sum_{j\in N(i)}(1-x_j)$

$$P_{(V,d)} = \frac{1}{2}\sum_{i\neq j} w_{ij}\left(x_i\overbrace{(1-x_j)}+x_j\overbrace{(1-x_i)}\right),$$

([AKK95], [FK00]) $\quad \sum_i x_i = n/2$

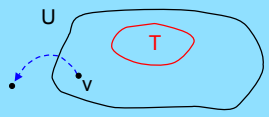
(SMOOTH, BUT UNBOUND. WEIGHT PR.)

17

BASIC METHOD:

METRIC SAMPLER FOR ESTIMATING $d(v,U)$, $U \subseteq V$,

$u \in_R U$ WITH PR. $= \frac{w_u}{W_U}$,



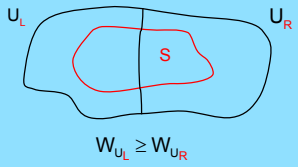
$T = \{U_1,\ldots,U_t\}$

$$\left|d(v,U) - \frac{W_U}{t}\sum_{u\in T}\frac{d(v,u)}{w_u}\right| \leq \varepsilon d(v,U)$$

WITH PR. $\geq 1 - 2e^{-t\varepsilon^2/8}$.

18

PARTITIONING (U_L, U_R) OF U :



$|S| = 3/\varepsilon^2$

$W_{U_L} \geq W_{U_R}$

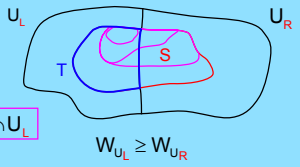
WE HAVE: $|S \cap U_L| \geq 1/\varepsilon^2$

WITH PR. $\geq 1-\varepsilon$

U_L IS UNKNOWN, SO WE

TRY ALL POSSIBLE SUBSETS T OF S .

PARTITIONING (U_L, U_R) OF U :



$T = S \cap U_L$

$|S| = 3/\varepsilon^2$

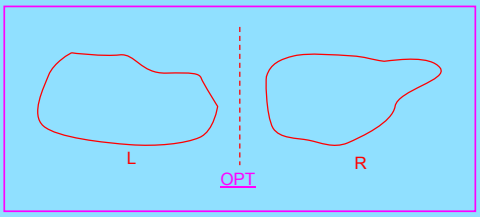
$W_{U_L} \geq W_{U_R}$

WE HAVE: $|S \cap U_L| \geq 1/\varepsilon^2$

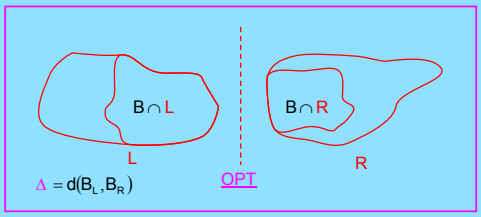
WITH PR. $\geq 1-\varepsilon$

U_L IS UNKNOWN, SO WE

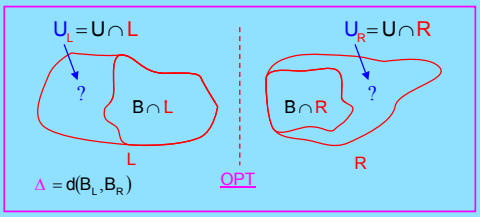
TRY ALL POSSIBLE SUBSETS T OF S .



1. CONSTRUCT A SET B OF 'LARGE' WEIGHT VERTICES $v \in V$ WITH $w_v \geq \varepsilon^2 W/100$; $U = V \setminus B$.
2. TAKE A RANDOM SAMPLE S OF SIZE $3/\varepsilon^2$ (OF U) WITH THE BIAS w_u/W_U .
3. GUESS $B_L = B \cap L$, $B_R = B \cap R$.



1. CONSTRUCT A SET B OF 'LARGE' WEIGHT VERTICES $v \in V$ WITH $w_v \geq \varepsilon^2 W/100$; $U = V \setminus B$.
2. TAKE A RANDOM SAMPLE S OF SIZE $3/\varepsilon^2$ (OF U) WITH THE BIAS w_u/W_U .
3. GUESS $B_L = B \cap L$, $B_R = B \cap R$.



1. CONSTRUCT A SET B OF 'LARGE' WEIGHT VERTICES $v \in V$ WITH $w_v \geq \varepsilon^2 W/100$; $U = V \setminus B$.
2. TAKE A RANDOM SAMPLE S OF SIZE $3/\varepsilon^2$ (OF U) WITH THE BIAS w_u/W_U .
3. GUESS $B_L = B \cap L$, $B_R = B \cap R$.

RANDOM SAMPLE S ON U_L :

GUESS $T = S \cap U_L$.

(ASSUME, $W_{U_L} \geq W_{U_R}$).

CONSTRUCT ESTIMATORS:

$$e_v = \frac{\widehat{W}_{U_L}}{t} \sum_{u \in T} \frac{d(v,u)}{w_u} + d(v, B_L)$$

RANDOM SAMPLE S ON U_L :

($|S| = 3/\varepsilon^2$) ON U.

GUESS $T = S \cap U_L$.

(ASSUME, $W_{U_L} \geq W_{U_R}$).

CONSTRUCT ESTIMATORS:

$$e_v = \frac{\widehat{W}_{U_L}}{t} \sum_{u \in T} \frac{d(v,u)}{w_u} + d(v,B_L)$$

→ LINEAR PROGRAM:

4. CONSTRUCT

LP(U)::

MIN $\sum_{v \in U} x_v e_v + \sum_{v \in U} (1 - x_v) d(v,B_R) + \Delta$

WITH CONSTRAINTS:

$\sum_{u \in U} (1 - x_u) d(u,v) \leq e_v (1 + \varepsilon)$

$\sum_{v \in U} x_v = \frac{n}{2} - |B_L|$, $0 \leq x_v, x_u \leq 1$

RR

COMPUTE OPTIMAL FRACTIONAL SOLUTION (x_v^*), $v \in U$ OF LP(U).

USE RANDOMIZED ROUNDING TO OBTAIN A PARTITION (V_1, V_2) OF U (A SOLUTION (y_v)).

"BALANCE" A PARTITION $(V_1 \cup B_L, V_2 \cup B_R)$ BY MOVING THE SMALLEST WEIGHT VERTICES.

MAIN STEP IN ANALYSIS OF RR:

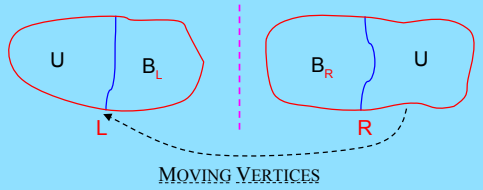
$$E\left[\left|\sum_{v \in U} (x_v^* - y_v)\right|\right] \leq \sqrt{n}/2$$

AND

OPT $\geq c(x_v^*) - 30 \varepsilon W$

W.H.P. (AT LEAST $89/100$)

(PROVED BY METRIC SAMPLER ESTIMATIONS.)



MOVING VERTICES

⇒ RESULTING BISECTION

(A,B) $((y'_v), v \in V)$

CLAIM: (A,B) APPROX. OPT TO WITHIN εW.

RUNNING TIME: $LP(n) \cdot 2^{O(1/\varepsilon^2)}$

COMBINATORIAL VERSION: $n^2 \cdot 2^{O(1/\varepsilon^2)}$

EXTENSION TO METRIC $(n_1, n_2, \ldots, n_K)$ MIN-PARTITIONING

(EXISTENCE OF PTASs)

- RUNNING TIME: $LP(n) \cdot 2^{o(1/\varepsilon^2)}$
- COMBINATORIAL VERSION: $n^2 \cdot 2^{o(1/\varepsilon^2)}$
- EXTENSION TO METRIC $(n_1, n_2, \ldots, n_K)$ MIN-PARTITIONING (EXISTENCE OF PTASS)

26

- EXTENSION TO QUASIMETRIC PARTITIONING AND CLUSTERING

($d(x,z) \le C(d(x,y) + d(y,z))$ FOR SOME POSITIVE CONSTANT C)

- → INCLUDES ALL "POWERS" OF METRIC FUNCTIONS LIKE $\ell_2^2, \ell_p^q, \ldots$ USED IN CLUSTERING APPLICATIONS.

27

IF $d(x,y)$ IS METRIC AND $\alpha > 0$, THEN $(d(x,y))^\alpha$ IS A QUASIMETRIC.

28

- FURTHER RESEARCH:

1. DESIGN THE PTASS (?) FOR "BALANCED" METRIC $(n_1, n_2, \ldots, n_K)$ CLUSTERING (EXTENSION OF [FKKR03]-TECHNIQUE ?)
2. IMPROVE EFFICIENCY

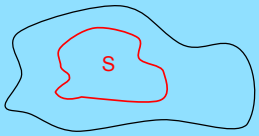
29

- FURTHER RESEARCH:

1. DESIGN THE PTASS (?) FOR "BALANCED" METRIC $(n_1, n_2, \ldots, n_K)$ CLUSTERING (EXTENSION OF [FKKR03]-TECHNIQUE ?)
2. IMPROVE EFFICIENCY (CONSTANT TIME ALGS ?)

29

- RANDOM CORE-SAMPLE COMPLEXITY :



$|S| = \tilde{O}\left(1/\varepsilon^4\right)$ IS ENOUGH FOR MAX-KCSP, K ARBITRARY.

([AFKK02] , [FKKV05])

30

Approximation Algorithms for Facility Location

Jens Vygen

University of Bonn

Outline

Introduction

Uncapacitated Facility Location

Capacitated and Universal Facility Location

Facility Location and Network Design with Service Capacities

Facility Location: Applications

- manufacturing plants
- storage facilities, depots
- warehouses, retail stores
- libraries, fire stations, hospitals
- servers in the internet
- base stations for wireless services
- buffers distributing signals on a chip
- ...

Goal: Optimum service for clients at minimum cost

Common features of facility location problems

- Two sets: clients and potential facilities
  - Each client must be served.
  - A potential facility can be opened or not.
  - Clients can only be served by open facilities.
- Two cost components: facility cost and service cost.
  - Opening a facility involves a certain cost.
  - Serving a client from a facility involves a certain cost.
- The total cost is to be minimized.

But there are many variants

- Can a client's demand be satisfied by more than one facility?
- Are there constraints on the total demand, or total service cost, that a facility can handle?
- Do the service costs satisfy the triangle inequality?
- Are there finitely or infinitely many potential facilities?
- Do the facility costs depend on the total demand served?
- Is it allowed to serve only a subset of clients, and pay for those that are not served?
- Is there a bound on the number of facilities that we can open?
- Does the total service cost of a facility depend on the sum of the distances to its clients, or the length of a shortest tour, or the length of an optimal Steiner tree?
- Are we interested in the sum of all service costs, or rather in the maximum service cost?
- Do we need to serve facilities by second-stage facilities (etc.)?

Example 1: Fermat-Weber Problem

The most prominent example for continuous facility location

Locating a single facility in $\mathbb{R}^n$: Given $a_1, \ldots, a_m \in \mathbb{R}^n$ and weights $w_1, \ldots, w_m \in \mathbb{R}_+$, find $p \in \mathbb{R}^n$ minimizing

$$\sum_{i=1}^{m} w_i ||p - a_i||.$$

- For ℓ_1-norm solvable in linear time (Blum et al. 1973)
- ℓ_2-norm, $n = 2$, $m = 3$: Simple geometric solution (Fermat, Torricelli, Cavalieri, Simpson, Heinen)
- For ℓ_2-norm: construction by ruler and compasses impossible (Bajaj 1988)
- Approximate solution for ℓ_2-norm: Weiszfeld's algorithm (Weiszfeld 1937, Kuhn 1973, Vardi and Zhang 2001, Rautenbach et al. 2004)

Example 2: Uncapacitated Facility Location (UFL)

The most prominent example for discrete facility location

Instance:

- a finite set $\mathcal{D}$ of clients;
- a finite set $\mathcal{F}$ of potential facilities;
- a fixed cost $f_i \in \mathbb{R}_+$ for opening each facility $i \in \mathcal{F}$;
- a service cost $c_{ij} \in \mathbb{R}_+$ for each $i \in \mathcal{F}$ and $j \in \mathcal{D}$.

We look for:

- a subset S of facilities (called *open*) and
- an assignment $\sigma : \mathcal{D} \to S$ of clients to open facilities,
- such that the sum of facility costs and service costs

$$\sum_{i \in S} f_i + \sum_{j \in \mathcal{D}} c_{\sigma(j)j}$$

is minimum.

More examples discussed later

- Capacitated Facility Location
- Universal Facility Location
- Facility Location and Network Design with Service Capacities

These are more general and more realistic in many applications.

Approximation Algorithms: Definition

Let f be a function assigning a real number to each instance. An f-**approximation algorithm** is an algorithm for which a polynomial p exists such that for each instance I:

- the algorithm terminates after at most $p(size(I))$ steps,
- the algorithm computes a feasible solution, and
- the cost of this solution is at most $f(I)$ times the optimum cost of instance I.

f is called the **approximation ratio** or **performance guarantee**. If f is a constant, we have a **(constant-factor) approximation algorithm**.

Uncapacitated Facility Location is as hard as Set Covering

Set Covering: Given a finite set U, a family $\mathcal{S}$ of subsets of U with $\bigcup_{S \in \mathcal{S}} S = U$, and weights $w : \mathcal{S} \to \mathbb{R}_+$, find a set $\mathcal{R} \subseteq \mathcal{S}$ with $\bigcup_{R \in \mathcal{R}} R = U$ with minimum total weight $\sum_{R \in \mathcal{R}} w(R)$.

- No $o(\log |U|)$-approximation algorithm exists unless $P = NP$. (Raz, Safra 1997)
- Greedy algorithm has performance ratio $1 + \ln |U|$. (Chvátal 1979)
- Set Covering is a special case of Uncapacitated Facility Location: define $\mathcal{D} := U$, $\mathcal{F} := \mathcal{S}$, $f_S = w(S)$ for $S \in \mathcal{S}$, $c_{Sj} := 0$ for $j \in S \in \mathcal{S}$ and $c_{Sj} := \infty$ for $j \in U \setminus S$.
- Conversely, the greedy algorithm for Set Covering can be applied to Uncapacitated Facility Location: Set $U := \mathcal{D}$, $\mathcal{S} = \mathcal{F} \times 2^{\mathcal{D}}$, and $w(i, D) := f_i + \sum_{j \in D} c_{ij}$. (Hochbaum 1982)

A natural assumption: metric service costs

Therefore we assume henceforth **metric service costs**:

$$c_{ij} \geq 0$$

and

$$c_{ij} + c_{i'j} + c_{i'j'} \geq c_{ij'}$$

for all $i, i' \in \mathcal{F}$ and $j, j' \in \mathcal{D}$.

Equivalently, we assume c to be a (semi)metric on $\mathcal{D} \cup \mathcal{F}$.

Motivation:

- The general problem is as hard as Set Covering.
- In many practical problems service costs are proportional to geometric distances, or to travel times, and hence are metric.

But: Greedy algorithm has performance guarantee $\Omega(\log n / \log \log n)$ even for metric instances. (Jain et al. 2003)

Integer Linear Programming Formulation

$$\text{minimize} \quad \sum_{i \in \mathcal{F}} f_i y_i + \sum_{i \in \mathcal{F}} \sum_{j \in \mathcal{D}} c_{ij} x_{ij}$$

subject to

$$\begin{aligned}
x_{ij} &\leq y_i && (i \in \mathcal{F}, j \in \mathcal{D}) \\
\sum_{i \in \mathcal{F}} x_{ij} &= 1 && (j \in \mathcal{D}) \\
x_{ij} &\in \{0,1\} && (i \in \mathcal{F}, j \in \mathcal{D}) \\
y_i &\in \{0,1\} && (i \in \mathcal{F})
\end{aligned}$$

(Balinski 1965)

Linear Programming Relaxation

$$\text{minimize} \quad \sum_{i\in\mathcal{F}} f_i y_i + \sum_{i\in\mathcal{F}}\sum_{j\in\mathcal{D}} c_{ij} x_{ij}$$

subject to

$$\begin{aligned} x_{ij} &\le y_i && (i\in\mathcal{F}, j\in\mathcal{D}) \\ \sum_{i\in\mathcal{F}} x_{ij} &= 1 && (j\in\mathcal{D}) \\ x_{ij} &\ge 0 && (i\in\mathcal{F}, j\in\mathcal{D}) \\ y_i &\ge 0 && (i\in\mathcal{F}) \end{aligned}$$

The Dual LP

$$\text{maximize} \quad \sum_{j\in\mathcal{D}} v_j$$

subject to

$$\begin{aligned} v_j - w_{ij} &\le c_{ij} && (i\in\mathcal{F}, j\in\mathcal{D}) \\ \sum_{j\in\mathcal{D}} w_{ij} &\le f_i && (i\in\mathcal{F}) \\ w_{ij} &\ge 0 && (i\in\mathcal{F}, j\in\mathcal{D}) \end{aligned}$$

First Approximation Algorithm: LP Rounding

- Compute an optimum solutions (x^*, y^*) and (v^*, w^*) to the primal and dual LP.
- By complementary slackness, $x^*_{ij} > 0$ implies $v^*_j - w^*_{ij} = c_{ij}$, and thus $c_{ij} \le v^*_j$.
- Let G be the bipartite graph with vertex set $\mathcal{F}\cup\mathcal{D}$ containing an edge $\{i,j\}$ iff $x^*_{ij} > 0$.
- Assign clients to clusters iteratively as follows.
  - In iteration k, let j_k be a client $j\in\mathcal{D}$ not assigned yet and with v^*_j smallest.
  - Create a new cluster containing j_k and those vertices of G that have distance 2 from j_k and are not assigned yet.
  - Continue until all clients are assigned to clusters.
- For each cluster k we choose a neighbour i_k of j_k with f_{i_k} minimum, open i_k, and assign all clients in this cluster to i_k.

Analysis of the LP Rounding Approximation Algorithm

- The service cost for client j in cluster k is at most
$$c_{i_k j} \le c_{ij} + c_{ij_k} + c_{i_k j_k} \le v^*_j + 2v^*_{j_k} \le 3v^*_j,$$
where i is a common neighbour of j and j_k.
- The facility cost f_{i_k} can be bounded by
$$f_{i_k} \le \sum_{i\in\mathcal{F}} x^*_{ij_k} f_i = \sum_{i\in\mathcal{F}:\{i,j_k\}\in E(G)} x^*_{ij_k} f_i \le \sum_{i\in\mathcal{F}:\{i,j_k\}\in E(G)} y^*_i f_i.$$
As j_k and $j_{k'}$ cannot have a common neighbour for $k\neq k'$, the total facility cost is at most $\sum_{i\in\mathcal{F}} y^*_i f_i$.
- The total cost is at most
$$3\sum_{j\in\mathcal{D}} v^*_j + \sum_{i\in\mathcal{F}} y^*_i f_i,$$
which is at most four times the LP value. Hence we get:

Theorem
This is a 4-approximation algorithm for metric UFL.
(Shmoys, Tardos and Aardal 1997)

Better approximation ratios for metric UFL

technique	ratio	RT	authors	year
LP-Rounding	3.16	–	Shmoys, Tardos, Aardal	1997
LP-Rounding+Greedy	2.41	–	Guha, Khuller	1998
LP-Rounding	1.74	–	Chudak	1998
Local Search	5.01	○	Korupolu, Plaxton, Rajaraman	1998
Primal-Dual	3.00	+	Jain, Vazirani	1999
Primal-Dual+Greedy	1.86	+	Charikar, Guha	1999
LP-Rounding+Primal-Dual+Greedy	1.73	–	Charikar, Guha	1999
Local Search	2.42	○	Arya et al.	2001
Primal-Dual	1.61	+	Jain, Mahdian, Saberi	2002
LP-Rounding	1.59	–	Sviridenko	2002
Primal-Dual+Greedy	1.52	+	Mahdian, Ye, Zhang	2002

RT : running time; – : slow; ○ : medium; + : fast

Primal-Dual Algorithm by Jain, Mahdian and Saberi (2002)

Start with $U := \mathcal{D}$ and time $t = 0$. Increase t, maintaining $v_j = t$ for all $j\in U$. Consider the following events:

- $v_j = c_{ij}$, where $j\in U$ and i is not open. Then start to increase w_{ij} at the same rate, in order to maintain $v_j - w_{ij} = c_{ij}$.
- $\sum_{j\in\mathcal{D}} w_{ij} = f_i$. Then open i. For all $j\in\mathcal{D}$ with $w_{ij} > 0$: freeze v_j and set $w_{i'j} := \max\{0, c_{ij} - c_{i'j}\}$ for all $i'\in\mathcal{F}$, and remove j from U.
- $v_j = c_{ij}$, where $j\in U$ and i is open. Then freeze v_j and set $w_{i'j} := \max\{0, c_{ij} - c_{i'j}\}$ for all $i'\in\mathcal{F}$, and remove j from U.

Improvement by Mahdian, Ye and Zhang (2002)

- Multiply all facility costs by 1.504.
- Apply the Jain-Mahdian-Saberi algorithm.
- Now consider the original facility costs.
- Apply greedy augmentation (Charikar, Guha 1999):
  Let g_i be the service cost saving induced by adding facility i.
  Iteratively pick an element $i \in \mathcal{F}$ maximizing $\frac{g_i}{f_i}$ as long as this ratio is greater than 1.

Theorem
This is a 1.52-approximation algorithm for metric UFL.

Lower bound on approximation ratios

Theorem
There is no 1.463*-factor approximation algorithm for metric UFL unless* $P = NP$.

(Sviridenko [unpublished], based on Guha and Khuller [1999] and Feige [1998])

Local Search as a general heuristic

Basic Framework:

- Define a neighbourhood graph on the feasible solutions.
- Start with any feasible solution x.
- If there is a neighbour y of x that is (significantly) better, set $x := y$ and iterate.

Features:

- Quite successful for many practical (hard) problems
- Many variants of local search heuristics
- Typically no guarantees of running time and performance ratio.

Local Search in Combinatorial Optimization

Example: TSP

- Even simple 2-opt typically yields good solutions. Variants (chained Lin-Kernighan) with empirically less than 1% error
- Worst-case running time of k-opt is exponential for all k.
- Performance ratio $\Omega(n^{\frac{1}{2k}})$.

(Applegate et al. 2003, Chandra, Karloff, Tovey 1999)

Example: Facility Location

- Probably the first nontrivial problem where local search led to constant-factor approximation algorithms.
  (Korupolo, Plaxton and Rajamaran 2000, Arya et al. 2004)
- But: for metric UFL worse in theory (maybe also in practice)
- The only known technique to obtain a constant-factor approximation for Capacitated Facility Location.

Capacitated Facility Location (CFL)

Instance:

- finite sets $\mathcal{D}$ (clients) and $\mathcal{F}$ (potential facilities);
- metric service costs $c_{ij} \in \mathbb{R}_+$ for $i \in \mathcal{F}$ and $j \in \mathcal{D}$;
- an opening cost $f_i \in \mathbb{R}_+$ for each facility $i \in \mathcal{F}$;
- a capacity $u_i \in \mathbb{R}_+$ for each facility $i \in \mathcal{F}$;
- a demand d_j for each client $j \in \mathcal{D}$.

We look for:

- a subset S of facilities (called *open*) and
- an assignment $x : S \times \mathcal{D} \to \mathbb{R}_+$ with $\sum_{i \in S} x_{ij} = d_j$ for $j \in \mathcal{D}$ and $\sum_{j \in \mathcal{D}} x_{ij} \leq u_i$ for $i \in S$
- such that the sum of facility costs and service costs

$$\sum_{i \in S} \left(f_i + \sum_{j \in \mathcal{D}} c_{ij} x_{ij} \right)$$

is minimum.

Splittable or Unsplittable Demands

Assume that facilities with given capacities are open.
Task: assign the clients to these facilities, respecting capacity constraints.

- Splittable (or uniform) demand:
  Hitchcock transportation problem.
- Unsplittable non-uniform demand:
  Generalizes bin packing.

Consequence: CFL with unsplittable demands has no approximation algorithm. It is strongly *NP*-hard to distinguish between instances with optimum cost 0 and ∞.

Hence consider splittable demands only.

Universal Facility Location (UniFL)

Instance:

- finite sets $\mathcal{D}$ (clients) and $\mathcal{F}$ (potential facilities);
- metric service costs, i.e. a metric c on $\mathcal{D} \cup \mathcal{F}$;
- a demand $d_j \geq 0$ for each $j \in \mathcal{D}$;
- for each $i \in \mathcal{F}$ a cost function $f_i : \mathbb{R}_+ \to \mathbb{R}_+ \cup \{\infty\}$, left-continuous and non-decreasing.

We look for:

- a function $x : \mathcal{F} \times \mathcal{D} \to \mathbb{R}_+$ with $\sum_{i \in \mathcal{F}} x_{ij} = d_j$ for all $j \in \mathcal{D}$

(a *feasible solution*), such that $c(x) := c_F(x) + c_S(x)$ is minimum, where

$$c_F(x) := \sum_{i \in \mathcal{F}} f_i\left(\sum_{j \in \mathcal{D}} x_{ij}\right) \quad \text{and} \quad c_S(x) := \sum_{i \in \mathcal{F}} \sum_{j \in \mathcal{D}} c_{ij} x_{ij}.$$

UniFL: Facility cost function given by an oracle

$f_i(z)$: cost to install capacity z at facility i.

Given by an oracle that, for each $i \in \mathcal{F}$, $u, c \in \mathbb{R}_+$ and $t \in \mathbb{R}$, computes $f_i(u)$ and

$$\max\{\delta \in \mathbb{R} : u + \delta \geq 0,\ f_i(u + \delta) - f_i(u) + c|\delta| \leq t\}.$$

Proposition

There always exists an optimum solution.

(Mahdian and Pál 2003)

UniFL: important special cases

- Uncapacitated Facility Location: $d_j = 1$ $(j \in \mathcal{D})$, and $f_i(0) = 0$ and $f_i(z) = t_i$ for some $t_i \in \mathbb{R}_+$ and all $z > 0$ $(i \in \mathcal{F})$.
- Capacitated Facility Location: $f_i(0) = 0$, $f_i(z) = t_i$ for $0 < z \leq u_i$ and $f_i(z) = \infty$ for $z > u_i$, where $u_i, t_i \in \mathbb{R}_+$ $(i \in \mathcal{F})$.
- Soft-Capacitated Facility Location: $d_j = 1$ $(j \in \mathcal{D})$, and $f_i(z) = \lceil \frac{z}{u_i} \rceil t_i$ for some $u_i \in \mathbb{N}$, $t_i \in \mathbb{R}_+$ and all $z \geq 0$ $(i \in \mathcal{F})$.

Simple local search operations

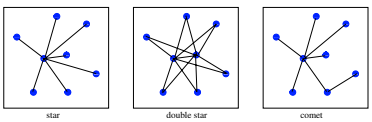
- Add: open a facility (CFL); add capacity to a facility (UniFL).
- Drop: close a facility (CFL).
- Swap: open one facility, close another one (CFL).

Even for CFL with non-uniform demands, these operations do not suffice:
When closing one facility, it may be necessary to open many other ones (and re-assign the demand along the edges of a star).

Previous approximation algorithms for CFL and UniFL

Kuehn, Hamburger 1963	add,drop,swap	CFL	—	
Korupolu, Plaxton, Rajaraman 1998	add,drop,swap	CFL	8.001	uniform capacities
Chudak, Williamson 1999	add,drop,swap	CFL	5.829	uniform capacities
Pál, Tardos, Wexler 2001	add,star	CFL	8.532	
Mahdian, Pál 2003	add,star	UniFL	7.873	
Zhang, Chen, Ye 2004	add,double-star	CFL	5.829	
Garg, Khandekar, Pandit 2005	add,double-star	UniFL	5.829	not polynomial!
Vygen 2005	add,comet	UniFL	6.702	

All based on local search.



Add Operation for UniFL

Let $t \in \mathcal{D}$ and $\delta > 0$. Replace current solution x by an optimum solution y of the transportation problem

$$\min\left\{ c_S(y) \;\middle|\; y : \mathcal{F} \times \mathcal{D} \to \mathbb{R}_+,\ \sum_{i \in \mathcal{F}} y_{ij} = d_j\ (j \in \mathcal{D}),\ \sum_{j \in \mathcal{D}} y_{ij} \leq \sum_{j \in \mathcal{D}} x_{ij}\ (i \in \mathcal{F} \setminus \{t\}),\ \sum_{j \in \mathcal{D}} y_{tj} \leq \sum_{j \in \mathcal{D}} x_{tj} + \delta \right\}.$$

We denote by

$$c^x(t, \delta) := c_S(y) - c_S(x) + f_t\left(\sum_{j \in \mathcal{D}} x_{tj} + \delta\right) - f_t\left(\sum_{j \in \mathcal{D}} x_{tj}\right)$$

the estimated cost (which is at least $c(y) - c(x)$).

How to find a profitable ADD operation

Lemma
Let $\epsilon > 0$ and $t \in \mathcal{F}$. Let x be a feasible solution. Then there is an algorithm with running time $O(|V|^3 \log |V| \epsilon^{-1})$ that

- *finds a $\delta \in \mathbb{R}_+$ with $c^x(t, \delta) \leq -\epsilon c(x)$*
- *or decides that no $\delta \in \mathbb{R}_+$ exists for which $c^x(t, \delta) \leq -2\epsilon c(x)$.*

(Mahdian, Pál 2003)

PIVOT Operation

Let x be a feasible solution. Let A be a graph with $V(A) = \mathcal{F}$ and

$$\delta \in \Delta_A^x := \left\{ \delta \in \mathbb{R}^{\mathcal{F}} \left| \sum_{j \in \mathcal{D}} x_{ij} + \delta_i \geq 0 \text{ for all } i \in \mathcal{F}, \sum_{i \in \mathcal{F}} \delta_i = 0 \right. \right\}.$$

Then we consider the operation $\textsc{Pivot}(A, \delta)$, which means:

- Compute a minimum-cost (w.r.t. c) uncapacitated δ-flow in (A, c).
- W.l.o.g., the edges carrying flow form a forest.
- Scan these edges in topological order, reassigning clients according to flow values.
- This increases the cost of the solution by at most the cost of the flow plus

$$\sum_{i \in \mathcal{F}} f_i \left(\sum_{j \in \mathcal{D}} x_{ij} + \delta_i \right) - f_i \left(\sum_{j \in \mathcal{D}} x_{ij} \right).$$

How to find a profitable PIVOT operation

But: how to choose δ?

- δ cannot be chosen almost optimally for the complete graph (unless $P = NP$).
- We show how to choose δ almost optimally if A is a forest.

Restrict attention to PIVOT on arborescences

Let A be an arborescence with $V(A) = \mathcal{F}$. Let x be a feasible solution.
For $\delta \in \Delta_A^x$ define

$$c_{A,i}^x(\delta) := f_i \left(\sum_{j \in \mathcal{D}} x_{ij} + \delta_i \right) - f_i \left(\sum_{j \in \mathcal{D}} x_{ij} \right) + \left| \sum_{j \in A_i^+} \delta_j \right| c_{ip(i)}$$

for $i \in \mathcal{F}$ and

$$c^x(A, \delta) := \sum_{i \in \mathcal{F}} c_{A,i}^x(\delta).$$

Here A_i^+ denotes the set of vertices reachable from i in A, and $p(i)$ is the predecessor of i.

How to find a profitable PIVOT for an arborescence

Lemma
Let $\epsilon > 0$. There is an algorithm with running time $O(|\mathcal{F}|^4 \epsilon^{-3})$ that

- *finds a $\delta \in \Delta_A^x$ with $c^x(A, \delta) \leq -\epsilon c(x)$*
- *or decides that no $\delta \in \Delta_A^x$ exists for which $c^x(A, \delta) \leq -2\epsilon c(x)$.*

(Vygen 2005)

Bounding the cost of a local optimum

Let $0 < \epsilon < 1$. Let x, x^* be feasible solutions to a given instance.

Lemma
If $c^x(t, \delta) \geq -\frac{\epsilon}{|\mathcal{F}|} c(x)$ for all $t \in \mathcal{F}$ and $\delta \in \mathbb{R}_+$, then

$$c_S(x) \leq c_F(x^*) + c_S(x^*) + \epsilon c(x).$$

(Pál, Tardos and Wexler 2001)

Lemma
If $c^x(A, \delta) \geq -\frac{\epsilon}{|\mathcal{F}|} c(x)$ for all stars and comets A and $\delta \in \Delta_A^x$, then

$$c_F(x) \leq 4c_F(x^*) + 2c_S(x^*) + 2c_S(x) + \epsilon c(x).$$

(Vygen 2005)

The total cost of a local optimum

These two lemmata imply:

Theorem
If $c^x(t,\delta) > -\frac{\epsilon}{8|\mathcal{F}|}c(x)$ *for* $t \in \mathcal{F}$ *and* $\delta \in \mathbb{R}_+$ *and*
$c^x(A,\delta) > -\frac{\epsilon}{8|\mathcal{F}|}c(x)$ *for all stars and comets* A *and* $\delta \in \Delta_A^x$*, then*

$$c(x) \leq (1+\epsilon)(7c_F(x^*) + 5c_S(x^*)).$$

By scaling facility costs by $\frac{\sqrt{41}-5}{2}$ we get a polynomial-time $(\frac{\sqrt{41}+7}{2}+\epsilon)$-approximation algorithm for UniFL.

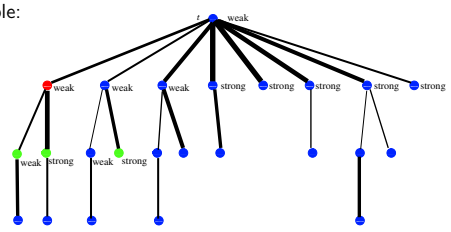
How to bound the facility cost

Let x be the current solution and x^* be an optimum solution.
Let $b(i) := \sum_{j\in\mathcal{D}}(x_{ij} - x^*_{ij})$ $(i \in \mathcal{F})$.
Let y be an optimum transshipment from $S := \{i \in \mathcal{F} : b(i) > 0\}$ to $T := \{i \in \mathcal{F} : b(i) < 0\}$.
W.l.o.g., the edges where y is positive form a forest F.
The cost of y is at most $c_S(x^*) + c_S(x)$.

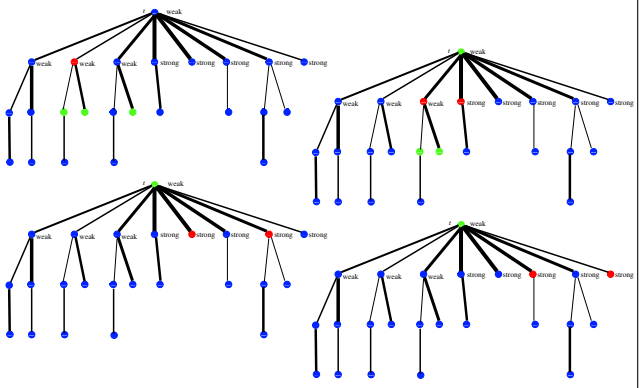
Using F and y, we will define a set of pivot operations on stars and comets, whose total estimated cost is at most $4c_F(x^*) - c_F(x) + 2c_S(x^*) + 2c_S(x)$.
An operation (A,δ) **closes** $s \in S$ if $\delta_s = -b(s) < 0$, and it **opens** $t \in T$ if $0 < \delta_t \leq -b(t)$.
Over all operations to be defined, we will close each $s \in S$ once, open each $t \in T$ at most four times, and use an estimated routing cost at most twice the cost of y.

How to define the operations (1)

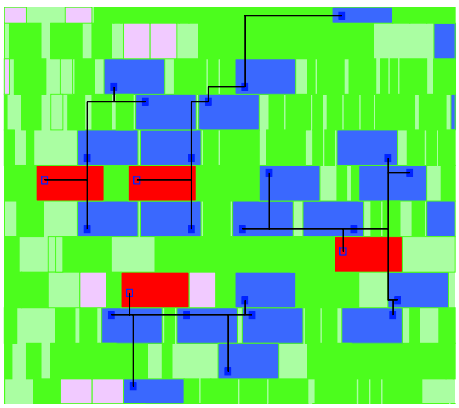
Orient F as a set of arborescences rooted at elements of T.
Call a vertex **weak** if there is more flow on downward than on upward incident arcs, otherwise **strong**. Let $t \in T$.
Open t up to twice if t is strong and up to three times if t is weak.
For each child s of t: Close s once, and open each child of s at most once (if weak) or twice (if strong).
Example:



How to define the operations (2)



VLSI Design: Distributing a signal to several terminals

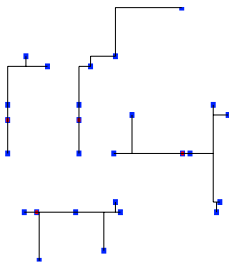


blue: terminals red: facilities

Problem Statement

Instance:

- metric space (V, c),
- finite set $\mathcal{D} \subseteq V$ (terminals/clients),
- demands $d : \mathcal{D} \to \mathbb{R}_+$,
- facility opening cost $f \in \mathbb{R}_+$,
- capacity $u \in \mathbb{R}_+$.



Find a partition $\mathcal{D} = D_1 \dot\cup \cdots \dot\cup D_k$ and Steiner trees T_i for D_i $(i = 1,\ldots,k)$ with

$$c(E(T_i)) + d(D_i) \leq u$$

for $i = 1,\ldots,k$ such that

$$\sum_{i=1}^{k} c(E(T_i)) + kf$$

is minimum.

Complexity Results

(All the following results are by Maßberg and Vygen 2005)

Proposition

- *There is no $(1.5-\epsilon)$-approximation algorithm (for any $\epsilon > 0$) unless $P = NP$.*
- *There is no $(2-\epsilon)$-approximation algorithm (for any $\epsilon > 0$) for any class of metrics where the Steiner tree problem cannot be solved exactly in polynomial time.*
- *There is a 2-approximation algorithm for geometric instances (similar to Arora's approximation scheme for the TSP). However, this is not practically efficient.*

Lower bound: spanning forests

Let F_1 be a minimum spanning tree for $(\mathcal{D}, c)$.
Let $e_1, \ldots, e_{n-1}$ be the edges of F_1 so that $c(e_1) \geq \ldots \geq c(e_{n-1})$.
Set $F_k := F_{k-1} \setminus \{e_{k-1}\}$ for $k = 2, \ldots, n$.

Lemma

F_k is a minimum weight spanning forest in $(\mathcal{D}, c)$ with exactly k components.

Proof.

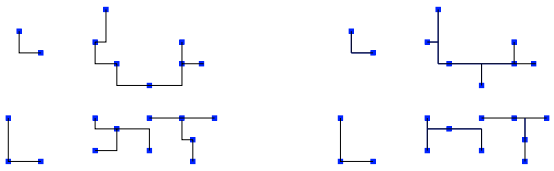
By induction on k. Trivial for $k = 1$. Let $k > 1$.
Let F^* be a minimum weight k-spanning forest.
Let $e \in F_{k-1}$ such that $F^* \cup \{e\}$ is a forest. Then

$$c(F_k) + c(e_{k-1}) = c(F_{k-1}) \leq c(F^*) + c(e) \leq c(F^*) + c(e_{k-1}).$$

□

Lower bound: Steiner forests

A k-Steiner forest is a forest F with $\mathcal{D} \subseteq V(F)$ and exactly k components.



Lemma

$\frac{1}{\alpha}c(F_k)$ is a lower bound for the cost of a minimum weight k-Steiner forest, where α is the Steiner ratio.

Lower bound: number of facilities

Let t' be the smallest integer such that

$$\frac{1}{\alpha}c(F_{t'}) + d(\mathcal{D}) \leq t' \cdot u$$

Lemma

t' is a lower bound for the number of facilities of any solution.

Let t'' be an integer in $\{t', \ldots, n\}$ minimizing

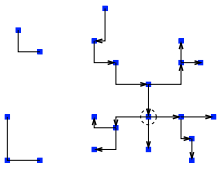
$$\frac{1}{\alpha}c(F_{t''}) + t'' \cdot f.$$

Theorem

$\frac{1}{\alpha}c(F_{t''}) + t'' \cdot f$ is a lower bound for the cost of an optimal solution.

Algorithm A

1. Compute a minimum spanning tree on $(\mathcal{D}, c)$.
2. Compute t'' and spanning forest $F_{t''}$ as above.
3. Split up overloaded components by a bin packing approach.



It can be guaranteed that for each new component at least $\frac{u}{2}$ of load will be removed from the initial forest.

Analysis of Algorithm A

Recall: $\frac{1}{\alpha}c(F_{t''}) + t'' \cdot f$ is a lower bound for the optimum.

We set $L_r := \frac{1}{\alpha}c(F_{t''})$ and $L_f := t'' \cdot f$.

Observe: $L_r + d(\mathcal{D}) \leq \frac{u}{f}L_f$.

The cost of the final solution is at most

$$c(F_{t''}) + t''f + \frac{2}{u}\Big(c(F_{t''}) + d(\mathcal{D})\Big)f$$

$$= \alpha L_r + L_f + \frac{2f}{u}(\alpha L_r + d(\mathcal{D}))$$

$$\leq \alpha L_r + L_f + 2\alpha L_f$$

Theorem

Algorithm A is a $(2\alpha + 1)$-approximation algorithm.

Algorithm B

Define metric c' by $c'(v,w) := \min\{c(v,w), \frac{uf}{u+2f}\}$.

1. Compute a Steiner tree F for $\mathcal{D}$ in (V,c') with some β-approximation algorithm.
2. Remove all edges e of F with $c(e) \geq \frac{uf}{u+2f}$.
3. Split up overloaded components of the remaining forest as in algorithm A.

Theorem

Algorithm B has perfomance ratio 3β.

Using the Robins-Zelikovsky Steiner tree approximation algorithm we get a 4.648-approximation algorithm.

With a more careful analysis of the Robins-Zelikovsky algorithm we can get a 4.099-approximation algorithm in $O(n^{2^{10000}})$ time.

Algorithm C

Define metric c'' by $c''(v,w) := \min\{c(v,w), \frac{uf}{u+f}\}$

1. Compute a tour F for $\mathcal{D}$ in (V,c'') with some γ-approximation algorithm.
2. Remove the longest edge of F.
3. Remove all edges e of F with $c(e) \geq \frac{uf}{u+f}$.
4. Split up overloaded components of the remaining forest as in algorithm A.

Theorem

Algorithm C has perfomance ratio 3γ.

Using Christofides' TSP approximation algorithm we get a 4.5-approximation algorithm in $O(n^3)$ time.

Comparison of the three approximation algorithms

- Algorithm A computes a minimum spanning tree.
- Algorithm B calls the Robins-Zelikovsky algorithm.
- Algorithm C calls Christofides' algorithm.
- Then each algorithm deletes expensive edges and splits up overloaded components.

algorithm	metric	perf.guar.	runtime
A	$(\mathbb{R}^2, \ell_1)$	4	$O(n \log n)$
A	general	5	$O(n^2)$
B	general	4.099	$O(n^{2^{10000}})$
C	general	4.5	$O(n^3)$

Experimental Results

Algorithm A on six real-world instances:

	inst1	inst2	inst3	inst4	inst5	inst6
# terminals	3675	17140	45606	54831	109224	119461
MST length	13.72	60.35	134.24	183.37	260.36	314.48
t'	117	638	1475	2051	3116	3998
L_r	8.21	31.68	63.73	102.80	135.32	181.45
$L_r + L_f$	23.07	112.70	251.06	363.28	531.05	689.19
# facilities	161	947	2171	2922	4156	5525
service cost	12.08	54.23	101.57	159.93	234.34	279.93
total cost	32.52	174.50	377.29	531.03	762.15	981.61
gap (factor)	1.41	1.55	1.59	1.46	1.44	1.42

Reduction of power consumption

Algorithm A on four chips, compared to the previously used heuristic:

chip	Jens	Katrin	Bert	Alex
technology	180nm	130nm	130nm	130nm
# clocktrees	1	3	69	195
total # sinks	3805	137265	40298	189341
largest instance	375	119461	16260	35305
power (W, old)	0.100	0.329	0.306	2.097
power (W, new)	0.088	0.287	0.283	1.946
difference	−11.1%	−12.8%	−7.5%	−7.2%

Some Open Problems

- Close the gap between 1.46 and 1.52 for the approximability of Uncapacitated Facility Location.
- Find better lower bounds than 1.46 for capacitated problems (such as CFL).
- Is Universal Facility Location really harder than CFL?
- Improve the approximation ratio for the problem with service capacities (in $(\mathbb{R}^2, \ell_1)$, with a practically efficient algorithm).
- In some real-world instances, there exists an interval graph on the terminals, and we have to partition this graph into cliques. Is there an approximation algorithm for the resulting problem?
- What other interesting problems combining facility location with network design, or routing, can be approximated?
- What about multi-stage extensions?

Further Reading

- J. Vygen. Approximation Algorithms for Facility Location Problems (lecture notes, with complete proofs and references). Can be downloaded at `http://www.or.uni-bonn.de/~vygen`
- B. Korte, J. Vygen. Combinatorial Optimization: Theory and Algorithms (Chapter 22). Springer, Berlin, third edition 2006. Also available in Japanese!
- J. Maßberg, J. Vygen. Approximation Algorithms for Network Design and Facility Location with Service Capacities. Proceedings of the 8th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems (APPROX 2005); LNCS 3624, Springer, Berlin 2005, pp. 158–169

Algorithms for a Networked World

Magnús M. Halldórsson

Dept. of Computer Science, University of Iceland

Abstract:

The realization of Moore's law has ensured that computing ability has increased dramatically in our times. The law has held not only for processor power and quantity of internal and external memory, but also for the ability to communicate information. The resulting impact on essentially all spheres of society and life has been nothing less than astounding.

Along with increased connectivity, we are also seeing the introduction of a wide range of compact computing entities, possibly mobile and often non-statically connected into largely wireless networks. The explosion of the web and the internet as not only a source of information but also as a resource of computational intelligence, is poised to lead to a dramatic change in the way we view computation. The traditional view of an algorithm with full random access to its input, operating serially on a single processor, is on the retreat.

In comparison, it can be said that changes in CS theory are less dramatic. Surely, each year and each conference brings new topics, new subjects, new treatments, and new directions. Yet, we can also easily detect a great deal of consistency [one that is certainly comforting at times], and a measured pace of change. Are we theoreticians then by nature reactionaries? One of the theses of this talk is that the objects of study in CS theory are inherently fundamental and long-lasting, applying also to this Panopticon world of global and ubiquitous computing.

Yet, we cannot rest on our laurels, with self-satisfied smugness. We must find ways to treat the new means, ways, possibilities and limitations of computation in a systematic framework that continues to provide applied fields with rigorous guidance. The aim of the talk is to discuss some objectives, measures, and paradigms that address the changing nature of computing in a networked world. The concrete examples discussed will mostly relate to problems of coloring and packing, the topics of main focus of the speakers research.

This will by no means be a comprehensive overview – in fact, it is unlikely to be even a balanced introduction. Instead, the hope is that by posing some questions, some members of the audience will eventually be prompted to find some of the answers.

Algorithms for Sequence Manipulation and Related Problems

D. T. Lee

Institute of Information Science
Academia Sinica
&
Department of Computer Science and Information Engineering
National Taiwan University

2006 NHC Spring School Workshop March 2-3, 2006

Combinatorial Optimization

- The combinatorial optimization typically deals with problems of *maximizing* or *minimizing* a function of one or many variables subject to a number of inequality constraints.
- Consider two categories of problems on sequences:
  - Optimization Problems
  - Range Search Problems

Optimization on Sequences

- Given a sequence $A = a_1, a_2, \ldots, a_n$, an optimization problem on sequences is to *maximize* or *minimize* some function, such as: *sum of subsequence*, *density of subsequence*, etc., with some constraints, such as: length, weight, etc.

Range Search Problems

- A *range* (*query*) *search problem* is typically to *report* the subset S' to *count* the total number of elements of the subset S' of a set S contained in a query range Q subject to certain conditions.

Range Search on Sequences

- Given a sequence A = $a_1, a_2, \ldots, a_n$, and a range query, we want to *report* or *count* some subsequences of A contained in the query range satisfying certain conditions.

5/92

Focus of Talk

- Focus on the optimization and range search problems on sequences, give a survey and present efficient problem-solving techniques for them.
- Many elegant and sometimes sophisticated techniques have been developed and applied to these problems in the past decade.
- Key: To exploit the combinatorial nature of these problems to obtain simpler and faster algorithms or algorithms with faster query time for range search problems.

6/92

Notations 1

- Given two positive real numbers ℓ and u with $\ell \leq u$, we say A(i, j) = $a_i, a_{i+1}, \ldots, a_j$ of A is **feasible** if $\ell \leq w(i, j) = j\text{-}i+1 \leq u$.
- **rank** r(x, S) of an element x in a set S: the number of elements in S no greater than x, i.e., $r(x, S) = |\{y \mid y \in S, y \leq x\}|$.

8/92

Notations 2

- Let A be a **sequence** of n real numbers $a_1, a_2, \ldots, a_n$.
- **segment** of A(i, j) is a *consecutive* subsequence $a_i, a_{i+1}, \ldots, a_j$
- **width** w(i, j) of A(i, j): j - i + 1
- **density** d(i, j) of A(i, j): $(a_i + a_{i+1} + \ldots + a_j)/w(i, j)$
- **sum** s(i, j) of A(i, j): $a_i + a_{i+1} + \ldots + a_j$.

7/92

Optimization Problems on Sequences

- Sum of subsequence,
- Density of subsequence
- Selection of subsequence
- subject to constraints on length, or weight of subsequences.

9/92

Max-Sum Segment Problem

- **Input:**
  - a sequence A of n real numbers $a_1, a_2, \ldots, a_n$
  - two nonnegative real numbers ℓ, u with $\ell \leq u$.
- **Output:**
  - a segment A(i*, j*) with maximum sum over all $O((u-\ell)\, n)$ feasible segments such that s(i*, j*) = max{ s(i, j) | A(i, j) is feasible.}

10/92

Example – Max-Sum Segment

- **Input:**
  - A = 3, -4, -2, 5, 6
  - $\ell = 2$, $u = 4$
- **Output: s(4, 5) = 11**

- Sums of all feasible segments:
  s(1, 2) = -1, s(1, 3) = -3, s(1, 4) = 2
  s(2, 3) = -6, s(2, 4) = -1, s(2, 5) = 5
  s(3, 4) = 3, s(3, 5) = 9
  s(4, 5) = 11

11/92

Application: Max-Sum Segment

- Finding the most rich GC-rich region in a DNA sequence can be cast as a maximum-sum segment problem.
- Input sequence A corresponds to a given DNA sequence, where $a_i = 1$ if the corresponding nucleotide in the DNA sequence is G or C, $a_i = 0$ otherwise.
- Output feasible segment corresponds to the GC-rich region of the given DNA sequence.

12/92

Applications in Bioinformatics

- Useful applications in bioinformatics including
  - finding tandem repeats, which are commonly used to map disease genes
  - locating DNA segments with rich CG content is a key step in gene finding and promoter prediction
  - low complexity filter, which is most commonly applied in sequence database search.

13/92

Max-Sum Segment Problem

- **Prior Results:**
  - O(n) time for the special case $\ell = 1$, $u = n$ Gries [Science of Computer Programming'82]
  - O(n) time for the special case $\ell = 1$, $u = n$ Bentely. [Commun. ACM '84]
  - O(n) time. Lin, Jiang and Chao. [Journal of Computer and System Sciences '02]
  - O(n) time. Fan, Lee, Lu, Tsou, Wang, and Yao. [CIAA '03]

14/92

Technique Used – Lin *et al.*

- Lin, Jiang and Chao gave an O(n) time algorithm based on a clever technique called *left-negative decomposition.*

  J. of Computer and System Sciences '02

15/92

Lin *et al.* Algorithm ['02]

- A sequence A= $a_1, a_2, \ldots, a_n$ is ***left-negative*** iff the sum of each proper prefix $a_1, a_2, \ldots, a_i$ is negative or zero for all $1 \le i \le n-1$.
- A partition of the sequence A= $A_1A_2 \ldots A_k$ is ***minimal left-negative*** if each A_i, $1 \le i \le k$, is l*eft-negative*, and, for each $1 \le i \le k-1$, the sum of A_i is positive.

16/92

Example – left-negative sequence

- The sequence -4, 1, -2, 3 is left-negative.
- The sequence -5, 3, 4, -1, 2, -6 is not left-negative.
- The partition (-5, 3, 4), (-1, 2), (-6) is minimal left-negative.
- For every suffix of a sequence we can find a minimal left-negative partition.
- (3)(4)(-1,2)(-6); (4)(-1,2)(-6); (-1,2)(-6), (2)(-6); (-6) are all possible minimal left-negative partitions

Example – left-negative sequence

- Lemma: Every sequence of real numbers can be uniquely partitioned in linear time into blocks of minimal left-negative segments, and the right end of a maximum sum segment must be at a block boundary.
- (-5, (3), (4)), (-1, (2)), (-6)
- Prefix sum sequence S= 0, -5, -2, 2, 1, 3, -3
- Sum(1st) = 2, Sum(2nd) = 1, Sum(3rd) = -6
- Max-Sum segment is a_2, a_3 a_4 a_5 of sum $s_5 - s_1 = 8$

Max-Density Segment Problem

- **Input:**
  - a sequence A of n real numbers a_1, a_2, …, a_n
  - two nonnegative real numbers ℓ, u with $\ell \le u$.
- **Output:**
  - a segment A(i*, j*) with maximum density over all O((*u*-ℓ) n) feasible segments such that d(i*, j*) = max{ d(i, j) | A(i, j) is feasible.}

Example – Max-Density Segment

- **Input:**
  - A = 3, -4, -2, 5, 6
  - ℓ = 2, u = 4
- **Output: d(4, 5) = 11/2**

- Densities of all feasible segments:
  d(1, 2) = -1/2, d(1, 3) = -1, d(1, 4) = 1/2
  d(2, 3) = -3, d(2, 4) = -1/3, d(2, 5) = 5/4
  d(3, 4) = 3/2, d(3, 5) = 3
  d(4, 5) = 11/2

Application: Max-Density Segment

- Finding the segment with the largest GC-ratio in a DNA sequence can be cast as a maximum-density segment problem.
- Input sequence A corresponds to the given DNA sequence, where $a_i = 1$ if the corresponding nucleotide G or C; and $a_i = 0$ otherwise.
- Output feasible segment corresponds to the region with the largest GC-ratio.

21/92

Application in Bioinformatics

- Maximum-Density Segment Problem arises from the investigation of non-uniformity of nucleotide composition within genomic sequences, which was first revealed through thermal melting and gradient centrifugation experiments.
- Researchers observed that the compositional heterogeneity is highly correlated to the **GC content** of the genomic sequences, and this motivates finding the segment with the largest GC-ratio.

22/92

Max-Density Segment Problem

- **Prior Results:**
  - O(n ℓ) time algorithm for the special case u = n Huang. [Computer Appl. in the Biosciences '94]
  - O(n log ℓ) time algorithm for the special case u = n Lin, Jiang, and Chao. [J. Comp. and Syst. Sci. '02]
  - O(n log (u-ℓ)) time algorithm. Goldwasser, Kao, and Lu. [J. of Comp. and Syst. Sci. '03]
  - O(n) time algorithm. Kim. [IPL '03]– has a flaw
  - O(n) time algorithm. Chung and Lu. [SICOMP '04]

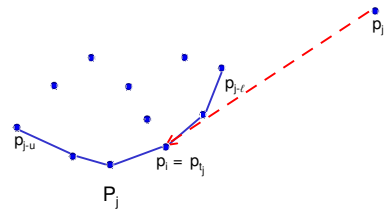
23/92

Technique Used – Kim. IPL '03 3

- Construct a point set in the plane $P = \{p_k \mid p_k = (k, s_k), k = 1, 2, \ldots, n$, where $s_k = a_1+a_2+\ldots+a_k$ is the prefix sum of sequence A.
- Construct lower hull of $P_j = \{p_{j-\ell}, p_{j-\ell+1}, \ldots, p_{j-u}\}$ and find tangent segment t_j from p_j to P_j.
- The tangent segment of the maximum slope is the maximum-density segment of A.

24/92

Technique-- Kim. IPL '03 2



$$\frac{p_j - p_i}{j-i} = \frac{a_j + a_{j-1} + \ldots + a_i}{j-i} = d(i+1, j)$$

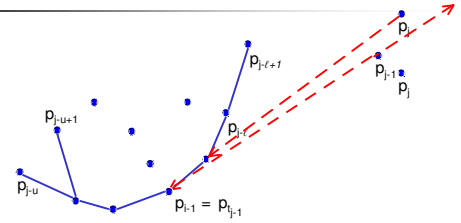
25/92

Technique– Chung & Lu

- Based on a clever observation that d(x, y), d(y+1, z) and d(x, z) with $x \le y < z$ are related as follows:
  - $d(x, y) \le d(y+1, z)$
  - $\Leftrightarrow d(x, y) \le d(x, z)$
  - $\Leftrightarrow d(x, z) \le d(y+1, z)$
- Chung and Lu, SIAM Journal on Computing '04.

27/92

Technique-- Kim. IPL '03 1



For each j,
(1) we need to do tangent query from p_j
If p_j lower than the line $p_{t_{j-1}}p_{j-1}$ we do nothing
If p_j higher than the line $p_{t_{j-1}}p_{j-1}$ we do tangent query from p_j
(2) we then delete p_{j-u} from P_j and insert $p_{j-\ell+1}$ into P_j to obtain P_{j+1}

26/92

k-Maximum Sums Problem

- **Input:**
  - a sequence A of n real numbers $a_1, a_2, \ldots, a_n$
  - two nonnegative real numbers ℓ, u with $\ell \le u$
  - a positive integer k.
- **Output:**
  - k feasible segments such that their sums are the k largest over all $O((u-\ell)\, n)$ feasible segments.

28/92

Example – k-Max. Sums

- **Input:**
  - A = 3, -4, -2, 5, 6
  - $\ell = 2$, $u = 4$
  - k = 3
- **Output: s(4, 5) = 11, s(3, 5) = 9 , s(2, 5) = 5**

- Sums of all feasible segments:
  s(1, 2) = -1, s(1, 3) = -3, s(1, 4) = 2
  s(2, 3) = -6, s(2, 4) = -1, s(2, 5) = 5
  s(3, 4) = 3, s(3, 5) = 9
  s(4, 5) = 11

k-Maximum Sums Problem

- **Prior Results:** (special case $\ell = 1$, $u = n$)
  - O(kn) time algorithm for the Bae and Takaoka. [Int'l Symp. on Parallel Architectures, Algorithms and Networks '04]
  - O(min {k + n $\log^2$n, nk$^{1/2}$) time algorithm Bengtsson and Chen. ISAAC 2004
  - O(n + k log(min{n, k})) time algorithm Cheng, Chen, Tien, and Chao. ISAAC 2005

Technique Used – Cheng *et al.*

- Prune-and-Search technique
  - There are n subsequences A(1, n), A(2, n), …, A(n, n) of A, where A(i, n) = a_i, a_{i+1}, …, a_n
  - At iteration i, it prunes away a fraction (½) of the n/2^{i-1} subsequences, so that no more than 2^ik/n segments are in the set of feasible k-maximum sum segments.
- Cheng, Chen, Tien, and Chao. ISAAC 2005.

Random Sampling Technique

- **Recent Result:**
  - We obtain an O(n log (u - ℓ) + h) time randomized algorithm based on random sampling technique. Lin and Lee. ISAAC 2005
- Solve the kth-Sum Selection Problem using random sampling technique.
- After finding the kth largest feasible segment s*, we can find k largest sum segments by sum range search algorithm, introduced later.

k-Maximum Densities Problem

- **Input:**
  - a sequence A of n real numbers $a_1, a_2, \ldots, a_n$
  - two nonnegative real numbers ℓ, u with $\ell \le u$
  - a positive integer k.
- **Output:**
  - the k segments such that their densities are the k largest over all $O((u-\ell)\, n)$ feasible segments.

33/92

Example – k-Max Densities

- **Input:**
  - A = 3, -4, -2, 5, 6
  - $\ell = 2$, $u = 4$
  - k = 3
- **Output: d(4, 5) = 11/2, d(3, 5) = 3, d(2, 5) = 5/4**

- Densities of all feasible segments:
  d(1, 2) = -1/2, d(1, 3) = -1, d(1, 4) = 1/2
  d(2, 3) = -3, d(2, 4) = -1/3, d(2, 5) = 5/4
  d(3, 4) = 3/2, d(3, 5) = 3
  d(4, 5) = 11/2

34/92

Random Sampling Technique

- **Recent Result:**
  - We obtain an $O(n \log (u - \ell) + h)$ time randomized algorithm based on random sampling technique.
- Solve the kth-Density Selection Problem using random sampling technique.
- After finding the kth largest density d*, we can find k largest density segments by density range search algorithm, introduced later.

35/92

k^{th}-Sum Selection Problem

- **Input:**
  - a sequence A of n real numbers $a_1, a_2, \ldots, a_n$
  - two nonnegative real numbers ℓ, u with $\ell \le u$
  - a positive integer k.
- **Output:**
  - the segment A(i*, j*) over all $O((u-\ell)\, n)$ feasible segments such that the rank of the sum s(i*, j*) in the set of sums of possible feasible segments is k.

36/92

k^{th}-Sum Selection Problem

- **Prior Result:**
  - O(n log n) time randomized algorithm for the special case $\ell = 1$, $u = n$ based on random sampling technique by Lin and Lee. ISAAC 2005
- **New results:**
  - We obtain an O(n log $(u - \ell)$) time randomized algorithm based on random sampling technique.

37/92

Technique – Random Sampling

- Contract initial interval $[s_l, s_r] = (-\infty, \infty)$ into a smaller subinterval $[s_l', s_r']$ such that it contains the kth largest feasible segment s* and the subinterval $[s_l', s_r']$ contains at most $O(n^2/n^{1/2}) = O(n^{3/2})$ feasible segments.
- Contract the interval $[s_l', s_r']$ into a smaller subinterval $[s_l'', s_r'']$ such that it contains not only s* but also at most $O(n^{3/2}/n^{1/2}) = O(n)$ feasible segments.
- If both steps are successful, output all the segments in $[s_l'', s_r'']$ and find the solution segment with an appropriate rank, whose sum is s*, by using any *standard selection* algorithm.

38/92

k^{th}-Density Selection Problem

- **Input:**
  - a sequence A of n real numbers $a_1, a_2, \ldots, a_n$
  - two nonnegative real numbers ℓ, u with $\ell \le u$
  - a positive integer k.
- **Output:**
  - the segment A(i*, j*) over all O($(u-\ell)$ n) feasible segments such that the rank of the density d(i*, j*) in the set of densities of possible feasible segments is k.

39/92

Sum Finding Problem

- **Input:**
  - a sequence A of n real numbers $a_1, a_2, \ldots, a_n$
  - two nonnegative real numbers ℓ, u with $\ell \le u$
  - a real number s*
- **Output:**
  - the segment over all O($(u-\ell)$ n) feasible segments such that its sum s(i*, j*) is closest to s*

40/92

Example – Sum Finding

- **Input:**
  - A = 3, -4, -2, 5, 6
  - $\ell = 2$, $u = 4$
  - s* = 1.5
- **Output: s(1, 4) = 2**

- Sums of all feasible segments:
  s(1, 2) = -1, s(1, 3) = -3, s(1, 4) = 2
  s(2, 3) = -6, s(2, 4) = -1, s(2, 5) = 5
  s(3, 4) = 3, s(3, 5) = 9
  s(4, 5) = 11

Open

Example – Density Finding

- **Input:**
  - A = 3, -4, -2, 5, 6
  - $\ell = 2$, $u = 4$
  - d* = 1.5
- **Output: d(3, 4) = 3/2**

- Densities of all feasible segments:
  d(1, 2) = -1/2, d(1, 3) = -1, d(1, 4) = 1/2
  d(2, 3) = -3, d(2, 4) = -1/3, d(2, 5) = 5/4
  d(3, 4) = 3/2, d(3, 5) = 3
  d(4, 5) = 11/2

Density Finding Problem

- **Input:**
  - a sequence A of n real numbers $a_1, a_2, \ldots, a_n$
  - two nonnegative real numbers ℓ, u with $\ell \le u$
  - a real number d*
- **Output:**
  - the segment over all $O((u-\ell)\, n)$ feasible segments such that its density d(i*, j*) is closest to d*

Density Finding Problem

- **Result to date:**
  - We obtain an $O(n \log^2 (u-\ell))$ time and $O(n \log (u-\ell))$ space algorithm based on maintaining a data structure of the left branch of an upper hull.

Technique – maintaining a data structure of left branch of upper hull 3

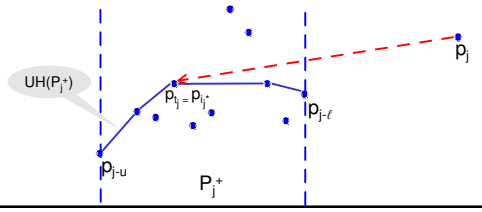
- We first reduce this problem to a geometric slope finding problem
- Input:
  - Given a set of points $P = \{p_0, p_1, \ldots, p_n\}$ in R^2, and
  - two integers ℓ, u
- Output:
  - a feasible line segment s(i, j) that minimizes the slope m(i, j), where $m(i, j) \geq 0$.

Technique – maintaining a data structure of left branch of upper hull 2

- Let $x_i = a_1 + \ldots + a_i$, i=1, 2, …, n, and let $x_0 = 0$.
- Let $P = \{x_0, x_1, \ldots, x_n\}$.
- Let $P_j = \{x_{j-u}, x_{j-u+1}, \ldots, x_{j-\ell}\}$.
- Let $P_j^+ = \{p_i \in P_j \mid m(i, j) \geq 0\}$.
- Let p_{t_j} be the tangent point of the upper hull $UH(P_j^+)$ from p_j.
- Lemma: p_{t_j} must be a hull point on the left branch of the upper hull $UH(P_j^+)$.

Technique – maintaining a data structure of left branch of upper hull 1

- $m(t_j, j) = \min \{m(i, j) \mid p_i \in P_j^+\} = m(i_j^*, j)$.
- Find $m(t_j, j)$ for each j and take the minimum.



Generalization to Higher Dimen.

- We can generalize the optimization problems on sequences to higher dimensional space.
- Given an m×n matrix, the *maximum subarray problem* is to find a rectangular subarray with the largest possible sum among all such subarrays.
- For example, the 2D maximum-sum segment problem with $\ell = 1$, $u = n$, referred to as *maximum sum subarray* problem, has many applications in graphics and data mining.

Range Search Problems

- Single-shot mode query: O(n) query time is optimal for this query mode.
- Repetitive mode query: Preprocessing allowed, and obtaining an o(n) time query time is the goal. A trade-off between storage and query time is expected.

Sum Range Search Problem single-shot mode

- **Input:**
  - a sequence A of n real numbers $a_1, a_2, \ldots, a_n$
  - two nonnegative real numbers ℓ, u with $\ell \le u$
  - two real numbers s_l, s_r with $s_l \le s_r$.
- **Output:**
  - the segments over all O((u-ℓ) n) feasible segments such that their sums are between s_l and s_r.

Sum Range Search Problem single-shot mode

- **Related work :**
  - O(n log (u-ℓ) + h) time algorithm, where h is the output size. Lin and Lee. ISAAC 2005
  - Straightforward
    - Ordinary binary search trees (order-statistic tree)

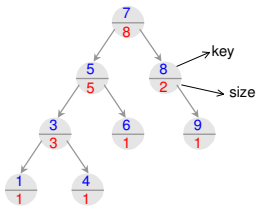
Technique – maintaining an order-statistic tree 2

- **prefix sum** x_i of the sequence A, $x_i = a_1 + \ldots + a_i$, i=1, 2, …, n, and let $x_0 = 0$.
- Let $P = \{x_0, x_1, \ldots, x_n\}$.
- Let $P_j = \{x_{j-u}, x_{j-u+1}, \ldots, x_{j-\ell}\}$.
- Maintain an **order-statistic tree** $T(P_j)$ on P_j. by scanning the sequence of prefix sums.

Order-Statistic Tree

- An order-statistic tree is a balanced binary search tree with size information, size[z], stored in each node z of the tree, and containing the total number of nodes in the subtree rooted at z.
- For an internal node z, size[z] = size[left[z]] + size[right[z]] + 1
- For a leaf node z, size[z]= 1.

Order-Statistic Tree: Example



Technique – maintaining an order-statistic tree 1

- To solve this problem, it suffices to iterate on each j finding all $x_i \in P_j$ such that $s_l \le x_j - x_i \le s_r$.
- At each iteration j,
  - maintain $T(P_j)$ dynamically such that we can find all the numbers $x_i \in [x_j - s_r, x_j - s_l]$ by binary search in $O(\log (u-\ell) + h_j)$ time
  - delete x_{j-u} and insert $x_{j-\ell+1}$ into $T(P_j)$ to obtain $T(P_{j+1})$ in $O(\log (u-\ell))$ time.

Basic Lemmas

- The rank $r(x, P_j) = |\{y \mid y \in P_j, y \le x\}|$ of any x not necessarily in P_j can be determined using $T(P_j)$ in O(log n) time.
- An element in $T(P_j)$ of a given rank can be found in O(log n) time.
- Both insertion and deletion operations in $T(P_j)$ can be done in O(log n) time.

Density Range Search Problem single-shot mode

- **Input:**
  - a sequence A of n real numbers $a_1, a_2, \ldots, a_n$
  - two nonnegative real numbers ℓ, u with $\ell \le u$
  - two real numbers d_l, d_r with $d_l \le d_r$.
- **Output:**
  - the segments over all $O((u-\ell)\, n)$ feasible segments such that their densities are between d_l and d_r

Density Range Search Problem single-shot mode

- **Recent result:**
  - We obtain an $O(n \log (u-\ell) + h)$ time algorithm, where h is the output size.
  - Use *problem transformation*
  - Maintain a ***priority search tree*** $T(P_j)$ on P_j.

Problem Transformation

- Transform the **Density Range** Search Problem into a geometric slope range query problem as follows.
- Consider the point set $P = \{p_0, p_2, ..., p_n\}$ in R^2 based on the prefix sums of the sequence A, where $p_i = (x_i, y_i) = (i, a_1 + a_2 + \ldots + a_i)$, i=1, 2, ..., n and $p_0 = (0, 0)$.
- Slope of segment connecting p_i and p_j corresponds to density d(i+1,j)

Geometric **Slope Range** Search

- **Input:**
  - A point set $P = \{p_0, p_2, ..., p_n\}$ in R^2,
  - two integers ℓ, u
  - two real numbers d_l, d_r,
- **Output:**
  - find all feasible line segments s(i, j) such that their densities m(i, j) satisfying $d_l \le m(i, j) \le d_r$.

Point-Line Duality Transform

- We can further transform this *geometric* ***slope range*** *search problem* into its dual problem, by mapping a *point* $p_i = (x_i, y_i)$ into its *dual line* ℓ_i: $y = x_i x - y_i$.
- For any two points p_i, and p_j, their corresponding dual lines ℓ_i, ℓ_j will intersect at the x-coordinate $x_{ij} = (y_j - y_i)/(x_j - x_i)$ which equals m(i, j).

61/92

Dual of **Geometric Slope** Range Search– Intersection Search

- **Input:**
  - a set of lines $L = \{\ell_0, \ell_1, ..., \ell_n\}$ in R^2, where each line ℓ_i: $y = x_i x - y_i$,
  - two integers ℓ, u
  - two real numbers d_l, d_r,
- **Output:**
  - find all intersection points $p_{ij}=(x_{ij}, y_{ij})$ of two feasible *dual lines* ℓ_i, ℓ_j such that their abscissae x_{ij} lie in $[d_l, d_r]$.

62/92

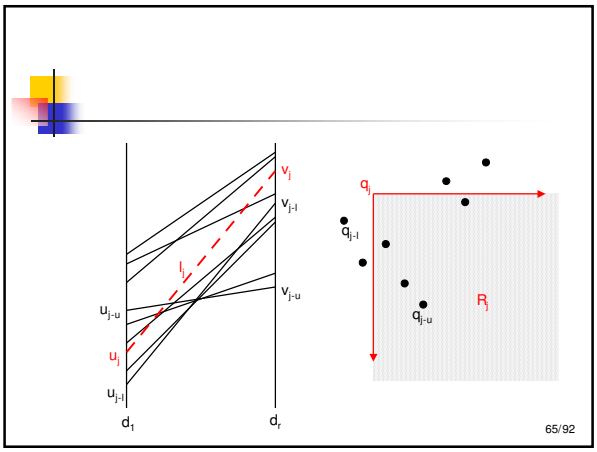
Intercept to Point Transform

- Let $u_k = x_k d_l - y_k$ denote the *y*-intercept of line ℓ_k at d_l and $v_k = x_k d_r - y_k$ .the *y*-intercept of line ℓ_k at d_r
- Denote $Q = \{q_0, q_1, ..., q_n\}$, where $q_k = (u_k, v_k) = (x_k d_l - y_k, x_k d_r - y_k)$.
- Let $Q_j = \{q_{j-u}, q_{j-u+1}, ..., q_{j-l}\} = Q_{j-u, j-l}$

63/92

- By the monotonically increasing property of the slopes of lines in L, i.e., the slope of ℓ_j is larger than each $\ell_i \in L_j$ for $i < j$, any dual line ℓ_i in L_j intersects ℓ_j in $[d_l, d_r]$ iff $u_i \geq u_j$ and $v_i \leq v_j$.

64/92



Algorithm for Intersection Search

- The *Intersection Search* problem is now equivalent to an orthogonal range search of the form $R_j = [u_j, \infty) \times (-\infty, v_j]$ to report all the points of Q_j which lie in R_j for each $j = 1, 2, \ldots, n$.
- We use a data structure called *priority search tree* to support the above orthogonal range queries in logarithmic time.

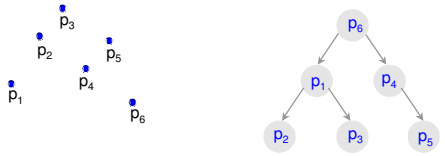
Priority Search Tree - Definition

- A *priority search tree* for a set of ordered pairs $\{(x_i, y_i) \mid i = 1, 2, \ldots, n\}$ is a hybrid of a heap (say in y) and a balanced binary search tree (say in x) used for orthogonal range query where at least one of sides of the query range is unbounded.

Priority Search Tree - Construction

- The priority search tree $T(\{P_i\})$ can be constructed in $O(n \log n)$ time using any balanced binary search tree as follows:
  - For a given set S of points P_i, if S is empty, then the priority search tree T(S) is null.
  - Otherwise, let point P_i be the point in S with the smallest y-coordinate and x_m be the median of the x-coordinates of the remaining point set $S\backslash\{P_i\}$. Let $S_l = \{ P_k (x_k, y_k) \in S\backslash\{P_i\} \mid x_k \le x_m \}$ and $S_r = \{ P_k (x_k, y_k) \in S\backslash\{P_i\} \mid x_k > x_m \}$.
  - The root of T(S) contains P_j (and key x_m) and its left child is $T(S_l)$ and right child is $T(S_r)$.

Priority Search Tree: Example



69/92

Sum Range Search Problem repetitive mode -- definition

- **Input:**
  - a sequence A of n real numbers $a_1, a_2, \ldots, a_n$.
  - two nonnegative real numbers ℓ, u with $\ell \le u$
  - two real numbers s_l, s_r with $s_l \le s_r$
- **Online Query:**
  - for an intervals $[s_l, s_r]$, reports the segments over all $O((u-\ell)\, n)$ feasible segments such that their sums are between s_l and s_r.

70/92

Sum Range Search Problem repetitive mode

- **Work to Do:**
  - Try to preprocess A into an appropriate data structure such that the query time is $o(n + h)$.

71/92

Density Range Search Problem repetitive mode -- definition

- **Input:**
  - a sequence A of n real numbers $a_1, a_2, \ldots, a_n$.
  - two nonnegative real numbers ℓ, u with $\ell \le u$
  - two real numbers d_l, d_r with $d_l \le d_r$.
- **Online Query:**
  - for an intervals $[d_l, d_r]$, reports the segments over all $O((u-\ell)\, n)$ feasible segments such that their densities are between d_l and d_r.

72/92

Density Range Search Problem repetitive mode

- **Work to Do:**
  - Try to preprocess A into a nice appropriate structure such that the query time is $o(n + h)$.

73/92

Aggregate Range Search Problem -- definition

- Given S and a range query Q, compute an *aggregate function* on the subset S'=S∩Q An aggregation function can be Min, Max, Sum, Count, Mean, Median (of S'), etc.

74/92

Range **Minimum Search** Problem -- definition

- **Input:**
  - a sequence A of n real numbers $a_1, a_2, \ldots, a_n$.
  - two real numbers i, j, $i \le j$.
- **Online Query:**
  - for each query interval [i, j], reports the index k with $i \le k \le j$ such that a_k achieves **minimum**.

75/92

Range **Minimum Search** Problem -- example

	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9
Sequence A	3	8	5	34	7	19	10	12	13	16

$RMS_A(3, 7) = 4$

$RMS_A(1, 6) = 2$

76/92

Range **Minimum Search** Problem

- **Related work :**
  - O(n) preprocessing time and O(1) query time under the unit-cost RAM model. -- Gabow, Bentley, and Tarjan. STOC 1984
  - O(n) preprocessing time and O(1) query time under the unit-cost RAM model. -- Bender and Colton. In Proc. the 4th Latin American Symposium on Theoretical Informatics 2000

77/92

Technique Used

- ±1RMS problem: adjacent elements of the input sequence A differ by +1 or -1
- Least Common Ancestor (LCA) problem reduces to ±1RMS problem by depth first search traversal of input tree T of LCA.
- An (O(n log n), O(1))-time table-lookup algorithm for RMS
- Using the above algorithm on a smaller array A' obtained by partitioning A into 2n/logn blocks, each of size (log n)/2 and making use of the ±1 property, we can solve ±1RMS in (O(n), O(1))-time.
- RMS reduces to LCA building the Cartesian tree of A.

78/92

Problem Reduction

- LCA problem reduces to ±1RMS problem
- Observation: The LCA of nodes u and v in T is the lowest node encountered between the visits to u and to v during a depth first traversal of T, where the depths of the nodes in T differ by exactly one.

79/92

(O(n log n), O(1))-time Algorithm for RMS

- Table-lookup algorithm
- Pre-compute the n by log n matrix M[i, j], $1 \le i \le n$, $0 \le j \le \log n$
  $M[i, j] = RMS(i, i + 2^j)$
- For any RMS(i, j) query:
  - Let $k = \max \{r | 2^r < j-i+1\}$
  - $RMS(i, j) = \min\{M(i, k), M(j-2^k+1, k)\}$

80/92

Problem Reduction

- *RMS can be reduced to LCA* by building a Cartesian tree of A.
- The root of a Cartesian tree is the minimum element of the array. The root is labeled with the position *k* of this minimum element.
- The left and right children of the root are the roots of recursively constructed Cartesian trees of the left and right subarrays respectively.

Range **Maximum-Sum Segment Search** Problem -- definition

- **Input:**
  - a sequence A of n real numbers $a_1, a_2, \ldots, a_n$ to be preprocessed.
  - real numbers i, j, $i \le j$ and k, *l*, $k \le l$.
- **Online Query:**
  - for two query intervals [i, j] and [k, *l*], reports A(x, y) with $i \le x \le j$ and $k \le y \le l$ that maximizes s(x, y).

Range **Maximum-Sum Segment Search** Problem

- **Related work :**
  - O(n) preprocessing time and O(1) query time under unit-cost RAM model by Chen and Chao. ISAAC 2004

Technique Used

- Let $S = s_1, s_2, \ldots, s_n$ be the sequence where $s_k = a_1+a_2+\ldots+a_k$ is the prefix sum of sequence A.
- Disjoint case: by min= RMinS(S, i, j), max= RMaxS(S, k, l), Ans.= $s_{max} - s_{min}$
- Overlapping case: Divide into 3 possible cases and take minimum of the outputs of these three cases.
  - [i, k] and [k, l]: by RMinS(S, i, k), RMaxS(S, k, l)
  - [k, j] and [j, l]: by RMinS(S, k, j), RMaxA(S, j, l)
  - [k, j] and [k, j]: by RMSSS(k, j), a special case!

Range **Maximum-Sum Segment Search** Problem- A Special Case

- **Input:**
  - a sequence A of n real numbers $a_1, a_2, \ldots, a_n$.
  - two real numbers i, j, $i \le j$.
- **Online Query:**
  - for any query interval [i, j], reports A(x, y) with $i \le x \le y \le j$ such that A(x, y) is the maximum-sum segment of A(i, j).

Range **Maximum-Sum Segment Search** Problem- A Special Case

- **Related work :**
  - O(n) preprocessing time and O(1) query time under the unit-cost RAM model by Chen and Chao. ISAAC 2004
- They solved RMSSS by using RMinS and RMaxS.

Algorithm

- Let C[·] be the array of prefix sum of A.
- Define: left bound L[k] of A at index k to be the largest index l with $1 \le l \le k-1$ such that $C[l] \ge C[k]$, and L[k]=0, if no such l exists.
- Define: partner P[k] of A at index k to be the largest index p with $L[k]+1 \le p \le k$ that minimizes C[p-1].
- A(P[k], k) is a candidate segment of A at index k with sum M[k] = s (P[k], k), for $1 \le k \le n$.

RMax-SumSegSearch

- Algorithm of RMSSS(A, i, j)

```
r ← RMaxS(M, i, j), i.e. M[r] is maximum
if P[r] < i then
    p ← RMinS(C, i-1, r-1)+1
    s ← RMaxS(C, i-1, r-1)+1
    if C[r]-C[p-1] < M(s)
    then output (P[s], s)
    else output (p, r)
else output (P[r], r)
```

Range **Maximum-Density Segment Search** Problem

- **Input:**
  - a sequence A of n real numbers $a_1, a_2, \ldots, a_n$
- **Online Query:**
  - for two intervals [i, j] and [k, l], reports A(x, y) with $i \le x \le j$ and $k \le y \le l$ that maximizes d(x, y).

89/92

Generalization

- We can also generalize the above aggregation range search problems to other aggregation functions or consider the dynamic range query problems which support insertion, deletion, concatenation operations.

91/92

Range **Maximum-Density Segment Search** Problem- A Special Case

- **Input:**
  - a sequence A of n real numbers $a_1, a_2, \ldots, a_n$.
  - two real numbers i, j, $i \le j$.
- **Online Query:**
  - for any query interval [i, j], reports A(x, y) with $i \le x \le y \le j$ such that A(x, y) is the maximum-density segment of A(i, j).

90/92

Conclusion

- We considered optimization and range search problems on sequences, gave a survey and presented recent results for these problems.
- Open problems
  - **Sum Range** Search Problem (repetitive mode)
  - **Density Range** Search Problem (repetitive mode)
  - Range **Maximum-Density Segment Search** Problem
  - Problems for which the elements are each chosen from an (error) interval

92/92

Dynamic Data Structures in Computational Geometry

Timothy M. Chan
School of Computer Science
University of Waterloo

Every student in computer science knows that we can maintain a set of n real numbers (in 1-d) to support insertions and deletions in $O(\log n)$ time and searches in $O(\log n)$ time, by his/her favorite kind of balanced search trees. The underlying question in this talk is: to what extent can this basic result hold in dimension beyond one? In other words, for what problems in computational geometry can we maintain solutions efficiently under insertions and deletions of data?

In the first part of the talk, we give a rough introduction to this fundamental and important topic called "dynamic computational geometry", which has been extensively studied for over three decades. We obviously do not have time to give a comprehensive survey (despite what the title says), but the purpose is to provide some examples to illustrate what types of problems have been studied, what types of results are possible, and what general techniques are available. Our focus is on fully dynamic algorithms that have guaranteed time bounds for arbitrary update sequences. We mention the following results:

- For *orthogonal range searching* or 2-d *point location*, dynamization with polylogarithmic update time is relatively easy, by directly applying standard balancing tricks to geometric search trees (such as range trees or segment trees); for these problems, research is thus all about removing logarithmic factors [16, 14, 10, 15]. The well-known dynamic 2-d *convex hull* problem [17, 5, 3] also fits in this category.

- Simple dynamization strategies (the "logarithmic method" and the "square-root method") are applicable to a general class of *decomposable search* problems [2].

- For some non-decomposable problems, like 2-d *smallest enclosing circle* and 3-d *linear programming*, dynamization can still be obtained by reducing them to decomposable problems through parametric search [13].

- A general technique by Eppstein [12] can solve dynamic max-max- or min-min-type problems like *bichromatic closest pair*. A key idea here is to handle deletions by re-insertions.

- For some other non-decomposable problems, like 2-d *width* [7] and *rectangle connectivity* [6], polylogarithmic dynamization is not known, but sublinear update time is possible.

- For even more challenging problems (like 2-d *smallest enclosing rectangle*), min-max-type problems (like 2-d *discrete 1-center*), and non-convex optimization problems (like 2-d *largest empty circle*), nothing is known at all, except in special cases (such as the insertion-only and offline settings) [8].

In the second part of the talk, we focus specifically on the dynamic 2-d *post office* problem, and discuss in more detail a new data structure recently discovered by this speaker [9], which is

the first polylogarithmic result known. The problem is to maintain a set of points in the Euclidean plane, to support exact nearest neighbor queries. (By a standard lifting transformation, it can also be viewed as a dynamic 3-d convex hull problem.) The previous solution by Agarwal and Matoušek [1] more than a decade ago has $O(n^\varepsilon)$ amortized update time and $O(\log n)$ query time, or $O(\log^2 n)$ amortized update time and $O(n^\varepsilon)$ query time, for any fixed $\varepsilon > 0$. The new solution has $O(\log^3 n)$ amortized insertion time, $O(\log^6 n)$ amortized deletion time, and $O(\log^2 n)$ query time. The techniques involved include removing "high-degree" elements (following Agarwal and Matoušek [1]), handling deletions by re-insertions (as in Eppstein [12]), and using geometric tools like "sampling" and "conflict lists" (as in [11, 4, 18]).

We conclude by mentioning applications of dynamic data structures in the design of geometric algorithms, and by listing some open problems in the area.

References

[1] P. K. Agarwal and J. Matoušek. Dynamic half-space range reporting and its applications. *Algorithmica*, 13:325–345, 1995. (Also in FOCS 1992.)

[2] J. Bentley and J. Saxe. Decomposable searching problems I: static-to-dynamic transformation. *J. Algorithms*, 1:301–358, 1980.

[3] G. S. Brodal and R. Jacob. Dynamic planar convex hull. In FOCS 2002.

[4] T. M. Chan. Random sampling, halfspace range reporting, and construction of ($\leq k$)-levels in three dimensions. *SIAM J. Comput.*, 30:561–575, 2001. (Also in FOCS 1998.)

[5] T. M. Chan. Dynamic planar convex hull operations in near-logarithmic amortized time. *J. ACM*, 48:1–12, 2001. (Also in FOCS 1999.)

[6] T. M. Chan. Dynamic subgraph connectivity with geometric applications. In STOC 2002.

[7] T. M. Chan. A fully dynamic algorithm for planar width. *Discrete Comput. Geom.*, 30:17–24, 2003. (Also in SoCG 2001.)

[8] T. M. Chan. Semi-online maintenance of geometric optima and measures. *SIAM J. Comput.*, 32:700–716, 2003. (Also in SODA 2002.)

[9] T. M. Chan. Dynamic data structures for 3-d convex hulls and 2-d nearest neighbor queries. In SODA 2006.

[10] Y.-J. Chiang and R. Tamassia. Dynamic algorithms in computational geometry. *Proc. IEEE*, 80:1412–1434, 1992.

[11] K. L. Clarkson and P. W. Shor. Applications of random sampling in computational geometry, II. *Discrete Comput. Geom*, 4:387–421, 1989.

[12] D. Eppstein. Dynamic Euclidean minimum spanning trees and extrema of binary functions. *Discrete Comput. Geom.*, 13:111–122, 1995. (Also in FOCS 1992.)

[13] J. Matoušek. Linear optimization queries. *J. Algorithms*, 14:432–448, 1993.

[14] K. Mehlhorn. *Data Structures and Algorithms 3: Multi-Dimensional Searching and Computational Geometry.* Springer-Verlag, 1984.

[15] C. W. Mortensen. Fully-dynamic two dimensional orthogonal range and line segment intersection reporting in logarithmic time. In SODA 2003.

[16] M. H. Overmars. *The Design of Dynamic Data Structures.* Springer-Verlag, 1983.

[17] M. H. Overmars and J. van Leeuwen. Maintenance of configurations in the plane. *J. Comput. Sys. Sci.*, 23:166–204, 1981. (Also in STOC 1980.)

[18] E. Ramos. On range reporting, ray shooting, and k-level construction. In SoCG 1999.

Dynamic Data Structures in Computational Geometry

Timothy M. Chan
School of CS
U of Waterloo

Theme

Dynamic data structures for searching in 1D:

balanced search trees

What about dynamic data structures in 2D (& beyond) ???

"Dynamic Computational Geometry"

Solve geometric problems under
insertion of an object &
deletion " " "
w. guaranteed worst-case/amortized time

Settings:

fully dynamic ⇐
insert-only
delete-only
offline (all updates known)
semi-online (delete times known)
random updates
kinetic

This Talk

Part I:
Survey

Part II:
A new result for
dynamic 3D convex hull/
2D post office [SODA'06]

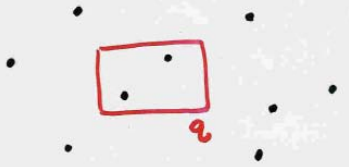
PART I:

SURVEY

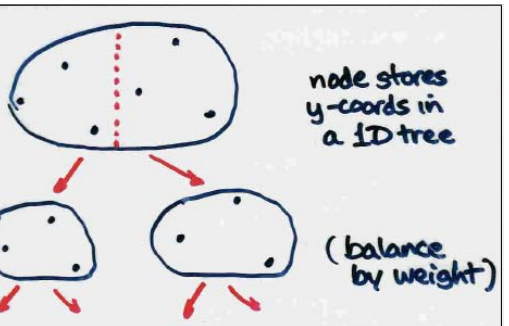


Ex 1: 2D Orthogonal Range Search

Maintain n pts in 2D s.t.
given rectangle q,
report/count all pts in q



General idea: just dynamize a geometric search tree,
here, a "range tree"



node stores y-coords in a 1D tree

(balance by weight)

$\Rightarrow$ $O(\log^2 n)$ update & query

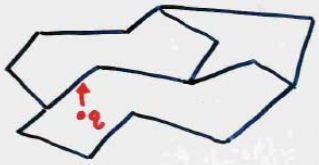
Various improvements:

$O(\log n \log\log n)$ update & query
[Mehlhorn, Näher '86]

$O(\log n)$ update & query
[Mortensen, SODA '03]

Ex 2: 2D Point Location

Maintain n disjoint line segments s.t.
given pt q,
find segment immediately above q



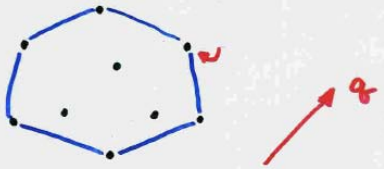
Similar idea: dynamize a "segment tree"

$\Rightarrow$ $O(\log^2 n)$ update & query [Overmars '85]

Various improvements on the logs ...

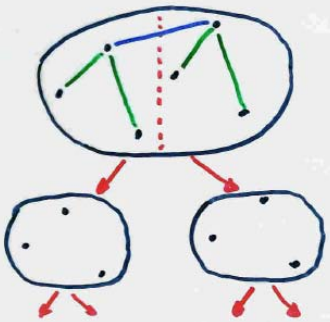
Ex 3 : 2D Convex Hull

Maintain n pts in 2D s.t.
given direction q,
find vertex of CH extreme along q



Rmk: CH may change a lot!

Similar idea: dynamize a "hull tree"



node stores a "bridge" (computable in log time)

$\Rightarrow$ $O(\log^2 n)$ update, $O(\log n)$ query
[Overmars, van Leeuwen, STOC'80]

Various improvements:
$O(\log^{1+\varepsilon} n)$ update, $O(\log n)$ query
[Chan, FOCS'99]
$O(\log n)$ update & query
[Brodal, Jacob, FOCS'02]

Ex 4 : 2D Post Office Problem

Maintain n pts in 2D s.t.
given pt q, find nearest neighbor to q

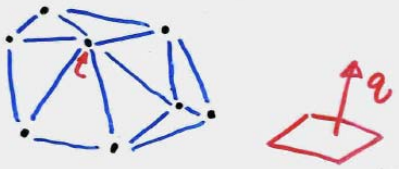


i.e. given (x,y), find
$\min_i (x-a_i)^2 + (y-b_i)^2$
i.e., $\min_i -2a_i x - 2b_i y + a_i^2 + b_i^2$

Rmk: viewing $(-2a_i, -2b_i, a_i^2+b_i^2)$ as a pt in 3D, this reduces to ...

Ex 5 : 3D Convex Hull

Maintain n pts in 3D s.t.
given direction q,
find vertex of CH extreme along q



Static soln: [classical CG]
$O(n \log n)$ preproc, $O(\log n)$ query

Rmk: but CH may change a lot!

Simple general idea for insert-only:

decompose into $O(\log n)$ subsets



$\Rightarrow$ $O(\log^2 n)$ insert & query

[Bentley, Saxe '80: the "logarithmic method" for "decomposable search problems"]

Simple general idea for fully dynamic:

decompose into $O(\sqrt{n})$ subsets



$\Rightarrow$ $O(\sqrt{n}\log n)$ insert/delete & query

A different idea for 3D CH:

dynamize a slower static soln, namely, a "partition tree" OR "cutting tree" [Matoušek '91]

$\Rightarrow$ $O(\log^2 n)$ update, $O(n^\varepsilon)$ query

OR $O(n^\varepsilon)$ update, $O(\log n)$ query

[Agarwal, Matoušek, FOCS'92]

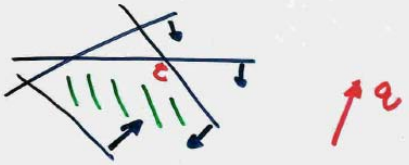
A new result for 3D CH:

$O(\text{polylog } n)$ update & query

[wait for 2nd half of talk!]

Ex 6: 3D Linear Programming

Maintain n halfspaces in 3D s.t.
given direction q,
find vertex in intersection extreme along q

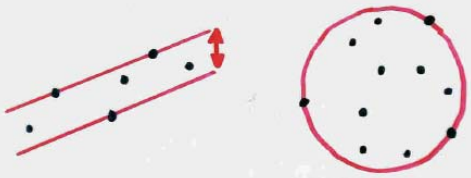


Rmk: "dual" to 3D CH but not decomposable!

Idea: (Megiddo '83 / Matoušek '92)
parametric search reduces LP to membership queries (which are decomposable)

$\Rightarrow$ O(polylog n) update & query
[by new result]

Appl'ns: 2D vertical width,
2D min enclos. circle



Ex 7: 2D Bichromatic Closest Pair

Maintain n red/blue pts in 2D to find $\min_{p \text{ red}} \min_{q \text{ blue}} d(p,q)$



Appl'n: 2D MST

Static sol'n: O(n log n) time

Rmk: but many nearest neighbors may change!



Eppstein's general technique: [FOCS '92]

Preprocessing: ("conga line")
for $i = 1, 2, \ldots$
p_i = nearest neighbor of p_{i-1}
delete p_i



Obs: closest pair is in conga line
each pt has const in-degree

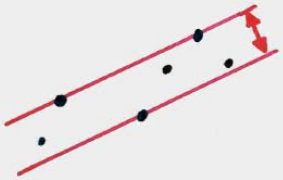
Old idea: handle insert by the logarithmic method

Extra idea: handle delete by re-insert!

$\Rightarrow$ O(polylog n) update
[using new result]

Ex 8: 2D Width

Maintain n pts in 2D to find min-width enclos. strip



Static sol'n: O(n log n)

Rmks: CH may change a lot!
not decomposable!
not linear/convex programming

Delete-only soln: [Eppstein, SODA '99/ Chan, SoCG '01]

$O(\log^3 n)$ delete time (amort.)

Fully dynamic idea: [Chan, SoCG '01]

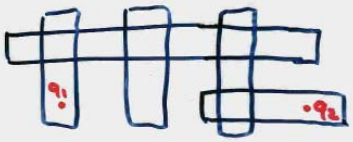
decompose into 2 subsets

delete-only $\leq \sqrt{n}$

$\Rightarrow O(\sqrt{n} \log^3 n)$ update

Ex 9: 2D Orthogonal Connectivity

Maintain n rectangles in 2D s.t.
given q_1, q_2,
decide if q_1 and q_2 connected



Similar idea: [Chan, STOC '02]

$\leq n^\alpha$

$\Rightarrow O(n^{0.94})$ update &
$O(n^{1/3})$ query

Ex 10: Even Tougher Problems

- 2D min encios. rectangle
- 2D max empty circle
- 2D discrete 1-center
  i.e. $\min_q \max_p d(p,q)$
- 3D convex hull volume

Similar idea for insert-only (or semi-online)
[Chan, SODA '02]

static $\leq n^\alpha$

$\Rightarrow O(n^{1-\alpha})$

Rmk: but nothing for fully dynamic !!

PART II:

THE NEW RESULT



Dynamic 3D Convex Hull / 2D Post Office

$O(\log^3 n)$ insert time (amort, rand)

$O(\log^6 n)$ delete time (amort, rand)

$O(\log^2 n)$ query time

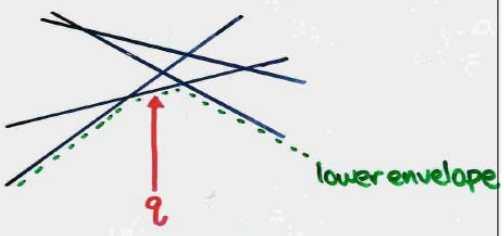
Overview of Ideas

- handle insert by the logarithmic method ($O(\log n)$ subsets)
- move "high-degree stuff" to new subsets during preprocessing
  [also done by Agarwal, Matoušek, FOCS'92]
- handle delete by re-inserts
  [inspired by Eppstein, FOCS'92]
- use $O(\log n)$ samples & "conflict lists"
  [inspired by skip list & a static structure by Chan, FOCS'98]

Dual Problem

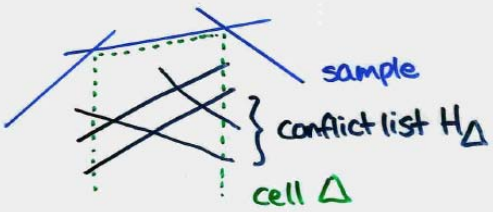
Maintain n halfspaces in 3D s.t.
given vertical line q,
find intersection at q

i.e. maintain n planes in 3D s.t.
given vertical line q,
find lowest plane at q



Sampling Lemma

For a random sample of r planes, triangulation of its lower envelope has $\sim r$ cells, each w. $\sim n/r$ conflicting planes



[Clarkson, Shor '88, Matoušek '91, Ramos '99: "shallow cuttings"]

Preprocessing a Subset

For $i = 1 .. \log n$
take sample of 2^i planes



$\sim 2^i$ cells, each w. $\sim n/2^i$ conflicts

move planes that have $\geq b$ conflicts to new subset

Analysis:

planes moved $\approx \frac{n}{b} \cdot \log n$

$\Rightarrow$ only a fraction moved, for $b \approx \log n$

$\Rightarrow$ preproc. time $O(n \log^2 n)$

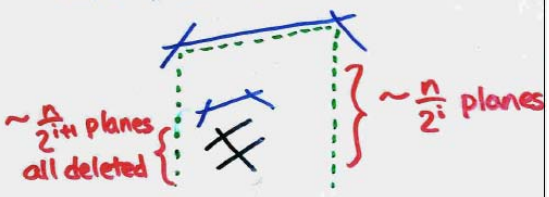
$\Rightarrow$ insert time $O(\log^3 n)$

Deleting h from a Subset

For $i = 1 .. \log n$
for each cell Δ in conflict with h
if a fraction of H_Δ was deleted
re-insert all planes in H_Δ

Correctness:

suppose answer is in a cell at layer i, but not $i+1$



Analysis:

re-inserts $\approx b \log n \approx \log^2 n$

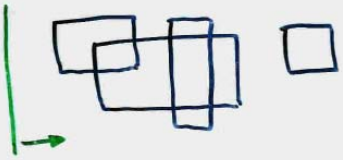
$\Rightarrow$ delete time $O(\log^2 n \cdot \log^3 n \cdot \log n)$

Conclusion

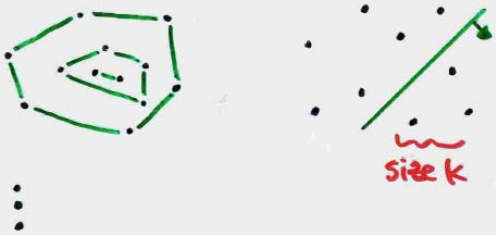


Exs of Appl'ns

- Klee's measure problem (compute volume of union of n boxes)



- 3D convex layers, k-sets



Open Problems

- dynamic 3D CH / 2D post office:
  $O(\log n)$ update & query ????
  & $O(n)$ space ??
- dynamic 2D point location:
  $O(\log n)$ update & query ??
- dynamic 2D width:
  $o(\sqrt{n})$??
- dynamic 3D approx. width (or "core-sets")
  $O(\log n)$??
- dynamic 2D connectivity for line segments
  $o(n)$??
- dynamic 2D centerpoint
  $o(n)$??

Geometric Networks: Integer Linear Programming and Combinatorial Algorithms

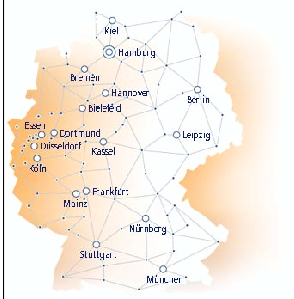
Alexander Wolff

Department of Computer Science
Karlsruhe University

Outline

1. Introduction
   - Geometric Networks
2. Drawing Metro Maps
   - Modeling the Metro Map Problem
   - MIP Formulation & Experiments
   - NP-Hardness
3. Spanning trees with few crossings
   - Non-Approximability
   - Fixed-Parameter Algorithms
   - MIP Formulation

Geometric Networks



modeled by graphs $G(V, E)$ with
– $V \subset \mathbb{R}^2$
– edge weights:
distances, travel time, ...

Applications:

- backbone of transportation networks
- model for communication networks
- ...

Outline

1. Introduction
   - Geometric Networks
2. Drawing Metro Maps
   - Modeling the Metro Map Problem
   - MIP Formulation & Experiments
   - NP-Hardness
3. Spanning trees with few crossings
   - Non-Approximability
   - Fixed-Parameter Algorithms
   - MIP Formulation

What is a Metro Map?





- schematic diagram for public transport
- visualizes lines and stations
- goal: ease navigation for passengers
  - "How do I get from A to B?"
  - "Where to get off and change trains?"
- distorts geometry and scale
- improves readability
- compromise between schematic road map ↔ abstract graph

More Formally

The Metro Map Problem

Given: planar embedded graph $G = (V, E)$, $V \subset \mathbb{R}^2$, line cover $\mathcal{L}$ of paths or cycles in G (the metro lines),
Goal: draw G and $\mathcal{L}$ nicely.

- What is a nice drawing?
- Look at real-world metro maps drawn by graphic designers and model their design principles as
  - *hard* constraints – must be fulfilled,
  - *soft* constraints – should hold as tightly as possible.

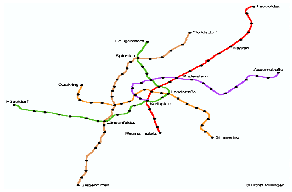
Hard Constraints

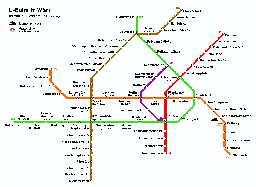
(H1) preserve embedding of G
(H2) draw all edges as octilinear line segments, i.e. parallel to a coordinate axes or at 45° degrees
(H3) draw each edge e with length $\geq \ell_e$
(H4) keep vertices $d_{\min}$ away from non-incident edges



Soft Constraints

(S1) draw metro lines with few bends
(S2) keep total edge length small
(S3) draw each octilinear edge similar to its geographical orientation: keep its relative position





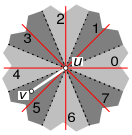
Mixed-Integer Programming

- Linear Programming: efficient optimization method for
  - linear constraints and objective function,
  - real-valued variables (domain $\mathbb{R}$).
- Mixed-Integer Programming (MIP):
  - allows also integer variables (domain $\mathbb{Z}$),
  - solution NP-hard in general.
- Still a practical method for many hard optimizat. problems.

Theorem (Nöllenburg & Wolff GD'05)

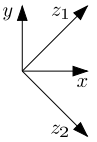
The problem MetroMapLayout can be formulated as a MIP s.th.
linear constraints → *hard constraints,*
objective function → *soft constraints.*

Example: Octilinearity and Relative Position



Sectors

– for each vtx. u partition plane into sectors 0–7
– number octilinear edge directions accordingly
- $\text{sec}_u(v) = 5$ (input)
- $\text{dir}(u, v) = 5$ (output)

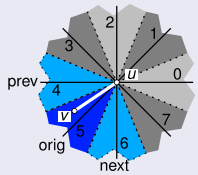


Coordinates

assign z_1- and z_2-coordinates to each vertex v:
- $z_1(v) = x(v) + y(v)$
- $z_2(v) = x(v) - y(v)$

Example: Octilinearity and Relative Position

Goal



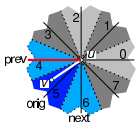
Draw edge uv
- with minimum length ℓ_{uv}
- restricted to 3 directions

How to model this using linear constraints?

Binary Variables

$$\alpha_{\text{prev}}(u, v) + \alpha_{\text{orig}}(u, v) + \alpha_{\text{next}}(u, v) = 1$$

Example: Octilinearity and Relative Position



Previous Sector

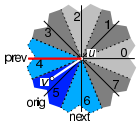
$$\begin{aligned} y(u) - y(v) &\leq M(1 - \alpha_{\text{prev}}(u, v)) \\ -y(u) + y(v) &\leq M(1 - \alpha_{\text{prev}}(u, v)) \\ x(u) - x(v) &\geq -M(1 - \alpha_{\text{prev}}(u, v)) + \ell_{uv} \end{aligned}$$

How does this work?

Case 1: $\alpha_{\text{prev}}(u, v) = 0$

$$\begin{aligned} y(u) - y(v) &\leq M \\ -y(u) + y(v) &\leq M \\ x(u) - x(v) &\geq \ell_{uv} - M \end{aligned}$$

Example: Octilinearity and Relative Position



Previous Sector

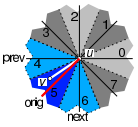
$$\begin{aligned} y(u) - y(v) &\leq M(1 - \alpha_{\text{prev}}(u,v)) \\ -y(u) + y(v) &\leq M(1 - \alpha_{\text{prev}}(u,v)) \\ x(u) - x(v) &\geq -M(1 - \alpha_{\text{prev}}(u,v)) + \ell_{uv} \end{aligned}$$

How does this work?

Case 2: $\alpha_{\text{prev}}(u,v) = 1$

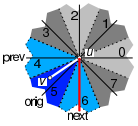
$$\begin{aligned} y(u) - y(v) &\leq 0 \\ -y(u) + y(v) &\leq 0 \\ x(u) - x(v) &\geq \ell_{uv} \end{aligned}$$

Example: Octilinearity and Relative Position



Original Sector

$$\begin{aligned} z_2(u) - z_2(v) &\leq M(1 - \alpha_{\text{orig}}(u,v)) \\ -z_2(u) + z_2(v) &\leq M(1 - \alpha_{\text{orig}}(u,v)) \\ z_1(u) - z_1(v) &\geq -M(1 - \alpha_{\text{orig}}(u,v)) + 2\ell_{uv} \end{aligned}$$



Next Sector

$$\begin{aligned} x(u) - x(v) &\leq M(1 - \alpha_{\text{next}}(u,v)) \\ -x(u) + x(v) &\leq M(1 - \alpha_{\text{next}}(u,v)) \\ y(u) - y(v) &\geq -M(1 - \alpha_{\text{next}}(u,v)) + \ell_{uv} \end{aligned}$$

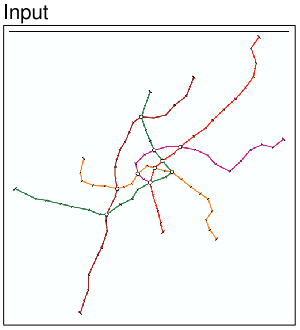
Summary of the Model

- The above constraints enforce
  - octilinearity,
  - minimum edge length,
  - (partially) relative position
- Similarly:
  - preservation of embedding
  - planarity
- Soft constraints: weighted sum in objective function

  minimize $\lambda_{\text{bends}}\,\text{cost}_{\text{bends}} + \lambda_{\text{length}}\,\text{cost}_{\text{length}} + \lambda_{\text{dir}}\,\text{cost}_{\text{dir}}$
- In total $O(|V|^2)$ constraints and variables

Results – Vienna

Input



Input	$\|V\|$	$\|E\|$	lines
normal	90	96	5
reduced	44	50	

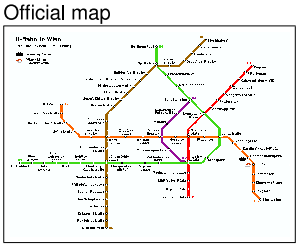
↓

MIP	constr.	var.
normal	39363	9960
improved	23226	6048
heuristic 1	5703	1800
heuristic 2*	1875	872

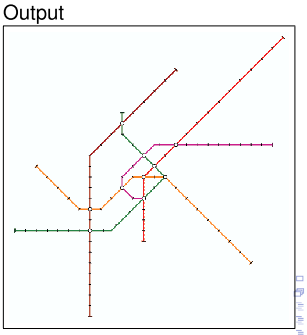
*) 29 seconds w/o proof of opt.

Results – Vienna

Official map

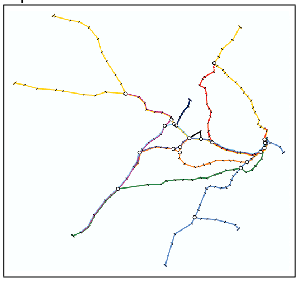


Output



Results – Sydney

Input



Input	$\|V\|$	$\|E\|$	lines
normal	174	183	10
reduced	62	71	

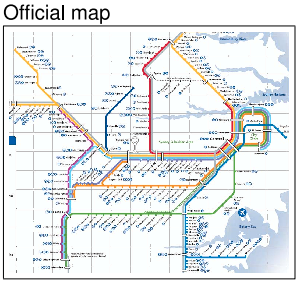
↓

MIP	constr.	var.
normal	81416	20329
improved	45182	11545
heuristic 1*	6242	2105
heuristic 2	3041	1329

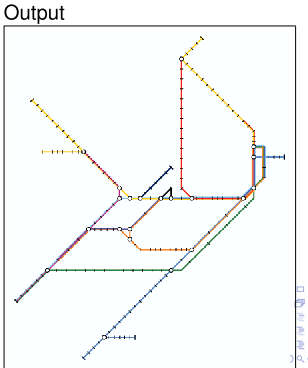
*) 22 minutes w/o proof of opt.

Results – Sydney

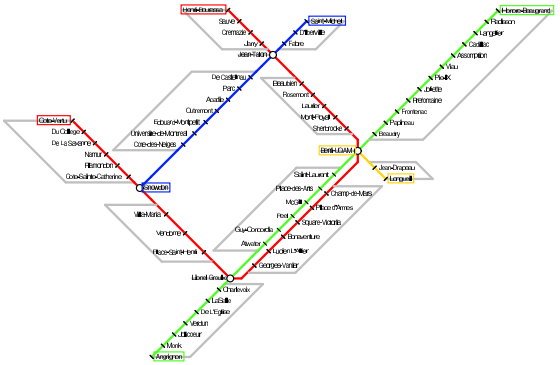
Official map



Output



Labeling



Labeling



A Similar Problem

RectilinearGraphDrawing Decision Problem

Given a planar embedded graph G with max degree 4.
Is there a drawing of G that

- preserves the embedding,
- uses straight-line edges,
- is rectilinear?

Theorem (Tamassia SIAMJComp'87)

RectilinearGraphDrawing *can be solved efficiently.*

Proof.

By reduction to a flow problem. □

Our Problem

MetroMapLayout Decision Problem

Given a planar embedded graph G with max degree 8.
Is there a drawing of G that

- preserves the embedding,
- uses straight-line edges,
- is octilinear?

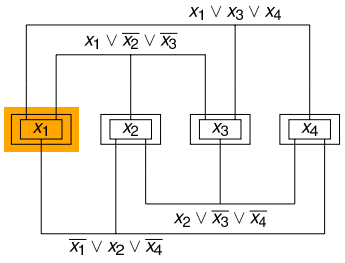
Theorem (Nöllenburg MSc'05)

MetroMapLayout *is NP-hard.*

Proof.

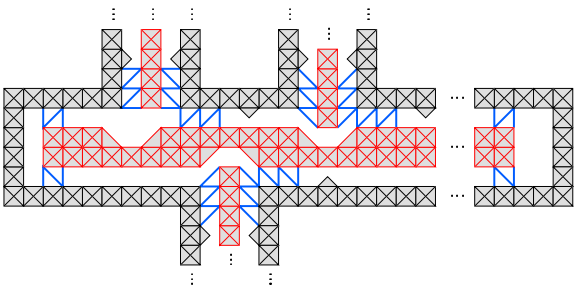
By reduction from Planar 3-Sat to MetroMapLayout. □

Outline of the Reduction



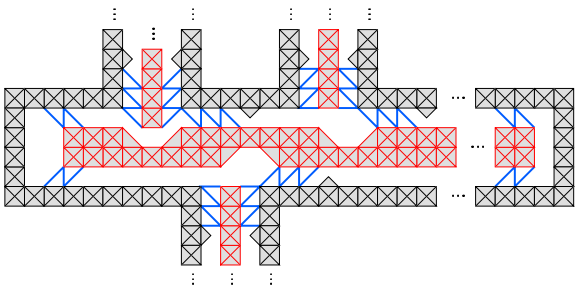
Input: planar 3-SAT formula $\varphi = (x_1 \vee x_3 \vee x_4) \wedge (x_1 \vee \overline{x_2} \vee \overline{x_3}) \wedge \ldots$
Goal: planar embedded graph G_φ with:
G_φ has a metro map drawing $\Leftrightarrow$ φ satisfiable.

Variable Gadget



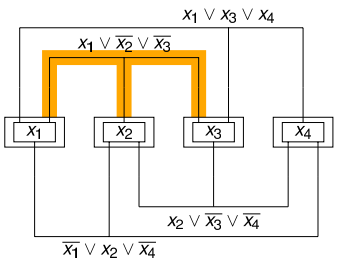
x = true

Variable Gadget



x = false

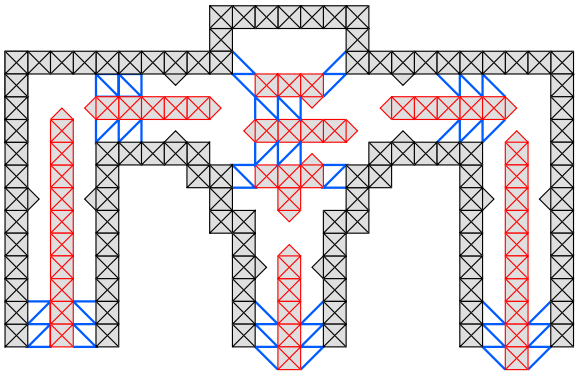
Outline of the Reduction



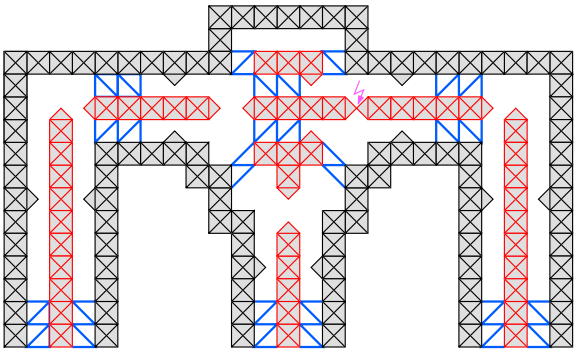
Input: planar 3-SAT formula $\varphi = (x_1 \vee x_3 \vee x_4) \wedge (x_1 \vee \overline{x_2} \vee \overline{x_3}) \wedge \ldots$

Goal: planar embedded graph G_φ with:
G_φ has a metro map drawing $\Leftrightarrow$ φ satisfiable.

Clause Gadget



Clause Gadget



Summary (metro maps)

- METROMAPLAYOUT is NP-hard.
- Formulated and implemented MIP.
- Our MIP can draw *any* kind of sketch "nicely".
- Results comparable to manually designed maps.
- Reduced MIP size & runtime drastically.

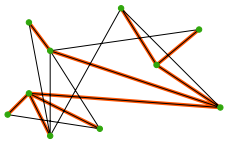
To Do

- rectangular stations
- multi-edges
- user interaction (e.g. fixing certain edge directions)

Outline

1. Introduction
   - Geometric Networks
2. Drawing Metro Maps
   - Modeling the Metro Map Problem
   - MIP Formulation & Experiments
   - NP-Hardness
3. Spanning trees with few crossings
   - Non-Approximability
   - Fixed-Parameter Algorithms
   - MIP Formulation

Spanning trees with few crossings



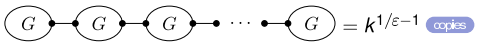
Given: geometric graph $G(V, E)$, i.e. $V \subset \mathbb{R}^2$.
Find: spanning tree in G with minimum number of crossings.
Known: Deciding "does G have a crossing-free spanning tree?" is NP-hard. [Jansen & Woeginger BIT'93]
We show: The problem is even hard to approximate.
But it is fixed-parameter tractable
and can be formulated as a mixed-integer program.

Crossing-free spanning trees

Let k = #crossings in G (crossing = pair of crossing edges).
$\varphi(G) = 1+$ minimum #crossings in spanning tree of G.

Theorem (Knauer, Schramm, Spillner, Wolff ISAAC'05)

If there is a poly-time $k^{1-\varepsilon}$-approximation algo $A_{1-\varepsilon}$ of $\varphi(G)$ for some $\varepsilon \in (0, 1]$, then $\mathcal{P} = \mathcal{NP}$.

Let $G' =$  $= k^{1/\varepsilon-1}$ copies

$\Rightarrow$ G' has $K = k \cdot k^{1/\varepsilon-1} = k^{1/\varepsilon}$ crossings.

$\varphi(G) = 1 \Leftrightarrow \varphi(G') = 1$	vs.	$\varphi(G) \geq 2 \Leftrightarrow \varphi(G') \geq 1 + k^{1/\varepsilon-1}$
$\downarrow A_{1-\varepsilon}(G')$		$\downarrow A_{1-\varepsilon}(G')$
$\leq K^{1-\varepsilon} = k^{1/\varepsilon-1}$ cross.		$\geq 1 + k^{1/\varepsilon-1}$ cross. in sp.-tree

Fixed-parameter tractability

Aim

Solve (NP-) hard problem by restricting combinatorial explosion to parameter independent from input size.

Definition

A decision problem Π is *FPT w.r.t. a parameter k* if there is an algorithm that decides in $O(f(k) \cdot \text{poly}(|I|))$ time, whether an instance I of Π is a yes- or a no-instance. ($f : \mathbb{N} \to \mathbb{N}$ arbitrary!)

Example

k-VertexCover (Can we cover all edges of G with k vertices?) is FPT.

VertexCover

Example

k-VertexCover is FPT.

Proof: search-tree method.

Take a node u with an uncovered edge $\{u, v\}$.
Either u is in a VC or the complete neighborhood of u.
Check both possibilities!
$\Rightarrow$ search tree T of size $S(k) \leq 2S(k-1) \leq 2^k$.
If in no leaf of T all edges of G are covered,
then G has no k-VC. Runtime: $O(2^k \cdot n)$ □

Example

k-DominatingSet is *not* FPT unless $\mathcal{P} = \mathcal{NP}$.

CrossingFreeSpanningTree

Theorem

CrossingFreeSpanningTree is FPT w.r.t. #crossings in the input graph.

i.e., can decide in $O(f(k) \cdot \text{poly}(n))$ time, whether a graph with n vertices and k crossings has a crossing-free spanning tree.

Proof by enumeration of edges.

$X :=$ set of crossings $\Rightarrow$ $E_X := \bigcup X$ contains $\leq 2k$ edges.
$G' := G \setminus E_X$
For each subset H of E_X check:
is H crossing-free? does $G' \cup H$ span G?
Runtime: $O(2^{2k} \cdot \text{poly}) = O(4^k \cdot \text{poly})$. □

Note: G has c-f spanning tree $\Leftrightarrow$ G has c-f spanning subgraph.

A faster algorithm

Theorem

CrossingFreeSpanningTree can be decided in $O(3^k \cdot \mathrm{poly})$ time.

Proof by enumeration of "crossing vectors".

$X := \{\{e_1, f_1\}, \ldots, \{e_k, f_k\}\}$ = set of crossings.

For each vector $x \in \{0,1,2\}^k$

$$H := \bigcup_{i=1}^{k} \begin{cases} e_i & \text{if } x_i = 1, \\ f_i & \text{if } x_i = 2, \\ \emptyset & \text{else.} \end{cases}$$

is H crossing-free? does $G' \cup H$ span G? □

A yet faster algorithm

Theorem

CrossingFreeSpanningTree can be decided in $O(2^k \cdot \mathrm{poly})$ time.

Proof by enumeration of *maximal* crossing-free edge sets.

Let $e \in E_X \quad \Rightarrow \quad e$ crosses $c \geq 1$ other edges.

If we put e into a crossing-free subset, we discard c crossings.

If we don't put e into a c-f subset, we discard c crossings.

$\Rightarrow E_X$ has $S(k) \leq 2S(k-c) \leq 2S(k-1) \leq 2^k$ max. c-f subsets

For each such subset H check:

does $G' \cup H$ span G? □

Our results

Theorem (KSSW'05)

CFST can be decided in $O(1.9999992^k \cdot \mathrm{poly})$ time.

Proof.

Exploit that edge sets H must make G' connected:

(1) if G' has many components, one must have low degree:
$\Rightarrow$ use search tree based on components.

(2) if G' has few components, there are few ways to connect G':
$\Rightarrow$ enumerate all possibilities. □

Theorem (KSSW'05)

There is a Monte-Carlo algo. (1-sided error, success prob. $> \frac{1}{2}$) for CFST that runs in $O(1.968^k \cdot \mathrm{poly})$ time.

Another parameter

Let ι = number of inner points:



Theorem (Deineko, Hoffmann, Okamoto, Woeginger ORL'06)

TravelingSalesPerson (TSP) is FPT w.r.t. ι.

Theorem (H., O. IWPEC'04; Grantson, Levcopoulos EWCG'06)

MinimumWeightTriangulation (MWT) is FPT w.r.t. ι.

Theorem (G. & L. JCDCG'04; Spillner CCCG'05)

MinimumConvexPartition (MCP) is FPT w.r.t. ι.

Theorem (Knauer & Spillner Manu'06)

CrossingFreeSpanningTree (CFST) is FPT w.r.t. ι.

A MIP for MinimumCrossingSpanningSubgraph

For each edge e of G let

$$y_e = \begin{cases} 1 & \text{if } e \text{ is in the desired spanning subgraph of } G, \\ 0 & \text{otherwise.} \end{cases}$$

We would like to have for each crossing $\{e, e'\} \in X$ a variable

$$x_{ee'} = \begin{cases} 1 & \text{if } y_e = y_{e'} = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Then we could state as objective function

$$\text{minimize} \sum_{\{e,e'\} \in X} x_{ee'}.$$

Clearly $x_{ee'} = y_e \cdot y_{e'}$

A MIP for MinimumCrossingSpanningSubgraph

For each edge e of G let

$$y_e = \begin{cases} 1 & \text{if } e \text{ is in the desired spanning subgraph of } G, \\ 0 & \text{otherwise.} \end{cases}$$

We would like to have for each crossing $\{e, e'\} \in X$ a variable

$$x_{ee'} = \begin{cases} 1 & \text{if } y_e = y_{e'} = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Then we could state as objective function

$$\text{minimize} \sum_{\{e,e'\} \in X} x_{ee'}.$$

Clearly $x_{ee'} = y_e \cdot y_{e'}$, but this is not linear!

Expressing $x_{ee'}$

Reminder: we want $x_{ee'} = \begin{cases} 1 & \text{if } y_e = y_{e'} = 1, \\ 0 & \text{otherwise.} \end{cases}$

We can also express this as $x_{ee'} = \min\{y_e, y_{e'}\}$.

So what about $x_{ee'} \le y_e$ and $x_{ee'} \le y_{e'}$ (and $x_{ee'} \ge 0$)?

Recall our objective function: minimize $\sum_{\{e,e'\} \in X} x_{ee'}$:-(

Now here's the trick: $x_{ee'} \ge 0$ and $x_{ee'} \ge y_e + y_{e'} - 1$:-)

To do: must make sure that edges e with $y_e = 1$ span G!

Idea: use flow to achieve connectivity!

skip one! skip two!

From flow to connectivity

[Williams'01, Shirabe'04]

Make two arcs (u, v) and (v, u) for each edge $\{u, v\}$ in G.
Let A = arc set. Let $f_a \in \mathbb{N}$ be the amount of flow on arc a.
Choose arbitrary *source* vertex s.
Make s "pour" $n - 1$ buckets of water into the graph G:

$$\sum_{(s,u) \in A} f_{(s,u)} = (n-1) + \sum_{(u,s) \in A} f_{(u,s)}$$

Make each other vertex v "drink" one bucket:

$$\sum_{(v,u) \in A} f_{(v,u)} = \quad -1 \quad + \sum_{(u,v) \in A} f_{(u,v)}$$

$\Rightarrow$ the set of arcs with non-zero flow is connected!

From paths to connectivity

Choose arbitrary *center* vertex s. Go through all $t \neq s$.

Idea: establish simple s–t path π^t. Let $p_e^t = \begin{cases} 1 & \text{if } e \in \pi^t \\ 0 & \text{else.} \end{cases}$

Make sure π^t leaves s and reaches t:

$$\sum_{e \text{ incident to } s} p_e^t \quad = \quad \sum_{e \text{ incident to } t} p_e^t \quad = \quad 1.$$

Make sure π^t does not stop in any vertex v other than s and t:

$$\{0, 2\} \quad \ni \quad \sum_{e \text{ incident to } v} p_e^t \quad = \quad 2d_e^t \quad \text{with } d_e^t \in \{0, 1\}.$$

Synchronize y_e with all variables of type p_e^t:

Summary (spanning trees)

- MinimumCrossingSpanningSubgraph:
  - hard to approximate,
  - MIP of size $O(mn + k)$.
- Fixed-parameter tractability:
  - interesting concept.
- CFST is FPT w.r.t.
  - #crossings,
  - #inner points.

To Do

- Beat running time of $O(1.9999992^k \text{poly})$ for CFST.
- Reduce size of MIP.
- Find other parameters – and motivate them!

Geometric embeddings and graph expansion

James R. Lee
jrl@ias.edu
Institute for Advanced Study (Princeton)
and University of Washington (Seattle)

Abstract

Beginning in the early-90's, it became gradually apparent that techniques from high-dimensional geometry were highly relevant for a variety of computational tasks. At the center of this connection is the study of *graph partitioning problems* which involve breaking a graph into two or more large parts while minimizing the size of the "interface" between them. These problems are of central importance in numerous computational settings like data clustering, divide and conquer algorithms, and packet routing in networks. Additionally, the techniques involved have applications to areas like Markov chains, nearest-neighbor search, and learning theory.

We will discuss an approach to these problems based on *geometric embeddings.* The basic idea is to represent a graph $G = (V, E)$ as a geometric object by mapping the vertices of G to points in a high-dimensional Euclidean space, and then to use geometric techniques to find good cuts in G—these are cuts which separate G into "large" pieces while minimizing the number of edges that are cut.

In the *Sparsest Cut problem*, the input is given as a graph $G = (V, E)$ along with a subset of pairs of vertices $D \subseteq V \times V$ called *demands.* For a subset $S \subseteq V$, let $E(S, \bar{S})$ be the set of edges crossing from S to its complement $\bar{S}$, and let $D(S, \bar{S})$ be the set of demands crossing from S to $\bar{S}$. The *sparsity of a cut* $(S, \bar{S})$ is defined as the ratio

$$\Phi(S) = \frac{|E(S, \bar{S})|}{|D(S, \bar{S})|},$$

and the goal of the Sparsest Cut problem is to find the cut $(S, \bar{S})$ which minimizes $\Phi(S)$. Since solving this problem exactly is NP-hard, we will instead search for a set $S \subseteq V$ for which $\Phi(S)$ is *approximately optimal,* i.e. is within some factor C of the sparsest cut.

During the talk, I will first explain the relationship between geometric embeddings and the Sparsest Cut problem, and then I will discuss the current state-of-the-art techniques in constructing such embeddings. These employ a beautiful mix of semi-definite programming, high-dimensional convex geometry, probability theory, and combinatorics. A brief outline of the talk (with references) now follows.

The relation of geometric embeddings to the Sparsest Cut problem was first realized in the two papers [LLR95, AR98]. The basic approach follows.

1. Associate a *metric* to the graph G. This is a value $d(u, v)$ for every pair of vertices $u, v \in V$ which is symmetric, i.e. $d(u, v) = d(v, u)$ and satisfies the triangle inequality

$$d(u, v) \leq d(u, w) + d(w, v)$$

for every triple of points $u, v, w \in V$. This metric is closely related to the structure of *multi-commodity flows in G,* and is the solution to a linear programming relaxation of the Sparsest Cut problem.

2. Given the metric d, we can think of (V, d) as a metric space. The second step is to *embed* this space into $\mathbb{R}^n$ (where $n = |V|$) such that the embedding preserves the structure of (V, d). Such a mapping is called a *low-distortion embedding.* This is a map $f : V \to \mathbb{R}^n$ which satisfies

$$d(u, v) \leq \|f(u) - f(v)\| \leq C \cdot d(u, v) \qquad \text{for all } u, v \in V.$$

The factor C is called the *distortion* of the map f, and our goal is to make C as small as possible. (Note that $\|f(u) - f(v)\|$ is the Euclidean distance between $f(u)$ and $f(v)$.)

3. The final step is to use the geometric embedding to find a cut in G. One way to do this is by projecting the image of G (under the embedding f) onto a randomly oriented line. If we number the points of G from left to right on the line $1, 2, \ldots, n$ then there are $n - 1$ cuts of the form $(\{1, 2, \ldots, i\}, \{i + 1, i + 2, \ldots, n\})$. The final step of the algorithm returns the cut $(S, \bar{S})$ among these which has the smallest sparsity $\Phi(S)$.

Remarkably, it turns out that with high probability, the cut we return after step (3) will be within a factor C of optimal, where C is the distortion of the embedding from step (2)!

After discussing this general approach, we will examine the new techniques that achieve the best-known approximation factor for Sparsest Cut. These are based on semi-definite programming and novel high-dimensional arguments from [ARV04] (see also [Lee05, CGR05]), as well as new techniques for constructing low-distortion embeddings [KLMN05, Lee05, ALN05].

References

[ALN05] S. Arora, J. R. Lee, and A. Naor. Euclidean distortion and the Sparsest Cut. In *37th Annual Symposium on the Theory of Computing*, pages 553–562, 2005. Full version available at `http://www.cs.berkeley.edu/~jrl`.

[AR98] Yonatan Aumann and Yuval Rabani. An $O(\log k)$ approximate min-cut max-flow theorem and approximation algorithm. *SIAM J. Comput.*, 27(1):291–301 (electronic), 1998.

[ARV04] Sanjeev Arora, Satish Rao, and Umesh Vazirani. Expander flows, geometric embeddings, and graph partitionings. In *36th Annual Symposium on the Theory of Computing*, pages 222–231, 2004.

[CGR05] S. Chawla, A. Gupta, and H. Räcke. Embeddings of negative-type metrics and an improved approximation to generalized sparsest cut. In *Proceedings of the 16th Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 102–111, Vancouver, 2005.

[KLMN05] R. Krauthgamer, J. R. Lee, M. Mendel, and A. Naor. Measured descent: A new embedding method for finite metrics. *Geom. Funct. Anal.*, 15(4):839–858, 2005.

[Lee05] James R. Lee. On distance scales, embeddings, and efficient relaxations of the cut cone. In *SODA '05: Proceedings of the sixteenth annual ACM-SIAM symposium on Discrete algorithms*, pages 92–101, Philadelphia, PA, USA, 2005. Society for Industrial and Applied Mathematics.

[LLR95] N. Linial, E. London, and Y. Rabinovich. The geometry of graphs and some of its algorithmic applications. *Combinatorica*, 15(2):215–245, 1995.

Distance Trisector curve and Voronoi diagram with neutral zone

Takeshi Tokuyama (Tohoku U)
joint work with Tetsuo Asano (JAIST)
and Jiri Matousek (Charles U)

Grand Challenge of NHC project

- Throw right on **Computational Barriers**
  - Identifying barriers (something **looking impossible**)
  - Breaking/proving/avoiding barriers
  - Making properties of barriers clearer
  - Well-known barriers in TCS
    - Computability
    - P vs NP, NP vs PSPACE etc
    - Approximation hardness, approximation ratio
    - Randomness (P vs PP, primarity checking, Yao's minmax principle)
    - Lower bounds for online algorithms
    - Cryptographic barriers (Discrete log etc)
  - Hopefully, find some more new barriers, because they will help progress of TCS

Classical barriers in math history

Let no one ignorant of Mathematics enter here. (plato)

- Incomputable geometric/arithmetic problems
  - Compute diagonal length of a unit square
  - Find a cube of volume 2
    - Dilemma of Pythagoreans
  - Draw a circle with the unit area
    - *It is easier to square the circle than to get round a mathematician.* *August de Morgan*
  - Draw regular n-gon
  - Trisect a given angle

Progress in math history

God created the integers, all else is the work of man.
(*Leopold Kronecker*)

- *Necessity is the mother of invention.*
  - Diagonal length computation — Irrational numbers
  - Cube with volume 2 — Radicals
  - Unit area circle — Transcendental number π
  - Draw regular n-gon
  - Trisect a given angle

  → "Solvability" of algebraic equations → Complex numbers, Groups, Elliptic functions

Inventing tools to measure what we cannot directly measure.

Same in CS: NP-complete theory, Proof checking,….

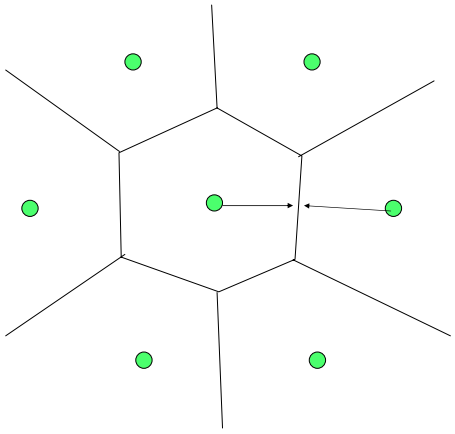
Tool to resolve a small but curious barrier.

Story of this talk

- In a computational geometric problem , we find a simple and natural geometric tool named *distance trisector curve*.
- A new transcendental curve??
- Some initial results have been obtained
  - Existence and uniqueness of the trisector curves
  - An algorithm to compute it.
  - Use of the trisector curves.
- A new possibility in computational geometry
  - Relaxed "computability" of geometric problems.

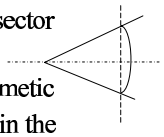
Voronoi diagram

- Subdivision of plane (space) into cells
  - $S = \{p_1, p_2, \ldots p_n\}$ points in the plane
  - $V(p_i) = \{ x : d(x, p_i) < d(x, p_j)$ for all $j \neq i\}$
    - Voronoi cell: dominating region of p_i
- Great geometric structure with many applications
  - Mesh generation , Graphics,
  - Simulating economic/political equilibrium
  - Simulating biological cells / crystallization
- Efficient algorithm : O(n log n) time
- Many variants: VD of lines/discs/regions, higher dimension, non-Euclidean metric, power diagrams.



Voronoi diagram is easy

- Drawn by using "perpendicular bisectors"
  - Anciently known how to draw the bisector
    - Tool to bisect an angle
  - Can be drawn by using rational arithmetic
  - It is trivial that a Voronoi diagram is in the arrangement of bisectors (size is polynomial)
    - Naïve polynomial time algorithm
    - Only need to speed up the computation
  - Known variants are also mathematically conventional



Motivation from nature

- We often see beautiful patterns with "objects" and "neutral zone" in natural structures
- Can we have a variation of Voronoi diagram to draw such a picture?

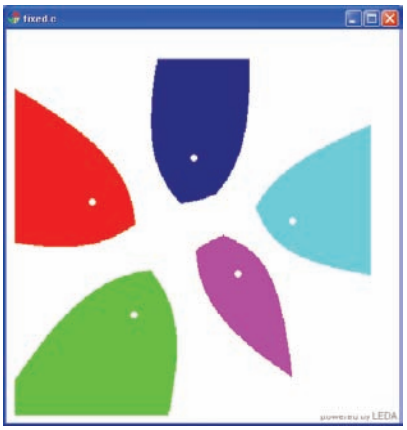






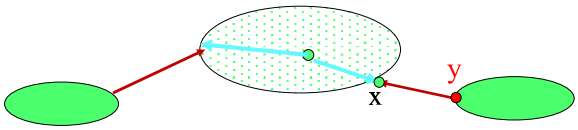
Voronoi diagram with neutral zone

- Classical Voronoi diagram: Partition the plane (space) into domination regions of input points.
- Idea: Partition the space (plane) into domination regions and a *neutral zone*
  - There may be many mathematical formulations
  - We adopt a natural formulation



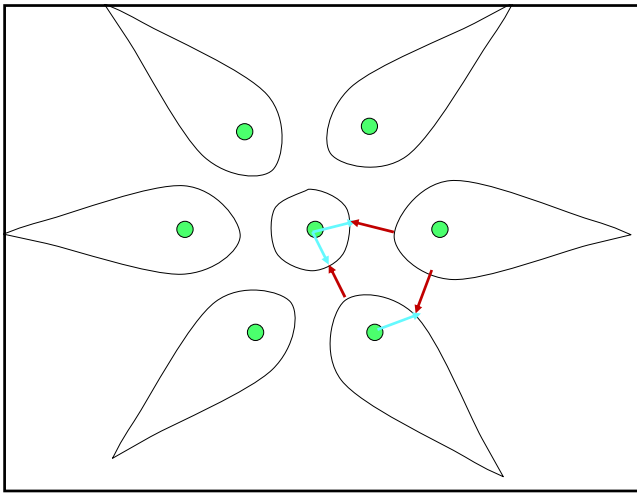
Definition of N-Voronoi diagram

- $S = \{p_1, p_2, \ldots p_n\}$ points in the plane
- $NV(p_i) = \{ x : d(x, p_i) < d(x, y)$ for every $y \in NV(p_j)$ for $j \neq i\}$



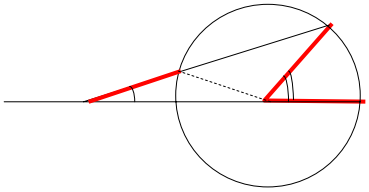
N-Voronoi diagram on 7 points

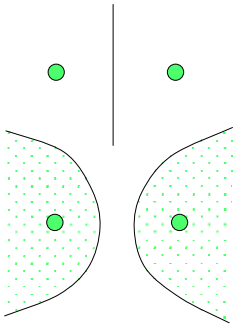




Questions

- Bisector ??
- **Distance trisector curves:**
  - Known or unknown?
  - As easy as angle trisection?

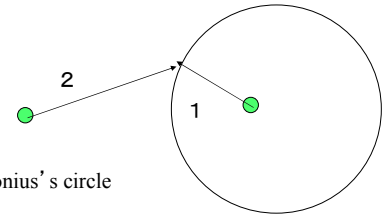




Ruler, Compass, and red-ink (Archimedes)

Distance trisector

- Different from Apollonius's circle
- Natural and simple definition (see next slide)
- Surprisingly, seems to be a new curve



Apollonius' s circle

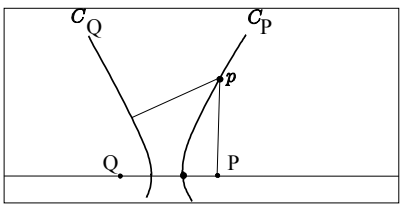
Distance Trisector Curves

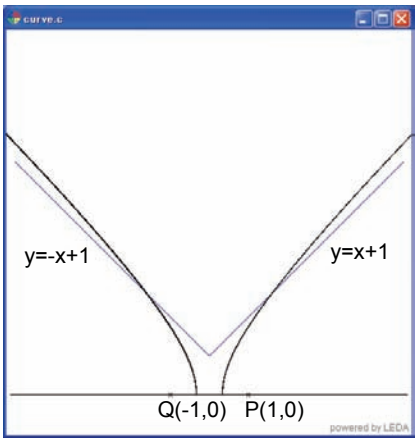
Equally-spaced curves C_P and C_Q:

for any point p on C_P, ***dist(p, P) = dist(p, C_Q)*** and

for any point q on C_Q, ***dist(q, Q) = dist(q, C_P)***.

where ***dist(p, C)*** is the distance from ***p*** to a point on ***C*** that is closest to p.

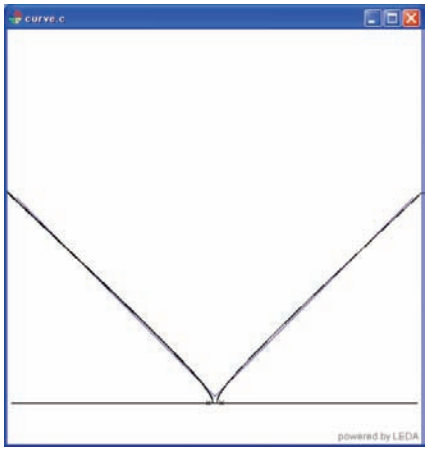




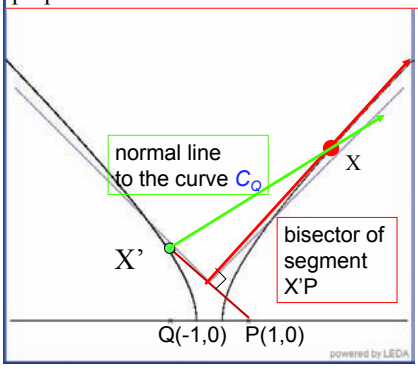
Note:

Drawing curves was not easy.

Only possible after revealing some theoretical results



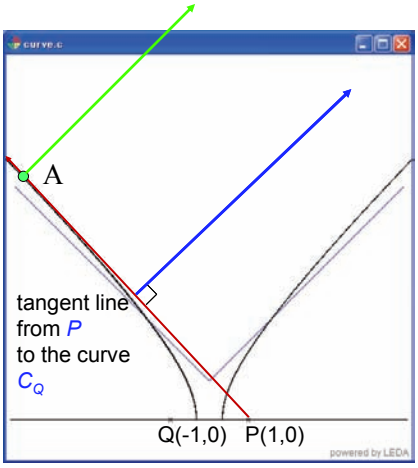
Observation: Each point X on C_P is the intersection of the normal line of C_Q at its partner point X' and the perpendicular bisector of X'P



Corollary.

If we exactly determine C_P at a small neighbor of P, we can determine whole C_P

We have a system of differential equation



Implication

•No point beyond the tangent point A can be a partner point of a point of NV(P)

Indeed, it suffices to compute C_P for x<5.65

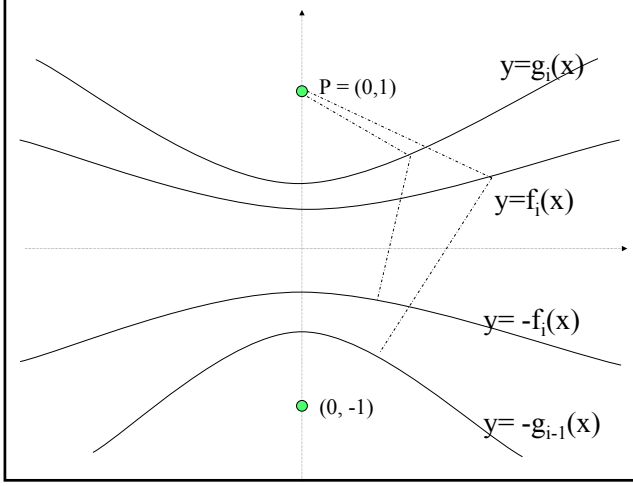
Nice nature of the curve

- Convex and smooth (revealed to be analytic)
- Satisfies a system of differential equations
  - Specialists did not know how to solve it
- It suffices to compute in the range [0, 5.65]
  - Important curves satisfy this
    - sin (x) $[0, 2\pi]$, log x [1,10]
- Problems: Existence, uniqueness, computation

Existence and uniqueness

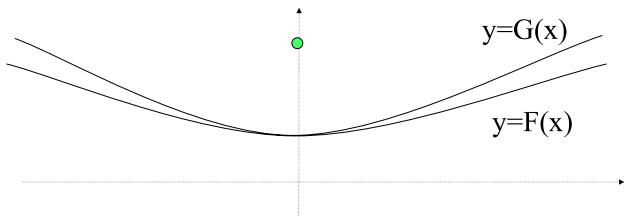
- P=(0,1), Q = (0,-1)
- $y=f_1(x)$ is x-axis (bisector of PQ)
- $y = g_1(x)$:bisector parabola of P and x-axis
- $y=f_j(x)$: bisector curve of P and $y=-g_{j-1}(x)$
- $y=g_j(x)$:bisector curve of P and $y= -f_j(x)$

Lemma. The trisecting curve C_P must be above $f_j(x)$ and below $g_j(x)$



Lemma: The series $f_j(x)$ and $g_j(x)$ converges to continuous functions F(x) and G(x),respectively

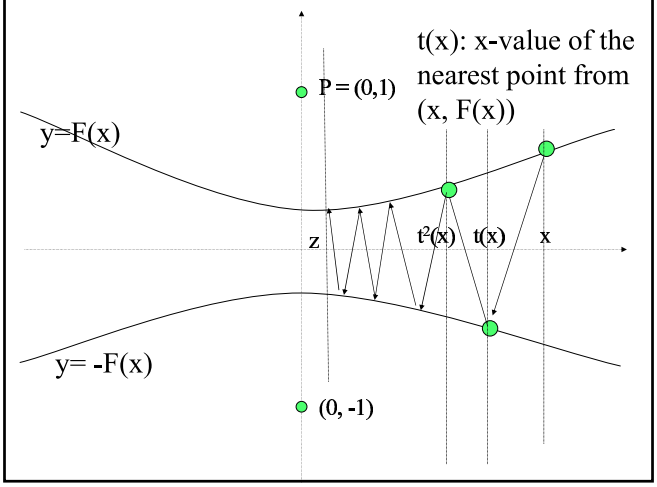
Theorem (**Existence and Uniqueness**) . G(x) ≡ F(x), and y= F(x) gives the trisector curve C_P

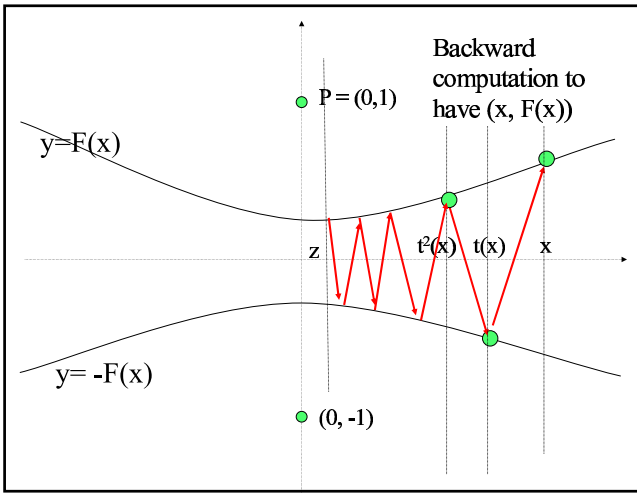


Computation of F(x)

- Given a value of x >0 , compute F(x) to any precision (error is smaller than given ε)

Theorem. We can compute F(x) to the accuracy ε in O(log ((1+x) / ε)) time





Idea for computing F(x)

- If -t(x) is the x-value of the partner point, $t(x) < \beta x$ for a constant $\beta < \sqrt{3} - 1 < 1$
- We can compute the Taylor expansion of F(x) and t(x) around zero to any precision.
  - F(x) and t(x) are computable if x < h for a small h.
- F(x) and x are computable from t(x), t(t(x)), F(t(x)), and F(t(t(x))).
- Guess $z = t^k(x) < h$, compute F(z) and F(t(z)), and recursively compute $t^i(x)$ for i=k, k-1, k-2, …, 0
- Determine correct value of z via binary search

Formulas to compute F(x)

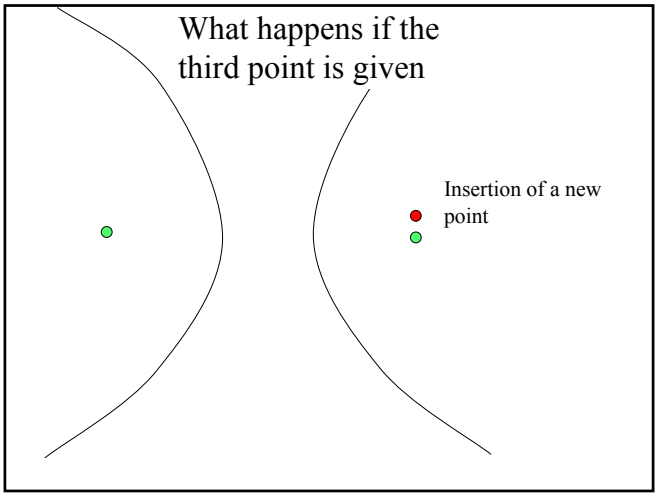
- $x = \Phi(t(x), t(t(x)), F(t(x)), F(t(t(x)))$
- $F(x) = \psi(t(x), t(t(x)), F(t(x)), F(t(t(x))))$

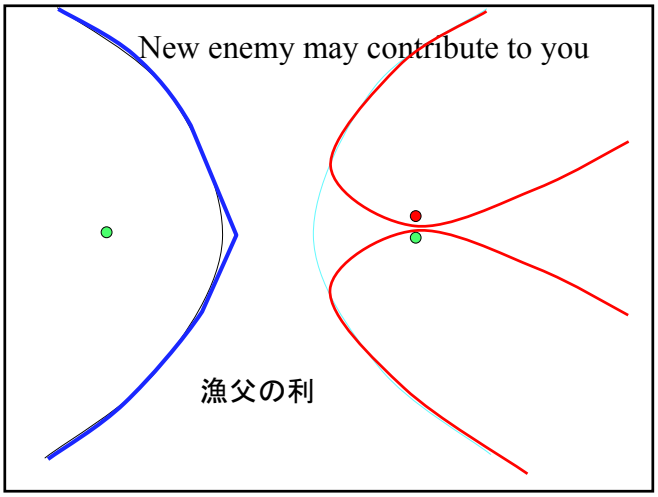
- $\Phi(x,y,u,w) = x + y(x^2+(1+u)^2)/2Q(x,y,u,w)$
- $\psi(x,y,u,w) = (2xyu +(1+u)(1+x^2-u^2)) /2Q(x,y,u,w)$
- $Q(x,y,u,w) = (1+u)(1+v)-xy$

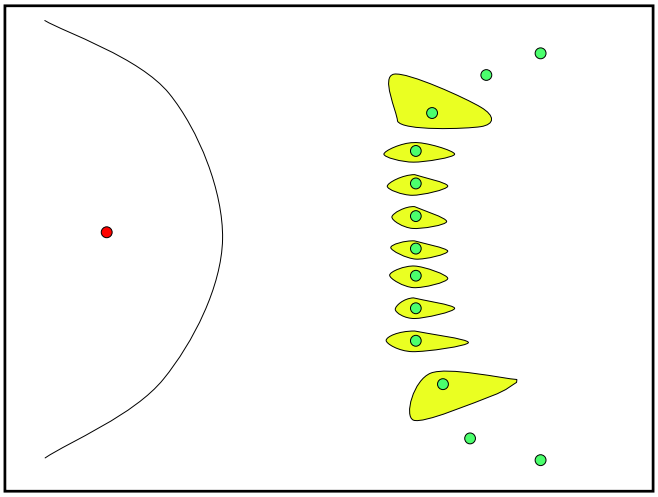
The above mentioned: STOC06, to appear

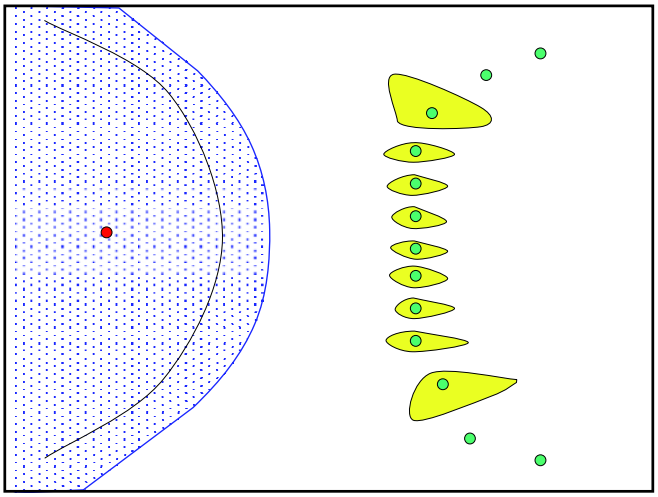
N-Voronoi diagram on many points

Now we have trisector curves.
Can we draw N-Voronoi diagram of more than two points by using them??







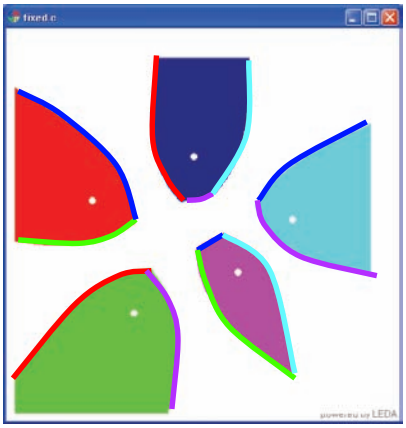


Basic properties

- Boundary curve of $NV(p_i)$ is the **bisector** between p_i and (the union of) boundary curves of other regions
- Each region is **convex** and nonempty
- It may happen that there is no unbounded region (different from an ordinary Voronoi diagram)

Voronoi edges

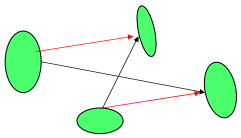
- Definition: If p is a boundary point on NV(p_i) and q is its nearest point among other region boundaries, we call q the partner point of p.
- Definition: The boundary of NV(p_i) is decomposed into curve segments each of which consists of points whose partner points are in a same region. The connected components are called Voronoi edges.



Combinatorial complexity

- Theorem. Number of Voronoi edges is O(n) in an N-Voronoi diagram on n points.

  Proof: Rays towards nearest enemy's-boundary do not cross each other (cheating a little) reduced to the linearity of number of edges in a planar graph +Davenport-Schinzel sequence argument.



Questions

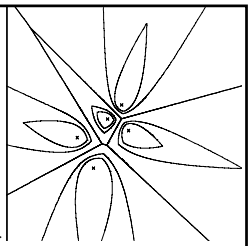
- N-Voronoi diagram always exists?
  - Yes
- Unique for a given point set?
  - Yes
- Efficient algorithm exist?
  - Yes, if we are given some oracles
- Really efficient in practice?
  - No……

Existence

Given a set of regions $R_1, R_2, \ldots R_n$ such that R_j contains p_j, consider an operator $\boldsymbol{F}$

$\boldsymbol{F}(R_1, R_2, \ldots R_n) = (Q_1, Q_2, \ldots Q_n)$

where $Q_j = \{ x: d(x, p_j) < d(x, y)$ for $\forall y \in \cup_{i \neq j} R_i \}$



Theorem. F has at least one fixed point

From Schauder-Kakutani's fixed point theorem

Corollary. N-Voronoi diagram is given as a fixed point of F

Note: Fixed point theorem

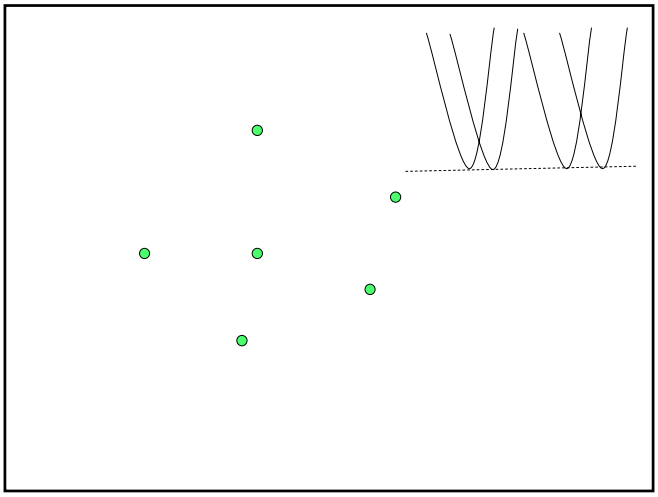
Brower(1910),Schauder(1930),Kakutani(1941)

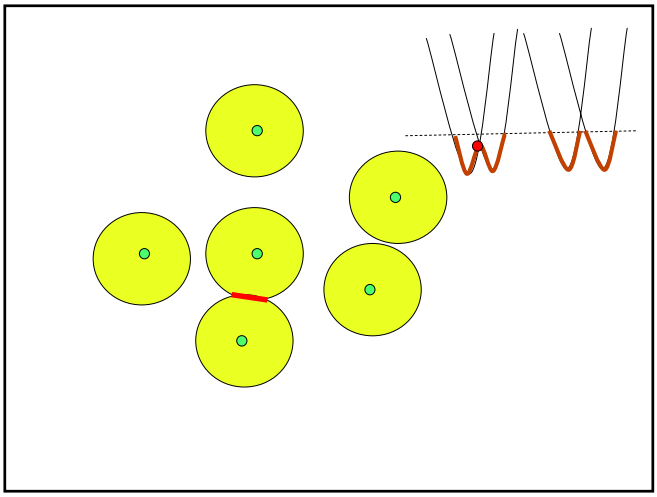
Z: Banach space,
K: Compact convex subset of Z (nonempty)
F: K K continuous map
Then, F has a fixed point

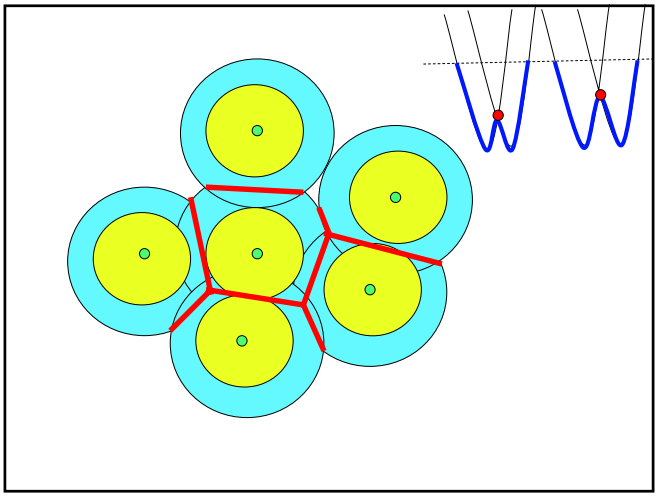
- Z: space of n-tupple of convex regions ($R_1, R_2, .. R_n$)
- We need to introduce norm, and define convexity etc…
- Continuous dimensional space (Shauder-Kakutani's version)

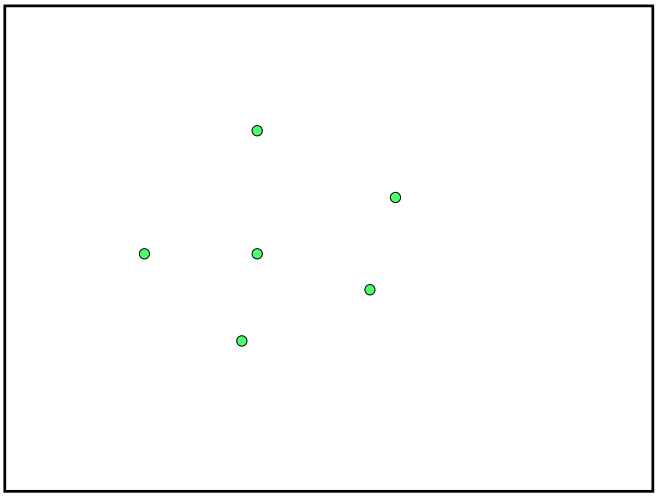
Uniquness

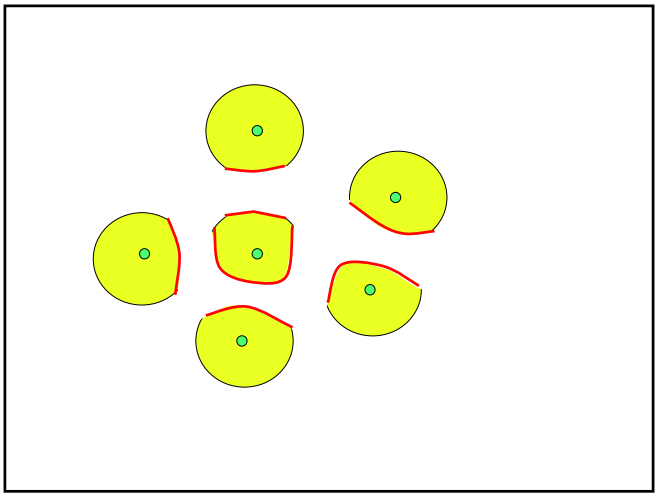
- Fixed point theorem does not assure uniqueness.
- Uniqueness is given in a constructive fashion
- Crystallization algorithm:
  - Growing radius of disks
  - Analogous to the space-sweep algorithm for computing a (classical) Voronoi diagram as a lower envelope of parabolic cylinders.

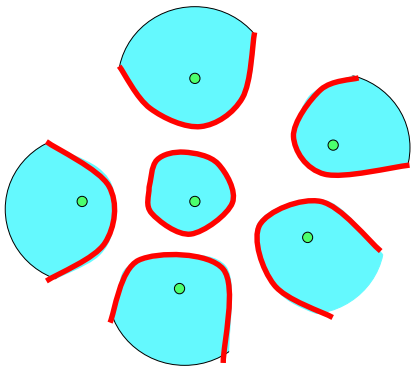












Curves in a N-Vonoroi diagram

Property 1: N-Voronoi diagram is a subset of an arrangement of curves in a curve family F

F consists of :

•Distance trisectors of pairs of input points are in F.

•Bisector curves of an input point and a curve (or point) C in F.

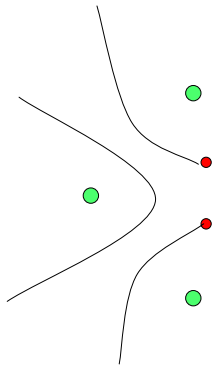
• Intersection points of curves in F.

Property 2: The number of applications of bisector operations is finite to obtain F

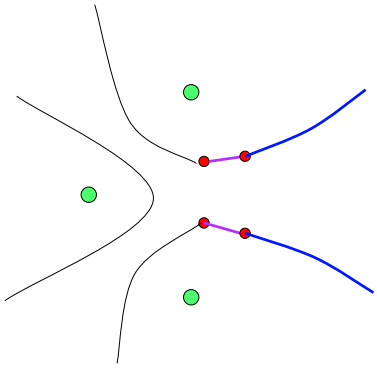
Analysis of crystallization algorithm

- For planar case, the algorithm shows uniqueness of N-Voronoi diagram
- Number of "structural changes" is O(n)
- Terminates in finite steps if we can draw
  1. bisector curve of a point and given point
  2. distance trisector curve
- Terminates in polynomial time if we assume that we can draw an "generalized" trisector curve

Generalized trisector curves



Generalized trisector curves



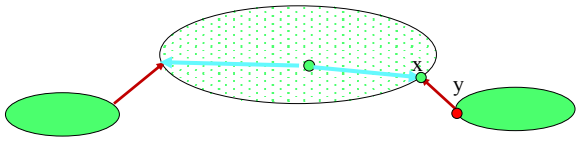
Some more ideas and problems

- Computability of geometric problems
  - Is the N-Voronoi diagram computable?
  - Bisector of a point and a curve not easy
    - Not difficult in digital (pixel) geometry
  - Especially, the trisector curves are only given by point-wise enumeration
    - Same situation as sin and cos curves.
  - Current algorithm needs iterative computation of bisectors accumulating error!
  - Is there fundamental difference from some "paper algorithms" in computational geometry?

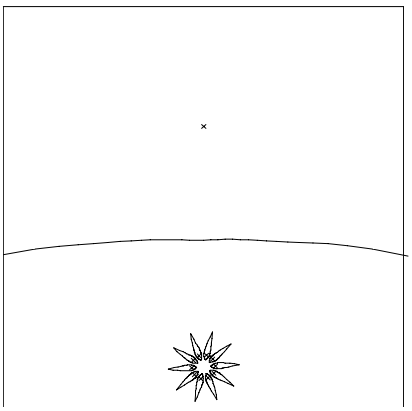
Generalized N-Voronoi diagram

- $S = \{p_1, p_2, \ldots p_n\}$ points in the plane
- $GNV(p_i) = \{ x : d(x, p_i) < \alpha\ d(x, y)$ for every $y \in GNV(p_j)$ for $j \neq i\}$

if $\alpha \to \infty$, Voronoi diagram.



Convexity fails in an N- Voronoi diagram for $\alpha = 1.5$

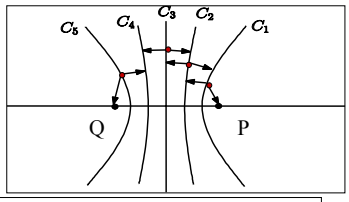


Multi-sector curves

- Given two points ***P*** and ***Q*** in the plane and an integer ***n***, draw *n* equally-spaced curves $C_1, C_2, \ldots, C_n$ between them s.t. for any point *p* on a curve C_i,

  $dist(p, C_{i-1}) = dist(p, C_{i+1})$

  $C_0 = P$, and $C_{n+1} = Q$



Trisector is the case where n=2

Conclusion

- N-Voronoi diagram: Interesting generalization of Voronoi diagram that admits a neutral zone.
- Many unsolved questions:
  - Is the trisector curve really transcendental?
  - Concrete analysis of N-Voronoi diagram algorithms.
  - Uniqueness of N-Voronoi diagram of a given point is not clear for high-dimensional cases
  - Generalization for $\alpha > 1$ (convexity fails)
  - N-sector curves