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18年度 成果報告書

平成19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 . . . 5
ミニプロジェクト . . . 6
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」 . . . 7
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」 . . . 8
国際ワークショップ Workshop on Improving Exponential-Time Algorithms . . . 10
NHC 秋学校 (NHC Autumn School on Discrete Algorithms) . . . 11
国際会議における特別セッション企画 . . . 13
第 19 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 . . . 14
ミニ研究集会 (列挙合宿) . . . 16
ミニシンポジウム「新世代計算限界と地球環境問題」 . . . 17
ミニ研究集会 (Complexity) . . . 19
ミニ研究集会 (暗号理論) . . . 21
ミニ研究集会 (組合せゲーム・パズル) . . . 24
電子情報通信学会 COMP-NHC 学生シンポジウム . . . 26
ミニ研究集会 (列挙合宿:その 2) . . . 27
第 20 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 . . . 41
A03: 論理関数表現のモデルとシンボリックアルゴリズム . . . 56
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 . . . 64
A05: ハードウェアアルゴリズムの性能評価に関する研究 . . . 75
A06: 幾何的配置問題の計算量限界と近似可能性の研究 . . . 83
A07: 現実的な状況下での量子計算の能力に関する研究 . . . 93
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 . . . 108
A09: 非明示的表現に対するアルゴリズムの開発 . . . 123
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 . . . 134
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 . . . 149
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 . . . 157
B03: 量子論理回路の最適化に関する研究 . . . 174
B04: 回路計算量の下限の研究とその応用 . . . 185
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 . . . 189

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 196
C01: グラフ描画アルゴリズムとその Web 情報検索への応用 213
C02: 連続と離散の統合によるロバストアルゴリズム構築 225
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 . 245
C04: 実践的な列挙アルゴリズムの理論構築 257
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 268
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 291
C07: Web コンテンツ活用に関連した離散最適化問題の研究 317
C08: 高性能近似アルゴリズムの設計法に関する研究 327
C09: ネットワーク問題のモデル化とアルゴリズムの研究 338
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 364
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 381

3. 各種資料 **391**
ニュースレター 第 5 号 393
ニュースレター 第 6 号 401
平成 18 年度 第 1 回 全体会議 講演資料 412
平成 18 年度 第 2 回 全体会議 講演資料 446
NHC Autumn School on Discrete Algorithms 講演資料 473

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 (京都大学)，堀山貴史 (埼玉大学)

1.1　活動の概略

今年度は，秋学校１件，国際会議ICALP'06のワークショップiETA，電子情報通信学会総合大会の第２回目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第２回目の招待講演セッション１件，ミニシンポジウム１件，ミニ研究集会５件，全体会議２件，幹事会１件，外部識者との意見交換会１件を行った．さらに教科書シリーズとして「アルゴリズム・サイエンス・シリーズ」を共立出版より発刊を開始し，電子情報通信学会誌和文論文誌Aおよび英文論文誌Dから、それぞれ特集号を発行した。また、計画中の企画として，国際会議HERCMA2007内のミニシンポジウム，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３回目の招待講演セッション，電子ジャーナルの発行の計画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15名の研究者を招聘（上記の秋学校の講師を含む）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．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．

秋学校

本特定領域研究の主催で，以下の秋学校を開催した．

会議名 NHC Autumn School on Discrete Algorithms

日程 2006年11月15日〜17日

場所 サンパレア瀬戸 愛知県労働者研修センター（愛知県瀬戸市）

内容 招待者による講義5件

参加登録者数 78名（うち学生51名）

国際ワークショップ iETA2006

ICALP'06のサテライト・ワークショップとして以下の企画を行った。

会議名 iETA2006

日程 2006年7月16日

場所 ベニス国際大学 (Venice International University)，ベニス

内容 招待チュートリアル講演3件，一般講演8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 2007年3月20日 13時55分〜17時30分

場所 名城大学 天白キャンパス

内容 学生講演7件，投票により優秀発表賞を1件選出．

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19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．

セッション名 新世代の計算限界

日時 2006年4月24日 13時30分〜17時

場所 軽井沢プリンスホテル西館

内容 講演3件．

ミニシンポジウム

企画名 新世代計算限界と地球環境問題

日時 2006年12月5日〜6日

場所 東京大学本郷キャンパス

内容 招待講演2件, 一般講演11件．

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．本年は以下の5件が実施された．

列挙アルゴリズム（１回目）

2006年9月28日〜30日, 群馬大学

Complexity

2006 年 12 月 28 日, 電気通信大学

暗号

2007 年 3 月 2 日〜3 日, 電気通信大学

組合せゲーム・パズル

2007 年 3 月 16 日, 豊橋技術科学大学

列挙アルゴリズム（2 回目）

2007 年 3 月 27 日〜29 日, 群馬大学

全体会議（2006 年度第 1 回目）

日時 2006 年 6 月 21 日〜22 日

場所 九州大学 箱崎キャンパス

内容 特別招待講演 1 件, 講演 3 件, 未解決問題セッション, 全体討論

全体会議（2006 年度第 2 回目）

日時 2006 年 11 月 18 日 10 時〜15 時 30 分

場所 名古屋大学

内容 本特定領域研究のまとめと今後の課題についてそれぞれ 1 件ずつの講演とディスカッション（全体討論）, 講演（研究発表）2 件

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．本年度は幹事会を 1 回行った．

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）．

幹事会 2006 年 6 月 22 日 11 時 30 分〜13 時, 九州大学

外部有識者との意見交換会

外部有識者を全体会議に招き，その後，本特定領域研究について忌憚の無い意見を聞き，意見交換を行った．

日時 2006 年 11 月 18 日　15 時 30 分〜17 時 30 分

場所 名古屋大学

参加者 外部有識者（12 名）： 稲垣康善教授（愛知県立大学），喜連川優教授（東京大学），小柳義夫教授（工学院大学），有村博紀教授（北海道大学），大堀淳教授（東北大学），五十嵐健夫助教授（東京大学），鳥居宏次特任教授（奈良先端科学技術大学院大学），田中和之助教授（東北大学），萩谷昌己教授（東京大学），岩野和生所長（日本アイ・ビー・エム株式会社執行役員・大和ソフトウエア開発研究所），市川晴久所長（NTT 先端技術総合研究所），松山隆司教授（京都大学）

特定領域研究側: 領域代表者他 9 名

招聘研究者

以下の研究者を招聘した．なお，*印は秋学校の講師でもある．

1. Andrzej Lingas (Lund University), 2006.5.10–2006.6.9
2. Ming-Yang Kao (Northwestern University), 2006.6.10–2006.8.20
3. Bruce Reed (McGill University), 2006.8.1–2006.9.1
4. Wolfgang W. Bein (University of Nevada, Las Vegas), 2006.8.6–2006.12.29
5. Oscar Ibarra (University of California-Santa Barbara), 2006.8.16–2006.9.17
6. M. Grazia Speranza (Universita' Degli Studi Di Brescia), 2006.10.10–2006.10.14
7. Tibor Szabo (ETH Zurich), 2006.11.8–2006.11.21 *
8. Kirk Pruhs (University of Pittsburgh), 2006.11.11–2006.11.18 *
9. Thomas Erlebach (University of Leicester), 2006.11.11–2006.11.19 *

10. Uri Zwick (Tel Aviv University), 2006.11.11–2006.11.21 *
11. Magnus Halldorsson (University of Iceland), 2006.11.12–2006.11.19 *
12. Rusins Freivalds (University of Latvia), 2006.11.17–2006.12.5
13. Bruce Reed (McGill University), 2006.12.16–2007.2.22
14. Mario Szegedy (Rutgers, the State University of NJ), 2007.1.8–2007.5.1
15. Dieter van Melkebeek (University of Wisconsin), 2007.3.4–2007.3.16

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** 玉置卓
   期間 2006.4.1–2007.3.31
   機関 京都大学
2. **氏名** 山本真基
   期間 2006.4.1–2007.3.31
   機関 京都大学

2　教科書シリーズ

担当：杉原厚吉 (東京大学)，室田一雄 (東京大学)，山下雅史 (九州大学)，渡辺治 (東京工業大学)

本特定領域を高校生および大学初年度生に紹介して，若い人たちへこの分野に対する興味を喚起するとともに，この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学習指針を整備することを目的として，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．共立出版社の理解を得ることができ，同社より順調に出版が進んでいる．今までに出版した本は次のとおりである．

1. 浅野哲夫：「アルゴリズム・サイエンス：入口からの超入門」
2. 岩間一雄：「アルゴリズム・サイエンス：出口からの超入門」
3. 荻原光徳：「複雑さの階層」
4. 浅野哲夫：「計算幾何」
5. 阿久津達也：「バイオインフォマティクスの数理とアルゴリズム」

全部で 16 巻を予定しており，以下順次刊行が進む見通しである．

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)

昨年度構築した論文サーバが，設置場所 (九州大学) の移転の際に壊れてしまった．そこで新しいマシンを用意し再度論文サーバを立ち上げた．URL は以前と同じ http://eprints.csce.kyushu-u.ac.jp である．使用しているソフトは前回同様 EPrints (http://www.eprints.org) であるが，バージョンが 3 になり，機能が追加されている．

平成 19 年度第 1 回全体会議 (2007 年 5 月, 東京大学) の全体討論において，特定領域に参加している研究者に使用方法等の詳細を周知する予定である．

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 5 号を 8 月中旬に，第 6 号を 12 月初旬に発行した．

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，現在

http://keisan-genkai.lab2.kuis.kyoto-u.ac.jp/newsletter/index.html

に掲載してある．

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 5 号・第 6 号について，それらの目次を示す．5 号では公立はこだて未来大学高木剛先生に，ドイツでの滞在体験を語っていただいた．また，第 6 号では広島大学の藤田先生による研究紹介，京都大学山本先生による ICALP 参加報告，豊橋技術科学大学岡本先生による秋学校の開催報告を掲載した。いずれも，執筆者の顔の見える報告・紹介となっており，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 5 号目次:

１．ドイツの長期滞在体験　　－ 高木 剛 (公立はこだて未来大学)
２．18 年度第１回全体会議を振り返って　　－ 山下 雅史 (九州大学)
３．2006 年度第 1 回全体会議討論会 － 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 6 号目次:

１．研究紹介 － 藤田 敏 (広島大学)
２．ICALP06 in Venice 報告書 － 山本 真基 (京都大学)
３．平成 18 年度秋学校で実現できたことと実現できなかったこと－ 岡本 吉央 (豊橋技科大)
４．2006 年度第 1 回全体会議討論会 － 事務局
５．イベントカレンダー ＋ 事務連絡
６．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)

昨年度のようなセミナーを開催することはしなかった．しかし、本特定領域における計算幾何学の研究者は連携を取って国内外の研究者と研究を推進することで，多くの成果を挙げることができた．次年度は 2 回目のセミナーを実施する計画である．

5.2　列挙アルゴリズム

担当： 中野 眞一 (群馬大学)

最適化，知識発見，データベース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みつつある．列挙アルゴリズムは本質的に大規模データを扱うため，様々な技術を用いて高効率化する必要がある．また，列挙アルゴリズムは，離散構造のランダム生成や，コンパクトなコード化等とも深い関連がある．本ミニプロジェクトでは，本年度も 2 回の 2 泊 3 日の研究集会を群馬大学伊香保研修所にて開催した．列挙をキーワードに多分野にわたる研究発表があり，これをきっかけとして多くの共同研究が進行中である．今後とも，様々な共同研究が生まれるよう，定期的に研究集会を開催する予定である．

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，昨年度の第 1 回目に引続き，組合せゲームとパズルに関する第 2 回目のミニ研究集会を，2007 年 3 月 16 日に京都大学で行った．8 件の一般講演が行われた．その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．昨年度からの進展の報告もあり，順調な進展を思わせた．

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)

本年度は周辺領域の研究者との積極的交流を強く意識しつつ２回のミニ研究集会を開いた．２００６年１０月開催の１回目の集会は暗号やアルゴリズムに関する講演を中心とした．２００６年１２月開催の２回目の集会は「数学基礎論と計算量理論」をテーマとし数学基礎論特に証明論と計算量理論の研究者が交流し議論する貴重な機会となった．ミニ研究集会以外に東工大における定期的 complexity セミナーなどが本分野の研究展開に効果的なものとなっており，全体的に「計算量・ブール関数」関連の研究は活発な展開が続いている．

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)

本特定領域で行っている研究テーマが，地球環境問題にどのように関わり得るか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，本ミニプロジェクトを遂行している．最適化は資源の有効利用を目指すものであるから，多くのアルゴリズムは，地球資源の有効利用につながるはずである．そこで，本領域の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，ミニシンポジウムを開催した．また，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した．

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した．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月に発行することができた．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．本特集号は Special Section on Invited Papers from New Horizons in Computing として 2006 年 8 月電子情報通信学会英文論文誌 (Volume E89-D, No. 8) に掲載された．タイトル, 著者及びページ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), pp.2332-2339.

(2) Online Allocation with Risk Information (Shigeaki Harada, Eiji Takimoto, Akira Maruoka), pp.2340-2347.

(3) Inserting Points Uniformly at Every Instance (Sachio Teramoto, Tetsuo Asano, Benjamin Doerr, Naoki Katoh), pp.2348-2356.

(4) A Polynomial Time Algorithm for Obtaining a Minimum Vertex Ranking Spanning Tree on Outerplanar Graphs (Shin-ichi Nakayama, Shigeru Masuyama), pp.2357-2363.

(5) Finding a Triangular Mesh with a Constant Number of Different Edge Lengths (Shinichi Tanigawa, Naoki Katoh), pp.2364-2371.

(6) An Efficient Algorithm for Evacuation Problem in Dynamic Network Flows with Uniform Arc Capacity, (Naoyuki Kamiyama, Naoki Katoh Atsushi Takizawa), pp.2372-2379.

(7) A $(2 - c\frac{logN}{N})$-Approximation Algorithm for the Stable Marriage Problem (Kazuo Iwama, Shuichi Miyazaki, Kazuya Okamoto), pp.2380-2387.

(8) Computing Automorphism Groups of Chordal Graphs Whose Simplicial Components Are of Small Size (Seinosuke Toda), pp. 2388-2401.

(9) The Even Outdegree Conjecture for Acyclic *PLCP*-Cubes in Dimension Five (Sonoko Moriyama, Yoshio Okamoto), pp. 2402-2404.

(10) Approximated Vertex Cover for Graphs with Perfect Matchings (Tomokazu Imamura, Kazuo Iwama, Tatsuie Tsukiji), pp. 2405-2410.

7.3 おわりに

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.

国際ワークショップ
Workshop on Improving Exponential-Time Algorithms

担当： 渡辺 治 (東京工業大学)

1 会議の概要

平成 18 年 7 月 16 日にイタリアヴェニスにおいて，Workshop on Improving Exponential-Time Algorithms — Strategies and Limitations と題する国際ワークショップを開催した．

このワークショップは，ヨーロッパ理論計算機科学学会 *European Association of Theoretical Computer Science* の年次総会として毎年行う国際会議 Intn'l Conference on Automata, Languages and Programming の第 33 回会議 ICALP'06 に連接して行われる 9 つの関連ワークショップの 1 つとして採択され開催されたものである．会議は，Rolf Niedermeier (Univ. Jena) と渡辺治（東京工業大学）を委員長とし，岩間一雄（京都大学），伊藤 大雄（京都大学），F. Fomin (Univ. Bergen), D. Kratsch (Univ. Metz), J. Rothe (Univ. Duesseldorf) の各委員からなる実行委員会により運営された．

2 会議の内容

このワークショップでは，困難といわれおり，指数関数的な計算量を持つアルゴリズムしか見つかっていない問題に対して，我々がどの程度のそれらのアルゴリズムを改良できるかを，関連の研究者で集中的に議論するためのものとして計画した．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，新たな手法や限界を見極めるための手法について活発な議論を行った．

プログラムと発表論文については以下の通り．

1. Improving exponential-time algorithms for NP-complete problems (tutorial), *T. Riege and J. Rothe*
2. An improved exact algorithm for the domatic number problem, *T. Riege, J. Rothe, H. Spakowski, and M. Yamamoto*
3. Inclusion-exclusion algorithms for counting set partitions, *A. Bjoerklund and T. Husfeldt*
4. Fast exponential-time algorithms for the forest counting in graph classes, *H. Gebauer and Y. Okamoto*
5. Algorithms for the full Steiner tree problem, *T. Ito Y. Okamoto and T. Tokuyama*
6. Lower bounds on exponential time algorithms (tutorial), *D. Kratsch*
7. Treewidth and exact algorithms, *F.V. Fomin*
8. An exact algorithm for solving Max-Cut on graphs with bounded maximum degree, *F. Della Croce, M. Kaminski and V. Paschos*
9. TSP for degree-restricted graphs, *K. Iwama and T. Nakashima*
10. Techniques for practical fixed-parameter algorithms (tutorial), *F. Hueffner, R. Niedermeier, and S. Wernicke*
11. Improved fixed-parameter algorithms for non-crossing subgraphs, *M.M. Halldorsson, T. Tokuyama and A. Wolff*

NHC秋学校
(NHC Autumn School on Discrete Algorithms)

担当： 岩間 一雄，伊藤 大雄，堀山 貴史 (京都大学),
平田 富夫，高木 直史，柳浦 睦憲，高木 一義，小野 孝男 (名古屋大学),
増山 繁，藤戸 敏弘，岡本 吉央 (豊橋技術科学大学)
和田 幸一 (名古屋工業大学)

1　秋学校の概要と目的

平成 18 年 11 月 15 日から 17 日までの 3 日間，サンパレア瀬戸 (愛知県労働者研修センター) において，NHC Autumn School on Discrete Algorithms (離散アルゴリズムに関する秋学校) を開催した．これは本特定領域研究における第 3 回国際研究集会として位置付けられるものであるが，第 1 回 (平成 17 年 1 月) はワークショップのみ，第 2 回 (平成 18 年 3 月) は春学校とワークショップの併設であったことに対して，今回は秋学校のみの開催とした．これは多様なバックグラウンドを持つ本特定領域研究メンバおよび学生に対して，基礎的な事項から最先端の研究成果までを俯瞰できる学校形式の方が効果が高いと思われることが前回までの経験から得られたので，それを参考にした結果である．実行委員会メンバ (アイウエオ順) は伊藤大雄 (京都大学)，岩間一雄 (本特定領域研究代表，京都大学)，岡本吉央 (豊橋技術科学大学)，小野孝男 (名古屋大学)，高木一義 (名古屋大学)，高木直史 (名古屋大学)，平田富夫 (実行委員長，名古屋大学)，藤戸敏弘 (豊橋技術科学大学)，増山繁 (豊橋技術科学大学)，柳浦睦憲 (名古屋大学)，和田幸一 (名古屋工業大学)，堀山貴史 (京都大学)，である．

秋学校の招待講師として，Tibor Szabó (ETH Zurich)，Thomas Erlebach (University of Leicester)，Magnús Halldórsson (University of Iceland)，Uri Zwick (Tel Aviv University)，Kirk Pruhs (University of Pittsburgh) の 5 氏を迎えた．いずれも離散アルゴリズム分野の一線で活躍する研究者であり，最先端の話題に関する基礎的な事項から最新の研究成果まで 2 時間の講義と 1 時間の演習で紹介された．各講義の中間には 10〜15 分程度の休憩を一度設けた．また，演習に対する討議を行なう時間や各参加者が自由に討論をできる時間も個別に設けた．

参加登録者は 78 名で，そのうち 51 名が学生であった．講師も含めてほとんどの参加者は秋学校開催地の併設施設に宿泊し，寝食を共にすることで包括的な研究交流が可能となるようにした．

2　秋学校の内容

スケジュールは以下の通りである．

- 11 月 15 日 (水)
  - 11:00– 受付
  - 12:30– 昼食
  - 14:00–17:00 講義および演習
    Making vs. avoiding in positional games
    Tibor Szabó (ETH Zurich)
  - 17:00–18:00 演習討論
  - 18:00– 夕食
  - 20:00–23:00 自由討論
- 11 月 16 日 (木)
  - 8:00– 朝食
  - 9:30-12:30 講義および演習
    Approximation algorithms for geometric intersection graphs

Thomas Erlebach (University of Leicester)

- 12:30– 昼食
- 14:00–17:00 講義および演習
  Approximation techniques for graph coloring problems
  Magnús Halldórsson (University of Iceland)
- 17:00–18:00 演習討論
- 18:00– 夕食
- 20:00–23:00 自由討論

- 11 月 17 日 (金)
  - 7:30– 朝食
  - 9:00–12:00 講義および演習
    Fast matrix multiplication and graph algorithms
    Uri Zwick (Tel Aviv University)
  - 12:00– 昼食
  - 13:30–16:30 講義および演習
    Scheduling algorithms for power management
    Kirk Pruhs (University of Pittsburgh)

講義の内容は組合せゲームと閾値現象 (Szabó), 幾何グラフに対する精度保証付き近似アルゴリズム (Erlebach), グラフ彩色およびスケジューリング問題に対する精度保証付き近似アルゴリズム (Halldórsson), 高速行列乗法のグラフアルゴリズムへの応用 (Zwick), 電力消費と CPU 速度のトレードオフを考慮したスケジューリング問題に対するオンラインアルゴリズム (Pruhs) といった基本的かつ最先端のトピックスであった. また, 演習においては 4〜6 人のグループに分かれて, 議論をしながら演習問題を解き, 講義内容を深く理解する助けになった. 演習討論では, 各グループの議論内容を発表し, 意見交換を行なった. 自由討論では, 泊り込みであることの利点を生かし, 小さなグループに分かれて様々な話題に関して自己組織的にディスカッションが始まり, 講師も交えて貴重な時間を過ごすことが出来た.

3 総括

昨年度開催の春学校の反省点を引き継ぎつつ今回の秋学校を開催したが, 口頭で参加者の感想を聞いたところ, 概ね良好だった. 参加者の感想を包括的にまとめて今後にフィードバックするため, 紙によるアンケートを行なうことも効果的であろう.

「講義内容や演習内容が難解であった」という指摘もあった. これは講師に対する依頼方法が曖昧であったため, 聴衆の前提知識の多様性や時間の制約に関する意図が講師に伝わり切っていなかったことが原因であったと思われる. 今後はその点を改善した企画・運営が必要である.

開催期間が 3 日間であったことは, 短すぎず長すぎず, 適当であった.

学校の主役は学生である. 日本各地から多くの学生の参加があり, 熱心な議論が展開されたことは大きな喜びであった. 学生がこの秋学校から研究内容だけでなく, 研究姿勢, 学習姿勢, 異文化理解, 異分野理解など多くのことを学び, 感じ取ったことを期待したい. また, 学生に積極的な参加を呼びかけてくれた関係諸氏にも感謝したい.

国際会議における特別セッション企画

担当： 浅野 哲夫 (北陸先端科学技術大学院大学)

1 国際会議 HERCMA

本特定研究の研究成果の一部を世界的に公表するために，ヨーロッパで開催される国際会議において特別セッションを設けて，そこで成果の報告を行うこととした．国際会議は，正式には

THE EIGHTH HELLENIC EUROPEAN RESEARCH ON COMPUTER MATHEMATICS AND ITS APPLICATIONS CONFERENCE

と呼ばれるものであるが，略して HERCMA2007 という名前でも知られている．この国際会議は，1992 年から隔年ごとに開催されている伝統のある国際会議であるが，コンピュータサイエンスと数学の接点を探ると共に，実際の問題への応用も対象とする幅の広い学会である．この国際会議は毎回ギリシャのアテネで開かれているが，下記の７つの学会から協賛を得ている．

ACM (Association for Computing Machinery),

SIGACT, SIGSAM ,

IMACS (Intern. Association for Maths and Computers in Simulation), USA

SEMA (Spanish Applied Maths Society), Spain

IMA (Institute of Mathematics and its Applications), England

GAMM (Gesellschaft fur Angewande Mathematik & Mechanik e.V.), Germany

JSIAM (Japan Society for Industrial & Applied Mathematics), Japan

この国際会議は２年に一度，ギリシャのアテネにおいて Athens University of Economics & Business (AUEB) のサポートの下に開催されるものである．１昨年は浅野が，今年に関しては杉原が招待講演者として招待されている．同じ特定研のメンバーが２人同時に招待講演を依頼されることは，本特定研究の成果が世界的に認められていることを示すものであろう．

2 発表論文

発表予定の論文は下記の通りである．

(1) “On-line Uniformity of Points,”

by Tetsuo Asano and Sachio Teramoto

(2) “Stable Computation of the Optimal Path for a Boat on a Water Stream and Its Applications”

by Kookichi Sugihara and Tetsushi Nishida

(3) “Snaky is a winner with one handicap”

by Hiro Ito and Hiromitsu Miyagawa

(4) “A Crash-tolerant COnsensus Algorithm in Presence of Probabilistic Message Omission”

by Taisuke Izumi and Koichi Wada

(5) “Theoretical and Practical Issues of Evacuation Planning in Urban Areas”

by Naoyuki Kamiyama, Naoki Katoh, and Atsushi Takizawa

(6) “Efficient $-\epsilon$-net Construction for an Application to Ad-hoc Network”

by Takeshi Tokuyama

第19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)

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2006年で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．

2006年度は次の講演からなるセッションを実施した．

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)
  （概要）本稿では，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，P2P システムのための新しい構造型オーバーレイネットワークを提案した．提案するオーバーレイネットワークは，スキップグラフの拡張であり，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を実現した．

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)
  （概要）The link structure of the Web is generally viewed as the webgraph. Web structure mining is a research area that aims to find hidden communities in the Web based on the webgraph, and communities or their cores are supposed to constitute dense subgraphs. Then, structure mining is realized by enumerating those substructures. In this paper, we focus on bicliques, cliques and isolated cliques as such candidate substructures, and attempt to investigate properties of the webgraph and to find useful information from the real web data. As a result, we

observed several interesting structural properties of the Web. Furthermore, we discovered that isolated cliques can be quite useful for detecting harmful link farms, while isolated cliques that lie over multiple domains sometimes stand for useful communities, which implies the validity of isolated cliques in web structure mining.

- 「The weakest failure detectors for the stable leader election」小野廣隆 (九大)
  （概要）耐故障分散計算における中心的な話題の一つに，基本的な合意問題の最弱故障検知器の解明がある．コンセンサス問題とその関連問題に関しては，最弱の故障検知器が近年明らかとなっている．本論文では基本合意問題の一つとしてリーダー選挙の一種である，安定リーダー選挙を取り上げる．まずモーダル故障検知器（L）という故障検知器クラスを導入し，これとコーラム故障検知器 Σ を用いて，(L, Σ) が安定リーダー選挙の最弱故障検知器であることを示した．

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．

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 28 日〜9 月 30 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．
多目的最適化に対する逆探索法 (岡本 吉央, 豊橋技科大)
ラーマングラフの列挙とその応用について (谷川眞一, 京都大学)
総頂点間経路長を最小にする完全K分木への辺追加 (澤田 清, 流通科学大学)
Efficient Algorithms for Airline Problem (上原 隆平, JAIST)
グレブナー基底のサンプリング・列挙に対する応用 (松井 泰子, 東海大学)
組合せ構造の擬似ランダム生成に関する考察 (岡本 吉央, 豊橋技科大)
飛び出す絵本の Computational Complexity (上原 隆平, JAIST)
Web グラフとそのアルゴリズムの最近の話題 (宇野 裕之, 大阪府立大)
同型性を考慮したインターバルグラフの列挙 (清見 礼, 情報研)
コーダルグラフのサンドイッチ問題 (来嶋 秀治, 東大)

岡本の発表では，多目的最適化問題に対する最適解を列挙する多項式時間アルゴリズムについて解説があった．今回のアルゴリズムは、初めての多項式時間アルゴリズムであるとともに、全域木を始め、列モジュラ多面体やシンプルな多面体上での問題に対しても適用可能である。

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．

全体を通して，非常に活発に議論が行れ，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．

ミニシンポジウム「新世代計算限界と地球環境問題」

世話役： 加藤 直樹 (京都大学)，杉原 厚吉 (東京大学)

科研費特定領域「新世代計算限界」で私たちが行っている研究テーマが，地球環境問題にどのように関わり得るかを考える機会を作りたいという目的で，2006 年 12 月 5 日 (火)，6 日 (水) に東京大学においてミニシンポジウム「新世代計算限界と地球環境問題」を開催した．

私たちは，普段の研究を進める上で，自分たちの研究と地球環境問題との関係を考えることはそれほど多くはない．しかし，最適化は資源の有効利用を目指すものであるから，多くのアルゴリズムは，地球資源の有効利用につながるはずである．たとえば，巡回セールスマン問題を解くことは，配送車の燃料消費量の節約や二酸化炭素排出量の削減につながり，より高速な計算アルゴリズムを設計し計算時間を短縮することは，計算に使う電力エネルギーの節約につながる，などである．

そこで，私たちの普段の研究を，地球環境問題という観点から解釈し直し，この分野へどのような貢献ができるかについて意見交換を行おうという主旨で講演を募集した．その結果，11 件の発表の申込みをいただき，それに 2 件の招待講演を加えて 1 日半のミニシンポジウムを開催することができた．

講演の内容は，車による荷物の配送計画，航空機の路線や経路の最適設計などの燃料の節約を目指すもの，計算資源の効率的運用によって電力エネルギーの節約を目指すもの，建物の最適設計によって建築資源の節約や太陽エネルギーの有効利用を目指すもの，センサーネットワークによる環境のモニタリング手法の開発，偏微分方程式のロバストな解法を利用して汚染の拡散の様子を予測するもの，環境アセスメントを配慮した地理情報データの国際標準化を目指すものなど多岐に渡った．

これらの中で特に印象深かったのは，エネルギーの節約を目指すものについては，計算限界上の工夫が，日本全体におけるエネルギー消費や二酸化炭素の排出量の削減に関してどれほどの効果をもたらすかについて，多くの講演者によってエネルギー統計に基づいた視点からの議論もなされたことである．このような視点は，最適化にかかわる多くの研究者にとって有用な情報である．

本ミニシンポジウムが新世代計算限界のメンバーが地球環境問題への関心を深めるきっかけとなれば幸いである．

以下に，本ミニシンポジウムのプログラムを掲げる．

=== 12 月 5 日 (火) ===

13:30–15:00

1. ボート航行距離方程式を利用した汚染拡散予測
   ◯ 杉原 厚吉，西田 徹志 (東京大学)
2. 時刻依存配送計画問題に対する反復局所探索法
   ◯ 橋本 英樹 (京都大学)，柳浦 睦憲 (名古屋大学)
3. 航路，飛行路の最適経路設計をめざして
   ◯ 西田 徹志，杉原 厚吉 (東京大学)

15:30–17:00

4. 剛性および外乱の変動に対するトラスのロバスト性能評価法
   ◯ 寒野 善博 (東京大学)，竹脇 出 (京都大学)
5. 歩行者と物流車両の便益を考慮した交通ネットワーク計画に関する研究
   ◯ 加藤 直樹 (京都大学)
6. 低消費電力アルゴリズムとデータ構造
   ◯ 定兼 邦彦 (九州大学)

=== 12 月 6 日 (水) ===

10:00–11:00

7. 燃料消費削減のための航空路線設計
   ◯ 岩佐 大 (東京大学)，齊藤 廣大 (JST，ERATO)，松井 知己 (中央大学)

8. 航空路線デザイン問題の効率の良いアルゴリズム
中野 眞一 (群馬大学), ○ 上原 隆平 (北陸先端大学), 宇野 毅明 (NII)

11:15–12:15 (招待講演 1)
輸送エネルギーの削減と都市空間構造の最適化
鈴木 勉 (筑波大学 大学院システム情報工学研究科 リスク工学専攻)

13:30–14:30 (招待講演 2)
環境配慮型プロダクトライフサイクルマネジメント
由良 憲二（電気通信大学 大学院電気通信学研究科 システム工学専攻)

14:45–16:15
9. 建築分野における地球環境問題の研究レビューと本研究室での取り組み
加藤 直樹, ○ 瀧澤 重志 (京都大学)
10. 最小節点ランキング全域木問題の環境モニタリングのためのセンサネットワークへの応用の試み
○ 増山 繁 (豊橋技術科学大学), 中山 慎一 (徳島大学)
11. ISO/TC211 地理情報の標準活動における計算限界
○ 今井 浩 (東京大学)

ミニ研究集会 (Complexity)

世話役： 垂井 淳 (電気通信大学)

本年度は２回の研究集会を開催した．

１回目の集会では５名の講演者による講演があった．特に計算量理論に密接に関連する周辺領域の研究の講演を重点的にプログラムに組み込んだ．特定領域外から小柴氏に暗号理論の最近の動向に関する招待講演をお願いした．約２０名の参加者があり活発な議論があった．

２回目の集会は数学基礎論と計算量理論の境界領域にフォーカスしたものとした．この２つの領域の研究者の交流を深めることも目的のひとつであった．参加者数は約２０名と予想を上回るものとなり日本におけるこの分野に興味をもつ研究者の多くが一同に会する機会ともなった．黒田氏に午後いっぱい使ったチュートリアルをお願いし後半は参加者からの活発な議論を交えるフリーディスカッションへと自然に移行した．この集会をきっかけとしてこの境界領域分野の活性化が期待される．

第１回集会

日時：１２月１日（金）　９：３０－－１７：００

場所：東工大大岡山キャンパス西８号館８０９号室

プログラム ：

1. 河内 亮周（東工大）：情報理論的安全性を持つ量子公開鍵暗号系

本講演では，2005 年に河内らによって提案された量子公開鍵暗号系を改良について述べる．以前の河内らの暗号系は基本的に計算量的仮定（グラフ自己同型性判定問題の困難性）に基づいていたが，今回は敵対者の計算能力を制限しない場合の安全性を与える．また量子公開鍵暗号系における汎用結合可能安全性についても議論する．本講演の内容は Christopher Portmann 氏との共同研究である．

2. 玉木久夫（明治大）：平面グラフの分枝分割とその応用

一般のグラフに対して最小幅の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，Seymour と Thomas による $O(n^4)$ 時間のアルゴリズムが知られている．この講演では，このアルゴリズムの $O(n^3)$ 時間への改良（Gu-Tamaki 2005）について述べる．また平面グラフの分枝分割の最適化問題への応用についても触れる予定である．

3. 戸田誠之助（日大）：グラフ自己同型群を求めるための動的計画アルゴリズム

適当な全順序集合の要素を成分とする $k \times n$ 行列からなる集合 $\mathcal{M} = \{M_1, M_2, ..., M_m\}$（一方の部集合を色分けし，かつ，辺にラベルを付けた二部グラフと見なすことができる）に対して，$\mathcal{M}$ の自己同型群を求めるための動的計画法に基づく $O(k!(nm)^{O(1)})$ 時間アルゴリズムを話します．

4. 小柴健史（埼玉大）：暗号理論における一方向性関数とその周辺の進展

Hastad, Impagliazzo, Luby, Levin(1989, 1990) により証明された任意の一方向性関数 (OWF) から擬似乱数生成器 (PRG) の構成は，一方向性置換 (OWP) からの PRG の (Blum-Micali-Yao) 構成や regular OWF(ROWF) からの PRG の (Goldreich-Krawczyk-Levin) 構成の発展でもある．OWF から PRG の構成に関して，今年になって大きく進展があり，これらの技術について紹介する．具体的には，Holenstein (TCC 2006) が導入した擬似エントロピー対 (PEP) という概念を利用し，OWF → PEP → PRG という流れのシンプルな構成法を与えている．PEP のアイデアと Impagliazzo (1995) に示した (non-uniform) Hard-Core Set Lemma の uniform 版 (by Holenstein) を組み合わせることにより証明が完成している．また，Haitner, Harnik, Reingold (CRYPTO 2006) は Randomized Iterate という技法の再検討を行い，GKL 構成法の単純化と，シンプルな PEP 構成法を与えることに成功している．これらの結果を組み合わせることによ

り OWF → PRG の構成がよりシンプルにすることができる．上記内容についてなるべく簡単に解説を行う．

5. 牧野和久（東大）：Minimum Transversals in Posi-modular Systems

Given a system (V, f, d) on a finite set V consisting of two set functions f and d, we consider the problem of finding a set $R \subseteq V$ of minimum cardinality such that $f(X) >= d(X)$ for all $X \subseteq V - R$, where the problem can be regarded as a natural generalization of the source location problems and the external network problems in graphs and hypergraphs. We give a structural characterization of minimal deficient sets of (V, f, d) under certain conditions. We show that all such sets form a tree hypergraph if f is posi-modular and d is modulotone, and that conversely any tree hypergraph can be represented by minimal deficient sets of (V, f, d) for a posi-modular function f and a modulotone function d. By using this characterization, we present a polynomial-time algorithm if, in addition, f is submodular and d is given by either $d(X) = \max\{p(v) : v \in X\}$ for a function $p : V \to R_+$ or $d(X) = \max\{r(v, w) : v \in X, w \in V - X\}$ for a function $r : V^2 \to R_+$. Our result provides first polynomial-time algorithms for the source location problem in hypergraphs and the external network problems in graphs and hypergraphs. We also show that the problem is intractable, even if f is submodular and $d \equiv 0$. This is a joint work with Mariko Sakashita, Hiroshi Nagamochi, and Satoru Fujishige.

第２回集会

日時：１２月２８日（木）　１１：００－－１８：００

場所：電通大総合研究棟６０１号室

プログラム ：

1. 鈴木登志雄（首都大）：
算術的フォーシングとフォーシング条件：クエリー記号付きブール式・計算量およびランダム性との関連

2. 黒田覚（群馬県立女子大）：
限定算術と proof complexity に関するチュートリアル

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)

昨年度，総括班の櫻井の呼びかけをきっかけに開催した研究集会に続き，今年度も特定領域研究「新世代の計算限界」暗号関係ミニ研究集会を開催した．本研究集会は，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開催された．電気通信大学の國廣が会場世話人，および，プログラムのとりまとめを行った．

昨年度は函館での開催，期間は 1 日であったが，今年度は東京での開催，期間は 2 日とした．参加者は，昨年度は約 20 名だったが，今年度は 1 日目が約 40 名，2 日目が約 30 名と増加した．また昨年度と異なり，企業の研究所からも多くの参加者がいた．

講演は下記の概要の通りであるが，1，10 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り，残りの講演は各自の研究成果に関する内容が中心であった．

参加者は少なくなかったものの自由に質問できる雰囲気が常にあった．実際に，講演の最中にも質問がでたり，講演直後の決められた時間以外にも活発な討論がされたりと，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．

研究集会 1 日目の後の懇親会では，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や，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が多く聞かれた．他にも研究集会に関して具体的に，一件あたりの発表および質疑応答の時間をもっと長くとりたい，チュートリアル講演を主体としたスクール的な研究集会をもちたいなどといった意見も聞かれた．

次年度も継続して，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予定である．

日時　2007 年 3 月 2 日 (金) 13:30–17:30, 3 日 (土) 9:30–15:45

場所　電気通信大学 総合研究棟 601 会議室 (〒182-8585 東京都調布市調布ヶ丘 1-5-1)

プログラム

1. 3 月 2 日 (金) 13:30–14:30
   証明可能安全性理論に向けて
   太田 和夫 (電気通信大学)

2. 14:45–15:15
   耐タンパ性を備えたユニークデバイスに基づく暗号認証基盤の検討
   今本 健二 (九州大学) (発表者: 蘇 春華 (九州大学))

3. 15:15–16:00
   ペアリング暗号の安全な高速実装について
   高木 剛 (はこだて未来大学)

4. 16:15–16:45
   指定検証者署名の定式化，および，送信者と受信者の匿名性について
   大山 千尋 (東京工業大学)

5. 16:45–17:30
   Concurrently Secure Password-based Authenticated Key Exchange without Random Oracles or Setup Assumptions
   米山 一樹 (電気通信大学)

6. 3 月 3 日 (土) 9:30–10:30
   スタンダードモデル PA の基礎に関して
   寺西 勇 (NEC)

7. 10:45–11:30
   Non-Malleability Definitions Reconsidered
   宮川 聡 (電気通信大学)

8. 11:30–12:15
   Collusion-resistant Private Association Rules Mining in Distributed Environment
   蘇 春華 (九州大学)

9. 13:30–14:15
   Revisiting Zero-Knowledgeness of an On the Fly Authentication Scheme
   Bagus Santoso (電気通信大学)

10. 14:15–15:45
    格子問題をベースとした暗号について
    草川 恵太 (東京工業大学)

各発表の概要

1. 証明可能安全性理論に向けて
   太田 和夫 (電気通信大学)
   概要: 実用的な暗号技術として，安全性が理論的に証明できる（証明可能安全な）方式が期待されている．公開鍵暗号の発明後しばらくの間『ある攻撃に対して安全な方式は，別の攻撃に対しては安全性証明がつかない』と信じられていた (Folklore)．本解説では,「folklore」の呪縛から逃れ,「安全性証明」への道筋を示した Goldwasser, Micali, Rivest による記念碑的な論文を紹介することで，本研究集会の導入とする．安全性定理に込められた「ココロ」，呪縛からの解放の「アイデア」などを解説した．

2. 耐タンパ性を備えたユニークデバイスに基づく暗号認証基盤の検討
   今本 健二 (九州大学)
   概要：従来，公開鍵証明書を用いた公開鍵基盤（PKI）や ID ベース暗号を利用した暗号化システムにおいては，数学アルゴリズムや第三者機関の利用など，様々な仮定に基づいた設計が行われている．本論文では，深谷らが提案したデバイス固有値を用いた対称暗号技術による ID ベース暗号化方式（IST 方式）に基づいた手法を検討し，本方式を用いることで認証を行う方式（3way 認証方式）を提案し，既存の認証方式との比較を行う．

3. ペアリング暗号の安全な高速実装について
   高木 剛 (公立はこだて未来大学)
   概要：ペアリング暗号の安全な高速実装について考察を行う．高速実装するにあたっては，ペアリングに関する演算の理論的改良，ペアリングをプログラミングコードで実装する際の種々の工夫を行っている．理論的改良については，３乗根を求めることなく EtaT ペアリングを演算する方法，および，トーラスを用いた最終的な結果を得るための指数演算の方法の２つを主に提案した．プログラミングコードで実装する際の種々の工夫に関しては，Java, C, BREW, FPGA の４つのコードにおいて高速実装を行った．さらには，ペアリングに関するサイドチャネル攻撃についても考察した．

4. 指定検証者署名の定式化，および，送信者と受信者の匿名性について大山 千尋 (東京工業大学)
   概要：本研究では，指定検証者署名における「受信者（指定検証者）の匿名性」という新しい安全性の概念を提案する．指定検証者署名を用いると，署名者が，特定の人にだけ検証が可能であるような署名を生成することができる．受信者の匿名性とは，攻撃者が署名を盗聴しても，その署名がだれに向けて指定されたのかが判別できないという性質である．我々は，この受信者の匿名性という概念を定式化するとともに，この性質をみたす方式を２つ提案する．

5. Concurrently Secure Password-based Authenticated Key Exchange without Random Oracles or Setup Assumptions
   米山 一樹 (電気通信大学)
   概要：本発表では，plain model におけるパスワード認証つき鍵交換の一般的な構成法を提案する．ここで plain model とは，その方式がランダムオラクル，あるいは，trusted

setup assumption を必要としないという意味である．さらに，我々の方式は複数のインスタンスが同時にプロトコルを実行したとしても（concurrent でも）安全である．我々の方式は plain model で concurrent な安全性を達成する初めての方式である．

6. スタンダードモデル PA の基礎に関して
寺西 勇 (NEC)
概要：plaintext awareness という安全性の概念についての考察を行った．plaintext awareness とは，公開鍵暗号の安全性についての概念であり，暗号文を作れる人はいうその平文を知っているはずであるという性質である．plaintext awareness は，もともとはランダムオラクルモデルという強い仮定の下で定義されていたが，近年はスタンダードモデルでの定義も提案されている．本発表では，現在の定義の問題点などを指摘するとともに，他の安全性の概念との関連性を示した．

7. Non-Malleability Definitions Reconsidered
宮川 聡 (電気通信大学)
概要：公開鍵暗号方式が 頑健性 (NM) を満たすとは，攻撃者が，暗号文から，対応する平文を改ざんした新たな暗号文を作成できないことをいう．この NM の概念を定式化するためには，攻撃者が作成すべき「新たな暗号文」に条件を付加する必要がある． この条件は 2 種類にわけられ，攻撃者は新たな暗号文に不正な暗号文を含めることはできないといった定義 (定義 1) と，攻撃者は新たな暗号文に不正な暗号文を含めることはできるが，含めた場合には実験に失敗するといった定義 (定義 2) がある．本研究では，NM に関する 3 種類の定義 (SNM, CNM, IND-P) について，SNM および CNM においては，定義 1 と定義 2 の間には攻撃者の能力の観点からすると差がないことを示した．また，IND-P においては，定義 2 のような方法では条件を付加することは不可能であることも示した．

8. Collusion-resistant Private Association Rules Mining in Distributed Environment
蘇 春華 (九州大学)
概要：相関ルールマイニングはデータベースに蓄積された大量のデータから，頻繁に同時に生起する事象同士を相関の強い事象の関係，すなわち相関ルールとして抽出する技術である．本論文では，相関ルールのプライバシー保護問題に着目し，結託を防止した安全なプライベート相関ルールマイニング手法を提案した．従来の提案では準同型性暗号の暗号を用いており，鍵の管理と生成，計算量と通信量はかなり大きいものだった．今回の我々のの提案では，分散ネットワークにおける n 個のパーティーがデータベースのプラバシーを保ったままで，共同の相関ルールマイニングを算出するシナリオを想定する．我々は，Han による Apriori algorithm の効率を大きく改善するアルゴリズムを使って，結託を防止できる効率のよい手法を提案した．

9. Revisiting Zero-Knowledgeness of an On the Fly Authentication Scheme
Bagus Santoso (電気通信大学)
概要：on-the-fly の認証方式である GPS のなりすましに対する安全性は，ゼロ知識性に依存して証明されているが，実際に使用した場合の安全性についての詳細な考察は行われていなかった．我々は，GPS に対して，正当な証明者と検証者の間での通信履歴を集めるだけで，秘密鍵の先頭ビットを計算することができることを示した．

10. 格子問題をベースとした暗号について
草川 恵太 (東京工業大学)
概要：格子問題に基づく暗号方式が注目を集めている．その理由は, 暗号方式の安全性を格子問題の最悪時の困難性から保証できることにある．また今のところ格子問題を解く量子アルゴリズムが知られていないことも格子問題に基づく暗号方式が注目を集める理由のひとつである．現在, 公開鍵暗号とハッシュ関数については安全性を格子問題の最悪時の困難性から保証できるものが知られている．本発表では，ハッシュ関数を攻撃することが，組合せ問題の最悪時の困難性と結びつくことを詳細に解説した．さらに，未解決問題についても解説を行った．

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), 岡本 吉央 (豊橋技術科学大学)

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，前年度より本研究集会は開催されている．今年度は第二回目である．

構成は８件の一般講演からなる．その内容は，理論からプログラミング，さらには実習報告まで広範囲におよび，活発な意見交換もなされた．詳細は以下の通りである．

日時 2007 年 3 月 16 日（金）　10:30 – 16:45

場所 豊橋技術科学大学 豊橋駅前サテライト・オフィス テクノス-U

参加者数 25 名（教員 15 名, 学生 10 名）

講演

1. 「整数計画法によるパズル解法」実習報告：岡本 吉央 (豊橋技術科学大学)

   要旨　平成18年8月上旬に高専4年生を対象として「整数計画法によるパズル解法」という体験実習を行なったので，その報告をする．この１週間に渡る実習では，論理のことばを算術のことばに置き換えるところから始めて，実際に魔方陣の作成や，数独，ののぐらむ，覆面算などのパズルを整数計画問題として定式化して，ソルバで解かせることまでを体験してもらい，最終日には各自のアイディアを報告する発表会を行なった．本発表では，実際の進め方，題材とするパズルの選定，注意点，解け具合などをまとめて報告する．

2. ヒントの位置が指定されたナンプレの高速な生成法：稲葉直貴（名古屋工業大学）

   要旨　ナンプレ（数独）と呼ばれているパズルに対して任意の指定された位置にヒントを持つような唯一解の問題を高速に生成する手法を開発した．

3. 戸神星也，渡辺治（東京工業大学）

   要旨　数独というパズルの全解に対してスパコンを用いて番号付けを行い，４G程度に圧縮したデータを作成し，それを元に，解⇔番号を１０秒程度で求めるプログラムを作成した．ちなみに，インデックスは２２桁の数になる．

4. スネーキーの置き石１の必勝法：宮川博光，伊藤大雄（京都大学）

   要旨　フランク・ハラリイの提案した一般化三並べとは，碁盤状の盤面に二者が交互に石を一つずつ置き，予め定められた，連結した石で定義されるある形を，回転と反転を許して，先に作った方が勝ちというゲームである．両者が最善を尽くしたとき，先手必勝である形を「勝ち型」，無限に続けても決着がつかない形を「負け型」と呼ぶ．なおゲームの性質上，後手必勝ではありえない．これまでの研究でスネーキーと呼ばれる図形のみ，勝ち型か負け型か未解明であり，さらにスネーキーのハンディキャップ数（勝ち型になる必要最小限の置き石数）についても，２以下であることが分かっているのみであった．本研究では，スネーキーの置き石１の先手必勝手順を示す．この結果，スネーキーのハンディキャップ数が０または１であることが分かった．

5. 正六角盤面上の一般化三並べ：入倉弘介，松浦昭洋（東京電機大学）

   要旨　正六角盤面上でハラリイの一般化三並べを考察した．これまでに明らかとなった，５細胞生物までの生物の勝ち型，負け型に関する結果を報告する．

6. 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の複雑さについて：高橋良介，瀧本英二（東北大学）

要旨　シャノンスイッチングゲームとは，与えられたグラフの頂点に 2 人のプレイヤーが交互に石を置いていくゲームである．先手の目的は指定された 2 頂点を結ぶパスの 1 つを自分の石で占有することで，後手の目的はそれを阻止することである．どちらのプレイヤーが必勝戦略を持つかを判定する問題は PSPACE 完全であることが知られている．
本発表では，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とき，後手が必勝戦略を持つかどうかを決定する問題の複雑さが Σ_2^P 完全であることを示す．

7. 重み付き半順序ゲームの必勝法：高田智史，伊藤大雄（京都大学），中村義作（東海大学）

要旨　本発表では「重み付き半順序集合ゲーム」というものを導入する．これは半順序集合ゲームの集合の要素に重みを付けて拡張したものである．両プレイヤーは非負の体力を持ち，要素を取る毎にその重みの合計だけ体力を失う．そして先に体力が負になったプレイヤーが負けである．我々はこのゲームにおける必勝法を考察した．まず第一に，重みが 0 か 1 かのどちらかである場合において以下の性質を発見した．

(1) 両者の体力が異なるなら，大きい体力を持つプレイヤーが必勝手順を持つ．
(2) 両者の体力が同じで，全ての極大要素が正の重みを持つなら，後手のプレイヤーが必勝手順を持つ．
(3) その他の場合は，問題を（従来の重み無しの）半順序集合ゲームに帰着できる．

そして第二に，一般の重みの場合において，半順序が全順序である場合における多項式時間必勝手順を発見した．

8. Rogue 脱出判定問題の PSPACE 完全性：新井滋，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問題が，空腹度のパラメータを設定した場合 PSPACE 完全であることを示す．

電子情報通信学会 COMP-NHC 学生シンポジウム

世話役： 渡辺 治 (東京工業大学), 有村 博紀 (北海道大学),
小柴 健史 (埼玉大学), 宮崎 修一 (京都大学)

平成 19 年 3 月 20 日〜23 日の日程で，名城大学天白キャンパスにおいて電子情報通信学会総合大会が開かれた．その初日の 20 日に，電子情報通信学会コンピュテーション研究会と本特定領域研究との共同で，昨年に引き続き COMP-NHC 学生シンポジウムを企画した．

理論計算機科学は取り扱われる分野が幅広く，特に学生においては異なる研究分野の研究者との情報交換が困難である．本シンポジウム最大の目的は，学生に研究交流の場を提供し，若手研究者を育成することである．その一環として，優秀な研究及び発表を行った学生には，COMP-NHC 論文賞を贈ることにした．

当日は 7 件の発表が行われ，約 30 名の聴衆が集まった．投票を元に審査した結果，神山直之氏（京都大学）が COMP-NHC 論文賞を受賞した．シンポジウムの概要は以下の通りである．

電子情報通信学会 2007 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」

日時: 2007 年 3 月 20 日 13:55 - 17:30

会場: 名城大学天白キャンパス (名古屋市) 共通講義棟北 N501

実行委員: 有村博紀 (北海道大), 岩間一雄 (京都大), 加藤直樹 (京都大), 小柴健史 (埼玉大), 徳山豪 (東北大), 宮崎修一 (京都大), 渡辺治 (委員長, 東工大)

最優秀発表賞選考委員： 上原隆平 (北陸先端大), 高木一義 (名古屋大), 瀧本英二 (東北大), 徳山豪 (東北大), 中西正樹 (奈良先端大), 宮崎修一 (京都大), 渡辺治 (委員長, 東工大)

プログラム:

13:55〜14:00 「開会に際して」渡辺治（東工大）

[**セッション COMP-NHC 1**] 座長：高木一義 (名古屋大)

14:00〜14:25 “Variations on Pseudo-Free Groups”, 平野貴人、田中圭介（東工大）

14:25〜14:50 “On formula size lower bounds for synthesis of Boolean functions over disjoint sets of variables”, Hideaki Fukuhara(Tohoku Univ.), Kzuyuki Amano (Gunma Univ.), Eiji Takimoto(Tohoku Univ.)

14:50〜15:15 “安定結婚問題に対する 1.8-近似アルゴリズム”, 山内直哉、宮崎修一、岩間一雄（京大）

15:15〜15:40 “日本語文字遷移における順方向・逆方向の情報量差異”, 朱碧蘭、中川正樹（東京農工大）

[**セッション COMP-NHC 2**] 座長：徳山豪 (東北大)

15:55〜16:20 “The Greedy Minimum Evolution Algorithm with an Appropriate Input Order”, Takeya Shigezumi (東工大)

16:20〜16:45 “An Efficient Algorithm for the Evacuation Problem in a Certain Class of a Network with Uniform Path-Lengths”, Naoyuki Kamiyama, Naoki Katoh, Atsushi Takizawa (Kyoto Univ.)

16:45〜17:05 “無交差ラーマンフレーム列挙アルゴリズム”, David Avis(McGill Univ.), 加藤直樹, 大崎純（京大）、Ileana Streinu(Smith College), 谷川眞一 (京大)

17:05〜17:30 「表彰式と講評」徳山豪 (東北大), 「閉会に際して」渡辺治 (東工大)

ミニ研究集会 (列挙合宿:その２)

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: 2007 年 3 月 27 日〜3 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)	河村 泰之 (石川高専)
山中 克久 (群馬大)	岡本 吉央 (豊橋技科大)
清見 礼 (JAIST)	下間直樹 (群馬大)
谷 聖一 (日大)	斎藤 寿樹 (JAIST)
藤芳明生 (茨城大)	有村 博紀 (北大)
元木 光雄 (JAIST)	来嶋 秀治 (東大)
澤田清 (流通科学大)	宇野 裕之 (大阪府立大)
宇野 毅明 (情報研)	

当日は，以下のような発表と議論が行われた．

・平面グラフの列挙 (山中克久 群馬大学)
・直線構造を持つネットワークのクラスタリングについて (宇野毅明 情報研)
・区間表現から MPQ-tree を効率よく構成するアルゴリズム (斎藤寿樹 JAIST)
・1 次元のボロノイゲームの解法 (清見礼 JAIST)
・コンパイラにおける組合せ最適化 (岡本吉央 豊橋技科大学)

前回は発表件数が多く，フリーディスカッションの時間が短かった，との要望があったので，今回は発表件数を抑えてディスカッションの時間を多くとった．そのため，全体を通して，各話題に関して深いレベルまで議論を行うことができた．

平面グラフの列挙では，多項式時間，多項式メモリで平面に埋め込んだグラフを重複なくもれなく列挙するアルゴリズムについて発表があった．重複の回避法や，コード化による標準形の作成，他のグラフクラスを簡単に扱う方法など，多くの議論が行われた．

コンパイラにおける組合せ最適化では，CPU のレジスタに対する変数の割当て方を最適化する方法について紹介があった．

区間表現から MPQ-tree を効率よく構成するアルゴリズムでは，MPQ ツリーの構成方法から，それを用いた列挙法に関する発表があった．MPQ ツリーは定義があいまいである部分があり，その点に関してきれいな特徴づけを与えることで，より効率良い列挙アルゴリズムと，アルゴリズムの単純化が得られるだろう，といったアイディアが，議論から生まれた．また，アノテーションの付いたビデオストリームの処理に関する応用について，議論が行われた．

フリーディスカッションでは，多くの問題について議論が行われた．グラフの bandwidth を最小化するアルゴリズムについての議論では，指数時間の厳密アルゴリズムの計算量を下げるアイディアについて議論が行われた．結果，既存の結果を改善するための基礎的なアイディアが示された．

全体を通して，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．

第 20 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 2007 年で 20 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．

2006 年度の企画が好評であったため，2007 年度も引き続き企画した．以下に関連プログラムを挙げる．

第 20 回 回路とシステム軽井沢ワークショップ

【日程】 2007 年 4 月 23 日 (月), 24 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 (4/23 13:30-15:00)
新世代の計算限界

- 「大規模データ処理に対するアルゴリズム理論からのアプローチ」宇野毅明 (国立情報学研究所)
- 「簡潔データ構造」定兼邦彦 (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ている．この目標を達成するため，今年度は，幅広い見地から次に述べる３つのアプローチを試みた．

１つめは，具体的な個々のオンライン最適化問題に対するアルゴリズムを開発し，その性能評価を厳密に与えることによって，一般的なオンライン意思決定問題に対する方法論や解析手法を確立するための手がかりに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（２章）．(1) 昨年度，オンラインオークションと呼ばれる商品売買のモデルに対し，Vovk の統合戦略と呼ばれるオンライン予測の手法を適用することによって，優れた利得下界を持つアルゴリズムを与えたが，今年度は，その下界導出の手法を単純化することに成功した．さらに，Vovk の統合戦略を適用する際の初期重みパラメータを最適化することによる，下界改善の可能性について検討を行った．(2) 銀行や理髪店の待合室における週刊誌の提供や，航空旅客機内における映画の上映など，待ち時間においてユーザを退屈させないためのサービスの費用対効果について考察した．このような読捨てコンテンツの提供においては，コンテンツの更新の頻度が低いと，ユーザが同一のコンテンツを再閲覧することが多くなりサービスの品質が低下する一方，更新の頻度を高くすると費用が高くなってしまう．我々は，この問題をオンライン最適化問題として定式化し，競合比解析を行った．

２つめは，さまざまな分野において，社会的・学術的に求められている品質保証の基準に基づいて問題をモデル化し，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３つの成果を得た（３章）．(1) 脳の計算素子であるニューロンは，発火するために一定のエネルギーを必要とするため，脳内では多くのニューロンが同時に発火することができないと考えられている．我々は，脳の計算機構をモデル化した閾値論理回路において，同時に発火し得る閾素子の数の最大値をエネルギー消費量を表す新しい尺度として導入し，エネルギー消費量を制限した場合の閾値論理回路の計算能力について考察した．その結果，エネルギー消費量と計算能力の間のトレードオフを表す不等式の導出に成功した．(2) ２つのゲノムのアラインメントを求める方法として，共通部分列のマッチングに基づく方法が提案されている．この手法においては，なるべく多くのマッチングを見つけることが求められるが，これは，２つの整数配列が与えられたとき，これらの配列に共通に含まれる最長の部分増加列を求める問題としてモデル化することができる．我々は，この問題を解く線形領域アルゴリズムを与えた．(3) ピラミッド型の階層構造を有する意思決定機構における情報の伝達コストを，完全 k 分木にいくつかのバイパス辺が付加されたグラフの平均頂点間距離とし

て与えられるとするモデルを提案し，最適なバイパス辺の付加条件を与えた．

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，以下の３つの成果を得た（４章）．(1) 否定素子数を限定した論理回路で，ソーティングや反転回路を構成する新しい手法を与えた．これらは，入力系列を k トニック列と呼ばれるものに限定すると，k が小さいときには従来の構成法より優れている．(2) ある条件のもとで，論理式のサイズの下界を再帰的に導出する方法を与えた．また，この手法を用いることにより，最簡形の論理式のみを列挙するアルゴリズムを与えた．(3) 論理回路のサイズの下界を求めるための，計算機支援による証明系の実現可能性について検討を行い，幾つかの知見を得た．

2 個々のオンライン最適化問題からのアプローチ

2.1 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なオンライン投資の問題へと還元される．まず，$[1, h]$ を離散化し，N 個の価格候補集合 $h \geq b(1) > b(2) > \cdots > b(N) \geq 1$ を考える．この離散化により，アルゴリズムの直接の目標は，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となる．ここで，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_T^* の比を十分小さく抑えることができる．還元は，価格候補集合を投資の対象であるオプション集合と考え，その集合上でオンライン投資アルゴリズムを走らせることによって行われる．各時刻 t において，投資アルゴリズムは，投資ベクトルとして，オプション集合上の確率分布 $p_t \in [0, 1]^N$ を出力する．これを見て，売り手は，$\Pr(r_t = b(i)) = p_t(i)$ という確率分布に従って価格 r_t を選ぶ．その後，入札者の入札金額 m_t が明かされたとき，売り手はこれを利得ベクトル $l_t = (0, \ldots, 0, b(k), b(k+1), \ldots, b(N))$ に変換し，投資アルゴリズムに与える．ここで，k は $b(k-1) > m_t \geq b(k)$ を満たす整数である．すると，時刻 t において売り手が得る利得の期待値は，$E[g_t] = p_t \cdot l_t = \sum_{i=1}^{N} p_t(i) l_t(i)$ のように，投資ベクトル p_t と利得ベクトル l_t の内積で表わされる．同様に，一定の価格 $b(i)$ で売り続けたとしたときの時刻 t における利得は，第 i 成分のみが 1 で他の成分が 0 の単位ベクトル u_i を用いて，$g_{t,i} = u_i \cdot l_t$ と表わされる．

このように，オンラインオークション問題は，環境との間で投資ベクトル p_t と利得ベクトル l_t を交互にやりとりし，それらの内積の総和 $E[G_t] = \sum_{t=1}^{T} p_t \cdot l_t$ を，一定の単位投資ベクトル u_i による内積の総和 $G_{T,i} = \sum_{t=1}^{T} g_{t,i}$ の最大値 $G_T^* = \max_{1 \leq i \leq N} G_{T,i}$ に匹敵させることを目標とする，オンライン投資の問題とみなすことができる．この目標は，オンラインオークション問題の目標と一致するため，従来のオンライン予測の手法を適用することができる．実際，我々は，初期重みベクトルと呼ばれるパラメータを $(v_1, \ldots, v_N)$ としたときの Vovk の統合戦略 [2] を適用し，次の利得下界を得た．

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，

$$E[G_T] \geq \frac{b(N)\ln\alpha}{D(r||s)+b(N)\ln\alpha}\log_\alpha\sum_{i=1}^{N}v_i\alpha^{G_{i,T}} \geq \frac{b(N)\ln\alpha}{D(r||s)+b(N)\ln\alpha}\left(G_T^*-\frac{\ln 1/v_{i^*}}{\ln\alpha}\right).$$

ここに，$D(r||s)$ は，KL ダイバージェンスである．従来のオンライン予測の解析においては，ほとんどの場合，一般性を失わずに初期重みを一様（$v_i = 1/N$）として良かったが，オンラインオークション問題においては，$\{G_{i,T} \mid 1 \leq i \leq N\}$ に互いに高い相関があるため，初期重みを工夫して選ぶことにより，より良い下界が得られる可能性がある．

2.2 読捨てコンテンツ更新タイミングのオンライン意思決定について

待ち時間を伴うサービスにおける読捨てコンテンツの提供はユーザを退屈させないための手法の一つである．銀行や理髪店の待合室における週刊誌の提供や，航空旅客機内における映画の上映などはその一例である．通常，ユーザを退屈させないという目的のもとでは，過去に閲覧したことのある読捨てコンテンツは，再度の閲覧においてその目的を果たさない．一方，古いコンテンツを新しいものに更新する際には，一般にコストが生じる．したがって，退屈させないことがサービスを継続的に利用するユーザの獲得に影響する状況のもとでは，どのようなタイミングでコンテンツを更新するかが問題となる．

このような状況を，ユーザによる同一コンテンツの再閲覧によって生じるコストを 1，古いコンテンツを新しいコンテンツに更新する際に生じるコストを m としたときに，u 人のユーザによる閲覧要求列に対してコストの総和を小さく抑えるための更新のタイミングを求める問題としてモデル化し，この問題を解く決定性オンライン更新アルゴリズムの競合比に関して評価した．ただし，閲覧要求列において複数のユーザは同一時刻に要求をしないものと仮定し，また，更新アルゴリズムは最初の閲覧要求が起こる前に必ず 1 回コンテンツを更新し，コンテンツの更新と閲覧要求は同一時刻に起こらないものと仮定した．

はじめに，競合比の下界に関して，どのような決定性オンライン更新アルゴリズムであっても，最適なオフライン更新アルゴリズムのコストの総和と比較して，漸近的に少なくとも，

- $u = \infty$ ならば，2 倍，
- $4m+1 \leq u < \infty$ ならば，$\dfrac{2\left\lfloor\dfrac{u-1}{2m}\right\rfloor - 1}{\left\lfloor\dfrac{u-1}{2m}\right\rfloor + \dfrac{1}{2}}$ 倍，
- $2m+5 \leq u \leq 4m$ ならば $\dfrac{3}{2+\dfrac{m}{2\left\lfloor\dfrac{u-1}{4}\right\rfloor}}$ 倍

のコストの総和を生じさせることを示した．

また，ユーザの人数に制限のない $u = \infty$ の場合に，漸近的に最適なオフライン更新アルゴリズムのコストの総和のたかだか 2 倍のコストの総和で更新をするという意味で最適な決定性オンライン更新アルゴリズムとして，以下の 2 つを提案した．

アルゴリズム 1：前回の更新の後に起こった再閲覧要求の回数がちょうど m になった直後に更新をする．

アルゴリズム 2：前回の更新の後に複数回閲覧要求をしたユーザの人数がちょうど m になった直後に更新をする．

特に，後者のアルゴリズムに関しては，漸近的に最適なオフライン更新アルゴリズムのコストの総和に対して，$m \leq u < 2m$ ならば，たかだか u/m 倍，$u < m$ ならば，たかだか 1 倍のコストの総和で更新をすることを示した．

更に，これらの二つのアルゴリズムを比較し，m が大きいときに，ある閲覧要求列に対しては前者のアルゴリズムのコストの総和が後者のアルゴリズムのコストの総和の 2 倍に近くなるのに対して，後者のアルゴリズムのコストの総和はどのような閲覧要求列に対しても前者のアルゴリズムのコストの総和のたかだか 1.5 倍に抑えられることを示した．また，m が大きくかつ $u \geq 2m$ の場合に，後者のアルゴリズムのコストの総和が実際に前者のアルゴリズムのコストの総和の 1.5 倍に近くなるような閲覧要求列が存在することを示した．

最後に，動的計画法に基づくオフライン更新アルゴリズムを提案し，このアルゴリズムが漸近的に閲覧要求列の長さの 2 乗に比例する時間で，任

意に与えられた閲覧要求列に対して最小のコストの総和を実現する更新のタイミングを求めることを示した．

3 新しい評価基準に基づく問題のモデル化からのアプローチ

3.1 エネルギー消費量に基づく脳の計算機構のモデル化

通常の半導体素子とは違い，ニューロンは，発火する（1を出力する）ときに消費するエネルギー量が，発火しない（0を出力した）ときに比べて大きいという性質がある．一方，脳全体の単位時間あたりのエネルギー代謝量は限られているので，脳におけるニューロンの発火活動は，極めて疎であると考えられている．にもかかわらず，実際に脳は複雑な計算を行っているように見える．このことは，脳の計算機構をモデル化して計算過程を論じる際，エネルギー消費量をパラメータの1つとして導入すべきであることを示唆している．本研究では，脳の計算機構モデルとして最も単純な閾値回路を考える．閾値回路とは，線形分離関数を計算する閾素子を単位素子とする組み合わせ論理回路である．さて，脳における上述の性質から，閾値回路の発火活動を制限したとき，その計算能力はどの程度の影響を被るのかという自然な疑問が生じる．閾素子や閾値回路は，意思決定アルゴリズムが保持する知識表現として広く用いられているため，この問は，本研究にとって基本的かつ重要なものである．Uchizawa らは，閾値回路が消費するエネルギー量を，その回路において同時に発火しうる閾素子の数の最大値と定義し，これをその回路のエネルギー複雑度と名付けた [3]．そして，n 変数関数の広いクラスが，$O(\log n)$ のエネルギー複雑度を持つ多項式サイズの閾値回路で計算できることを示した．そのクラスには，線形分離関数が分類規則として各内部頂点に割り当てられた決定木などが含まれる．この結果は，素子の発火活動が疎でも，回路は複雑な計算を行えることを意味している．

一方，我々は，計算量理論の見地から，エネルギー複雑度を制限することによる否定的な側面に着目し，閾値回路のエネルギー複雑度と計算能力の関係を調べた．その結果，それらの間にトレードオフがあることを意味する不等式の導出に成功した．特に，エネルギー複雑度を $n^{o(1)}$ に制限し，さらに深さを定数に制限すると，ある自然な条件を満たす論理関数を計算するには，指数的な素子数を必要とすることを示した．そのような関数の1つに，内積関数 $IP(x,y) = x_1y_1 \oplus x_2y_2 \oplus \cdots \oplus x_ny_n$ がある．内積関数は，エネルギー複雑度を $O(n)$ に緩めると，深さが3で線形サイズの閾値回路で計算できるので，この結果は，エネルギー消費量の制限が，閾値回路の計算能力に本質的な影響を与えていることを示している．

3.2 最長共通増加部分配列問題の線形領域解法について

最長共通増加部分配列問題は，与えられた複数個の整数配列において共通に含まれる部分配列の中で，各要素である整数の値が先頭から末尾に向かって真に増加する最長の部分配列を求める問題である．ただし，配列に含まれる部分配列とは，元の配列の任意の位置から任意の個数の要素を削除して得られる配列のことをいう．この問題は，古くから知られている単一の整数配列に対する最長増加部分配列問題を，複数個の配列を扱う形に一般化した問題である．また，同じく古くからよく知られている複数個の配列に対する最長共通部分配列問題とも密接な関係があり，この関係に基づく応用の一例として，複数本のゲノム同士のアラインメントを求める際の，最長共通増加部分配列問題の解の利用が考えられる．

2つの整数配列 X，Y に対する最長共通増加部分配列問題に対しては，Yang らによって提案された $O(|X|\cdot|Y|)$ 時間 $O(|X|\cdot|Y|)$ 領域アルゴリズムが知られている [5]．そこで，本研究では，アルゴリズムが計算に用いる領域が，2つの配列の長さの積に比例する大きさではなく，長さの和に比例する大きさで十分であるような，$O(|X|\cdot|Y|)$ 時間 $O(|X|+|Y|)$ 領域アルゴリズムを提案した．

配列 X，Y に対する最長共通部分配列に対しては，$O(|X|)$ 領域を用いて $O(|X|\cdot|Y|)$ 時間で解くアルゴリズムが古くから Hirschberg によって与えられている [4]．このアルゴリズムでは，配列 Y を半分の長さの接頭辞と接尾辞に分割し，Y の接

頭辞に対しては，X の各長さの接頭辞との最長共通部分配列の長さを $O(|X| \cdot |Y|)$ 時間 $O(|X|)$ 領域で求め，同様に Y の接尾辞に対しては，X の各長さの接尾辞との最長共通部分配列の長さを求める．そして，得られた X の各接頭辞と Y の接頭辞の最長共通部分配列の長さと，X からその接頭辞を取り除いて得られる接尾辞と Y の接頭辞の最長共通部分配列の長さの和が最大になるように，X を接頭辞と接尾辞へ分割する．この結果として，X と Y の最長共通部分配列問題は，X と Y の接頭辞の最長共通部分配列問題と接尾辞の最長共通部分配列問題に分割されるため，再帰的にこの分割を繰り返すことによって解を求める．

この分割統治法に基づく手法は、整数配列 X, Y の最長共通増加部分配列問題を線形領域で解く際にも利用できる．ただし，X と Y それぞれの接頭辞の最長共通増加部分配列の長さと，それらの接頭辞を取り除くことによって得られる X と Y それぞれの接尾辞の最長共通増加部分配列の長さの和の最大値は，必ずしも X と Y の最長共通増加部分配列の長さに一致するわけではない．なぜなら，接頭辞に関する最長共通増加部分配列の末尾の整数が接尾辞に関する最長共通増加部分配列の先頭の整数よりも大きいか等しい場合には，これら二つの配列の連接は，各要素である整数が先頭から末尾に向かって真に単調に増加するという条件を満たさないからである．

上記の問題点は，X と Y のある最長共通増加部分配列が部分配列として現れる Y 上の位置の中で Y の長さが半分の接尾辞の最も先頭よりの位置に現れる整数を z とすると，この z が現れる位置で Y を接頭辞と接尾辞に分割し，また，同じ最長共通増加部分配列が部分配列として現れる X 上の位置における z が現れる位置を，X における接頭辞と接尾辞への分割位置とすることによって回避できる．この X と Y それぞれの接頭辞、接尾辞への分割のもとで，X と Y の接頭辞については末尾が z 未満である最長共通増加部分配列を求め，一方，接尾辞については先頭が z を超える最長共通増加部分配列を求めれば，前者に整数 z を連接し，これに後者を連接することによって，X と Y 全体の最長共通増加部分配列が得られるからである．X と Y の各長さの接頭辞の対に対して，上記の分割位置を長さが 1 だけ短い接頭辞に関する値から帰納的に求める漸化式を与えることによって，Hirschberg [4] の分割統治法に基づく $O(|X| \cdot |Y|)$ 時間 $O(|X| + |Y|)$ 領域アルゴリズムを得た．

4 論理関数の複雑さ

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．これら表現のサイズは，様々な意思決定アルゴリズムが保持する知識表現の構築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，本研究においても基本的研究課題として位置づけている．本研究では，前年に引き続き，論理回路，論理式，決定木，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 否定数限定論理回路の複雑さ

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．論理回路を計算モデルとして計算の複雑さを解析する手法は，理論計算機科学における最大の未解決問題である P≠NP 予想の解決にも直結する有望なアプローチの 1 つと考えられている．論理回路モデルにおいては，計算の複雑さは回路のサイズや深さで評価されるが，それらは，使用できる否定素子の個数を制限すると，制限しない場合に比べて大きいオーダーの量を必要とすることがある．本研究では，そのようなギャップのある問題として，入力ビット系列を昇順に（0*1*の形に）並び変えるソートと入力ビット系列の 1 の補数を求めるビット反転問題を取り上げ，否定素子数と回路のサイズとの間の関係を調べた．このとき，入力ビット系列 $x = (x_1, x_2, \ldots, x_n)$ において，値が 0 から 1 へ，あるいは 1 から 0 へ変化する回数

$A(x) = |x_2 - x_1| + \cdots + |x_n - x_{n-1}|$ をパラメータとして解析を行った．以下では，入力ビット系列 x を，$A(x) \leq k$ を満たす系列（k トニック列と呼ぶ）に限定する．

ソートについては，$k = O(1)$ で否定素子数を $\log\log n$ に制限したとき，サイズが，ある定数 $c \in (0,1)$ に対して $O(n(\log n)^{1-c})$ となる回路を構成した．マージは $k = 2$ におけるソート問題とみなせるので，この結果はマージに対する同様の結果 [7] の拡張となっている．

ビット反転問題については，否定素子数を $O(k \log n)$ に制限したとき，深さが $O(k \log n)$ でサイズが $O(kn)$ の回路を構成した．この結果は，$k = o(\log n)$ のときは，従来の構成法 [8] を改善したものとなっている．さらに，$k = O(1)$ のときは，我々の構成法は本質的にこれ以上改善できない最適なものとなっている．

4.2 論理式のサイズの下界の構成的証明

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，論理式のサイズの下界導出手法としても利用可能であるという報告 [6] を受けて，その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．ここで，論理式とは，論理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．本手法は，SumPI と呼ばれるブール関数の複雑さを表す指標によって特徴づけられる．SumPI は，ブール関数 f が与えられたとき，f の真理値表によって規定されたある半正定値問題の最適解として定義され，その 2 乗値 $\mathrm{SumPI}(f)^2$ が，f を表わす論理式のサイズの下界を与えるという性質がある．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．特に，f と g が互いに素な変数集合を持つブール関数のとき，任意の 2 項演算 $\otimes$ に対し，$\mathrm{sumPI}(f \oplus g)$ が $\mathrm{sumPI}(f)$ と $\mathrm{sumPI}(g)$ の簡単な関数で表わされることを示した．これにより，互いに素な変数集合を持ついくつかのブール関数を合成することによって得られるブール関数の論理式複雑さの下界を，効率よく再帰的に求めることができる．

さらに，この結果から，f と g に対する最簡の論理式表現が与えられていると仮定したとき，$f \oplus g$ の最簡論理式を簡単に構成できるための条件を与えている．これにより，最簡な論理式のみを列挙するアルゴリズムを構築することができる．

4.3 計算機支援下界証明系の開発にむけて

明示的に与えられた関数を計算する論理回路のサイズの下界を与える，計算機支援による証明の実現可能性に対する検討を行った．四色問題の解決に端を発する計算機支援証明は，近年の著しい計算機性能の向上のもと，より一層の広がりを見せることが予想されている．本研究では，岩間らによる論理回路サイズに対する既知の最良の下界を与える証明 [9] を，計算機支援のもとで再構成することを試み，その実現可能性や，より強い下界導出手法へと発展させる際に必要となる技術に対する幾つかの知見を得た．

参考文献

[1] Z. Bar-Yossef, K. Hildrum and F. Wu, Incentive-Compatible Online Auctions for Digital Goods, *Proceedings of 13th SODA*, 964–970, 2002.

[2] V. Vovk, A game of prediction with expert advice, *Journal of Computer and System Sciences*, 56(2):153–173, 1998.

[3] K. Uchizawa, R. Douglas and W. Maass, Energy complexity and entropy for threshold circuits. *Proceedings of 33rd ICALP*, (1):631–642, 2006.

[4] D.S. Hirschberg, A linear space algorithm for computing maximal common subsequence, *Communications of ACM*, 18(6):341–343, 1975.

[5] I.H. Yang, C.P. Huang and K.M. Chao, A fast algorithm for computing a longest

common increasing subsequence, *Information Processing Letters*, 93, 249–253, 2005.

[6] S. Laplante, T. Lee and M. Szegedy, The quantum adversary method and classical formula size lower bounds, *Proceedings of 20th IEEE Conference on Computational Complexity*, 76–90, 2005.

[7] K. Amano, A. Maruoka and J. Tarui, On the Negation-Limited Circuit Complexity of Merging, *Discrete Applied Mathematics*, 126(1):3–8, 2003.

[8] R. Beals, T. Nishino and K. Tanaka, More on the Complexity of Negation-Limited Circuits, *SIAM Journal on Computing*, 27(5):1334–1347, 1998.

[9] K. Iwama and H. Morizumi, An Explicit Lower Bound of $5n - o(n)$ for Boolean Circuits, *Proceedings of 27th MFCS*, 353–364, 2002.

研究業績一覧

学術論文

1. 瀧本英二:
"オンライン予測の理論に基づく意思決定", 電子情報通信学会論文誌 A, J89-A (6), 405–418, 2006.
概要: 計算学習理論の枠組みの一つとして開発され発展してきたオンライン予測の方法論は，情報圧縮，資源配分，ゲームの戦略選択，線形回帰，ネットワークルーチングなど，様々な領域における意思決定問題に適用できることが明らかになってきた．本解説では，この普遍性を支えるオンライン予測アルゴリズムの設計と解析の原理を，いくつかの応用例とともに紹介する．

2. Shigeaki Harada, Eiji Takimoto and Akira Maruoka:
"Online Allocation with Risk Information", IEICE Transactions on Information and Systems, E89-D (8), 2340–2347, 2006.
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 Vovk's Aggregating Algorithm to this problem and give a tight performance bound. The results support our intuition that it is safe to bet more on low-risk options. Surprisingly, the loss bound of the algorithm does not depend on the values of relatively small risks.

3. Shigeaki Harada, Eiji Takimoto and Akira Maruoka:
"Aggregating Strategy for Online Auctions", Proceedings of the 12th Computing and Combinatorics Conference (COCOON 2006), Lecture Notes in Artificial Intelligence, 4112, 33–41, Aug. 2006.
概要: We consider the online auction problem in which an auctioneer is selling an identical item each time when a new bidder arrives. It is known that results from online prediction can be applied and achieve a constant competitive ratio with respect to the best fixed price profit. These algorithms work on a predetermined set of price levels. We take into account the property that the rewards for the price levels are not independent and cast the problem as a more refined model of online prediction. We then use Vovk's Aggregating Strategy to derive a new algorithm. We give a general form of competitive ratio in terms of the price levels. The optimality of the Aggregating Strategy gives an evidence that our algorithm performs at least as well as the previously proposed ones.

4. Yoshifumi Sakai:
"A linear space algorithm for computing a longest common increasing subsequence", Information Processing Letters, 99 (5), 203–207, Jul. 2006.
概要: Let X and Y be sequences of integers. A common increasing subsequence of X and Y is an increasing subsequence common to X and Y. In this note, we propose an $O(|X|\cdot|Y|)$-time and $O(|X|+|Y|)$-space algorithm for finding one of the longest common increasing subsequences of X and Y, which improves the space complexity of Yang et al. [Inform. Process. Lett. 93 (2005) 249–253]'s $O(|X|\cdot|Y|)$-time and $O(|X|\cdot|Y|)$-space algorithm, where $|X|$ and $|Y|$ denote the lengths of X and Y, respectively.

5. 酒井義文, 上原稔, 佐藤永欣:
"読捨てコンテンツをいつ更新するべきか", 電子情報通信学会論文誌 D-I, J89-D (9), 1913–1922, 2006 年 9 月.
概要: ユーザが以前に閲覧したことのある読捨てコンテンツを再閲覧したときのコストを 1，読捨てコンテンツを新しいものに更新する際に生じるコストを m としたときの，u 人のユーザによる閲覧要求列に対する決定性オンライン更新アルゴリズムの競合比を，競合解析の手法により評価する．

6. Kazuyuki Amano, Akira Maruoka:
"Better Upper Bounds on the QOBDD Size of Interger Multiplication", Discrete Applied Mathematics, (掲載予定), 2007.
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 (J. Comp. Sys. Sci. 71(4) pp. 520–534, 2005). The experimental results suggest that our exponent of $6n/5$ is optimal or 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 is also presented.

7. Kazuyuki Amano, Akira Maruoka:
"On the Monotone Circuit Complexity of Quadratic Boolean Functions", Algorithmica, 46 (1), 3–14, Sep. 2006.
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.

8. Takayuki Sato, Kazuyuki Amano, Akira Maruoka:
"On the Negation-Limited Circuit Complexity of Sorting and Inverting k-tonic Sequences", Proceedings of the 12th Computing and Combinatorics Conference (COCOON 2006), Lecture Notes in Computer Science, 4112, 104–115, Aug. 2006.
概要: A binary sequence $x_1,\ldots,x_n$ is called k-tonic if it contains at most k changes between 0 and 1, i.e., there are at most k indices such that $x_i \neq x_{i+1}$. A sequence $\neg x_1,\ldots,\neg x_n$ is called an *inversion* of $x_1,\ldots,x_n$. In this paper, we investigate the size of a negation-limited circuit, which is a Boolean circuit with a limited number of NOT gates, that sorts or inverts k-tonic

input sequences. We show that if $k = O(1)$ and $t = O(\log \log n)$, a k-tonic sequence of length n can be sorted by a circuit with t NOT gates whose size is $O((n \log n)/2^{ct})$ where $c > 0$ is some constant. This generalizes a similar upper bound for merging by Amano, Maruoka and Tarui (Disc. Appl. Math. 126(1) 3–8, 2003), which corresponds to the case $k = 2$. We also show that a k-tonic sequence of length n can be inverted by a circuit with $O(k \log n)$ NOT gates whose size is $O(kn)$ and depth is $O(k \log^2 n)$.

研究会等

1. 内沢啓，瀧本英二:
"エネルギー計算量に制限のあるしきい値論理回路のサイズの下界について", 電子情報通信学会技術研究報告（コンピュテーション）, COMP2006 (40), 71–76, 2006 年 10 月.
概要: エネルギー計算量とは，脳が計算過程で消費するエネルギーと計算能力の関係を調べるために，しきい値論理回路に対して提案されたパラメータである．脳内のニューロンが "発火する "時に，"発火しない "時と比べて非常に大きなエネルギーを必要とするという事実に基づき，エネルギー計算量は，計算過程で "発火する（1 を出力する）"素子の個数として定義される．実際の脳内の計算は，非常に少ない発火回数で行われることが知られているため，本稿ではこの事実に着目し，エネルギー計算量の制限がしきい値論理回路の計算能力にどのように影響を与えるかについて理論的に解析した．具体的には，しきい値論理回路のエネルギー計算量，素子数，深さの 3 つのパラメータに関する関係式を導き，この関係式から，あるクラスに属するブール関数を計算する，エネルギー計算量と深さに制限のあるしきい値論理回路は，素子数が入力数に対して必ず指数的であることを示す.

2. Hideaki Fukuhara, Kazuyuki Amano and Eiji Takimoto:
"On formula size lower bounds for synthesis of Boolean functions over disjoint sets of variables", 電子情報通信学会 2007 年総合大会, DS-1-2, 2007 年 3 月.
概要: Recently, it shown that a complexity measure called sumPI which originates from quantum computing provides a good lower bound on the size of Boolean formulas. In this paper, we evaluate sumPI($f \oplus g$) in terms of sumPI(f) and sumPI(g), where f and g are "disjoint" Boolean functions, i.e., the sets of variables for f and g are disjoint, and $\oplus$ is an arbitrary Boolean operator. Applying this result recursively, we obtain formula size lower bounds for any synthesis of disjoint Boolean functions. Moreover, we give conditions under which the bounds are tight.

3. Kazuyuki Amano:
"A Procedure that Generates a Class of Optimal Boolean Formulas", 情報処理学会アルゴリズム研究会, 2006-AL-106, 1–8, 2006 年 5 月.
概要: In this paper, we investigate the size of Boolean formulas for composite functions. For two Boolean functions $f : \{0,1\}^n \to \{0,1\}$ and $g : \{0,1\}^m \to \{0,1\}$, $f \otimes g$ denotes a Boolean function on nm variables defined by $(f \otimes g)(x_1, \ldots, x_{nm}) = f(g(\tilde{x}_1), \ldots, g(\tilde{x}_n))$ where $\tilde{x}_i = (x_{(i-1)m+1}, \ldots, x_{im})$. We give a class of base functions G such that for every function of the form $f = f_1 \otimes \cdots \otimes f_k$ with $f_1, \ldots, f_k \in G$, a "naive" construction yields an optimal formula for f. The class G contains every two-variable functions, 134 out of 256 three-variable functions, and more. This can be viewed as a generalization of Khrapchenko's result that says that the formula size of the parity function on $n = 2^k$ variables is n^2, which corresponds to the case $f_i = x_1 \oplus x_2$ for every i. We also give a procedure that recursively generates Boolean formulas whose

optimality is guaranteed. Our results are based on a careful inspection of a recently proposed complexity measure called SumPi, which originated from the quantum adversary method.

4. 天野 一幸:
“回路計算量の線形下界に対する計算機支援証明について”, 電子情報通信学会技術研究報告（コンピュテーション）, COMP2006-39, 65–70, 2006 年 10 月.
概要: 近年の計算機の著しい性能向上を受けて，組み合わせ論的問題に対する計算機支援証明の適用可能性が広がっている．本稿では，明示的論理関数に対する回路計算量の線形下界の導出問題を取り上げ，これに対する計算機支援証明を構成する試みについて報告する．まず，この問題に対する証明手法として広く用いられるゲート除去法を，四色定理の証明との類似性についても言及しつつ，より機械的取り扱いが容易となるよう定式化する．次いで，岩間ら (MFCS ’02) による現在最良の線形下界の証明を，計算機支援のもとで再構成する試みを通じて得られた知見について述べる．

5. 澤田 清，天野 一幸:
“完全 k 分木型組織構造の多階層関係追加モデル”, 情報処理学会 アルゴリズム研究会, 2007-AL-110, 47–54, 2007 年 1 月.
概要: 本研究では，高さ H の完全 K 分木型組織構造に関係を追加するモデルを提案する．ここでは，$L(L = 1, 2, \cdots, H)$ 個の階層それぞれのすべての頂点対に辺を追加する場合に，完全 K 分木の全頂点対の最短経路の短縮長さを合計した総頂点間短縮経路長を最大にする最適深さの組 $\{N_1, N_2, \ldots, N_L\}$ $(N_1 > N_2 > \cdots > N_L)$ を求める．その結果，$\{N_1, N_2, \ldots, N_L\} = \{H, H-1, \ldots, H-L+1\}$ が示される．

学会大会等

1. 福原秀明，天野一幸，瀧本英二:
“パリティ合成関数に対するブール式のサイズの下界について”, 2006 年度 夏の LA シンポジウム, 2006 年 8 月.

2. 内沢啓，瀧本英二:
“エネルギー計算量に制限のあるしきい値論理回路について”, 2006 年度 冬の LA シンポジウム, 2007 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 †　全　眞嬉 †　河原林　健一 ‡

† 東北大学 大学院 情報科学研究科
{tokuyama, shioura, jinhee}@dais.is.tohoku.ac.jp

‡ 国立情報学研究所
k-keniti@nii.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．

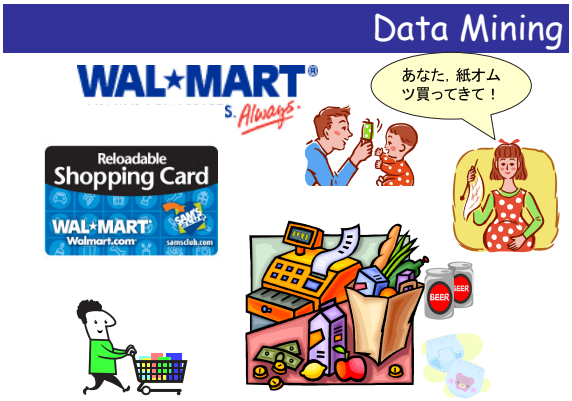


図 2.1: データマイニングのイメージ：紙おむつを買う人は高い確率でビールも同時に買う

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．

図 2.2: 書籍販売でのデータマイニング

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 18 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 18 年度の具体的な成果目標としては，柔軟かつ実用的なデータマイニング手法の実現と，関連する基礎理論とその利用についての研究を行った．また、全と、博士研究員として参加した Ashkan Sami 研究員は、ＷＥＢデータや医療データなどでの問題への応用研究を行った。さらに、データマイニングで広く使われるクラスタリングのための基礎理論であるボロノイ図についても研究を行い、さまざまな拡張について成果を得た。特にゾーン図という新しいボロノイ図に関する成果は非常に高い国際評価を得ている。また、モデル班のメンバーとして，近年のさまざまの新しい計算モデルについてスタディーと研究を行った。特に河原林はグラフマイナーを考慮した最適化アルゴリズムの設計理論について世界的なブレークスルーであると評価の高い研究を行なった。その一部は本特定領域の経費で招聘した Bruce Reed 教授との共同研究であり、データマイニングで用いるグラフの視覚化に応用できる非常に優れた成果である。また、徳山と塩浦はパラメトリック複雑度モデルでの計算量の理論と離散凸解析モデルでの計算理論での成果をあげた。そのほかに、徳山と塩浦は計算幾何学を用いた金融工学における新しいアルゴリズム設計モデルについていくつかの研究成果を得た。

本年度の具体的な主な成果としては，下記のものがある．

1. 柔軟な決定木の構築と実験
2. 階層ルールの一般化に対する計算量の探求と高速アルゴリズムの設計
3. 計算幾何学の最適化理論の研究
4. WEB データや医療データにおけるデータマイニングの実用研究
5. パラメトリック複雑度やグラフマイナーを考慮した新しいモデルでのアルゴリズム設計理論と解析
6. 計算幾何学手法を用いた金融工学におけ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，河原林は新しいモデルでの最適化とグラフアルゴリズムの研究，全は階層ルールを用いた柔軟な決定システムの実装と実験及び改良、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．

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１０本，研究協力者の塩浦は同 4 本を発表している．また、河原林健一は権威ある STOC、SODA などの国際会議での発表を行い、国際会議 ISAAC では最優秀論文賞を獲得した。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．総じて、研究グループにおいて STOC の論文 3 件 (2007 年採録分含む)、SODA の論文 2 件、ISAAC での最優秀論文を含む 18 件の質の高い研究論文の発表を行い，十分高い評価を受ける事が出来る活動成果であると判断する。また、徳山は市民講座での講演など本研究テーマに関連した啓蒙活動も行った。

経費について

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．徳山は STOC、SODA 国際会議などのアルゴリズム分野での最高レベルのシリーズ国際会議で研究成果発表経費、ISAAC 国際会議 (プログラム委員）の参加経費、その他国内旅費を本研究費から拠出した。さらに塩浦はヨーロッパ各国の研究者との共同研究を行い，広く国際的に活動したが、それらの旅費の一部を本研究費から拠出した。全はデータベースでの一流国際会議である VLDB 国際会議への参加費用や国内旅費を本研究費から拠出した。また，博士研究員として採用（採用経費は他の経費から拠出）した Ashkan Sami 研究員はデータマイニングと人工知能の 2 つの国際会議での研究発表を行い、その経費を本特定領域研究費から拠出した。更に、NHC プロジェクトの春、秋の強化合宿には，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，その旅費及び国内研究会発表のための旅費も本研究費から拠出した．

4　研究成果の概要

4.1　柔軟な決定木の構築と実験

本テーマについては前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．実装は平成 17 年度に行い、本年度は、さまざまな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．実験の成果は共同研究者の全による博士論文にまとめられている。

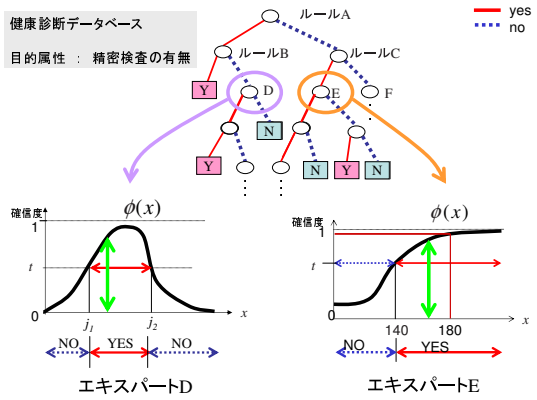


図 2.3: エキスパート付き決定木

4.2　階層ルールの一般化に対する計算量と高速アルゴリズムの設計

上記の数値属性用のエキスパート設計に用いられる階層化ルールでは、ルールの基本形状が「1 点を共有する長方形領域の和」の形状に限られており、より広いクラスへの拡張が望まれていた。この手法は、有向グラフの最大重み支配閉包が多項式時間で計算できる事を用いて設計されており、未解決問題として、2 つの異なったグラフの支配閉方の和集合で最大重みであるものの計算の複雑度の同定が求められていた。平成 18 年度の成果の

一つとして、上記の未解決問題は、グラフが木である場合でも NP 完全であり、かつ近似アルゴリズムの設計も困難である事を証明した。さらに、有向グラフの最大重み支配集合の理論を用いた新しい階層化ルールの設計として、ディジタル平面やディジタル空間での（中心を固定した）星型領域の集合を最大重み支配集合の集合とするグラフの設計に成功した (図 2.4)。これらの仕事は、全、徳山と、博士学生として滞在したドイツ、カールスルーエ大学の Martin　Nöllenberg 君（博士課程学生）の共同研究である。学会での成果発表は次年度となる予定である。

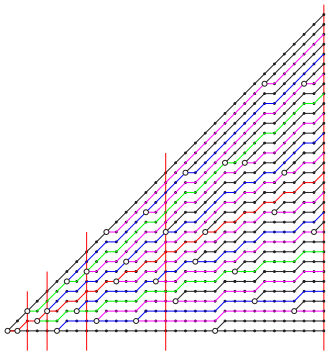


図 2.4: ディジタル星型領域を定義するグラフ

4.3　計算幾何学の最適化理論の研究

知識抽出において、特にイメージや幾何学データからの知識抽出にあたっては幾何学的最適化技法は要素技術として必須である。さまざまな研究を行ったが、ここでは特にゾーン図に対する研究について記述する。この成果は浅野哲夫教授 (JAIST)、Jirka Matousek 教授 (チェコ、チャールス大学) と共同研究の成果であり、計算理論分野で最高レベルの国際会議 STOC (ACM Symposium on Theory of Computing), SODA (ACM-SIAM Symposium on Discrete Algorithms) などで発表されている。また、成果の一部は数学分野での一流専門誌である Advances in Mathematics に掲載が決定している。

ボロノイ図は平面上のデータに対応する勢力図として与えられる平面分割であり、知識抽出に必須であるクラスタリングやベクトル量子化を行うための基本技法である。本年度の大きな成果として、ボロノイ図の新しい変種であるゾーン図の性質の解明があげられる。

平面上の 2 点が与えられたとき，コンパスと定規を用いてそれらの垂直二等分線を作図するのは，小学校で習う初歩の作図法であると共に，ギリシャでの「幾何算術」の基本であり，四則計算や根号計算などを作図を用いて行うための基本技法である．垂直二等分線は 2 点からの等距離点の集合であり，同様に平面上の 3 点に対して，2 点からの等距離点は 3 点を通るユニークに定まる円の中心であり，三角形の外接円の中心（外心）であるが，これが 3 本の垂直二等分線（三角形の 3 つの辺の二等分線たち）の交点として求める事ができることは中学校で学ぶ事実である．3 点 $\mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3$ に対して，平面を，どの点に一番近いかで 3 つの領域（支配領域）に分けることが出来る．これは外心から放射状にこれら 3 本の垂直二等分線を三角形の対応する辺に向けて書くことで実現できる．これを一般化して，平面上の n 点集合 $\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_n$ に対して，

$$Vor(\mathbf{p}_i) = \{\mathbf{z} \in \mathbb{R}^2 : d(\mathbf{z}, \mathbf{p}_i) \leq d(\mathbf{z}, \mathbf{p}_j) \text{ for } 1 \leq j \leq n\}$$

を点 $\mathbf{p}_i$ の支配領域とし，平面分割を行ったものがボロノイ図である．ボロノイ図は垂直二等分線を用いて比較的容易に描くことができる．さて，ここで，ボノロイ図の変種を一つ考えてみよう．図 2.5 の左図は通常のボロノイ図であり，右図は新たに導入した概念であるゾーン図 (zone diagram) である．

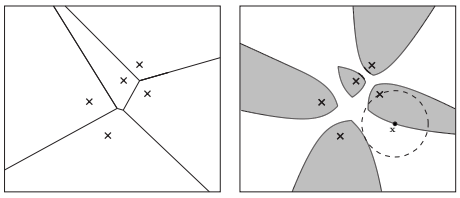


図 2.5: 5 つの母点が×印で描かれている．左は古典的ボロノイ図．右のゾーン図では母点 $\mathbf{p}_i$ は R_i を領域として持ち，R_i の境界上の点 $\mathbf{x}$ から $\mathbf{p}_i$ への距離は他の領域たちへの最短距離と等しい

平面上の点 $\mathbf{a}$ と集合 $X \subseteq \mathbb{R}^2$ に対して $\mathbf{a}$ の X

に対峙する支配領域 (*dominance region*) を

$$\mathrm{dom}(\mathbf{a}, X) = \{\mathbf{z} \in \mathbb{R}^2 : d(\mathbf{z}, \mathbf{a}) \leq d(\mathbf{z}, X)\},$$

で定義する．ここで $d(\cdot,\cdot)$ はユークリッド距離であり $d(\mathbf{z}, X) = \inf_{\mathbf{x}\in X} d(\mathbf{z}, \mathbf{x})$ である．

古典的なボロノイ図では, 母点 $\mathbf{p}_i$ の支配領域は $\mathrm{dom}(\mathbf{p}_i, \{\mathbf{p}_j : j \neq i\})$ であり, これらの領域は平面を敷き詰める．ゾーン図では, $\mathbf{p}_i$ の支配領域は

$$R_i = \mathrm{dom}\Big(\mathbf{p}_i, \bigcup_{j\neq i} R_j\Big) \text{ for all } i = 1, 2, \ldots, n \tag{2.1}$$

で定まる．すなわち，支配領域は，他のどの支配領域よりも母点に近い点の集合である．支配領域 R_i たちの集合和は中立地帯 (*neutral zone*) と呼ばれる空でない補集合を持つ．

ゾーン図の概念を「戦国時代」の均衡を例にして説明しよう．互いに敵対する n 国の領主たちがいるとしよう．領国 i はその居城を母点 $\mathbf{p}_i$ にもち，領国 R_i をその周りに持っている．これら n 個の領国は中立地帯で隔てられている．領国 R_i が他の領主から攻撃された場合，迎撃隊が居城 $\mathbf{p}_i$ から出発する．迎撃隊が R_i の境界にある攻撃地点に，敵軍よりも早く到着した場合に撃退に成功する．しかしながら，攻撃側は自分の領内では秘密に部隊の移動を行うことが出来，迎撃隊の出発は攻撃側がその領国の境界を離れたときに始めて居城を出発できる．ゾーン図は上記の状況での均衡図であり，どの国も領土を守ることが出来，更にどの国も他の国からの侵略のリスクなしに領土の拡大が出来ない状態である．

ゾーン図の概念は非常に面白く，多くの数学的, アルゴリズム論的なチャレンジを提供してくれる．さらに，以下の理由により，ゾーン図やその変種は自然界の現象のモデル化に活用できるように思える．古典的なボロノイ図は基本的な幾何学構造であるが，さまざまの分野で利用され，中でも多体の成長過程（細胞成長や結晶格子，地理的パターン，社会科学における領域均衡など）の数学的モデル化に利用される．今までのボロノイ図やその多くの一般化は，空間を母点たちに対応する領域に分割する．しかし，自然界における幾何学的構造においては，支配領域が全空間を覆っているとは限らない．例えば，成長過程において，支配領域たちが接する前に成長が停止したような場合や，何らかの非接触（遠隔）作用によって領域成長が抑えられるような場合である．このような場合にはゾーン図のように中立地帯のあるモデルが適当である．

先に書いたように古典的なボロノイ図の定義は直接的であり，存在は自明である．しかしながら，ゾーン図の定義は陰的に与えられ，各々の領域の定義に他の領域が使用されている．従って，この定義を満たすような領域族の存在は非自明であり，また，一意に存在するかどうかも明らかでない．本研究ではこの 2 つの問題を肯定的に解決した．すなわち，下記の定理である．

Theorem 1 平面上の任意の n 点の集合 $\mathbf{p}_1, \ldots, \mathbf{p}_n \in \mathbb{R}^2$ に対して，領域族 $(R_1, \ldots, R_n)$ で *(2.1)* を満たすものが存在し，一意である．

驚くべきことに，母点数が 2 である場合にすら上記定理は自明でない．この場合，2 つの領域は互いの鏡映像であり，境界線は *distance trisector curve* と呼ばれる面白い曲線になる．これは垂直二等分線の自然な拡張であるが，この曲線は代数的でなく，基本的な関数たちを用いて表示できないのではないかと予想されている．一方，曲線上の点は任意の精度までビット数の多項式の時間で計算することが出来る．

定理 1 のうち，存在証明は，解析学でよく知られた角谷-Shauder のバナッハ空間における不動点定理を利用することで与えられる．バナッハ空間の一点は領域の n 個の組に対応し，従ってこの空間は連続無限次元を持つ．証明は概念的にシンプルであり，d 次元空間におけるゾーン図において成立する．さらに，幾何学物体たちのゾーン図, α-ゾーン図 (R_i たちの点と $\mathbf{p}_i$ の距離が $\bigcup_{j\neq i} R_j$ への距離の α 倍以下, ここで $\alpha > 0$ は任意のパラメタ) などゾーン図のさまざまな自然な拡張に対して存在性の証明は適用できると思える．

一意性の証明では，ゾーン図を近似する自然な繰り返しプロシージャを考える．母点 $\mathbf{p}_1, \ldots, \mathbf{p}_n$ を固定し，$\mathbf{R} = (R_1, \ldots, R_n)$ を平面上の領域の n 組で $\mathbf{p}_1 \in R_1, \ldots, \mathbf{p}_n \in R_n$ を満たすものとする．これに対して，新しい領域の n 組 $\mathbf{Dom}(\mathbf{R}) = \mathbf{S} = (S_1, S_2, \ldots, S_n)$ を $S_i = \mathrm{dom}(\mathbf{p}_i, \bigcup_{j\neq i} R_j)$ として定義する．このようにすると，**Dom** は領域の n 組全体の集合に作用する作用素（ドミナンス

作用素）であり，ゾーン図の定義は下記のように書き直すことが出来る．

> 領域の n 組 $\mathbf{R} = (R_1, \ldots, R_n)$ が点集合 $\mathbf{p}_1, \ldots, \mathbf{p}_n$ のゾーン図であるとは，作用素 **Dom** の不動点である，すなわち，$\mathbf{R} = \mathbf{Dom}(\mathbf{R})$ であることである．

二つの n 組 $\mathbf{R} = (R_1, \ldots, R_n)$ と $\mathbf{S} = (S_1, \ldots, S_n)$ に対して，$R_i \subseteq S_i$ for all $i = 1, 2, \ldots, n$ であるとき，$\mathbf{R} \preceq \mathbf{S}$ と表記する．

定義から $\mathbf{R} \preceq \mathbf{S}$ であれば $\mathbf{Dom}(\mathbf{R}) \succeq \mathbf{Dom}(\mathbf{S})$，すなわち **Dom** は $\preceq$ に関して反単調作用素である．初期状態 $\mathbf{I}^{(0)} = (\{\mathbf{p}_1\}, \ldots, \{\mathbf{p}_n\})$ を単一点集合領域からなるシステムとし，$\mathbf{O}^{(0)} = (O_1^{(0)}, \ldots, O_n^{(0)}) = \mathbf{Dom}(\mathbf{I}^{(0)})$ を $\mathbf{p}_1, \ldots, \mathbf{p}_n$ たちの古典的なボロノイ領域たちからなるシステムとする．帰納的に $k = 1, 2, \ldots$ に対して $\mathbf{I}^{(k)} = \mathbf{Dom}(\mathbf{O}^{(k-1)})$, $\mathbf{O}^{(k)} = \mathbf{Dom}(\mathbf{I}^{(k)})$ と定義する．

作用素 **Dom** の反単調性と帰納的定義により $\mathbf{I}^{(0)} \preceq \mathbf{I}^{(1)} \preceq \mathbf{I}^{(2)} \preceq \cdots$ かつ $\mathbf{O}^{(0)} \succeq \mathbf{O}^{(1)} \succeq \mathbf{O}^{(2)} \succeq \cdots$ となる．さらに，もし R がゾーン図であれば，$\mathbf{R} = \mathbf{Dom}(\mathbf{R})$ かつ $\mathbf{I}^{(0)} \preceq \mathbf{R}$ なので，帰納法と反単調性から任意の k に対して $\mathbf{I}^{(k)} \preceq \mathbf{R} \preceq \mathbf{O}^{(k)}$ が成立する．すなわち図 2.6に示すように，$\mathbf{I}^{(k)}$ はゾーン図を内側から近似する増加列であり，一方 $\mathbf{O}^{(k)}$ は外側から近似する減少列である．

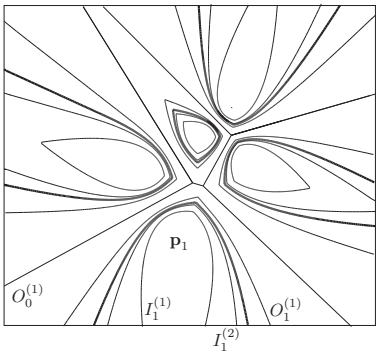


図 2.6: ゾーン図の内側近似と外側近似 $\mathbf{I}^{(k)}$ と $\mathbf{O}^{(k)}$.

内側近似と外側近似が同一の極限に収束することを示す事により，ゾーン図が一意に存在することが示される．この証明は同時にゾーン図を構成する実用的なアルゴリズムを与える．領域族 $\mathbf{I}^{(k)}$, $\mathbf{O}^{(k)}$ に属する領域たちは凸多角形を用いて近似することにより，証明に沿ったアルゴリズムの実行が可能になり，この論文にあるゾーン図の絵はこのアルゴリズムで描画したものである．実装に注意は要るが，これらの凸多角形たちが実際にゾーン図の領域たちの内側近似と外側近似になっているようにアルゴリズムを設計できる．小規模データでの実験結果では，このアルゴリズムの収束は非常に早いことが示されている．

4.4 WEB データや医療データにおけるデータマイニングの実用研究

WEB データでのデータ切り分け.

HTML で表現されたリスト形式のデータを切り分けて表形式のテーブルにする事は、知識抽出の道具として、さまざまの応用がある。これは、リストに対する詳細ページ情報を用いたデータ切り分けによって実現する事が出来、充足制約問題として定式化できる。　全と修士学生の小沼らにより、従来の研究の実装と改良、書籍販売 WEB データ等での実験を行い、更にグラフアルゴリズムを用いた高速計算法の研究を行った。研究成果は一部研究会で発表したが，次年度以降に続けて発表する。

医療データでのデータ抽出.

データマイニング技術の実データへの適用の試みとして、博士研究員 Ashkan Sami、東北大学医学研究科永富教授との共同研究を行い、データマイニングにおけるデータ評価指標として、SDI (Shape Distribution Indicator) を提案し、医療の実データに適応し、いくつかの新しい知見を得た。成果はデータマイニングと AI 分野の 2 つの国際会議で発表を行った。

4.5 パラメトリック複雑度やグラフマイナーを考慮した新しいモデルでのアルゴリズム設計理論と解析

知識抽出に必要な最適化問題の多くはグラフ上の最適化問題として定式化されるが、それらの多くが NP 完全である事が知られている。しかしな

がら、グラフマイナー理論において、パーフェクトグラフ予想の解決や Hadwiger 予想 (4 色問題の拡張）での研究成果など、多くの理論的な道具立てがそろい、その結果、特定のマイナーを含まないグラフでは多くの最適化問題が効率的に解けるということが明らかにされてきている。河原林はこのテーマに網羅的に取り組み、多くの新しい成果をあげた。これらは最高レベルの国際会議 STOC 及び SODA で論文発表され，また、権威ある国際会議である ISAAC での最優秀論文賞を受けるなど理論的には非常に高い評価を上げている。但し、多項式時間解法ではあるが、計算時間は非常に掛かるので、知識抽出への利用はまだ先のことであり、実装等は行っていない。さらに、グラフマイナー理論から発展した特筆すべき成果は、交差数が定数であるグラフの最小交差数描画を求める線形時間アルゴリズムの開発である。これは河原林と、東北大学で本特定領域の研究費（総括班）を用いて平成 18 年度に 2ヶ月間招聘したカナダ、マクギル大学の Bruce Reed 教授との共同研究である。交差がなく平面に描画できるグラフ (平面グラフ）の描画を行うアルゴリズムは Hopcroft と Tarjan によって 1970 年代 (JACM 1974) に提案され、アルゴリズム理論の一つの金字塔とされる。しかしながら、データマイニングの関係描画など多くの応用では、疎ではあるが必ずしも平面的でないグラフを視覚化させる必要があり、そのため、Hopcroft と Tarjan の手法を拡張し、与えられたグラフの最小交差数を計算し、かつ最小交差数を持つ描画の実現を行うアルゴリズム設計は広く知られていた未解決問題であった。河原林らは、この未解決問題を解決し、最小交差数が定数である場合は線形時間で作動するアルゴリズムの設計に成功した。数学的にも非常に深い結果であり、最高レベルの国際会議 STOC で 2007 年 6 月に発表される予定である。

これに関連し、徳山は Halldorsson 教授 (アイスランド大学）Knauer 教授（ベルリン自由大学）Spillner 教授（East Anglia 大学、英国）との共同研究で、グラフの非交差全域木の計算アルゴリズムに関して、入力グラフの交差数をパラメタとした時に従来より格段に高速なアルゴリズムの設計を与えた。

4.6 計算幾何学手法を用いた金融工学における近似アルゴリズムの設計

塩浦と徳山は，パス依存型オプションの一種である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，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．

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，行使期日の固定されたヨーロピアンアジアンオプションに対し、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，$O(\sqrt{n}X/k)$ 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，$O(n^{1/4}X/k)$ という近似誤差を実現した．

本年度では，前年度に提案した、ヨーロピアンアジアンオプションに対して、計算時間がこれまでと同じ $O(kn^2)$ であり，かつより小さい近似誤差 $O(X/k)$ をもつランダム化アルゴリズムを国際論文誌で発表した．さらに継続研究として、より複雑なアメリカンアジアンオプションに対して、計算幾何学手法を用いて誤差をパラメタとする多項式時間アルゴリズムの設計に成功した。また，本研究で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. T. Asano, J. Matousek, T. Tokuyama:
"The Distance Trisector Curve", Proceedings of the 38th ACM Symposium on Theory of Computing, STOC06, 336-343, 2006.
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 $f : \mathcal{R} \to \mathcal{R}$, 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. We provide an algorithm that, given $x \in \mathcal{R}$ and $\epsilon > 0$, computes an approximation to $f(x)$ with error at most ϵ in time polynomial in $\log \frac{1+|x|}{\epsilon}$. The separation of two points by two "trisector" curves considered here is a special (two-point) case of a new kind of Voronoi diagram, which we call the *zone diagram* and which we investigate in a companion paper.

2. B. Aronov, T. Asano, N. Katoh, K. Mehlhorn, T. Tokuyama:
"Polyline Fitting of Planar Points under Min-sum Criteria", Int. J. Comput. Geometry Appl., 16(2-3), 97-116, 2006.
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.

3. M. Halldorsson, T. Tokuyama:
"Minimizing Interference of a Wireless Ad-Hoc Network in a Plane", LNCS4240, ALGOSENSORS 2006, 71-82, 2006.
概要: We consider the problem of topology control of a wireless ad-hoc network on a given set of points in the plane, where we aim to minimize the maximum interference by assigning a suitable transmission radius to each point. By using computational geometric ideas and ϵ-net theory, we attain an $O(\sqrt{\Delta})$ bound for the maximum interference where Δ is the interference of a uniform-radius ad-hoc network. This generalizes a result given by Rickenbach et al. for the special case of highway model (i.e., one-dimensional problem) to the two-dimensional case. We also give a

method based on quad-tree decomposition and bucketing that has another provable interference bound in terms of the ratio of the minimum distance to the radius of a uniform-radius ad-hoc network.

4. A. Sami, R. Nagatomi, M. Takahashi, T. Tokuyama:
"OSDM: Optimized Shaper Distribution Method", LNCS 4093, ADMA2006, 1057-1064, 2006.
概要: Comprehensibility is vital in results of medical data mining systems since doctors simply require it. Another important issue specific to some data sets, like Fitness, is their uniform distribution due to tile analysis that was performed on them. In this paper, we propose a novel data mining tool named OSDM (Optimized Shape Distribution Method) to give a comprehensive view of correlations of attributes in cases of uneven frequency distribution among different values of symptoms. We apply OSDM to explore the relationship of the Fitness data and symptoms in medical test dataset for which popular data mining methods fail to give an appropriate output to help doctors decisions. In our experiment, OSDM found several useful relationships.

5. A. Sami, R. Nagatomi, M. Takahashi, T. Tokuyama:
"SDI: Shape Distribution Indicator and its Application to Find Interrelationships between Physical Activity Tests and Other Medical Measures", LNAI, 4304, 383-392, 2006.
概要: Comprehensibility is driving force in medical data mining results since doctors utilize the outputs and give the final decision. Another important issue specific to some data sets, like physical activity, is their uniform distribution due to tile analysis that was performed on them. In this paper, we propose a novel data mining tool named SDI (Shape Distribution Indicator) to give a comprehensive view of co-relations of attributes together with an index named ISDI to show the robustness of SDI outputs. We apply SDI to explore the relationship of the Physical Activity data and symptoms in medical test dataset for which popular data mining methods fail to give an appropriate output to help doctors decisions. In our experiment, SDI found several useful relationships.

6. T. Asano, N. Katoh, H. Tamaki, T. Tokuyama:
"Angular Voronoi Diagram with Applications", Proceedings of the 3rd International Symposium on Voronoi Diagrams in Science and Engineering, 18-24, 2006.
概要: Voronoi diagram for a set of geometric objects is a partition of the plane (or space in higher dimensions) into disjoint regions each dominated by some given object under a predetermined criterion. This paper defines a new Voronoi diagram called an angular Voronoi diagram for a set of line segments in the plane and investigate its combinatorial and structural properties. Given a set of line segments, an angular Voronoi diagram partitions the plane into regions so that a point belongs to a Voronoi region of a line segment if the visual angle of the line segment from the point is smallest (or largest) among all line segments. For simplicity we assume that given line segments are transparent when computing their visual angles. In other words, the visual angle of a line segment from a point is defined without considering other line segments.

7. 徳山豪:
"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（招待解説論文）", 電子情報通信学会論文誌 A, J89-A, 419-429, 2006.
概要: データの単純化は現代の情報社会では

非常に重要なテーマである．生のデータは通常巨大なサイズを持ち，分布関数としてみるとサンプル誤差や例外データ，誤入力などによる揺らぎを持っている．したがって，データマイニングなどのデータ解析においては，入力データをシンプルな関数に近似して利用する事が重要である．関数の近似においてはさまざまなアプローチがあり，関数解析的な手法，学習による手法などとともに離散アルゴリズムを用いた計算幾何学的な最適近似のアプローチは広く研究されている．しかしながら，計算幾何学的な手法においては，従来の応用はパターンマッチなどであり，データ解析に用いる場合は定式化や最適化基準を適当なものに変更する必要がある．それにしたがってアルゴリズム理論上のさまざまな困難や計算限界が生じ，それらを打破あるいは回避する必要が生じる．本稿では，計算幾何学におけるデータ近似の説明と現状の上で，著者たちの最近の研究を中心にした動向を解説する．

8. T. Itoh, Y. Okamoto, T. Tokuyama:
"Algorithms for the full Steiner tree problem", Proceedings of IETA(Improving Exponential Time Algorithms), 39-45, 2006.
概要: Assume that each edge of a graph $G = (V, E)$ is assigned a nonnegative real number cost, and that a set $K \subseteq V$ of vertices, called *terminals*, is given. A *full Steiner tree* (or a *terminal Steiner tree*) of G with respect to K is a subtree of G whose leaf set is K. The (minimum-cost) *full Steiner tree problem* is to find a full Steiner tree for K which has the minimum total cost of edges. In this paper we first give an exact algorithm to solve the problem for general graphs in time $O(3^k)$ where $k = |K|$, and hence it shows the fixed-parameter tractability of the problem. We then show that the problem can be solved in polynomial time for plane graphs if all the terminals lie only on a fixed constant number of face boundaries.

9. M. Halldorsson, A. Wolff, and T. Tokuyama:
"Improved fixed-parameter algorithms for non-crossing subgraphs", Proceedings of IETA(Improving Exponential Time Algorithms), 31-37, 2006.
概要: We consider the problem of computing non-crossing spanning trees in topological graphs. It is known that it is NP-hard to decide whether a topological graph has a non-crossing spanning tree, and that it is hard to approximate the minimum number of crossings in a spanning tree. We give improved fixed-parameter algorithms, where we use the number k of crossing edge pairs and the number μ of crossing edges in the given graph as parameters. The running times of our algorithms are $O^*(k^{O(\sqrt{k})})$ and $O^*(\mu^{O(\mu^{2/3})})$, where the O^*-notation neglects polynomial terms. Our method can be applied to several other non-crossing subgraph problems in topological graphs.

10. Takeshi Tokuyama:
"Recent Progress on Geometric Algorithms for Approximating Functions：Towards Applications to Data Analysis", Electronics and Communications in Japan, 90-3, 1-12, 2007.
概要: Data simplification is an extremely important issue in our current information-oriented society. Normally, a real-world database contains there exists a massive amount of raw data, and when we an attempt is made to consider the that data as a distribution function, it has fluctuations due to sampling errors, outliersexception data, and/or invalid inputs. Therefore, for data analysis technology such as data mining, it is important to approximate the input data by a simplifiede function. There are various approaches to function approximation, and including functional analytical methods techniques, and learning-based

techniques are quite popular. and computational geometric Apart from them, computational geometric approach based on optimizational approximation approaches using discrete algorithms, which have been is widely studied. However, the conventional application of computational geometrical techniques is pattern matching, and to applyuse them to for data analysis, their formulation and or optimization criteria must be changed accordingly. Therefore, various difficulties and or computational barriers arise, which must be eliminated or avoided. In this paper, we discuss the author explains data approximation in computational geometry and describes current trends centered on the author's his latest research.

11. T.Asano, J. Matousek, T. Tokuyama:
"Zone Diagrams, Existence, Uniqueness, and Algorithmic Challenge", Proceedings of the ACM-SIAM Symposium on Discrete Algorithms, SODA2007, 756-765, 2007.
概要: A *zone diagram* is a new variation of the classical notion of Voronoi diagram. Given points (sites) $p_1, \ldots, p_n$ in the plane, each p_i is assigned a region R_i, but in contrast to the ordinary Voronoi diagrams, the union of the R_i has a nonempty complement, the *neutral zone*. The defining property is that each R_i consists of all $x \in \mathcal{R}^2$ that lie closer (non-strictly) to p_i than to the union of all the other R_j, $j \neq i$. Thus, the zone diagram is defined implicitly, by a "fixed-point property," and neither its existence nor its uniqueness seem obvious. We establish existence using a general fixed-point result (a consequence of Schauder's theorem or Kakutani's theorem); this proof should generalize easily to related settings, say higher dimensions. Then we prove uniqueness of the zone diagram, as well as convergence of a natural iterative algorithm for computing it, by a geometric argument, which also relies on a result for the case of two sites in an earlier paper. Many challenging questions remain open.

12. K. Kawarabayashi, B. Mohar:
"Approximating the list-chromatic number and the chromatic number in minor-closed and odd-minor-closed classes of graphs", Proceedings of the 38th ACM Symposium on Theory of Computing, STOC06, 401–406, 2006.
概要: It is well-known (Feige and Kilian, Hastad) that approximating the chromatic number within a factor of $n^{1-\epsilon}$ cannot be done in polynomial time for $\epsilon > 0$, unless coRP = NP. Also, it is known that computing the list-chromatic number is much harder than the chromatic number. In fact, it is known that the problem of deciding if the list-chromatic number is k for $k \geq 3$ is Π_2^p-complete. In this paper, we focus on minor-closed and odd-minor-closed families of graphs. In doing that, we may as well consider only graphs without K_k-minors and graphs without odd K_k-minors for a fixed value of k, respectively. Our main results are that there is a polynomial time approximation algorithm for the list-chromatic number of graphs without K_k-minors and there is a polynomial time approximation algorithm for the chromatic number of graphs without odd-K_k-minors. Their time complexity are $O(n3)$ and $O(n4)$, respectively. The algorithms have multiplicative error $O(\sqrt{\log k})$ and additive error $O(k)$, and the multiplicative error occurs only for graphs whose list-chromatic number and chromatic number are $\Theta(k)$, respectively. Let us recall that H has an odd complete minor of order at least l if there are l vertex disjoint trees in H such that every two of them are joined by an edge, and in addition, all the vertices of trees are two-colored in such a way that the edges within the trees are bichromatic, but the edges between trees are monochromatic.

Hence it is easy to see that odd minor is a generalization of minor. Let us observe that the complete bipartite graph $K_{n/2,n/2}$ certainly contains a K_k-minor for $k \leq n/2$, but on the other hand, it does not contain any odd K_k-minor for any $k \geq 3$. Odd K_5-minor-free graphs are closely related to one field of discrete optimization which is finding conditions under which a given polyhedron has integer vertices, so that integer optimization problems can be solved as linear programs. Also, the odd version of the well-known Hadwiger's conjecture has been paid attention by many researchers. This is our motivation to consider odd minor-closed class of graphs. Our main idea involves precoloring extension. This idea is used in many results; one example is Thomassen's proof on his celebrated theorem on planar graphs. The best previously known approximation for the first result is a simple $O(k\sqrt{\log k})$-approximation following algorithm that guarantees a list-coloring with $O(k\sqrt{\log k})$ colors for K_k-minor-free graphs. The best previous approximation for the second result comes from the recent result of Geelen et al. who gave an $O(k\sqrt{\log k})$-approximation algorithm. We also relate our algorithm to the well-known conjecture of Hadwiger and its odd version of the conjecture. In fact, we give an $O(n^3)$ algorithm to decide whether or not a weaker version of Hadwiger's conjecture is true. Here, by a weaker version of Hadwiger's conjecture, we mean a conjecture which says that any $27k$-chromatic graph contains a K_k-minor. Also, we shall give an $O(n^{2500k})$ algorithm for deciding whether or not any $2500k$-chromatic graph contains an odd-K_k-minor.

13. E.D. Demaine, M. Hajiaghayi, K. Kawarabayashi:
"Algorithmic Graph Minor Theory: Improved Grid Minor Bounds and Wagner's Contraction", Proceedings of The 17th International Symposium on Algorithms and Computation, ISAAC2006, 3–15, 2006.
概要: We explore the three main avenues of research still unsolved in the field of algorithmic graph-minor theory, which all stem from a key min-max relation between the treewidth of a graph and its largest grid minor. This min-max relation is a keystone of the Graph Minor Theory of Robertson and Seymour, which ultimately proves Wagner's Conjecture about the structure of minor-closed graph properties. First, we obtain the only known polynomial min-max relation for graphs that do not exclude any fixed minor, namely, map graphs and power graphs. Second, we obtain explicit (and improved) bounds on the min-max relation for an important class of graphs excluding a minor, namely, $K_{3,k}$-minor-free graphs, using new techniques that do not rely on Graph Minor Theory. Third, we disprove Wagner's Conjecture in the context of graph contractions for general graphs, and in a sense characterize which graphs satisfy the conjecture. Our results have several combinatorial and algorithmic implications.

14. K. Kawarabayashi:
"Half-integral packing, Erdos-Posa Property and Graph Minors", Proceedings of the ACM-SIAM Symposium on Discrete Algorithms, SODA2007, 1187–1196, 2007.
概要: We consider the following problem: Given a graph G. Decide whether or not G has k half-integral packing of an H-minor for fixed k and H. Here, "k half-integral packing of an H-minor" is that there are k H-minors such that each vertex is used at most twice. Let us observe that if G contains H as a minor, then G has $|H|$ disjoint trees such that after contracting all the trees, we can get an H. So k half-integral packing of an H-minor means that there are

$k|H|$ trees $T_{1,1}, \ldots, T_{1,|H|}, T_{2,1}, \ldots, T_{k,|H|}$ such that trees $T_{i,1}, \ldots, T_{i,|H|}$ are disjoint for $1 \leq i \leq k$, and after contracting all these trees $T_{i,1}, \ldots, T_{i,|H|}$, we can get an H for $1 \leq i \leq k$, but each vertex is used at most twice in these trees $T_{1,1}, \ldots, T_{1,|H|}, T_{2,1}, \ldots, T_{k,|H|}$. This problem is motivated by the study of the half disjoint paths problem and unspilittable flow problem, . Let us observe that when $k = 1$, this case is exactly testing a given minor. So our problem includes Robertson-Seymour's result. Also, it would not follow from the existence of kH-minors. Furthermore, the algorithm of the half disjoint paths problem by Kleinberg does not give our algorithm. Hence, our setting is not directly comparable to Robertson and Seymour's result, and Kleinberg's result. We prove that when $H = K_6$ or K_7, this problem is solvable in polynomial time. Our motivation for the K_6-minor is that the structure of graphs with no K_6-minors. Unfortunately, it is not known at all, although the structure of graphs without K_5-minors is well known from 1930's. Moreover, we prove that Erdős-Pósa property holds for k half-integral packing of a K_6-minor (a K_7-minor, respectively). More precisely, either G has k half-integral packing of a K_6-minor (a K_7-minor, respectively) or G has a vertex set T of order at most $f(k)$ for some function of k such that $G-T$ does not contain any K_6-minor (K_7-minor, respectively). This settles the conjecture of Thomas for the K_6-minor case and the K_7-minor case. Finally, we shall address why our approach works for the K_6-minor case and the K_7-minor case, but does not work for the K_8-minor case.

15. K. Kawarabayashi, B. Reed:
"Computing crossing number in linear time", Proceedings of the 38th ACM Symposium on Theory of Computing, STOC07, to appear, 2007.

概要: We show that for every fixed k, there is a linear time algorithm that decides whether or not a given graph has crossing number at most k, and if this is the case, computes a drawing of the graph in the plane with at most k crossings. This answers the question posed by Grohe (STOC'01 and JCSS 2004). Our algorithm can be viewed as a generalization of the seminal result by Hopcroft and Tarjan, which determines if a given graph is planar in linear time. Our algorithm can also be compared to the algorithms by Mohar (STOC'96 and Siam J. Discrete Math 2001), for testing the embeddability of an input graph in a fixed surface. For each surface S, Mohar describes an algorithm which yields either an embedding of G in S or a minor of G which is not embeddable in S and is minimal with this property. The same approach allows us to obtain linear time algorithms for the same question for a variety of other crossing numbers. We can also determine in linear time if an input graph can be made planar by the deletion of k edges (for fixed k).

16. A. Shioura, N. Sun, Z. Yang:
"Efficient Strategy Proof Fair Allocation Algorithms", Journal of the Operations Research Society of Japan, 42 (2), 144–150, 2006年6月.

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.

17. A. Shioura, T. Tokuyama:
"Efficiently Pricing European-Asian Options: Ultimate Implementation and Analysis of the AMO Algorithm", Information Processing Letters, 100 (6), 213–219, 2006 年 12 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 $\mathrm{O}(kn2)$ time with the error bound $\emptyset(X/k)$ 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.

18. A. Shioura, K. Tanaka:
"Polynomial-time Algorithms for Linear and Convex Optimization on Jump Systems", SIAM Journal on Discrete Mathematics, (掲載予定).
概要: The concept of jump system, introduced by Bouchet and Cunningham (1995), is a set of integer points with a certain exchange property. In this paper, we discuss several linear and convex optimization problems on jump systems and show that these problems can be solved in polynomial time under the assumption that a membership oracle for a jump system is available. We firstly present a polynomial-time implementation of the greedy algorithm for the minimization of a linear function. We then consider the minimization of a separable-convex function on a jump system, and propose the first polynomial-time algorithm for this problem. The algorithm is based on the domain reduction approach developed in Shioura (1998). We finally consider the concept of M-convex functions on constant-parity jump systems which has been recently proposed by Murota (2006). It is shown that the minimization of an M-convex function can be solved in polynomial time by the domain reduction approach.

研究会等

1. 徳山豪:
"風変わりなボロノイ図と計算可能性", 日本 OR 学界 RAMP シンポジウム, 2006 年 7 月.
概要: 垂直二等分線とその一般化であるボロノイ図は計算幾何学ではもっともポピュラーな研究対象である．その定義を少し変更し，垂直二等分線ではなく三等分線を用いたボロノイ図であるゾーン図（zone diagram) を考察する．本公演では，このような変更により生じる，数学的な困難，及び計算可能性に対する新しい問題点について述べる.(浅野哲夫氏，Jiri Matousek 氏との共同研究）.

2. 岡田有司，徳山 豪:
"点と直線間の 3 等分線と 2 点間の 6 等分線", LA シンポジウム, 2006 年 8 月.
概要: 平面上に点 p と直線 ℓ を与え, これらを次の条件を満たす曲線 C_1, C_2 で分割する.C_1 の全ての点から点 p への距離と C_2 への距離が等しく, また C_2 の全ての点から直線 ℓ への距離と C_1 への距離が等しい．我々は C_1,C_2 が一意に存在することを示す.

3. 田代 太一，Magunus Halldorsson，徳山 豪:
"Wireless Ad-Hoc Network における干渉の軽減法", LA シンポジウム, 2006 年 8 月.
概要: 本研究では, 平面上に与えられた点集合を用いて Ad-Hoc ネットワークを構築する際, 各端末の電波送信半径を調整することによって, 最も干渉が起こる端末の干渉レベルを抑える手法を考える．本論分では, ϵ-ネットの理論と計算幾何のアイディアを用いることで, 干渉を $O(\sqrt{\Delta})$ に抑える手法を提案する．ここでの Δ は, 全端末を同じ電波送信半径としてネットワークを構築した場合の最大干渉レベルである．この手法は一次元モデルにおける結果を二次元に拡張したものである．さ

らに 4 分木を用いた手法も提案し, 最大干渉レベルの下界を考察する

4. 小沼寛明，全眞嬉，徳山豪:
“Web データの自動抽出とデータ変換”, FIT2006, D-036, 2006 年 9 月.
概要: 複数の web ページからデータを自動的に抽出しデータ変換を行い XML にまとめる．本稿では，リストページとディテールページの構造を持った web ページ群から情報を自動抽出する Lerman らの手法の実装と改善方法を提案し実験を行った．Lerman らの手法ではタグに挟まれている文字列を extract とし，リストページとディテールページの完全一致する文字列のみを抽出し，CSP の制約式を立ててレコード分割に用いる．完全一致した文字列のみ抽出されるため，情報ロスが生じる．本稿では上記の問題を回避するための改善法を提案する．

5. T. Asano, J. Matousek, T. Tokuyama:
“Zone Diagram, Existence, Uniqueness and Algorithmic Challenge”, 電子情報通信学会コンピュテーション研究会, 2006 年 9 月.
概要: SODA 2007 と同文に近いので省略

6. 渋谷彰信，塩浦昭義，徳山豪:
“アメリカン・アジアンオプションの価格付けに対する計算幾何手法を用いた近似アルゴリズム”, LA シンポジウム, 2007 年 1 月.
概要: 本論文は，金融市場で取引されている金融派生商品 (デリバティブ) の一つである，オプションの価格付け (価格の計算) という問題を扱う．本論文では，アメリカン・アジアンオプションと呼ばれるオプションに対し，計算幾何学の手法を用いて、オプション価格の近似値を効率的に求めるアルゴリズムを提案する．

7. 田代太一，M. Halldorsson，徳山豪:
“Wireless Ad-Hoc ネットワークにおける干渉の軽減法に関する研究”, 電子情報通信学会コンピュテーション研究会, 2007 年 3 月.
概要: 本研究では, 無線通信形態の一つである Ad-Hoc ネットワークに着目し, 平面上に与えられた点集合を用いて Ad-Hoc ネットワークを構築する際の電波干渉を抑える手法を議論する．各端末の電波送信半径を調整することによって, 連結性を保ちながら, 最も干渉が大きい端末の干渉レベルを抑えることが可能となる．本論分では, 計算幾何における ϵ-net のアイディアを用いることで, 干渉を $O(\sqrt{\Delta})$ に抑える手法を提案する．ここでの Δ は, 全端末を同じ電波送信半径としてネットワークを構築した場合の最大干渉レベルである．この手法は一次元モデルにおける Rickenbach らの結果を二次元に拡張したものである．さらに 4 分木を用いた手法も提案し, 最大干渉レベルの下界を考察する．

学会大会等

1. 徳山豪:
“数学の使い方：コンピュータサイエンスでの利用”, 茨城大学イブニングセミナー（公開市民セミナー）, 2006 年 12 月.

2. 徳山豪:
“計算理論の現状と未来”, 特定領域研究 NHC 全体会議, 2006 年 11 月.

3. 徳山豪:
“計算理論の現場での応用例：講演者の経験から”, 情報処理学会全国大会（特別セッション基調講演）, 2007 年 3 月.

4. K. Murota, A. Shioura:
“Substitutes and Complements in Network Flows Viewed as Discrete Convexity”, ECCO XIX – CO 2006 Joint Meeting, 2006 年 5 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、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。

また、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。第一に、OBDD を用いたシンボリックアルゴリズムに関して、与えられたグラフの全ての可能なトポロジカルソートの列挙を行なうアルゴリズムの提案、実装を行なった。OBDD を用いると多数の解を比較的小さなサイズで保持できるため、全ての解を求め、記憶する処理に向いていると考えられる。本研究では、特に規則的なグラフに対しては、極めて多数の解を小さなサイズの OBDD で表現できることを明らかにし、またその効率的な計算法について考察を進めた。

第二に、画像データの OBDD による表現法と、その上での基本的な画像処理アルゴリズムの設計を行なった。画像データの表現法としては、1 個の OBDD で表現する方法と、画像の濃度の各ビットをそれぞれ OBDD で表現する方法を提案した。この上で、閾値処理、平行移動・回転、エッジ抽出などのフィルタ処理等の画像処理アルゴリズムを提案、実装した。

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、chordal グラフに、高々k_1 本の辺を追加し、高々k_2 本の辺を除去した、chordal+k_1e−k_2e グラフに対する頂点彩色問題のアルゴリズムを設計し、パラメータ k_1、k_2 に関して fixed parameter tractable であることを示した。これは、知る限りでは辺の追加と削除をはじめて同時に

扱った、パラメータ付きグラフに対するアルゴリズムである。

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 OBDD によるトポロジカルソートの列挙

2.1 概論

Ordered Binary Decision 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る。多くの実用的な論理関数を効率的に表現できる、変数順序を決めれば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、実用的な研究が進められてきている。

解の列挙とは、問題の条件を満たす解を全て求めることである。問題の解を 2 進符号化して表現すると、解集合は x が解の符号化となるときそのときに限り、$f(x) = 1$ となる論理関数で表現できる。この論理関数を OBDD を用いて表現することにより、多数の解が存在する場合においても、部分グラフの共有が行なわれるため、比較的小さなサイズで表現可能になると期待できる。指数的な個数の解を多項式サイズで表現できる場合も存在する。特に解の集合は問題の条件を満たすために、共通の性質を持つ部分が存在することから、適切な符号化や変数順序の選択により、効率的な OBDD 表現が可能となる場合が多いと考えられる。また、解集合を OBDD で表現することにより、多数の解の中から、与えられた条件を満たす解を容易に抽出することができる利点がある。

本研究では、与えられた有向非巡回グラフに対し、その全てのトポロジカルソートの結果を列挙するアルゴリズムの提案、実装評価を行なった。入力のグラフは OBDD の形で与えられるものとし、論理演算などのシンボリック操作のみにより、トポロジカルソートの列挙を行なう。複数の列挙アルゴリズムを実装し、それらの比較を行なった。その結果、非常に多くの解を小さなサイズの OBDD で表現でき、特に規則的な構造を持つグラフに対してはその効果が顕著であることが明らかになった。しかし、演算結果は小さく表現できるが、計算途中の OBDD のサイズが非常に大きくなる場合がある。しかし、この問題点は各頂点の開始頂点からの距離を求めるアルゴリズム [2] の適用により大幅に改善可能であることが示された。

2.2 二分決定グラフ (OBDD)

二分決定グラフ (Ordered Binary Dicision Diagram：OBDD) とは、論理関数を表現する有向非循環グラフである。変数でラベル付けされ 0 枝、1 枝の 2 つの出枝を持つ内部節点と、論理値でラベル付けされた終端節点を持つ。各変数の値にしたがって 0 枝、1 枝をたどっていき到達した終端節点のラベルが関数値となる。OBDD のすべてのパスで現れる変数の順序は変数順序と呼ばれる全順序に従う。冗長な節点と等価な節点を持たない OBDD を既約な OBDD と呼ぶ。変数順序を一つ決めたとき論理関数を表す既約な OBDD は一意に定まり、論理関数の標準形となる。

2.3 トポロジカルソートの列挙アルゴリズム

トポロジカルソートの OBDD 表現

有向非巡回グラフ $G = (V, E)$ のトポロジカルソートとは、$(v_1, v_2) \in E \Leftrightarrow \pi^{-1}(v_1) < \pi^{-1}(v_2)$ の条件を満たす頂点順序 $v_{\pi(1)}, \ldots, v_{\pi(n)}$ を求めることである。グラフ G の頂点は、$0, \ldots, |V| - 1$ の数字でラベル付けされているものとする。

グラフを OBDD で表現する際には、頂点のラベルを n ビットで 2 進符号化し、2 頂点間に辺が存在するときのみ 1 を返す関数で表現する。トポロジカルソートは $n \times |V|$ 変数の入力 x をとる論理関数 f で表す。頂点の並び順 $(x_0 \ldots x_{n-1}), (x_n \ldots x_{2n-1}), \ldots, (x_{n(|V|-1)} \cdots x_{n|V|-1})$ がトポロジカルソートになっているとき、f は 1 になる。

$S(i, v)$ はソートの i 番目に頂点 v が現れることを表す関数である。つまり、v の符号を変数 $x =$

$x_{n\times(i-1)}\cdots x_{n\times i-1}$ としたとき、1 になる関数である。

列挙アルゴリズム

本研究では、3 通りの方法でトポロジカルソートの列挙を行った。

追加法では、従来の方法と同様、1 個ずつソート結果を求め、それを OBDD に追加する。OBDD で与えられたグラフより、深さ優先で次に選択できる頂点を選ぶ操作をシンボリック操作により実現した。

削除法では、次の手順で全ての頂点の組合せから条件に当てはまらないものを削除していく。

step1　全ての頂点の組合せを作る。

$$f = \neg(\bigvee_{i=0}^{|V|-1} \bigvee_{|V|\le x<2^n} S(i,x))$$

n ビットで表せる数のうち、$|V|$ 以上は不要なので削除する。

step2　同じ頂点が 2 回以上出現する組合せを削除する。

$$\forall u \in V : f = f \wedge \neg(\bigvee_{0\le i<j<|V|} S(i,u) \wedge S(j,u))$$

頂点 u が 2 度以上でるような全ての組の論理和をとり、その否定と全体の論理積をとることで全体から削除する。

step3　辺の向きに矛盾する組合せを削除する。

$$(u,v) \in E : f = f \wedge \neg(\bigvee_{0\le i<j<|V|} S(i,v) \wedge S(j,u))$$

$(u,v) \in E$ なら、u より前に v が出るような全ての組の論理和をとり、その否定と全体の論理積をとることで全体から削除する。

削除法+最大距離では、それぞれの頂点の、開始頂点（終端頂点）からの最大距離を求めるアルゴリズム [2] を用い、あらかじめ不要な順列を削除することで、計算途中の OBDD のサイズを小さくする。

頂点 v の開始頂点からの最大距離 d は、頂点 v のソート順が d 以上であることを保証する。したがって、次の操作により条件を満たさない順列を除去する。

$$f = f \wedge \neg(\bigvee_{v=0}^{|V|-1} \bigvee_{0\le i<DIST(v)} S(i,v))$$

同様に、終端頂点からの最大距離 d は、頂点 v のソート順が $|V|-1-d$ 以下であることを保証する。

3　実験結果と考察

OBDD ライブラリは CMU の bddlib を利用し、Opteron265*2CPU、8GB メモリの計算機上で実験を行なった。入力のグラフとして、$k\times k$ のグリッドグラフ、これから指定した確率で辺を除去したグラフ、表 2.3は 2 個の頂点を長さ $m+1$ のパス l 本で結んだ l 行 m 列グラフをなどを用いた。

図 2.1に、グリッドグラフにおける、全ての解を保持する OBDD の頂点数を示す。

表 2.1: 解の個数と OBDD サイズ

頂点数	解の個数	OBDD サイズ
4	2	13
9	42	87
16	24024	431
25	–	1925

解の個数の増加に対し、非常に小さいサイズの OBDD で全ての解を保持できることがわかる。

しかし、計算途中において、OBDD サイズが非常に大きくなる場合がある。表 2.2は 4×4 グリッドグラフでの実行結果である。

追加法では、計算途中の OBDD のサイズが結果と比べてそれほど大きくならないが、当然解が非常に多い場合には計算時間が長くなり、5×5 グリッドグラフでは計算不能となる。削除法は、計算途中の最大 OBDD サイズが大きくなり、1 回の演算に時間がかかる。削除法+最大距離では最大サイズが小さくなり、実行時間も最速となる。

表 2.3は 3 行 m 列グラフに対する、削除法+最大距離による実行結果である。解の数が爆発的に

表 2.2: 4×4 グリッドグラフでの実行結果

アルゴリズム	実行時間 (秒)	最大サイズ
追加法	9.37	465
削除法	3.04	209782
削除法+最大距離	0.53	25164

増えているのに対し、結果の OBDD サイズや実行時間はそれほど大きくなっていない。

表 2.3: 3 行 M 列グラフでの実行結果

m	解の数	OBDD サイズ	実行時間 (秒)
2	90	112	0.01
3	1680	398	0.07
4	34650	773	0.55
5	756756	1662	6.66

4 OBDD を用いた画像処理アルゴリズム

4.1 概論

OBDD を用いることにより、様々な離散的なデータを、効率的に表現できる場合がある。本研究では、画像データを OBDD で表現することを考える。画像の性質によってはかなり効率的に画像データを表現できることが期待できる。さらに、OBDD 表現を用いる事により、OBDD 上の操作によって種々の画像の処理をより効率的に実行できる可能性がある。特に画像処理では、画像の全画素に対して同じ処理を施すことが非常に多いため、OBDD 上の演算により全画素に対して同時に操作を実行できる点で OBDD 表現の利用が有効であると考えられる。しかも、これらの処理は OBDD 表現により圧縮されたデータのまま実行することができる。

本研究では、多値画像データの OBDD による表現方法として、1 個の OBDD で表現する方法、複数の OBDD を用いて SBDD(Shared OBDD) で表現する方法の 2 種類を考えた。そして、この 2 種類の表現方法の上での、閾値処理、平行移動・回転、エッジ抽出などのフィルタ処理等の画像処理アルゴリズムを提案、実装した。

4.2 OBDD を用いた画像の表現

画像を OBDD で表現する際には、x 座標、y 座標、画素の濃度 z をそれぞれ $x = x_{n-1}x_{n-2}\cdots x_0$ などと 2 進表現により符号化する。また論理関数 $f(x_{n-1}x_{n-2}\cdots x_0, y_{n-1}y_{n-2}\cdots y_0, z_{n-1}z_{n-2}\cdots z_0)$ を $f(\mathrm{x,y,z})$ のように表す。OBDD により画像を表現する方法として、x 座標、y 座標を表す節点の後に z を表す節点を持つ 1 つの OBDD で表す方法と、複数の OBDD で z の各ビットをそれぞれ個別に表し、その複数の OBDD を SBDD で保持する方法の 2 通りが考えられる。なお以下では、簡単のため画像のサイズは $2^n \times 2^n$ とする。

・1 個の OBDD による表現

この方法では x 座標、y 座標、画素の濃度 z を表す $x_0, \cdots, x_{n-1}$, $y_0, \cdots, y_{n-1}$, $z_0, \cdots, z_{m-1}$ を変数として持ち、1 つの OBDD で画像を表現する。座標 (x, y) の画素の濃度が z のとき、$f(\mathrm{x,y,z}) = 1$ となる OBDD により画像を表現する。

・SBDD による表現

この方法では、OBDD の変数は x, y のみで各 OBDD が z の各ビットを表し、それら全ての OBDD を SBDD として保持する。座標 (x, y) の画素の濃度 z の z_i が 1 のとき、$f_i(\mathrm{x,y}) = 1$ $(i = 0, \cdots, m-1)$ となる OBDD により画像を表現する。

4.3 OBDD を用いた画像処理

本章では OBDD 上での画像処理を行うシンボリックアルゴリズムを提案する。以下では、x 軸にあたる横の軸は処理後は u 軸に、y 軸にあたる縦の軸は処理後は v 軸に変換されるものとする。

閾値処理

閾値処理とは、画像を 2 値化しモノクロ画像にする処理である。まず基準となる値 (閾値：$t =$

$t_{m-1}t_{m-2}\cdots t_0$ とする) を設定し、各画素に対してその値より大きければ黒、小さければ白の 2 色に変換する処理を行う。OBDD 表現を用いた場合のアルゴリズムを以下に示す。

1. $g(\mathrm{z}) = 1$ を初期値とする。
2. $i = 0, \cdots, m-1$ に対し、$t_i = 0$ なら $g(\mathrm{z}) = g(\mathrm{z}) + z_i$、$t_i = 1$ なら $g(\mathrm{z}) = g(\mathrm{z}) \cdot z_i$.
3. $f'(\mathrm{x}, \mathrm{y}, z_0) = \exists z_{m-1}, \cdots, z_1[f(\mathrm{x}, \mathrm{y}, \mathrm{z}) \cdot g(\mathrm{z})]$. f' が求める画像を表現する OBDD である。

平行移動

平行移動は、x 軸方向または y 軸方向に距離 d だけずらす操作である。OBDD 表現に対するアルゴリズムを以下に示す。

1. $g(\mathrm{x}, \mathrm{u}) = 1 \Leftrightarrow u - x = d$ となるような g を作る。
2. $f'(\mathrm{u}, \mathrm{y}, \mathrm{z}) = \exists \mathrm{x}[f(\mathrm{x}, \mathrm{y}, \mathrm{z}) \cdot g(\mathrm{x}, \mathrm{u})]$

g は k-variate 閾値関数のクラスに属している [2]。そのため g は x, u の変数順序を $x_0, u_0, x_1, u_1, \cdots, x_{n-1}, u_{n-1}$ のように入れ子にすることによって定数幅で表すことができ、f のサイズを w とすると $f \cdot g$ の OBDD の幅は $O(w)$、計算量は $O(nw)$ で抑えられる。$\exists$ をとる操作は OBDD のある変数 x について $x = 0$ の場合の OBDD と $x = 1$ の場合の OBDD で OR 演算を行う操作であり、幅は最大で w^2 となる。それを $x_0, \cdots, x_{n-1}$ の n 個に対して行うため、f' の幅は最大で w^{2^n} である。

回転の操作も同様の考え方で実現できる。

OBDD 表現によるエッジ抽出

エッジ抽出とは画像の中の図形の輪郭を抽出する処理である。エッジ抽出は、2 次の微分演算の近似値を算出するラプラシアンフィルタを用いた処理を行うことで実現できる。この処理を行う際は画像を 2 値化しておく必要がある。注目画素とその 4 方向、あるいは 8 方向の画素値が等しい場合に注目画素を 0 にする処理を行う。アルゴリズムを以下に示す。

1. 平行移動処理を用い、4 方向 (8 方向) に移動した OBDD を求める。
2. 元の OBDD $f(\mathrm{x}, \mathrm{y}, \mathrm{z})$ と、1. で作った 4 個または 8 個の OBDD との AND をとる。

SBDD 表現によるフィルタ処理

多値のままフィルタをかける処理は、OBDD 表現での効率的実現は困難であると考えられる。しかし SBDD 表現では、これらを含めた様々なフィルタ処理を行うことが出来る。SBDD 表現によるフィルタ処理のアルゴリズムを以下に示す。

1. 周囲 8 方向への平行移動処理を行う。
2. 1. で作った 8 個の画像の SBDD と元の画像の SBDD に対し、フィルタの対応する要素の絶対値との乗算を行う。
3. フィルタの対応する要素の符号がプラスのもの同士を加算したものを $g(\mathrm{x}, \mathrm{y})$、マイナスのもの同士を加算したものを $h(\mathrm{x}, \mathrm{y})$ とする。
4. $g(\mathrm{x}, \mathrm{y}) - h(\mathrm{x}, \mathrm{y})$ の減算を行う。結果が濃度の最大値を超えた場合は最大値に、マイナスになった場合は 0 にする。

これらの処理は最悪の場合入力 OBDD サイズに対して指数時間かかるものもあるが、画像の画素数に対しては最悪でも多項式時間となる。今後、実際の画像データを用いて、これらのアルゴリズムの実際的な効率を実験的に示す予定である。

5 $\mathcal{F} + k_1\mathrm{e} - k_2\mathrm{e}$ グラフの頂点彩色問題

5.1 概論

頂点彩色問題とは、グラフの隣接する頂点が異なる色になるように頂点に色を割り当てるために必要な最小の色数を求める問題であり、この問題を少しでも効率的に解くことは、計算機科学において重要な課題である。頂点彩色問題は一般に NP 完全であるが、特定のグラフ族に対しては多項式時間で解くことができる場合がある。そのため、

そのグラフ族に“ 近い ”グラフに対しても、多項式時間で解ける可能性がある。

そのようなグラフとして、グラフ族 $\mathcal{F}$ に対して辺や頂点を付加、あるいは削除して得られるグラフである $\mathcal{F}+k$e、$\mathcal{F}-k$e、$\mathcal{F}+k$v、$\mathcal{F}-k$v グラフなどについて研究が行われている。Chordal グラフ、split グラフや非隣接頂点の同一化に関して閉じているグラフ族の $+k$e に対する頂点彩色問題は fixed parameter tractable であることが知られている [3, 4]。また、辺の縮退に関して閉じているグラフ族の $-k$e に対する頂点彩色問題も fixed parameter tractable であることが知られている [3]。

本研究では、$\mathcal{F}$ グラフに辺の付加、削除の両方を行って得られるグラフを扱う。頂点彩色問題を多項式時間で解くことが出来るグラフ族 $\mathcal{F}$ に含まれるグラフに高々k_1 本の辺を追加し、高々k_2 本の辺を削除して出来る $\mathcal{F}+k_1$e $-k_2$e グラフを考える。追加された高々k_1 本の辺の集合と、削除された高々k_2 本の辺の集合をそれぞれプラスモジュレータ、マイナスモジュレータと呼び、合わせてモジュレータと呼ぶ。またプラスモジュレータの端点を正特殊頂点、マイナスモジュレータの端点を負特殊頂点と呼び、合わせて特殊頂点と呼ぶ。

第一に、$\mathcal{F}$ が辺の縮退・非隣接頂点の同一化という 2 つの操作に対して閉じているなら、そのグラフの頂点彩色問題はパラメータ k_1、k_2 に関して fixed parameter tractable、すなわち $f(k_1,k_2)p(n)$ 時間で解けることを示した。第二に、chordal+k_1e $-$ k_2e グラフに対する頂点彩色問題を扱った。辺の縮退に関しては閉じているが非隣接頂点の同一化に関しては閉じていないグラフとして、chordal グラフを取り上げる。本研究では chordal+k_1e$-k_2$e グラフに対する頂点彩色問題のアルゴリズムを設計し、パラメータ k_1、k_2 に関して fixed parameter tractable であることを示した。

5.2 $\mathcal{F}+k_1$e $-k_2$e グラフの頂点彩色問題

$\mathcal{F}+k$e、$\mathcal{F}-k$e グラフの頂点彩色問題に関して Cai[3] は、グラフ族 $\mathcal{F}$ が非隣接頂点の同一化、辺の縮退に関して閉じているという性質を持つ場合 fixed parameter tractable となることを示している。

非隣接頂点の同一化とは、非隣接である 2 頂点を、それらに接続している辺全てと接続する新しい 1 つの頂点に置き換える操作であり、辺の縮退とは、隣接している 2 頂点間の辺を削除し、それら 2 頂点に対して上の同一化を行う操作である。本研究では、縮退・同一化の両方に関して閉じているグラフ族について、以下の結果を得た。

Theorem 1 $\mathcal{F}$ を辺の縮退、非隣接頂点の同一化に関して閉じているグラフ族とし、$\mathcal{F}$ グラフの最適彩色の計算時間を $T(m,n)$ で表現する。このとき、$\mathcal{F}+k_1$e $-k_2$e グラフ G の最適彩色は、G のモジュレータが与えられているなら、$O(2^{k_1+k_2}maxT(m+k_2,n),m+n+k_2)$ で計算できる。

5.3 Chordal+k_1e $-$ k_2e グラフの頂点彩色問題

本研究のアルゴリズムは、グラフの tree decomposition を用いた、Marx の chordal+ke グラフの頂点彩色問題に対するアルゴリズム [4] をもとに、マイナスモジュレータに対する処理を可能にしたものである。

Tree Decomposition

グラフ G に対し、以下を満たす木 T を G の tree decomposition と呼ぶ。「木 $T(U,F)$ と、各 $v\in V$ に対するその部分木 $T_v\subseteq V$ が存在し、$u,v\in V$ がグラフ $G(V,E)$ 内で隣接している必要十分条件は、$T_u\cap T_v\neq\phi$ である。」G が chordal グラフの場合、G の tree decomposition は多項式時間で求められる。

ノード $x\in U$ に対して、V_x により x または x の子孫を含む部分木を構成する頂点の集合を表す。また、V_x によって誘導される G の部分グラフを $G_x=G[V_x]$ で表す。T のノード $x\in U$ に対して、K_x で x に含まれる頂点集合を表す。

Nice tree decomposition とは、さらに以下の条件を満たすものを言う。

・全てのノード $x\in U$ が高々2 つの子を持つ。

・もし $x\in U$ が 2 つの子 y、$z\in U$ を持つならば、$K_x=K_y=K_z$ である (x は join ノード)。

・もし $x \in U$ が 1 つの子 $y \in U$ しか持たないならば、ある $v \in V$ に対して $K_x = K_y \cup \{v\}$(introduce ノード) か、$K_x = K_y \backslash \{v\}$(forget ノード) のどちらかである。
・もし $x \in U$ が子を持たないならば、K_x はちょうど 1 つの頂点を含む (leaf ノード)。

アルゴリズム

[4] のアルゴリズムの概要は以下の通りである。色集合 C による彩色が可能かどうかを判定する。G_x にモジュレータを加えて出来るグラフを H_x と表し、$|C| - |K_x|$ 個の頂点 $u_1, u_2, \ldots, u_{|C|-|K_x|}$ からなるクリークを H_x に加え、K_x の各頂点と繋げて出来るグラフを H_x^* とし、その時出来る $|C|$ クリークは K_x^* で表す。アルゴリズム中では、部分グラフ H_x^* の彩色は「同じ色で彩色する頂点の組」を要素とする集合を S_x で表す。Set system $\mathcal{S}_x$ とは、部分グラフ H_x^* の彩色の方法 S_x の集合となる。Set system の各集合の要素数 n が指数的に増加することを抑えるために、representative system を用いる。木 T の葉ノードから順に、ノードの種類ごとの操作を行なうことにより、H_x^* に対する set system を求める。根ノードに達した時に set system が空でなければ、グラフ G 全体に対する C 彩色が存在する。モジュレータの両端が H_x^* に含まれた時点で、両端が同じ色になる彩色は排除される。

本研究では、マイナスモジュレータに対する処理を行なうため、次の概念を導入した。マイナスモジュレータの端点のうち後で introduce されるものを後入負特殊頂点、先に forget されるものを先忘負特殊頂点と呼ぶ。Chordal+ke グラフの頂点彩色問題アルゴリズムとの大きな違いは、後入負特殊頂点によって K_x 内にマイナスモジュレータが現れ、その両端が同色の彩色パターンを考えることが必要になり、先忘負特殊頂点によって K_x 内のペアが無くなったマイナスモジュレータの組を別の同色の頂点で置き換える操作が必要になることである。

K_x 内で構成されているマイナスモジュレータの両端が同色になっている場合、$|K_x|'$ を K_x で使用している色数とし、頂点 $u_1, u_2, \ldots, u_{|C|-|K_x|'}$ からなるクリークを付け加える。

以下では本研究で提案したアルゴリズムについて、マイナスモジュレータの主な処理の方針のみを示す。

Introduce v. y を x の子とする。v が後入負特殊頂点である時、$\mathcal{S}_y$ の各集合 S に対して以下の 1,2 を行う。
1. K_y に含まれる、v とマイナスモジュレータを成す負特殊頂点のうち同色の組それぞれに対し、v をこれらと同色にする頂点の組を作成する。
2. K_y に含まれる、v とマイナスモジュレータを成す負特殊頂点のうちの、どれとも異なる色で彩色する場合に対応し、$u_{|C|-|K_x|'}$ を v に置き換える。

Forget v. v が先忘負特殊頂点の時、マイナスモジュレータ vv^- に対応する組 (v, v^-) を集合 S 内に含む場合は、同色で彩色する頂点の組から v を除く処理を行なう。

Join node. K_x に含まれる頂点の組がすべて同じ集合同士のみをマージして、ひとつの set system を作る。

K_x 内の頂点で構成されるマイナスモジュレータの集合は高々 2^{k_2} 種類存在する。このそれぞれに対して、k_1 の関数で表される計算時間で、k_1 の関数で表されるサイズに抑えることができるため、$\mathcal{S}_x^*$ のサイズは常に k_1, k_2 の関数で抑えられる。これより以下の定理が得られる。

Theorem 2 *Chordal*$+k_1\mathrm{e}-k_2\mathrm{e}$ グラフの頂点彩色問題は、パラメータ k_1、k_2 に関して *fixed parameter tractable* である。

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

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

[4] D. Marx,“Parameterized coloring problems on chordal graphs”, LNCS 3162 (2004) pp.83-95.

研究業績一覧

学術論文

1. Yasuhiko Takenaga and Kenichi Higashide: “Vertex Coloring of Comparability+ke and -ke Graphs”, 32nd International Workshop on Graph-Theoretic Concepts in Computer Science, Lecture Note in Computer Science 4271, pp.102-112, June 2006.
   概要: $\mathcal{F}+k$e and $\mathcal{F}-k$e graphs are classes of graphs obtained by adding or deleting at most k edges from a graph in $\mathcal{F}$. In this paper, we consider vertex coloring of comparability+ke and comparability$-k$e graphs. As vertex coloring can be solved in polynomial time for comparability graphs, it may also be easy for such graph classes. For comparability+ke graphs, we show that vertex coloring can be solved in polynomial time for $k = 1$, and is NP-complete for $k \geq 2$. For comparability-ke graphs, we show that vertex coloring can be solved in polynomial time for $k = 1$.

2. Yasuhiko Takenaga and Toby Walsh: “TETRAVEX is NP-complete”, Information Processing Letters, Vol.99, No.5, pp.171-174, Sept. 2006.
   概要: Tetravex is a widely played one person game in which you are given n^2 unit tiles, each edge of which is labelled with a number. The objective is to place each tile within a n by n square such that all neighbouring edges are labelled with an identical number. In this paper, we prove that deciding if there exists a tiling for the given unit tiles is NP-complete.

研究会等

1. Yasuhiko Takenaga: “Coloring Comparability-ke Graphs”, 京都大学数理解析研究所講究録, 1489, pp.239-244, May 2006.
   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 $\mathcal{F}$. 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.

2. 三浦勇介，武永康彦: “Chordal+k_1e$-k_2$e グラフの頂点彩色問題”, 電子情報通信学会コンピュテーション研究会, COMP2006-53, pp.21-27, 2007 年 3 月.
   概要: $\mathcal{F}+k_1$e$-k_2$e グラフとは、グラフ族 $\mathcal{F}$ に含まれるグラフに高々k_1 本の辺を追加し、高々k_2 本の辺を削除して得られるグラフ族である。本稿では、$\mathcal{F}+k_1$e$-k_2$e グラフの頂点彩色問題を考える。$\mathcal{F}$ が辺の縮退、非隣接頂点の同一化の両方に関して閉じているならば、そのグラフに対する頂点彩色問題は fixed parameter tractable であることを示す。また、chordal+k_1e$-k_2$e グラフの頂点彩色問題のアルゴリズムを提案し、パラメータ k_1,k_2 に関して fixed parameter tractable であることを示す。

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　概要

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) において、技法の核にあるのは、グラフやハイパーグラフの再帰的分割であり、幅の小さい木分割 [3] や分枝分割 [2] 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、分枝分割を求める多項式時間のアルゴリズムが知られている [4]。我々はこれまでの研究で、この分枝分割アルゴリズムの計算時間を $O(n^4)$ から $O(n^3)$ に改良することに成功している。今年度は、前年度に引き続きこのアルゴリズムを効率的に実装するための研究を行った。詳細については2節で述べる。

(B) においては、巡回セールスマン問題、平面グラフの低縮退描画問題、集合被覆問題に対して具体的な研究を行った。巡回セールスマン問題については、グラフ分割に基づいた動的計画法による平面グラフ巡回セールスマン問題の解法プログラムを公開可能な形に整備した。この解法プログラムを近傍内最適化に用いることを前提に、平面ユークリッド距離巡回セールスマン問題に対する指数サイズ近傍の設計を行い、種々の案について実装と実験をおこなった。年度末に、これらの努力を総括し、研究の新しい方向性を探るために巡回セールスマン問題研究の精力的な研究者である Bill Cook を訪問した。この訪問により得られた今後の研究の方向性については、3節で述べる。集合被覆問題においては、近傍内最適化の方法として集合と要素の関係を表す木分割に基づいた動的計画法とハイパーグラフの分枝分割に基づいた動的計画法を実装し、実験を行った。平面グラフの低縮退描画問題については、素朴な小近傍局所探索アプローチと指数サイズ近傍アプローチの比較実験を行い、後者の方が計算時間はかかるものの、描画の質において大きく優る解を得ることができることを確認した。この問題の定義、解法と実験結果については、4節で述べる。

指数サイズ近傍アプローチを具体的な問題に適用する試みの全体としては、期待された効果をあげることができない場合が多いことが判明しつつあり、打開策を模索中である。

(C) については、巡回セールスマン問題の近傍内最適化のための動的計画法で用いる解の合成関数の部分について準ハードウェア化のための予備的な実験を行った。この詳細については、5節で述べる。

2　分枝分割アルゴリズムの実装

グラフの分枝分割 (branch decomposition) と分枝幅 (branch width) の概念は Robertson と Seymour[2] により、よりよく知られた木分割と木幅の概念と関連して導入された。木幅と分枝幅

は線形の関係にあることが知られている。多くの組み合わせ問題に対して、グラフのサイズに関して線形時間で分枝分割幅に関して指数時間で動作するアルゴリズムが存在する。したがって、与えられたグラフの分枝幅を決定する問題や最適な分枝分割を構成する問題は重要である。

与えられたグラフ G の分枝幅を決定する問題はＮＰ完全問題であるが、G が平面グラフである場合、Seymor と Thomas[4] の「ネズミ捕りアルゴリズム」と呼ばれるアルゴリズムによって $O(n^2)$ 時間で解くことができる。彼らはまた、このネズミ捕りアルゴリズムをサブルーチンとして用い、平面グラフの最適分枝分割を構成する $O(n^4)$ 時間のアルゴリズムを与えた。Gu と Tamaki[5] は、ネズミ捕りアルゴリズムの呼び出し回数を減らすことにより、計算時間を $O(n^3)$ に改良した。

ネズミ捕りアルゴリズムを実装するためには、$O(n^2)$ のメモリが必要であるため、これがこのアルゴリズムを実用に供する際の大きな制約となっている。Hicks は [6] で、メモリを節約するために、基礎情報を格納せずに再計算する手法を提案している。我々は、再計算によらずにメモリを節約するためにアルゴリズムの背後にあるネズミ捕りゲームの性質を用い、できるだけ局所的に計算を完結させる方針で実装上の改良を行った。これらの手法により、素朴な実装ではメモリ不足のために解く事ができない例を扱うことができるようになった。以下でこれらの手法の詳細について述べる。

諸定義

グラフ G の分枝分割 B は、B の葉頂点の集合が $E(G)$ であり、B の任意の内部頂点の次数が 3 であるような木である。B の各辺 b は、$E(G)$ の 2 分割 (E_1, E_2) と自然に対応する。ここで、E_1 と E_2 は B を b によって切断して得られる 2 つの部分木における葉の集合を表す。E_1 と E_2 の共有する頂点の個数を B における辺 b の幅と呼ぶ。B の幅とは、B の辺の幅の最大値のことであり、G の分枝幅とは、G の分枝分割を全て考えたときのそれらの幅の最小値のことである。

ST アルゴリズムでは、平面グラフの分枝分割の問題を次に述べる刻み分割の問題に帰着する事によって解く [4]。分枝分割がグラフの辺の集合の階層的分割を表すのに対し、刻み分割は同様な表現でグラフの頂点の集合の階層的分割を表わす。

グラフ G の刻み分割 C は、C の葉頂点の集合が $V(G)$ であり、C の任意の内部頂点の次数が 3 であるような木である。G の刻み分割 C の各辺 c は、$V(G)$ の 2 分割 $(V1, V2)$ と自然に対応する。ここで、$V1$ と $V2$ は C を c によって切断して得られる 2 つの部分木における葉の集合を表す。$V1$ と $V2$ を結ぶ辺の本数を C における辺 c の幅と呼ぶ。刻み分割 C の幅とは、C の辺の中で一番大きい辺の幅のことであり、グラフ G の刻み幅とは、G の刻み分割を全て考えたときのそれらの幅の最小値のことである。

平面グラフの刻み幅決定アルゴリズム

平面グラフ G の分枝分割問題は実際は G を変換して得られる多重平面グラフの刻み分割に帰着される。以下では記述の簡明さのために単純平面グラフについての刻み幅決定について述べるが、多重平面グラフへの一般化は容易である。また、平面グラフ G に対しては固定した平面描画が与えられていると仮定する。刻み幅決定をするために、ネズミ捕りゲーム $RC(G, k)$ を考える。

ネズミ捕りゲーム $RC(G, k)$

プレイヤーはネズミとネズミ捕りの二人である。ゲームは G の平面描画上で行われる。ネズミは頂点に位置し、辺を通って移動する。ネズミ捕りは面に位置し、辺を横切って移動する。移動の途中でいったん辺上に停止する。ネズミとネズミ捕りはグラフ全体の構造を知っており、また自分と相手のグラフ上での位置を知っている。ネズミ捕りは、ネズミの移動を妨害するためにノイズを発生させる。ネズミ捕りの位置が f （f は G の辺また面）であるとき、G の各辺 e は、「G の平面双対グラフ上で f と e をとおる長さ k 以内の閉じた歩道が存在する」という条件のもとで通行不能となる。ここで、k は G とともに与えられたゲームのパラメータである。ゲームは次の手順で進行する。

1. ネズミ捕りが最初に自分が位置する面を選ぶ。

2. それに応じてネズミは自分の位置する頂点を選ぶ。

3. もしネズミが次数が k 以下の頂点にいて、ネズミ捕りがネズミのいる頂点と接する面にいるならばネズミ捕りの勝ちでゲームを終える。

4. ネズミ捕りは自分がいる面と接する面の中から、移動先の面を選び、現在面と移動先の面の共有する辺上に移動する。

5. ネズミは、通行不能でない辺を0個以上任意個通って移動する。

6. ネズミ捕りは予定していた面に移動し、3に戻る。

ネズミが永久に負けを免れて逃げ続けるとき、ネズミをゲームの勝者とする。

定理 1 (Seymour and Thomas[4]) 平面グラフ G が幅 k 以下で刻み分割可能であることの必要十分条件は $RC(G,k)$ においてネズミ捕りが必勝であることである。

ゲームのグラフ化

ネズミ捕りアルゴリズムに対する我々の実装手法を説明しやすくするために、アルゴリズムをSeymout と Thomas のオリジナルとは多少異なる形で定式化する。$RC(G,k)$ のゲームの状態を頂点、状態遷移を辺とする二部グラフ $H(G,k)$ を次のように定義する。ネズミ捕りが面 r にいるときにノイズが通過する辺を G から取り除くことによってできる G の部分グラフを G_r とする。同様に、ネズミ捕りが辺 e にいるときにノイズが通過する辺を取り除くことによってできる G の部分グラフを G_e とする。G_r、G_e の連結成分の集合をそれぞれ、C_e、C_r と表す。G の辺 e と面 r が接しているとき、$E(G_r) \subseteq E(G_e)$ であり、従って、$V(G)$ の分割 C_r は C_e の細分である。よってネズミ捕りが面 r から辺 e に移動したいときに、ネズミが移動できる頂点集合 $c \in C_e$ は、ネズミがどの $c' \in C_r$ の中にいたかだけに依存し、c' のどの頂点にいたかには依存しない。つまり、ネズミ捕りが面 r にいるとき、ゲームの状態は (r,c') によって表すことができる。

$H(G,k)$ の頂点集合は S,T であり、$R(G)$ を G の面の集合とすると、$S = \{(r,c)|r \in R(G), c \in C_r\}$ はネズミ捕りが面にいるときの状態の集合である。$T = \{(e,c)|e \in R(G), c \in C_e\}$ はネズミ捕りが辺にいるときの状態の集合である。そして、$(r,c) \in S$ と $(e,c') \in T$ の間に $H(G,k)$ の辺があるのは、これらの状態間で遷移が可能であるときである。すなわち、r と e が接していて、かつ、$c \subseteq c'$ であるときである。S の頂点 (r,c) からは、ネズミ捕りが次に向かう面 r' と r の間の辺 e を選択することによって、T の頂点 (e,c') へ遷移する。一方、T の頂点 (e,c) からの遷移はネズミの選択した頂点 v とネズミ捕りが移動する先である面 r' によって、$v \in c''$ である S の頂点 (r',c'') と決まる。

ネズミ捕りゲームの勝敗判定

もし、グラフ G の最大次数が k より大きい場合、ネズミは k よりも大きい次数を持つ頂点にいれば捕まることはないので、ネズミ必勝が自明であう。よってこれ以後はグラフ G の最大次数が k 以下である場合の判定法を述べる。$RC(G,k)$ における、ネズミ捕り必勝の状態を表す集合を以下のように帰納的に定義する。

1. $\hat{T}_0 = \phi$

2. $\hat{S}_0 = \{(r,\{v\})|G$ の面 r と頂点 v は接している $\}$

3. $\hat{T}_{i+1} = \{(e,c)|e$ と接しているある面 r と $c' \subseteq c$ なるすべての $c' \in C_r$ に対して $(r,c') \in \hat{S}_i\} \cup \hat{T}_i$

4. $\hat{S}_{i+1} = \{(r,c)|r$ と接しているある辺 e と $c' \supseteq c$ なるある $c' \in C_e$ に対して $(e,c') \in \hat{T}_{i+1}\} \cup \hat{S}_i$

$\hat{S} = \bigcup_i S_i, \hat{T} = \bigcup_i T_i$ とおく。各 $\hat{S}_i$ に属する状態がネズミ捕り必勝状態であることと $S - \hat{S}$ に属す状態はネズミ必勝であるはともに数学的帰納法によって証明することができる。

勝敗判定アルゴリズムの実装においては、$H(G,k)$ から頂点を削除することにより $\hat{S}$、$\hat{T}$ を表現する。実装を工夫することにより、この計算は $O(n^2)$ 時間で実行することができる [4]。また、

次の観察により、$\hat{S}$ を全て計算しなくても判定できる場合がある。

観察 1 ある面 r に対して、すべての $(r,c), c \in C_r$ が $\hat{S}$ に属するならば、$S = \hat{S}$ である。つまり、ゲームはネズミ捕り必勝である。

実装上の改良

改良を述べるために以下の定義を行う。R を G の平面双対グラフにおいて連結な面の集合とし、E_R を R の面と接する辺の集合とする。S, T の部分集合 S_R, T_R を $S_R = \{(r,c)|r \in R, c \in C_r\}, T_R = \{(e,c)|e \in E_R, c \in C_e\}$ と定義し、H_R を $S_R \cup T_R$ によって誘導される $H(G,k)$ の部分グラフとする。$\hat{S}, \hat{T}$ の構成規則を H_R の中だけで、適用して得られる $\hat{S}, \hat{T}$ の部分集合を $\hat{S}_R, \hat{T}_R$ で表す。$\hat{S}_R$ はネズミ捕りが R, E_R を動いて勝つことのできる状態の集合を表している。

面 $r \in R$ に対して $(r,c) \in S_R - \hat{S}_R$ なる $c \in C_r$ が唯一であるとき、c を R における面 r のサバイバル成分と呼ぶ。サバイバル成分が $\hat{S}$ に属さないことは、ネズミが勝つために必要である。$\hat{S}$ の帰納的定義において、$\hat{S}_0$ を $\hat{S}_0 \cup X \subseteq S$ で、$\hat{T}_0$ を $Y \subseteq T$ で置き換えて得られる集合を、それぞれ $\hat{S}(X,Y), \hat{T}(X,Y)$ で表す。$\hat{S}_R(X,Y), \hat{T}_R(X,Y)$ も同様に定義する。

改良 1．局所的な計算により、ネズミ捕り必勝であることが判る状態を見つける

ネズミ捕りが面 r にいて、ネズミが頂点 v から一歩も動けずにネズミ捕りに近づかれて、捕まってしまうための十分条件の真偽を調べる。次の定理を用いる。

定理 2 次数が k 以下である平面グラフ G において、r を G の面、v を G の頂点とする。以下の 2 条件を同時に満たす、ある二つの面 s, t があるならば、 $(r,v) \in \hat{S}$ である。

1. G の平面双対グラフにおいて r から最短距離で s まで行き、v の周りを時計回りして t まで行き、 r へ最短距離で戻ってくる閉じた歩道 C_1 の長さが k 以下である
2. 同じく G の平面双対グラフにおいて r から最短距離で s まで行き、v の周りを反時計回りして t まで行き、r へ最短距離で戻ってくる閉じた歩道 C_2 の長さが k 以下である

改良 2．$H(G,R)$, および、$\hat{S}, \hat{T}$ の漸増的な構成

G のある面 r_0 から、幅優先探索で面の集合 R を次第に増大させながら、$S_R, T_R, \hat{S}_R, \hat{T}_R$ を計算していく。

前に述べたように, $\hat{S}, \hat{T}$ は S, T から要素を削除することによって表現するので、使用メモリ量の節約が期待できる。実験により、改良 1 と組み合わせたときに効果が著しいことが判った。観察 1 から、$H(G,k)$ 全体を構成せずともアルゴリズムを停止することができる場合があるので、この方法は計算時間の改良にもなる可能性がある。

改良 3. サバイバル成分の特別扱い

以下の定理を用いる。

定理 3 R を G の平面双対グラフにおいて連結な面の集合とし、各 $r \in R$ がサバイバル成分 C_r を持つと仮定する。$\tilde{E}_R$ によって R に属する面と R に属さない面を隔てる辺の集合を表す。R を G の平面双対グラフから除いて作られる各連結成分 Q に対して $Y_Q = \{(e,c)|e \in \tilde{E}_R \cap \tilde{E}_Q, (e,c) \in \tilde{T}_R\}$ と定義する。$\hat{S} = S$ と次の条件は同値である。

> ある辺 $e \in \tilde{E}_R$ と e に接する面 $r \in R$ があって、C_r を包含する C_e の要素を c_e とするとき、$(e, c_e) \in \hat{T}_Q(\phi, Y_Q)$ である。但し Q は G の平面双対グラフから R を取り除いたときにできる連結成分のうち、e を境界に持つようなものの集合である。

上の定理より、サバイバル成分を持つ連結な面の集合 R と E_R については $\tilde{E}_R$ に属す辺 e についてのみの状態集合だけを保持すればよく、メモリ節約効果が期待できる。

表 2.1: 例題ごとの分枝幅決定計算時間

例題名	辺数	分枝幅	計算時間 (sec)	
			素朴	改良
eil51	140	8	0.937	0.265
lin105	292	8	4.44	0.625
ch130	377	10	23.1	0.735
pr144	393	9	4.50	0.500
kroB150	436	10	11.7	0.828
tsp225	622	12	37.1	1.16
pr226	586	7	7.64	1.13
rd400	1183	17	×	3.58
u574	1708	17	×	11.2
p654	1806	10	×	11.3
d657	1958	22	×	7.28
pr1002	2972	21	×	27.9
rl1323	3950	22	×	75.9
d1655	4890	29	×	57.8
rl1889	5631	22	×	188
u2152	6312	31	×	76.2
pr2392	7125	29	×	158
fl3795	11326	25	×	502
fnl4461	13359	48	×	622
rl5934	17770	41	×	1690
pla7397	21865	33	×	2370
usa13509	40503	63	×	9230
brd14051	42128	68	×	6680

実験

素朴な実装と以上の改良を組み込んだ実装を比較する実験結果を表 2.1に示す。実験に使用したグラフは巡回セールスマン問題のベンチマークライブラリ TSPLIB にある点集合を delaunay 三角形分割をしたものであり、Hicks[6] が使用したグラフと同じものである。例題名中の数値は点の個数を示している。Pentium4 3.2GHz の CPU を使用した。使用言語は java である。また、使用ヒープメモリ上限は６００ＭＢバイトとした。

3　巡回セールスマン問題

この研究課題のテーマとして指数サイズ多項式近傍アプローチをとりあげるにいたった経緯において、過去における巡回セールスマン問題でのこのアプローチの成功が大きな位置を占めている。すなわち、最適にかなり近い巡回路をさらに改良しようとする場合に、現在の巡回路に改良に役立ちそうな辺を加えたグラフをつくり、このグラフ上の巡回路の集合を近傍とし、近傍内の最適化をグラフ分割に基づいた動的計画法で行うことが有効であることがわかっている。これは、最終的には最適解を得ようとする努力のなかで大量のＣＰＵ時間を消費することが許される領域での話である。今年度は、より実用に近い領域、すなわち、妥当な計算時間内である程度の質の巡回路を得るために同様のアプローチを適用する研究に多くの努力を費やした。この領域での標準手法は、高速の巡回路構成法に Lin-Kernighan による局所探索法（解の逐次改善法）を組み合わせるものである。この標準手法と同等以上の性能を持つ指数サイズ近傍アプローチヒューリスティックを開発することを目標とし、種々の案を実装し実験を行なった。

これらの研究努力を総括し、研究の新しい方向を探るためにジョージア工科大学の Bill Cook を訪問した。教授らのグループを対象として Euclidean TSP heuristics based on exact solvers on planar graphs と題した講演を行い、意見を交換した。Cook は、Applegate, Bixby, Chvatal らとともに、巡回セールスマン問題の厳密解法について精力的に研究を行い、最近その研究成果をまとめた大著 [1] を出版している。この書のなかに述べられているように、彼らは巡回セールスマン問題の古典的なベンチマークライブラリである TSPLIB の例題を（最大の８５９００都市の例題も含めて）すべて厳密に解くことに成功している。

この訪問で得た最大の収穫は、厳密解法のなかのさまざまなアルゴリズム的課題の存在を学んだことである。Cook を引用すると「我々は、良い巡回路を見つけることはうまくできるようになったが、（cutting-plane 法における）カットをみつけるのはまだまだ稚拙であると確信している。」

特に、カットをある程度蓄積して厳密解に接近してきたＬＰ解のサポートグラフが、平面グラフに近くかつかなり疎であること、したがってカット発見のアルゴリズムにおいても分枝分割等に基づいたアプローチが有望であるとの指摘を受けたことは、今後の研究方向に対して大きな意味を持

つ。すなわち、分枝分割の応用をこれまでのように巡回路の構築・改良のみに限定するのではなく、厳密解法にも広げて研究して行きたい。

4　平面グラフの低縮退描画問題

平面グラフ G が与えられたとき、すべての辺が直線分となるように G を平面描画し、隣接する２辺のなす角の正弦の絶対値の最小値ができるだけ大きくなるようにしたい。この問題は、二次元凸包の分割統治法アルゴリズムのトレース例題を学生の自習用にランダムに生成する必要から生まれた。このトレースの課題においては、学習者は平面上の２０点程度の点集合を図で与えられて、分割統治法アルゴリズムを紙上で実行することを要求される。コピー解答の誘惑から学習者を解放するために、例題は乱数によって学習者ごとに生成される。与えられた点集合に対して、分割統治法アルゴリズムが再帰の各レベルで生成するすべての凸包の辺の和集合からなるグラフ G を考える。このグラフ G のなかで、隣り合う２辺のなす角が小さいかまたは π に近いと、アルゴリズムの実行に必要な３点の位置関係に対する判断を正しくできない可能性がある。そのために、G は上に述べたような基準によって描画されていることが望ましい。

この問題に対する厳密アルゴリズムはおそらく難しいので、次のような指数サイズ近傍を設計した。まず、頂点は整数座標の点のみに配置することにする。現在の描画を D とし、d を $(1,0)$、$(1,1)$、$(0,1)$、$(-1,1)$、$(-1,0)$、$(-1,-1)$、$(0,-1)$、$(1,-1)$ の８つのベクトルのうちのひとつとする。このとき、D の d-近傍 $N_d(D)$ は $N_d(D) = \{D_i \mid 0 \leq i < 2^n\}$ で定義される。ここで、n は G の頂点数であり、D_i は「D において頂点 j を、もし i の第 j ビットが１ならば d によって動かし、０ならば動かさない」という規則により得られる描画である。$N_d(D)$ 内の最適化には、D の平面双対グラフの分枝分割に基づいた動的計画法を用いる。アルゴリズム全体では、d を８通りに変化させながら近傍内最適化を行うフェーズを改良ができなくなるまで繰り返す。また、目的関数は隣接２辺の角の正弦の絶対値の辞書式列として、最小値が変化しない場合も改良が起きる可能性があるようにした。

この指数サイズ近傍を実装し、小近傍の局所探索との比較を行った。小近傍の探索では、各頂点に対して上の８通りのベクトルを足して改良が起きる場合にはその移動を施すということを変化がなくなるまで繰り返した。実験対象は、実際の教育で使用する問題のサイズと同様の２０頂点のランダムな例題１００題を用いた。指数サイズ近傍の結果の質が一貫して小近傍の結果を上回った。特に小近傍の場合には、まれに 0.04 などの非常に小さい値に収束するのに対し、指数サイズ近傍では、もっとも小さい場合でも収束値が 0.2 を下回ることはなかった。小近傍で他の工夫をすることにより同等の効果をあげることができないか、さらなる検討が必要だが、指数サイズ近傍によって素朴な小近傍の欠陥を補うことができることは明らかになった。

5　準ハードウェア化の準備

平面描画グラフ TSP を動的計画法を用いて専用ハードウェアで解く準備について本節で述べる.

専用ハードウェアで, マイクロプロセッサとソフトウェアとの組合せより高速に解を得るためには, 次の 2 つの工夫が必要である.

1. 並列度を上げること,
2. 解を予め計算する. これを圧縮して格納し, 使用時に効率良く検索できること.

並列度を上げるためには, グラフを再帰的に分割し, 個々のグラフで解を求めればよい. 個々に求めた解を併合するときに, それがまた TSP としての解の性質を満たしているかの判定を行う. また, 併合後のグラフの内部接続を高速に求めたい. グラフをその度に辿って解を求めると時間がかかりすぎるので, 予め計算しておきそれを表に蓄える.

図 2.1にグラフ G_1 と G_2 とからなるグラフを示す. G_1 は, 下から反時計回りに $0, 1, 2, \ldots, 7$ とラベル付けされた 8 本の辺によって外部と接続している. 内部では, 0 と 7, 1 と 6, 2 と 3, 4 と 5 とが内部の太い実線で表されたツアーで接続されている.　これを ((()())) で表現する.

一方, G_2 は時計回りに $0, 1, 2, \ldots, 5$ とラベル付けされた 6 本の辺がグラフから出ている. 内部で

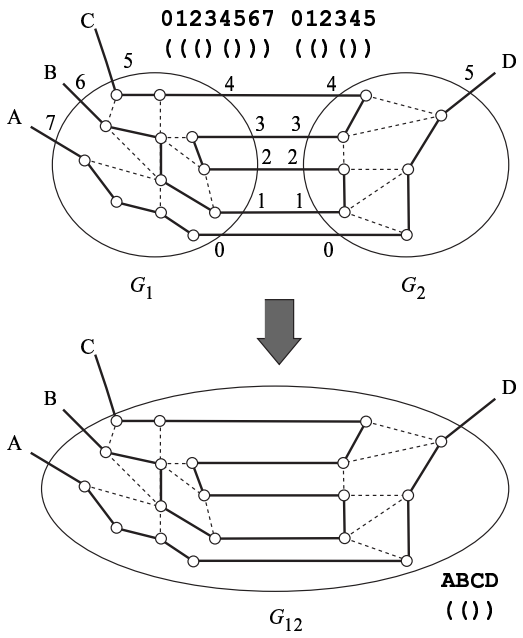


図 2.1: 解の合成

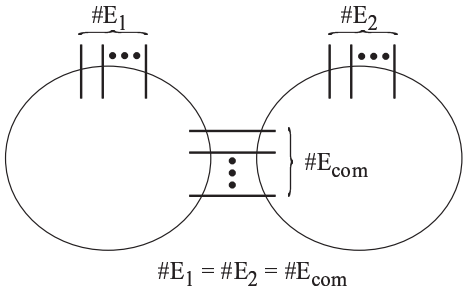


図 2.2: 取り扱うグラフ

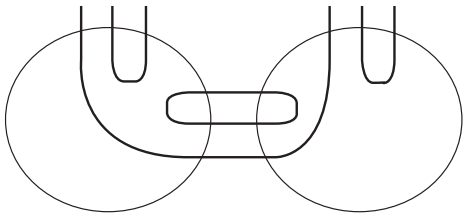


図 2.3: 内部ループが存在するグラフ

は, 0 と 5, 1 と 2, 3 と 4 とが接続されている．これは (()()) と表現する．

この 2 つのグラフを図 2.1にあるように 5 本の共通辺で接続し，一つのグラフ G_{12} に併合する．このグラフから出る辺 A,B,C,D は, 図から明らかなように A と D, B と C とでグラフ内部で接続されている．これは (()) で表せる．

ここで，入力として解の型 ((()())), および, (()()) を与えると, 合成結果の型 (()) を高速に出力する方法を考える．一番単純な方法は，予めすべての解をグラフを辿ることで求めておき表に蓄え, 実際に値が必要なときは表引きによる求めることである．この括弧を用いた記法は, 左括弧を 0, 右括弧を 1 とすれば 2 進数で表せる．本例では, 14 ビット入力, 4 ビット出力の論理関数で表現できる．

ここでは, 問題を簡単にするために図 2.2のように, 2 つのグラフ G_1 と G_2 の共通辺の個数 $\#E_{com}$ とその他のグラフから出る辺の個数 $\#E_1$, および, $\#E_2$ とが全て等しい場合についての結果を示す．

無効な入力（それぞれの部分グラフにおいて括弧の対応が正しくない入力）が多いから, すべての有効な解 (TSP として成立する解) は, 入力の全ての組合せに比べるとわずかである．無効な入力は, 計算時（表引き時）には，与えないので出力は don't care としてよい．

また, 図 2.3のように併合したグラフ内に内部ループが存在する場合は, TSP の解として不適当である．この場合は, TSP の解としては成立しないという出力を出す．

例 1 図 *2.2*において, $\#E_1 = \#E_2 = \#E_{com} = 3$ の場合を考えてみよう．この場合, 入力は *12* ビット, 出力は *6* ビットとなる．単純にメモリで記憶させると $2^{12} \times 6 = 4096 \times 6 = 24576$ ビットの記憶容量を必要とする．一方, *TSP* として意味のある接続は表 *2.2*に示すように *17* 通りのみである．(例終り)

例 1では, 意味のある答えは 17 通りだけであった．これを記憶する場合は, 入力と出力のペアで記憶させればよいので $(12 + 6) \times 17 = 306$ ビットあれば十分である．なお, このように格納した場合は, 表引きにはハッシュ関数や連想メモリ, および, 連想メモリを模擬する専用ハードウェアを用いれば高速に検索が可能となる [8, 9].

このように, 有効な解の個数は, 入力の全ての組合せに比べて少ない．ソフトウェアで TSP の解を求めるとき, この計算を表引きに変えれば高速化の可能性がある．また, ハードウェアで計算する場合も, この方法は利用できる．

表 2.2: 12 入力 6 出力の論理関数で表したグラフの意味のある接続

in	*out*
((()))((()))	((()))
((()))(()())	(()())
((()))(())()	(())()
((()))()(())	()(())
((()))()()()	()()()
(()())((()))	(()())
(()())()(())	(()())
(()())()()()	(())()
())(()((()))	()(())
())()()(())	()(())
())()()()()	()()()
()(())((()))	(())()
()(())(()())	(()())
()(())(())()	(())()
()()()((()))	()()()
()()()(()())	()(())
()()()(())()	()()()

そこで, 実際にメモリに蓄えられる大きさがどのくらいか, 解を圧縮して記憶させたいので実際の解のパターンを全て求めてみた. 計算結果を表 2.3 に示す. 計算に用いた計算機は, Intel Xeon CPU 3.2GHz×2, 3.5GB RAM, Windows XP Professional V.2002 Service Pack 2 の PC (Personal Computer) を用いた. 使用言語は, C 言語であり, コンパイラには gcc を用いた. 表 2.3に入力ビット数の増加に対して, 有効な解の個数とその解全てを求めるのに要した計算時間, 有効解の割合を示す. 例 1の例は, 表 2.3では, $in = 12$ の場合に相当する. この場合, 意味のある解は 17 個であり, 17 個の解を求めるのに $6.8\mu s$ 要している. 有効な組合せは 4096 個中 17 個であるので, これを $17 \div 2^{12} \times 100 = 0.41\%$ と示した.

表より, 意味のある組合せは割合としては, わずかであることがわかる. しかし, 48 入力のときの全ての解の個数は 10G 個を超えているこれをそのままメモリなどに記憶するのは難しい

今後, 2 つのグラフの併合で入力数が異なる場合, また, 効率的な圧縮法の考案, もしくは, 一部を

表 2.3: 意味のある解の種類

in	有効な解の個数	計算時間	有効解の割合 [%]
4	1	93ns	6.2000
8	3	580ns	1.2000
12	17	6.8μs	0.4100
16	117	100μs	0.1800
20	955	2ms	0.0910
24	8,389	36ms	0.0500
28	79,889	630ms	0.0300
32	791,905	11s	0.0180
36	8,228,777	210sec	0.0120
40	87,675,915	1hours	0.0080
44	963,501,291	17hours	0.0055
48	10,771,003,505	12days	0.0038

表引きに変えるなどの検討が必要であることがわかった. これには LUT カスケード [10] を用いた方法などを適用する予定である. LUT カスケードが基本技術となる可能性が高いので, LUT カスケードの基本技術と応用技術の検討を並行して行っている. LUT カスケードチップに関する成果と基数変換の基本技術なども開発できた [11, 12, 13, 14].

参考文献

[1] D.L. Applegate and R.E. Bixby and V. Chvátal and W.J. Cook, The Traveling Salesman Problem - A Computational Study, Princeton University Press, 2006.

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

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

[4] P.D. Seymour and R. Thomas, Call Routing and the Ratcatcher. Combinatorica, 14(3), 217-241,1994.

[5] Q.-P. Gu and H. Tamaki, Optimal Branch-decomposition of planar graphs in $O(n^3)$time. ICALP 2005, 373-384.

[6] I.V. Hicks,Planar Branch Decomposition I:The Ratcatcher,INFORMS Journal on Computing. Vol.17, No.4, Fall2005, pp.402-412.

[7] H. Tamaki, A liner time heuristic for the branch-decomposition of planar graphs. ESA2003, 765-775.

[8] T. Sasao, "A Design method of address generators using hash memories," *International Workshop on Logic and Synthesis(IWLS06),* Vail, Colorado, U.S.A, June 7-9, 2006, pp.102-109.

[9] H. Nakahara, T. Sasao and M. Matsuura, "A CAM emulator using look-up table cascades," *14th Reconfigurable Architectures Workshop RAW 2007*, March 2007, Long Beach California, USA. CD-ROM RAW-9-paper-2.

[10] T. Sasao, M. Matsuura, and Y. Iguchi, "A cascade realization of multiple-output function for reconfigurable hardware," *International Workshop on Logic and Synthesis(IWLS01),* Lake Tahoe, CA, June 12-15, 2001, pp. 225-230.

[11] K. Nakamura, T. Sasao, M. Matsuura, K. Tanaka, K. Yoshizumi, H. Nakahara and Y. Iguchi, "A memory-based programmable logic device using look-up table cascade with synchronous static random access memories," Japanese Journal of Applied Physics, Vol. 45, No. 4B, pp. 3295-3300, April 2006.

[12] Y. Iguchi, T. Sasao, and M. Matsuura, "On designs of radix converters using arithmetic decompositions," IEEE Proc. of ISMVL-2006 (CD-ROM), May 17-20, 2006.

[13] Y. Iguchi, T. Sasao, and M. Matsuura, "On designs of radix converters using arithmetic decompositions, — Binary to Decimal Converters —," IEEE Proc. of ISMVL-2007, (Accepted).

[14] Y. Iguchi, T. Sasao, and M. Matsuura, "Design methods of radix converters using arithmetic decompositions," IEICE Trans. on Information and Systems, Vol. E90-D (Accepted).

研究業績一覧

学術論文

1. K. Nakamura, T. Sasao, M. Matsuura, K. Tanaka, K. Yoshizumi, H. Nakahara and Y. Iguchi:
"A memory-based programmable logic device using look-up table cascade with synchronous static random access memories", Japanese Journal of Applied Physics, Vol. 45, No. 4B, pp. 3295-3300, April, 2006.
概要: A large-scale memory-technology-based programmable logic device (PLD) using a look-up table (LUT) cascade is developed in the 0.35-mm standard complementary metal oxide semiconductor (CMOS) logic process. Eight 64 K-bit synchronous SRAMs are connected to form an LUT cascade with a few additional circuits. The features of the LUT cascade include: 1) a flexible cascade connection structure, 2) multi phase pseudo asynchronous operations with synchronous static random access memory (SRAM) cores, and 3) LUT-bypass redundancy. This chip operates at 33MHz in 8-LUT cascades at 122mW. Benchmark results show that it achieves a comparable performance to field programmable gate array (FPGAs).

2. Y. Iguchi, T. Sasao, and M. Matsuura:
"On designs of radix converters using arithmetic decompositions", IEEE Proc. of

ISMVL-2006, May 17-20, 2006.
概要: In arithmetic circuits for digital signal processing, radixes other than two are often used to make circuits faster. In such cases, radix converters are necessary. However, in general, radix converters tend to be complex. This paper considers design methods for p-nary to binary converters. It introduces a new design technique called arithmetic decomposition. It also compares the amount of hardware and performance of radix converters implemented on FPGAs.

3. Y. Iguchi, T. Sasao, and M. Matsuura:
"On designs of radix converters using arithmetic decompositions
— Binary to Decimal Converters —", IEEE Proc. of ISMVL-2007, (Accepted).
概要: In digital signal processing, radixes other than two are often used for high-speed computation. In the computation for finance, decimal numbers are used instead of binary numbers. In such cases, radix converters are necessary. This paper considers design methods for binary to qnary converters. It introduces a new design technique based on weighted-sum (WS) functions. The method computes a WS function for each digit by an LUT cascade and a binary adder, then adds adjacent digits with q-nary adders. A 16-bit binary to decimal converter is designed to show the method.

4. Y. Iguchi, T. Sasao, and M. Matsuura:
"Design methods of radix converters using arithmetic decompositions", IEICE Trans. on Information and Systems, Vol. E90-D, (Accepted).
概要: In arithmetic circuits for digital signal processing, radixes other than two are often used to make circuits faster. In such cases, radix converters are necessary. However, in general, radix converters tend to be complex. This paper considers design methods for p-nary to binary converters. First, it considers Look-Up Table (LUT) cascade realizations. Then, it introduces a new design technique called arithmetic decomposition by using LUTs and adders. Finally, it compares the amount of hardware and performance of radix converters implemented by FPGAs. 12-digit ternary to binary converters on Cyclone II FPGAs designed by the proposed method are faster than ones by conventional methods.

5. Qian-Ping Gu, Hisao Tamaki:
"Optimal branch-decomposition of planar graphs in $O(n^3)$ time", ACM Transaction on Algorithms, （掲載予定）.
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. 井口幸洋, 笹尾勤, 松浦宗寛:
"算術分解を用いた基数変換回路の構成法", 電子情報通信学会, ディペンダブルコンピューティング研究会, DC2006-23, pp. 61-66, 2006年8月1日.
概要: デジタル信号処理用の算術演算回路などでは, 基数が2以外の論理回路を用いて, 高速かつコンパクトな回路を実現する場合がある．この場合, 基数変換回路が必要であるが, 一般には複雑な回路となる．本論文では, p進数を2進数に変換する基数変換回路の構成法を提案する．本構成法では, 算術分解と呼ぶ新しい方法を用いる．また, FPGA(Field Programmable Gate Array) 上に基数変改回路を実現したときのハードウェア量と性能の比較を行う.

2. 井口幸洋、笹尾勤、松浦宗寛:
"算術分解を用いた基数変換回路の構成法(2)", 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, RECONF2006-47,

pp. 19-24, 2006-11-30.
概要: デジタル信号処理では, 高速演算のために 2 以外の基数がよく用いられる．また, 金融計算では，10 進数が 2 進数の代わりに用いられる．このような場合, 基数変換回路が必要である．本論文では, 2 進数を q 進数に変換する新しい基数変換回路の構成法を提案する．これは, weighted-wum (WS) 関数の概念に基づく新しい方法である．各桁の WS 関数を LUT カスケードと 2 進加算器とで計算し, それらを q 進加算器で足し合わせることで基数変換器を構成する．16 ビットの 2 進 10 進変換器を例にその構成法を説明する．

3. 井口幸洋、笹尾勤、松浦宗寛:
“算術分解を用いた基数変換回路の構成法 (3)”, 電子情報通信学会 VLSI 設計技術研究会, VLD2006-135, 2007 年 03 月 8 日.
概要: デジタル信号処理では, 高速演算のために 2 以外の基数がよく用いられる．また, 金融計算では，10 進数が 2 進数の代わりに用いられる．このような場合, 基数変換回路が必要である．我々は, 2 進数を q 進数に変換する新しい基数変換回路の構成法を提案している．これは, weighted-wum (WS) 関数の概念に基づく新しい方法である．各桁の WS 関数を LUT カスケードと 2 進加算器とで計算し, それらを q 進加算器で足し合わせることで基数変換器を構成する．本稿では, 基数変換の合成ツールを開発したので報告する．これは, FPGA 上の組込みメモリのデータ・パターンと Verilog-HDL での回路記述を生成する．16 ビットの 2 進 10 進変換器を例にその結果を示す．

4. 玉木久夫、吉武由実:
“平面グラフの分枝幅決定アルゴリズムの効率的実装”, 情報処理学会アルゴリズム研究会, SIGAL-109-4, 19-26, 2006 年１１月.
概要: 平面グラフの分枝幅を決定するための、Seymour と Thomas によるネズミ捕りアルゴリズムについて主にメモリを節約するための工夫を施した上で実装し、素朴な実装では実行できない規模の例題に対して実行することを可能とした。

5. 玉木久夫、土屋裕希:
“平面ユークリッドＴＳＰの分割統治法ヒューリスティック”, 情報処理学会アルゴリズム研究会, SIGAL-111-17, 125-132, 2007 年３月.
概要: 平面ユークリッドＴＳＰの初期解構築法として、分割統治法によるアプローチを提案した。この方法は、部分解（巡回路）の統合のステップにおいてふたつの部分巡回路にさらに多数の辺を付加した統合グラフを作成して、その上での最適巡回路を動的計画法によって求めることに特徴がある。

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。

前年度に、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。その結果、近年の VLSI の配線層数の増加がハードウェアアルゴリズムの性能に与える影響を調査する必要があるという考えに至った。

平成 18 年度は、前年度までに提案した新しいハードウェアアルゴリズムを含む、乗算のいくつかのハードウェアアルゴリズムについて、それらに基づく乗算器の回路面積が、VLSI の配線層数によりどのような影響を受けるかを調査した。また、信号処理や暗号処理で出現する演算に対する新しいハードウェアアルゴリズムを設計し、シミュレーションによる評価を行った。具体的には、以下の研究を行った。

1. 前年度までに提案した Karatsuba の方法に基づく新しいハードウェアアルゴリズムを含む 6 種類のアルゴリズムについて、それらに基づく乗算器の回路面積が、VLSI の配線層数によりどのような影響を受けるかを調査した。

2. 冗長 2 進表現の絶対値計算を用いた新しい整数開平のハードウェアアルゴリズムを開発し、シミュレーションによる評価を行った。アルゴリズムに基づく開平回路は組合せ回路モデル上での段数が演算数の長さに比例し、素子数が演算数の長さの平方に比例する。また、VLSI モデル上での面積が演算数の長さの平方に比例する。

3. 公開鍵暗号の一種である楕円曲線暗号等の処理で用いられるガロア体 GF(2^m) 上の乗算と逆元計算の統合ハードウェアアルゴリズムを開発し、シミュレーションによる評価を行った。

以下、これらの研究の詳細を述べる。

2 配線層数の乗算器の回路面積への影響

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、平成 16 年度に、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]。平成 17 年度には、この乗算器の詳細設計を行い、ＬＳＩを試作した。今年度は、この乗算器と、広く用いられている配列型乗算器、Wallace 木を用いた乗算器、および、これらのそれぞれに 2 ビット Booth の方法を適用した、合計 6 種類の乗算器について、配線層数の回路面積への影響を調べた。

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、$XY = 2^{2k_L} X_H Y_H + 2^{k_L}(X_H Y_L + X_L Y_H) + X_L Y_L = 2^{2k_L} P_1 + 2^{k_L}(P_3 - P_1 - P_2) + P_2$ となる。ここに $P_1 = X_H Y_H$、$P_2 = X_L Y_L$、$P_3 = (X_H + X_L)(Y_H + Y_L)$ 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。

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。

$P_4 = -2^{\frac{n}{2}} P_1 + P_2$ を導入し、$XY = (-2^{\frac{n}{2}} + 1)P_4 + 2^{\frac{n}{2}} P_3$ とすることによって素子数を削減した [3]。この構成では、P_4 を求めるために、P_1、P_2 の部分積をまとめて加算している。

2.2 回路面積の評価

前述の Karatsuba アルゴリズムに基づく乗算器（Karatsuba 乗算器）と配列型乗算器（Array 乗算器）、Wallace 木を用いた乗算器（Wallace 乗算器）、および、これらのそれぞれに 2 ビット Booth の方法を適用した乗算器（Karatsuba+Booth 乗算器、Array+Booth 乗算器、Wallace+Booth 乗算器）の計 6 種類の乗算器を、用いる配線層数を変えてレイアウトを行った。

Karatsuba 乗算器の部分積加算では、配列型乗算器の構成を用いた。Karatsuba+Booth 乗算器では、内部で用いる三つの乗算器のそれぞれに 2 ビット Booth の方法を適用し、部分積加算では [2] で提案した遅延を考慮して部分積をビット単位で加算していく手法を用いた。両乗算器とも、内部の加算器には順次桁上げ加算器を用いた。

乗算器は Verilog HDL を用いて記述し、ROHM $0.18\mu m$ プロセスを用いてレイアウトを行った。セルライブラリは東京大学大規模集積システム設計教育研究センター（ＶＤＥＣ）の ROHM $0.18\mu m$ プロセス用ライブラリを用い、レイアウトツールは Cadence 社の SOC Encounter を用いた。このプロセスでは配線層を 5 層利用できる。ただし、1 層目には電源用の配線があるため、1 層目は信号配線にはほとんど利用できない。

レイアウトは配線が可能な範囲で回路面積が最小になるように行った。レイアウトが可能かどうかは SOC Encouter による DRC(Design Rule Check) を行って判定した。DRC では配線の最小間隔や短絡、接続性などの幾何的なバイオレーションのみを考慮し、これらのバイオレーションがなければレイアウト可能と判断した。

配線に 5 層すべてを用いるレイアウトと、3 層のみを用いるレイアウトを行った。3 層のみの配線では、5 層の配線層のうち、4 層目と 5 層目の回路領域全体に配線禁止の領域を設定し、配線が行われないようにした。

乗算器のセル面積および配線層 3 層、5 層の場合それぞれの回路面積を表 2.1に示す。面積増加率はセル面積に対する回路面積の増加率を示す。

表 2.1: レイアウト結果

			3 層			5 層		
		セル面積 (μm^2)	回路面積 (μm^2)	総配線長 (μm)	増加率 (%)	回路面積 (μm^2)	総配線長 (μm)	増加率 (%)
32bit	Array	99813	101333	108958	1.5	101333	116749	1.5
	Wallace	101245	102787	167065	1.5	102787	158746	1.5
	Karatsuba	84336	85623	102435	1.5	85623	100927	1.5
	Array+Booth	77447	81525	150266	5.3	78627	161320	1.5
	Wallace+Booth	78472	104632	207152	33.3	79668	186336	1.5
	Karatsuba+Booth	76011	89425	160781	17.6	77169	139270	1.5
64bit	Array	404413	410573	423456	1.5	410573	446090	1.5
	Wallace	409054	415284	736326	1.5	415284	684370	1.5
	Karatsuba	320140	325019	411950	1.5	325019	390066	1.5
	Array+Booth	290543	363178	711159	25.0	294969	724458	1.5
	Wallace+Booth	294023	490043	1064182	66.7	298505	845112	1.5
	Karatsuba+Booth	253342	506686	1021491	100.0	257201	691701	1.5

どちらの入力サイズの乗算器でも、Array 乗算器と Wallace 乗算器はほぼ同じ面積となっている。Karatsuba 乗算器は Array 乗算器や Wallace 乗算器よりもセル面積が小さくなっている。２ビット Booth の方法を用いた場合には、用いない場合よりもセル面積が小さくなっている。

配列型乗算器、Wallace 乗算器、Karatsuba 乗算器はほとんどがセル面積に対し 1.5%の面積増加率でレイアウトできている。1.5%の面積増加率はセルの配置効率によるものであり、配線量によるものではない。Wallace 乗算器は配列型乗算器や Karatsuba 乗算器よりも配線量が多い。一方、２ビット Booth の方法を用いた乗算器では、用いない乗算器と比較して面積増加率が大きくなっている。そのため、回路面積はセル面積に比べて大きく増加している。Wallace+Booth 乗算器と Karatsuba+Booth 乗算器の回路面積は Wallace 乗算器、Karatsuba 乗算器よりも大きくなっている。

配線層を５層用いた場合には、すべて面積増加率 1.5%でレイアウトができている。そのため、ほとんどの乗算器ではセル面積の大きさが回路面積に強く反映されており、セル面積が最も小さい Karatsuba+Booth 乗算器の回路面積が最も小さくなっている。

３層を用いたレイアウトに比べ、５層を用いたレイアウトでは回路面積の面積増加率が低下している。この結果より、配線層が増加することにより、配線が回路面積に及ぼす影響が小さくなっているといえる。また、どちらのビット数においても、配線層を５層用いた Karatsuba+Booth 乗算器の回路面積が最小となっている。Karatsuba+Booth 乗算器は素子数が少なくなることを重視した乗算器である。そのため、配線層数が多い場合には、素子数を重視した構成をとることにより、回路面積の小さな乗算器を構成することができるといえる。

3 冗長２進表現の絶対値計算を用いた整数開平のハードウェアアルゴリズム

整数開平は、信号処理等で現れ、いくつかの整数開平回路が市販のＩＰライブラリに登録されている [4]。整数開平は、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、整数開平のハードウェアアルゴリズムを提案する。アルゴリズムは基数２の減算シフト型の非回復型開平法に基づいている。

専用回路によって計算を高速化するには、部分残余の表現に桁上げ保存形や符号付きディジット表現 [5] を導入し、漸化式の計算を桁上げの伝搬なしに高速に行う手法がよく用いられる [6]。しかし、そのためには、演算数を正規化する必要が

あり、したがって、大きな面積を要する先頭１検出器やバレルシフタが必要となる。

本研究で提案するハードウェアアルゴリズムでは、部分残余を冗長２進表現（２進ＳＤ表現）で表し、漸化式の計算を桁上げの伝搬なしに高速に行い、かつ、演算数の正規化を必要としない。部分残余を符号と絶対値の組で保持し、絶対値を冗長２進表現で表す。商の各桁は部分残余の符号から決定する。

3.1 非回復型整数開平

ここでは、n ビット符号なし２進整数である演算数 X から、$Z = \lfloor X \rfloor$ を満す、$\frac{n}{2}$ ビット符号なし２進整数の平方根 Z を求めるものとする。

提案アルゴリズムは、以下に示す基数２の非回復型整数開平アルゴリズムに基づく。

[Algorithm ISQRT]

$Z_{\frac{n}{2}} := 0$;
$R_{\frac{n}{2}-1} := X - 2^{n-2}$;
for $j := \frac{n}{2} - 2$ downto 0 do
  if $R_{j+1} < 0$ then
    $z_{j+1} := 0$;
    $R_j := R_{j+1} + 2^{j+1} \cdot (Z_{j+2} + 2^{j+1}) - 2^{2j}$;
  else $z_{j+1} := 1$;
    $R_j := R_{j+1} - 2^{j+1} \cdot (Z_{j+2} + 2^{j+1}) - 2^{2j}$;
  endif;
  $Z_{j+1} := Z_{j+2} + 2^{j+1} z_{j+1}$;
endfor;
if $R_0 < 0$ then $z_0 := 0$ else $z_0 := 1$;
$Z_0 := Z_1 + z_0$;
$Z := Z_0$ □

3.2 整数開平のハードウェアアルゴリズム

提案アルゴリズムは [Algorithm ISQRT] に基づく。数列 $\hat{R}_j = sign(R_{j+1}) \cdot R_j$ を導入し、$\hat{R}_j$ を冗長２進表現で表す。冗長２進表現は桁集合が $\{-1, 0, 1\}$ の２進表現である。ここに、$sign(R_{j+1})$ は、$R_{j+1} \geq 0$ なら $+1$、< 0 なら -1 である。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 $R_j := R_{j+1} + 2^{j+1} \cdot (Z_{j+2} + 2^{j+1}) - 2^{2j}$、他のとき $R_j := R_{j+1} - 2^{j+1} \cdot (Z_{j+2} + 2^{j+1}) - 2^{2j}$ であるから、

$\hat{R}_j = |\hat{R}_{j+1}| - 2^j \cdot (2Z_{j+1} + 2^{j+1} \bar{z}_{j+1} + 2^j)$

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。

以下に提案する整数開平のハードウェアアルゴリズムを示す。

[VLSI Algorithm ISQRT-VA]

$\hat{R}_{\frac{n}{2}-1} := X - 2^{n-2}$;
if $sgn(\hat{R}'_{\frac{n}{2}-1}) = -1$ then $z_{\frac{n}{2}-1} := 0$
  else $z_{\frac{n}{2}-1} := 1$;
$Z_{\frac{n}{2}-1} := 2^{\frac{n}{2}-1} z_{\frac{n}{2}-1}$;
for $j := \frac{n}{2} - 2$ downto 0 do
  $\hat{R}_j := abs(\hat{R}_{j+1}) - 2^j \cdot (2Z_{j+1} + 2^{j+1} \bar{z}_{j+1} + 2^j)$;
  if $sgn(\hat{R}'_j) = -1$ or
    $(sgn(\hat{R}'_j) = 0$ and $z_{j+1} = 0)$
    then $z_j := \bar{z}_{j+1}$ else $z_j := z_{j+1}$;
  $Z_j := Z_{j+1} + 2^j z_j$;
endfor;
$Z := Z_0$ □

アルゴリズムに基づく開平回路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。

3.3 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開平回路を組合せ回路として設計し、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 高速版セルライブラリを用いて合成した。また、基数２の回復型整数開平法に基づく整数開平回路を同様に合成した。表１ (a) と (b) に、それぞれ 32 ビットと 64 ビットの整数開平回路の遅延とセル面積の見積りを示す。

表 2.2: 整数開平回路の見積り ($0.35\mu m$ CMOS)

(a) 32-bit

	遅延 $[ns]$	面積 $[mm^2]$
提案法	28.29	0.487
従来法	46.78	0.261

(b) 64-bit

	遅延 $[ns]$	面積 $[mm^2]$
提案法	60.95	1.990
従来法	180.00	0.992

4 GF(2^m) 上の乗算・逆元計算の統合ハードウェアアルゴリズム

ガロア体 GF(2^m) は、公開鍵暗号の一種である楕円曲線暗号において重要な役割を担っており、その上の乗算と逆元計算の高速化が望まれている。

本研究では乗算と逆元計算のための統合ハードウェアアルゴリズムを提案する。乗算と逆元計算アルゴリズムに出現する計算の類似性に着目して二つのアルゴリズムを統合する。このアルゴリズムに基づく複合回路は、乗算回路と逆元計算回路を別々に実現するよりも小さな面積で構成される。

4.1 GF(2^m) 上の乗算および逆元計算

多項式 G(x) を GF(2) 上の m 次既約多項式とすると、$G(x)$ によって定義される GF(2^m) 上の元 $A(x)$ は、$m-1$ 次以下の GF(2) 上の多項式として表現される。

GF(2^m) 上の乗算 "$\cdot$" は、$A(x)\cdot B(x) = A(x)\times B(x) \bmod G(x)$ と定義される。ここで、演算 "$\times$" は GF(2) 上の多項式乗算を表す。乗算アルゴリズムとして、MSB-first アルゴリズム等が知られている [7]。

GF(2^m) 上の零元を除く任意の元 $B(x)$ の乗法逆元 $B^{-1}(x)$ は、GF(2^m) 上の乗算を用いて $B(x)\cdot B^{-1}(x) = 1$ と定義される。逆元計算アルゴリズムとして、拡張ユークリッド法に基づくアルゴリズム等が知られている [8]。

4.2 統合ハードウェアアルゴリズム

MSB-first の乗算アルゴリズムと拡張ユークリッド法に基づく逆元計算アルゴリズムを統合した。二つのアルゴリズムで出現する計算の類似性に着目し、演算を区別する mode 信号を導入して、相違点には初期値の設定と mode 信号による簡単な制御で対処している。以下にアルゴリズムを示す。

[Algorithm GF-MULINV]

Input:

$mode \in \{0, 1\}$

$A(x), B(x)$: $m-1$ 次以下多項式

$G(x)$: m 次既約多項式

Output:

$B^{-1}(x)$ (if $mode = 0$)

$A(x) \cdot B(x)$ (if $mode = 1$)

Algorithm:

if $mode = 0$ then
  $R(x) := x \times B(x)$;
  $U(x) := x^3$; $V(x) := 0$;
  $\delta := -1$; $n := 2m - 1$;
else
  $R(x) := x \times B(x) + 1$;
  $U(x) := 0$; $V(x) := A(x)$;
  $\delta := m - 1$; $n := m + 1$;
endif
$S(x) := G(x)$;
for $i = 1$ to n
  if $r_m = 0$ then
    $R(x) := R(x) \times x$;
    $U(x) := U(x) \times x$;
  else
    if $\delta \geq 0$ then
      $R(x) := (R(x) + \overline{mode} \cdot S(x)) \times x$;
      $U(x) := (U(x) + V(x)) \times x$;
    else
      $\left\{ \begin{array}{l} R(x) := (R(x) + S(x)) \times x, \\ S(x) := mode \cdot S(x) + \overline{mode} \cdot R(x) \end{array} \right\}$;
    $\{U(x) := (U(x)+V(x)) \times x, V(x) := U(x)\}$;
      $\delta := -\delta$;
    endif
  endif
  if $u_{m+1} = 1$ then
    $U(x) := U(x) + x^{m+1}$
      $+ \sum_{k=1}^{m-1} mode \cdot s_t x^{k+1} + \overline{mode}$;

表 2.3: 統合ハードウェアアルゴリズムの各ステップでの計算

r_m	$\delta \geq 0$	$R(x), S(x)$	$U(x), V(x)$	δ
0	*don't care*	$R(x) := x \times R(x);$	$U(x) := x \times U(x) \bmod F(x);$	$\delta := \delta - 1;$
1	*false*	$R(x) := x \times (R(x) + \overline{mode} \cdot S(x));$ $S(x) := mode \cdot S(x) + \overline{mode} \cdot R(x);$	$U(x) := x \times (U(x) + V(x)) \bmod F(x);$ $V(x) := U(x);$	$\delta := -\delta - 1;$
1	*true*	$R(x) := x \times (R(x) + \overline{mode} \cdot S(x));$	$U(x) := x \times (U(x) + V(x)) \bmod F(x);$	$\delta := \delta - 1;$

$$F(x) = \begin{cases} x^{m+1} + 1 & mode = 0 \\ S(x) \times x = G(x) \times x & mode = 1 \end{cases}$$

表 2.4: GF(2^m) 上の演算回路の見積り ($0.18\mu m$ CMOS)

	遅延 $[ns]$	面積 $[mm^2]$
乗算回路	1.1397	0.3489
逆元計算回路	1.2554	0.3754
複合回路 (提案回路)	1.3409	0.4343

endif
$\delta := \delta - 1;$
endfor
output $V(x)/x$ as the result; □

各ステップにおける計算は表2.3のようになる。

4.3 ハードウェアアルゴリズムの評価

統合アルゴリズムに基づく複合回路を、$m = 163, 233, 283, 409, 571$ について、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 $0.18\mu m$ CMOS 用セルライブラリを用いて合成した。また、単体の乗算回路と逆元計算回路を同様に合成した。表 2.4に $m = 571$ の場合の遅延とセル面積の見積りを示す。提案回路の面積は、乗算回路及び逆元計算回路を別々にもつ場合と比較して４割程度小さい。計算時間は同等である。

5 まとめ

集積回路の最新技術の諸側面を反映した新しい回路モデルの構築を目指し、前年度までに提案した新しいハードウェアアルゴリズムを含む、乗算のいくつかのハードウェアアルゴリズムについて、それらに基づく乗算器の回路面積が、VLSI の配線層数によりどのような影響を受けるかを調査した。さらに、信号処理等で出現する整数開平および楕円曲線暗号処理で出現するガロア体 GF(2^m) 上の乗算と逆数計算に対する新しいハードウェアアルゴリズムを設計し、シミュレーションによる評価を行った。これらを通し、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。

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] 川島裕崇，高木直史，高木一義：「Karatsuba 乗算器の設計と評価」，2006 年電子情報通信学会ソサエティ大会，A-3-8，2006 年９月.

[4] Synopsys Inc.: 'DesignWare Building Block IP,' 2003.

[5] A. Avizienis: 'Signed-digit number representations for fast parallel arithmetic,' IRE Trans. Elec. Comput., vol. EC-10, no. 3, pp. 389-400, Sept. 1961.

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

[7] S. K. Jain, L. Song and K. K. Parhi: 'Efficient Semisystolic Architectures for Finite-Field Arithmetic,' IEEE Trans. VLSI Systems, vol. 6, no. 1, pp. 101–113, March 1998.

[8] Z. Yan and D. V. Sarwate: 'New Systolic Architectures for Inversion and Division in GF(2^m),' IEEE Trans. Computers, vol. 52, no. 11, pp. 1514–1519, Nov. 2003.

研究業績一覧

学術論文

1. F. Kumazawa, N. Takagi:
   “Hardware algorithm for computing reciprocal of Euclidean norm of a 3-D vector”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E89-A, No. 6, pp. 1799–1806, June, 2006.
   概要: A hardware algorithm for computing the reciprocal of the Euclidean norm of a 3-dimensional (3-D) vector which appears frequently in 3-D computer graphics is proposed. It is based on a digit-recurrence algorithm for computing the Euclidean norm and an on-line division (on-line reciprocal computation) algorithm. These algorithms are modified, so that the reciprocal of the Euclidean norm is computed by performing on-line division where the divisor is the partial result of Euclidean norm computation. Division, square-rooting, and reciprocal square-root computation, which are important operations in 3-D graphics, can also be performed using a circuit based on the proposed algorithm

2. N. Takagi, S. Kadowaki, K. Takagi:
   “A hardware algorithm for integer division using the SD2 representation”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E89-A, No. 10, pp. 2874–2881, October, 2006.
   概要: A hardware algorithm for integer division is proposed. It is based on the radix-2 non-restoring division algorithm. Fast computation is achieved by the use of the radix-2 signed-digit (SD2) 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, and sequential implementation yields compact dividers.

3. N. Takagi, K. Takagi:
   “A VLSI algorithm for integer square-rooting”, Proc. of 2006 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS2006), pp. 626–629, December, 2006.
   概要: A VLSI algorithm for integer square-rooting is proposed. It is based on the radix-2 non-restoring square-rooting algorithm. Fast computation is achieved by the use of the radix-2 signed-digit representation. Nonetheless, the algorithm does not require normalization of the operand. Combinational (unfolded) implementation of the algorithm yields a regularly structured array square-rooter. Its delay is proportional to n, the bit length of the operand, while that of conventional ones is at least proportional to $n \log n$.

研究会等

1. 川島裕崇，高木直史，高木一義:
   “配線層数の乗算器の回路面積への影響について”，電子情報通信学会技術研究報告, VLD2006-141, pp. 7–12, 2007 年 3 月.
   概要: 近年の VLSI 製造技術の進歩により、配線に用いることができるメタル層数が増加している。使用できる配線層数が増えると、セルの上を通過することができる配線の量も増加する。そのため、配線のための面積は小さくなり、より小さい回路面積で回路が構成できる。乗算は基本的な算術演算のひとつであり、多数の特定用途向けの集積回路 (ASIC, Application Specific Integrated Circuit) で乗算器が搭載されている。ASIC において乗算器は大きな面積を占めるため、乗算器の面積は ASIC の面積や製造コストに大きな影響を与える。本稿では複数の構成法を用いて乗

算器を構成し、配線層数が回路面積に及ぼす影響を確認した。

2. 小林克希，高木直史:
“拡張ユークリッド法に基づく GF(2^m) 上の乗算・逆元計算のための複合回路”, 電子情報通信学会技術研究報告, VLD2006-142, pp. 13–18, 2007 年 3 月.
概要: GF(2^m) 上の乗算及び逆元計算のための複合回路を提案する。提案回路は、これまでに提案されている複合回路と異なり、構成が GF(2^m) を定義する既約多項式に依存せず、また、入出力される多項式の係数の順序を反転する必要がない。提案回路において、逆元計算は拡張ユークリッド法に、乗算は MSB-first アルゴリズムに基づいており、それぞれのアルゴリズムの類似性に着目して回路の大部分を共用できるように複合した。複合には乗算と逆元計算で剰余多項式の次数が同一である必要があるため、乗算の場合の剰余多項式を変形して次数を揃え、他の変数もその変形に合わせた。提案回路を論理合成して回路の規模を見積もったところ、面積はそれぞれの回路を別々に持つよりも 4 割程度小さかった。

学会大会等

1. 小林克希，高木直史，高木一義:
“GF(2^m) 上の乗除算のためのハードウェアアルゴリズム”, 2006 年電子情報通信学会基礎・境界ソサイエティ大会, 51(A-3-7), 2006 年 9 月.

2. 川島裕崇，高木直史，高木一義:
“Karatsuba 乗算器の設計と評価”, 2006 年電子情報通信学会基礎・境界ソサイエティ大会, 52(A-3-8), 2006 年 9 月.

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 †, 田村 明久 ‡

† 京都大学 大学院 工学研究科
〒 606-8540 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

‡ 慶應義塾大学 理工学部 数理科学科
〒 223-8522 横浜市港北区日 3-14-1
aki-tamura@math.keio.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、平成 17 年度までの研究成果を踏まえて、これまでに残されている課題、新たに生じた課題も含めて、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った。本年度の研究成果を以下に示す。

1. 静定構造物の位相的な特徴はラーマングラフによって特徴付けられる。構造最適化への応用を考慮すると、辺が交差しないことが重要である。そこで、与えられた点集合に対して辺が交差しないラーマングラフをすべて列挙する問題を考察した。本問題で考えるグラフのクラスは pseudo-triangulation を含み、より難しい問題である。この問題に対して、逆探索法を基礎にした効率のよい列挙アルゴリズムを開発した。また、あらかじめ指定された辺集合を必ず含むような無交差ラーマングラフをすべて列挙する問題も考察し、効率のよいアルゴリズムを提案した。

2. 逆探索法によって列挙された静定構造物 (ラーマングラフ) に対して，節点座標と部材断面積を連続変数として，指定された性能（大変形挙動）を満たすコンプライアントメカニズムを求める手法を開発した。この方法によって、これまでにないさまざまな形状のコンプライアントメカニズムを生成することに成功した。

3. 総和が一定の長さの直線分（曲線分）集合で表現される道路を配置することにより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、最適化アルゴリズムを構築した。

4. 災害発生時における建物内部から安全な外部への最適避難経路や、津波や大地震発生時の安全な建物・地域への最適避難経路を求める問題を考察した。実用的な観点から、格子状ネットワーク、木構造ネットワークに限定し、通路幅も一定という制約や、避難経路が途中で枝分かれすることを許さない、または交差しないという制約下での最適経路群を求める問題を考察した。

5. 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、計算量限界、近似性能比を明らかにした。

6. 棒材とケーブルで構成されるテンセグリティに対し，釣合い行列の特異値分解と固有値解析によって，形態（節点位置）と，張力の長さに対する比を制御する方法を提案し，その計算量限界を明らかにした。

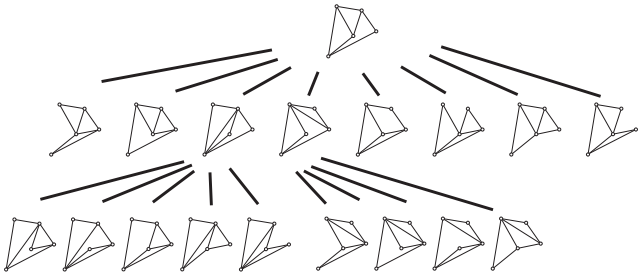


図 2.1: 頂点数 5 の頂点集合上の無交差ラーマングラフ列挙の様子.

2 無交差ラーマンフレームワークの列挙

頂点数 n の頂点集合 $V = \{1, \ldots, n\}$ と辺数 m の辺集合 E から成るグラフ $G = (V, E)$ について，$m = 2n - 3$ でかつ任意の n' 個の頂点部分集合においてその誘導部分グラフの辺数が $2n' - 3$ 以下である時，G は**ラーマングラフ**である．平面上の点集合 $P = \{p_1, \ldots, p_n\} \subset \mathbf{R}^2$ が与えられた際，頂点 $i \in V$ を点 $p_i \in P$ へ，辺 $ij \in E$ を伸び縮みのできない線分 p_ip_j へと埋め込んで得られる幾何グラフを棒とジョイントからなる**フレームワーク**と呼び，$G(P)$ と表される．組合せ剛性理論とは，平面や空間内に棒とジョイントを用いて構成されたフレームワークの剛性，安定性を組合せ的に特徴付ける理論である．フレームワークの安定性に関する研究は多数の工学分野の研究者によって行われてきたが，近年，ロボットアームやリンク機構の設計，立体抽出等，その応用の多様さからますます注目を集めることとなった．特に G がラーマングラフである時，G を一般の点配置上に埋め込む事で得られるフレームワークを**ラーマンフレームワーク**と呼び，ラーマンフレームワークは P 上の最小数の棒から成る安定したフレームワークである事が知られている．また一般の点集合上のラーマンフレームワークの集合は，辺集合を台集合をする**剛性マトロイド**基を構成するなど，優れた組合せ的特徴を有している．

$G(P)$ のすべての直線分対 p_ip_j, p_kp_l に対して，p_ip_j と p_kp_l がその端点以外で共有点を持たないとき $G(P)$ は無交差であるという．本稿では P 上のすべての無交差ラーマンフレームワークの列挙を行うアルゴリズムを考える．

幾何グラフの列挙問題は，多数のグラフクラスに対して効率的なアルゴリズムの構築がなされている．列挙を行うオブジェクト (幾何グラフ) の集合を $\mathcal{O}$ とした時，あるオブジェクト $o_1 \in \mathcal{O}$ から辺を一本取り除き新たに一本加えることによって新たなオブジェクト $o_2 \in \mathcal{O}$ を得る局所探索操作を**フリップ**と呼ぶ．2 つのオブジェクトが一回のフリップによって相互に変換可能である時，それらは**隣接**しているものと捉え，各オブジェクトを頂点とし，隣接しているオブジェクトの頂点間を辺で結ぶことでグラフ $\mathcal{G}_\mathcal{O}$ が得られる．列挙アルゴリズムの基本的な考えはこの $\mathcal{G}_\mathcal{O}$ 上を効率よく辿ることにあるが，列挙アルゴリズムのみならず近傍探索に基づく最適化アルゴリズムやヒューリスティックの多くは $\mathcal{G}_\mathcal{O}$ 上の探索を行う事により実現されている．そのため $\mathcal{G}_\mathcal{O}$ の性質を解明することは，各種アルゴリズムの有効性や性能を評価する際の重要な理論を与える．

ラーマンフレームワークの集合に対して，頂点集合上の (無交差とは限らない) ラーマンフレームワークの集合 $\mathcal{L}$ は，剛性マトロイドの基であることから，フリップ (基底変換) を用いて $\mathcal{G}_\mathcal{L}$ は連結であり，その列挙も容易である．しかしその部分集合である無交差ラーマンフレームワークの集合 $\mathcal{NL}$ は必ずしもフリップを用いて連結であるとは限らず，$\mathcal{G}_\mathcal{NL}$ が連結である事は自明ではない．我々は，全ての無交差ラーマンフレームワークは $O(n^2)$ 回のフリップで互いに変換可能である事を新たに示した．またさらに異なる証明の方針で，指定された辺集合 F を必ず含む無交差ラーマンフレームワーク，F 制約付き無交差ラーマンフレームワークの集合に関しても $O(n^2)$ 回のフリップを用いて互いに変換可能である．

Avis and Fukuda による逆探索手法に基づき，新たに定義したフリップを用いて列挙アルゴリズムの設計を行った．

剛性マトロイドの剛体成分を保持するデータ構

造等を用い，局所探索を行う辺のペアを適切に特徴づけることにより与えられた頂点集合上の F 制約付き無交差ラーマンフレームワークの集合を $O(n^2)$ のメモリを用いてオブジェクト 1 つあたり $O(n^3)$ の計算時間で求めることができる事を新たに示した．図 2.1に 5 頂点の平面頂点集合上の列挙の様子を例示する．

3 コンプライアントメカニズムの形状設計

不安定なリンク機構（剛な棒材と回転の自由な節点で構成される機構）とは異なり，構造物の節点あるいは部材の柔性を利用した安定なメカニズムを，コンプライアントメカニズムという。

棒材で構成されるコンプライアントメカニズムを対象として，本研究グループでは，昨年までに以下のような形状最適化手法を提案した。

Step 1: 存在可能な節点と部材の配置（トポロジー）と，入出力節点，支点及び要求される変形性能を定める。

Step 2: 部材断面積と節点位置の初期値を，乱数を発生させてランダムに定める。

Step 3: 所要の条件を満たし，全部材体積を最小化するようなメカニズムを，部材断面積と節点位置を変数とした非線形計画問題を解き，不要な部材を除去することによって求める。

Step 4: 他の形状のメカニズムが必要であれば Step 2 へ戻る。

本手法によって，さまざまな形状のメカニズムを生成することができる。しかし，上記の Step 3 で解かれる最適化問題は極めて非線形性が強いので，実際的に意味のあるメカニズムを得るためには最適化問題を多数回解かなければならない。

ところで，最適化によって得られるコンプライアントメカニズムは，静定構造であり，ラーマングラフの性質を満たすことが知られている。そこで，本年度は，ラーマングラフ列挙手法にによって得られた種々のトポロジーを初期解として，節点位置のみを変数として最適化を行う方法を提案した。本手法によると，最適化問題が極めて単純

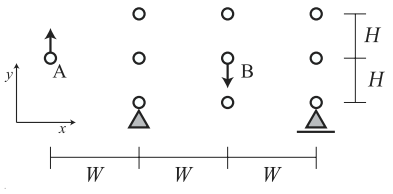
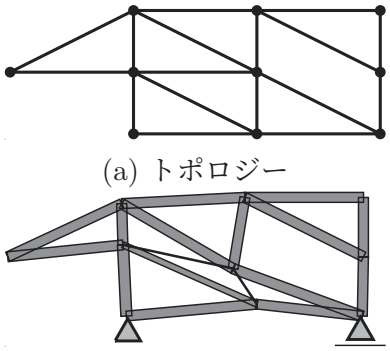
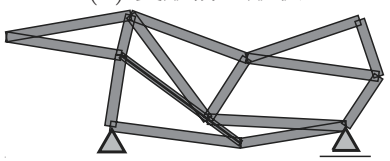


図 2.2: 節点，支点と荷重の配置

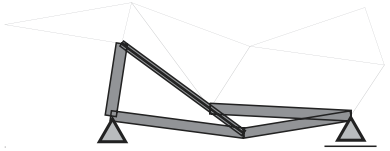


(a) トポロジー

(b) 変形前の形状



(c) 変形後の形状



(d) 変形後の形状（弾性変形部材のみ）

図 2.3: 節点，支点と荷重の配置

な形式となり，収束性が向上するので，さまざまなトポロジーを持つコンプライアントメカニズムを容易に求めることができる。

例として，図 2.2のような節点・支点配置を持つ構造において，節点 B を下方に移動させたときに，節点 A が上方に所定の量変位するメカニズムを求めた。詳細は省略するが，ラーマングラフの列挙によって，図 2.2から 7793 個のトポロジーが得られ，それらを初期値として，1148 個の異なるトポロジーを持つメカニズムを得ることが出来た。得られたトポロジーの 1 例を図 2.3(a) に示す。図 2.3(b) は変形後の形状であり，弾性変形している部材のみを図 2.3(c) に示す。

4 避難計画問題に対する効率的なアルゴリズムの研究

本論文は、大地震や火事、そして津波といった大規模災害に対する危機管理システム構築のための理論的基礎研究である。最も効率的な避難計画を求める問題は、**動的ネットワークフロー**を用いた**避難計画問題**として定式化される。避難計画問題においては、n 個の要素を持つ点集合 V と m 個の要素を持つ辺集合 A を持つ有向グラフ $D = (V, A)$、容量関数 $c\colon A \to \mathbb{R}_+$、移動時間関数 $\tau\colon A \to \mathbb{Z}_+$、サプライ関数 $b\colon V \to \mathbb{R}_+$、そしてシンク $s \in V$ で構成される動的ネットワーク $\mathcal{N} = (D = (V, A), c, \tau, b, s)$ が与えられる。ただし、$\mathbb{R}_+$ と $\mathbb{Z}_+$ は、それぞれ非負の実数と非負の整数の集合である。辺 $e \in A$ に対して、容量 $c(e)$ は単位時間当たり e を通過することのできる人数を、移動時間 $\tau(e)$ は e を通過するのに必要な時間を表している。点 $v \in V$ に対して、サプライ $b(v)$ は v に存在する人の数を表している。この時、避難計画問題は全てのサプライをシンクまで流すことが可能な最小時間を求める問題である。

避難計画問題に対する唯一の多項式時間アルゴリズムが Hoppe と Tardos によって提案されているが、計算時間が高次元の多項式となっているゆえ、実用的なネットワークのサブクラスに対する効率的なアルゴリズムの開発が必要となる。我々は、それぞれの点 v に対して v から s への任意のパスの長さが一定であり（**単一パス長**)、それぞれの点 v に対して最小 v-s カットが s に接続している辺のうち、その始点が v から到達可能なものによって構成されている (**完全連結**) 動的ネットワーク（図 2.4）に対する高速なアルゴリズムを開発した。このネットワークのクラスはグリッドネットワークの一般化となっており、都市や建物の構造をモデル化する際に頻繁に現れる構造である。また、単一パス長は最短路のみを使用して避難することを想定した問題ともみなすことができる。

具体的には避難計画問題を**限定パラメトリックフロー問題**に帰着することによって高速なアルゴリズムを実現した。我々がこれまでに開発したグリッドネットワークに対するアルゴリズムは避難計画問題を資源配分問題に帰着していたのだが、この限定パラメトリックフロー問題への帰着により、さらに高速化を実現することが可能となった。帰着の具体的な内容は省略するが、得られた結果を以下の定理にまとめる。

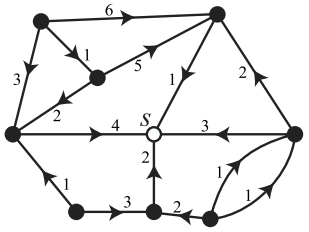


図 2.4: 単一パス長完全連結ネットワークの例。(辺に付された数字は移動時間を表わしている。全ての辺の容量は 1 とする)

Theorem 1 単一パス長と完全連結性を満たす動的ネットワークに対する避難計画問題は以下の計算時間で解くことができる。ただし k は全ての点からシンクまでのパス長の異なった種類である。

単位容量の場合	$O(m^2 \log m)$
整数容量場合	$O(mn + kn^3 \log n)$
s の入次数が定数の場合	$O(m + n^2 \log n)$

この結果は、既存の結果を我々のケースにそのまま適用した場合の計算時間 $O(k^3 m^2 n \log(kn^2/m))$ にくらべ非常に高速になっている。

研究業績一覧

学術論文

1. Shin-ichi Tanigawa and Naoki Katoh: “Finding a Triangular Mesh with a Constant Number of Different Edge Lengths”, IEICE TRANSACTIONS on Information and Systems, E89-D(8), 2364–2371, 2006.
概要: We consider the problem of triangulating an x-monotone polygon with a small number of different edge lengths using Steiner points. Given a parameter α, where $0 < \alpha < 1$, we shall present an algorithm for finding an almost uniform triangular mesh with $3\pi/8\alpha^2 + o(1/\alpha^2)$ different edge lengths such that every edge length is between $\underline{l}$ and

$(2+\sqrt{2}\alpha)\underline{l}$. Experiments demonstrate the effectiveness of this algorithm.

2. David Avis, Naoki Katoh, Makoto Ohsaki, Ileana Streinu and Shin-ichi Tanigawa:
"Enumerating Non-crossing Minimally Rigid Frameworks", Graph and Combinatorics, to appear, 2007.
概要: In this paper we present an algorithm for enumerating without repetitions all the non-crossing generically minimally rigid bar-and-joint frameworks (simply called non-crossing Laman frameworks) on a given generic set of n points. Our algorithm is based on the reverse search paradigm of Avis and Fukuda. It generates each output graph in $O(n^4)$ time and $O(n)$ space, or, with a slightly different implementation, in $O(n^3)$ time and $O(n^2)$ space. In particular, we obtain that the set of all non-crossing Laman frameworks on a given point set is connected by flips which remove an edge and then restore the Laman property with the addition of a non-crossing edge.

3. Naoyuki Kamiyama, Katoh Naoki, Astushi Takizawa:
"An Efficient algorithm for Evacuation Problem in Dynamic Network Flows with Uniform Arc Capacity", IEICE Transaction on Fundamentals, E89-D(8), 2372-2379, 2006.
概要: In this paper, we consider the evacuation problem in a network which consists of a directed graph with capacities and transit times on its arcs. We present an $O(n \log n)$ time algorithm for the evacuation problem in a network of grid structure with uniform arc capacity which has a single sink where n is the number of vertices in the network.

4. Sachio Teramoto, Tetsuo Asano, Benjamin Doerr, Naoki Katoh:
"Inserting Points Uniformly at Every Instance, The Institute of Electronics", IEICE Transaction on Fundamentals, E89-D(8), 2348-2356, 2006.
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 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.

5. Boris Aronov, Tetsuo Asano, Naoki Katoh, Kurt Mehlhorn:
"Polyline Fitting of Planar Points under Min-Sum Criteria ", International Journal of Computational Geometry & Applications, to appear, 2006.
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. J. Y. Zhang and M. Ohsaki:
"Adaptive force density method for form-finding problem of tensegrity structures", Int. J. Solids and Struct., 43, 5658–5673, 2006.
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.

7. S. Fujishige and A. Tamura:
"A general two-sided matching market with discrete concave utility functions", Discrete Applied Mathematics, 154, 950–970, 2006.3.
概要: In the theory of two-sided matching markets there are two standard models: (i) the marriage model due to Gale and Shapley and (ii) the assignment model due to Shapley and Shubik. Recently, Eriksson and Karlander introduced a hybrid model, which was further generalized by Sotomayor. In this paper, we propose a common generalization of these models by utilizing the framework of discrete convex analysis introduced by Murota, and verify the existence of a pairwise-stable outcome in our general model.

8. S. Fujishige and A. Tamura:
"A two-sided discrete-concave market with possibly bounded side payments: An approach by discrete convex analysis", Mathematics of Operations Research, 32, 2007.3.
概要: The marriage model due to Gale and Shapley and the assignment model due to Shapley and Shubik are standard in the theory of two-sided matching markets. We give a common generalization of these models by utilizing discrete concave functions and considering possibly bounded side payments. We show the existence of a pairwise stable outcome in our model. Our present model is a further natural extension of the model examined in our previous paper (Fujishige and Tamura (2006)), and the proof of the existence of a pairwise stable outcome is even simpler than the previous one.

研究会等

1. 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. 2nd International Conference on Algorithmic Aspects in Information and Management (AAIM 2006), Hong Kong, LNCS 4041, 161–172, 2006.
概要: For a given x-monotone polygonal curve each of whose edge lengths is between $\underline{l}$ and $2\underline{l}$, we consider the problem of approximating it by another x-monotone polygonal curve using points of a square grid so that there exists a small number of different edge lengths and every edge length is between $\underline{l}$ and $\beta\underline{l}$, where β is a given parameter satisfying $1 \leq \beta \leq 2$. Our first algorithm computes an approximate polygonal curve using fixed square grid points in $O((n/\alpha^4)\log(n/\alpha))$ time. Based on this, our second 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, where α is a parameter that controls the closeness of approximation. Based on the approximate

polygonal curve, we shall give an algorithm for finding a uniform triangular mesh for an x-monotone polygon with a constant number of different edge lengths.

2. David Avis, Naoki Katoh, Makoto Ohsaki, Ileana Streinu and Shin-ichi Tanigawa:
"Enumerating Non-crossing Minimally Rigid Frameworks", Proc. 9th Japan-Korea Joint Workshop on Algorithms and Computation, Sapporo, 73–78, 2006.
概要: 概要

3. David Avis, Naoki Katoh, Makoto Ohsaki, Ileana Streinu and Shin-ichi Tanigawa:
"Enumerating Non-crossing Minimally Rigid Frameworks", Proc. 12th International Computing and Combinatorics Conference (COCOON 2006), Taipei, LNCS 4112, 205–215, 2006.
概要: In this paper we present an algorithm for enumerating without repetitions all the non-crossing generically minimally rigid bar-and-joint frameworks (simply called non-crossing Laman frameworks) on a given generic set of n points. Our algorithm is based on the reverse search paradigm of Avis and Fukuda. It generates each output graph in $O(n^4)$ time and $O(n)$ space, or, with a slightly different implementation, in $O(n^3)$ time and $O(n^2)$ space. In particular, we obtain that the set of all non-crossing Laman frameworks xson a given point set is connected by flips which remove an edge and then restore the Laman property with the addition of a non-crossing edge.

4. Naoki Katoh, Makoto Ohsaki, Takuya Kinoshita, Shin-ichi Tanigawa, David Avis and Ileana Streinu:
"Enumeration of Optimal Pin-Jointed Bistable Compliant Mechanisms", Proc. 4th China-Japan-Korea Joint Symposium on Optimization of Structural and Mechanical Systems (CJK-OSM4), Kunming, China, 2006.
概要: In this paper we present an algorithm for enumerating without repetitions all the non-crossing generically minimally rigid bar-and-joint frameworks (simply called non-crossing Laman frameworks) on a given generic set of n points. Our algorithm is based on the reverse search paradigm of Avis and Fukuda. It generates each output graph in $O(n^4)$ time and $O(n)$ space, or, with a slightly different implementation, in $O(n^3)$ time and $O(n^2)$ space. In particular, we obtain that the set of all non-crossing Laman frameworks on a given point set is connected by flips which remove an edge and then restore the Laman property with the addition of a non-crossing edge.

5. Naoyuki Kamiyama, Katoh Naoki, Astushi Takizawa:
"An Efficient algorithm for Evacuation Problem in Dynamic Network Flows with Uniform Arc Capacity", The Second International Conference on Algorithmic Aspect in Information and Management (AAIM2006), Hong Kong, China, LNCS4041, 231-242, 2006.
概要: In this paper, we consider the evacuation problem in a network which consists of a directed graph with capacities and transit times on its arcs. We present an $O(n \log n)$ time algorithm for the evacuation problem in a network of grid structure with uniform arc capacity which has a single sink where n is the number of vertices in the network.

6. Naoyuki Kamiyama , Katoh Naoki , Atsushi Takizawa:
"An Efficient algorithm for Evacuation Problem in a Certain Class of Layered Networks", The 9th Japan-Korea Joint Workshop on Algorithms and Computation (WAAC2006), 2006.
概要: In our previous paper, we proposed an $O(n \log n)$ time algorithm for the evacuation problem in a grid network with uni-

form arc capacity. In this paper, we extend the classes of networks to which we can apply the algorithm of our previous paper.

7. Naoyuki Kamiyama , Katoh Naoki , Atsushi Takizawa:
"An Efficient algorithm for the Evacuation Problem in a Certain Class of a Network with Uniform Path-Lengths", The Third International Conference on Algorithmic Aspect in Information and Management (AAIM2007), to appear, 2007.
概要: In this paper, we consider the evacuation problem for a network which consists of a directed graph with capacities and transit times on its arcs. We consider a dynamic network with a single sink s such that (1) for each vertex v the sum of transit times of arcs on any path from v to s takes the same value, and (2) for each vertex v the minimum v-s cut is determined by the arcs incident to s whose tails are reachable from v. This class of networks is a generalization of the grid network studied in the previous paper.

8. Naoyuki Kamiyama , Katoh Naoki , Atsushi Takizawa:
"Generalization of the theorem Edmonds", Kyoto International Conference on Computational Geometry and Graph Theory (KyotoCGGT2007), to appear, 2007.
概要: In this paper, given a directed graph $D = (V, A)$ and a set of specified vertices $S = \{s_1, s_2, \ldots, s_d\} \subseteq V$ with $|S| = d$ and a function $f : S \to \mathbb{N}$ where $\mathbb{N}$ denotes the set of natural numbers, we consider the necessary and sufficient condition such that there exist arc-disjoint in-trees T_i^j rooted at s_i spanning the vertices which are reachable to s_i for $i = 1, \ldots, d$ and $j = 1, \ldots, f(s_i)$. In fact, this is the generalization of the result of Edmonds, i.e., the necessary and sufficient condition such that given a directed graph $D = (V, A)$ with a specified vertex $s \in V$, in D there are k arc-disjoint in-trees rooted at s which span V.

9. Naoyuki Kamiyama , Katoh Naoki , Atsushi Takizawa:
"Theoretical and Practical Issues of Evacuation Planning in Urban Areas", The 8th Hellenic European Research on Computer Mathematics & Conference its Applications (HERCMA 2007), to appear, 2007.
概要: In the evacuation problem by using dynamic network flow, we need to consider several other features from the viewpoint of actual evacuation planning. (a) All the supplies at the same vertex flow through a single path from each vertex to a sink. Moreover, these evacuation paths for different vertices should not cross each other. (b)Theoretically, it is know that storage at intermediate vertices is unnecessary for an optimal flow of the evacuation problem. However, people at sources can not wait if the outgoing arc is not full. (c) We take into consideration the difference of the transition speed of people. In the model taking the difference of the speed of people, there exist multi-commodities in the network, and arcs have to be given several transit times for each commodity. In our paper, we present the well-define theoretical models in order to solve the above problems, and the results concerning these models.

10. Tetsuo Asano, Hisao Tamaki, Naoki Katoh, Takeshi Tokuyama:
"Angular Voronoi Diagram with Applications", The 3rd International Conference on Voronoi Diagrams in Science and Engineering (ISVD 2006), Banff, Canada, IEEE Computer Society, 18-24, 2006.
概要: we define a new Voronoi diagram for a set of line segments in the plane, which is called an aspect-ratio Voronoi diagram. We show several interesting properties of this diagram. it looks quite different from an

ordinary Voronoi diagram defined for a set of points. Voronoi edges consist of plane curves of degree-4 polynomial in x and y. A Voronoi cell associated with a line segment is not always connected. It may be divided into a number of connected regions. This fact causes high complexity of the diagram.

11. J. Y. Zhang and M. Ohsaki:
"Multiobjective optimization for force design of tensegrity structures", Proc. Fourth China-Japan-Korea Joint Symposium on Optimization of Structural and Mechanical Systems (CJK-OSM4), 485–490, 2006.11.
概要: In this paper, we present a multiobjective optimization approach for force design of tensegrity structures, where their geometries are assumed to be determined a priori; we search for the optimal distribution of member forces that leads to the maximum stiffness, and that is closest to the target values assigned by the designers as well. The Pareto optimal solutions of the problem are presented for a tensegrity grid as an example to demonstrate the methodology

学会大会等

1. 谷川眞一, 加藤直樹:
"グリッドを用いた多角形近似", 電子情報通信学会コンピュテーション研究会, comp2006-3, 25–32, 2006.

2. 谷川眞一, 加藤直樹, 大崎純:
"平面無交差静定構造列挙アルゴリズム", 日本建築学会大会学術講演集梗概集, A-2, 457–458, 2006.

3. David Avis, 加藤直樹, 大崎純, Ileana Streinu, 谷川眞一:
"辺制約付き非交差静定グラフ列挙アルゴリズム", 情報処理学会アルゴリズム研究会, 2006-AL-108, 33–40, 2006.

4. David Avis, 加藤直樹, 大崎純, Ileana Streinu, 谷川眞一:
"メカニズム最適化のための平面無交差静定構造列挙アルゴリズム", 第 7 回最適化シンポジウム講演論文集, 209–214, 2006.

5. 加藤直樹, 谷川眞一:
"辺制約付き無交差全域木列挙アルゴリズム", 情報処理学会アルゴリズム研究会, 2006-AL-111, 発表予定, 2007.

6. David Avis, 加藤直樹, 大崎純, Ileana Streinu, 谷川眞一:
"無交差ラーマンフレームワーク列挙アルゴリズム", 電子情報通信学会 2007 年総合大会, 発表予定, 2007.

7. Naoyuki Kamiyama, Katoh Naoki, Astushi Takizawa:
"An Efficient algorithm for Evacuation Problem in Dynamic Network Flows with Uniform Arc Capacity", 情報処理学会 COMP 研究会, 京都大学吉田キャンパス, 41-48, 2006.

8. 神山直之, 加藤直樹, 瀧澤重志:
"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", RIMS 研究集会「モデリングと最適化の理論」, 232-240, 2006.

9. 神山直之, 加藤直樹, 瀧澤重志:
"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", 日本建築大会, 465-466, 2006.

10. Naoyuki Kamiyama, Katoh Naoki, Astushi Takizawa:
"An Efficient algorithm for Evacuation Problem in a Certain Class of Layered Networks", 日本オペレーションズ・リサーチ学会秋季研究発表会, 230-231, 2006.

11. 神山直之, 加藤直樹, 瀧澤重志:
"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”, 日本建築学会大会, A-2, 2006.

12. 神山直之, 加藤直樹, 瀧澤重志:
“避難計画問題”, 京都大学 アルゴリズム・計算量・数理計画・OR・etc. 合同研究会 (KIDS), 発表予定, 2007.

13. Naoyuki Kamiyama, Katoh Naoki, Astushi Takizawa:
“An Efficient algorithm for the Evacuation Problem in a Certain Class of a Network with Uniform Path-Lengths”, 電子情報通信学会 2007 年総合大会, 発表予定, 2007.

14. Naoyuki Kamiyama, Katoh Naoki, Astushi Takizawa:
“An Efficient algorithm for the Evacuation Problem in a Certain Class of a Network with Uniform Path-Lengths”, 研究集会「最適化：モデリングとアルゴリズム」, 発表予定, 2007.

15. M. Ohsaki:
“M. Ohsaki, Design of tensegrity and flexible structures”, Proc. Conf. Computational Eng. Sci., Japan Soc. Comp. Eng. Sci., 11, 855-858, 2006.

16. 木下拓也，大崎 純:
“コンプライアントメカニズムを利用した可動建築構造物”, 日本建築学会大会学術講演梗概集, B-1, 725–726, 2006.

17. 大崎 純，西脇眞二:
“幾何学的非線形性を考慮したトラスの形状・トポロジー最適化によるリンク機構の生成”, 第 7 回最適化シンポジウム講演論文集，日本機械学会, 173–178, 2006.

18. 木下拓也，大崎 純，加藤直樹，谷川眞一，D. Avis:
“静定トラス列挙アルゴリズムを利用した柔構造物の最適設計”, 第 7 回最適化シンポジウム講演論文集，日本機械学会，203–208, 2006.

19. 田村明久:
“離散凸解析を利用したマッチング市場モデル”, 日本応用数理学会年会講演予稿集, 178–179, 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

量子計算および量子通信は，現在の計算・通信方式より本質的に勝る点があると広く信じられている一方で，その能力や具体的な利用方法に関してはまだ明らかになっていない点が多い．そのため，完全にその物理的な実現ができていない今日からでも，計算科学の立場から多くの研究をしておく必要がある．そこで，本研究では，量子計算が実際に利用されるような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る場合や，量子計算の一部分がエラーを含む場合に関する計算能力の解析，量子情報処理の通信プロトコルへの利用方法，量子回路の設計方法などに関して研究を行ってきた．今年度は更に研究を展開し，物理的なエラーと量子計算の関係，古典通信ではできない量子通信による暗号やマジックプロトコル，量子回路設計などに関して多角的に研究を進めた．それらの主要な研究成果の概要は以下の通りである．

量子文字列封印における情報流出の上下界

量子封印とは，乱数と量子ビットを用いてメッセージを符号化することにより，第三者がそのメッセージを復号すると量子状態が壊れ，メッセージが読まれたことが確認できるというものである．1 ビットの値を封印する量子ビット封印に関しては，安全なプロトコルが存在しないことがすでに知られている．しかし，量子ビット封印が安全でないからと言って量子文字列封印も安全でないとは限らない．そこで，量子文字列封印の可能性について様々な議論がなされている．しかし，今まで盗聴者が盗聴できる情報量と検出率の関係については知られていなかった．本研究では，盗聴される情報量の上界が自明な下界に一致するプロトコルを提案し，盗聴者が盗聴できる情報量と検出率のトレードオフの関係を明らかにした．

量子回路を二分決定グラフ構造から合成する手法

ブール関数を計算する量子回路の組織的な設計手法を提案した．提案手法は，既存の手法が入力数に関して指数的な精度のゲートを必要とするのに比べ，3 種類のゲートしか用いないという点でより実用的であると言える．また，提案手法の導入のために，量子回路の動作を記述する行列関数という概念を新たに導入し，行列関数を二分決定グラフで表現する *Decision Diagram for a Matrix Function (DDMF)* というデータ構造も提案した．これらの概念も理論的に興味深いと考えられる．

多準位系の量子ゲートによる量子回路設計のためのユニタリ行列近似

近年，量子計算において多準位系を用いることが提案されている．本研究では，多準位系の量子ゲートによる量子回路設計のために，与えられた任意の n 次元のユニタリ行列を決められたいくつかの n 次元のユニタリ行列（基本ゲートに相当）の積で近似する手法を提案した．提案手法は，与えられた行列を n 次元だが「2 準位にしか作用しない行列」に分解し，その行列を基本ゲートの積に分解するという手法をとる．これにより，既存の手法（Solovay-Kitaev (SK) theorem およびそれに基づいた Dawson らによる手法）に比べて，合成される回路の規模はほぼ同じままで，アルゴリズムの前段階で要する処理時間を大幅に短縮することができるようになった．

Pure Dephasing を考慮した量子オラクル計算モデル

本研究では，量子オラクルと呼ばれる量子のブラックボックスがデコヒーレンスのエラーを受けた状況を計算科学の視点から考察を行った．まず，計算量とデコヒーレンスのエラーの度合いとの関係を解析するためにオラクルの出力に pure dephasing のエラーが起こってもそのようなオラクルを複数用いて pure dephasing のエラーを軽減する手法を提案した．これは，古典計算においてエラーのあるオラクルに対処するための最も基本的な手法である多数決による成功確率の増幅に対応する．我々の知る限りでは，我々の問題設定はオラクル計算の枠組みでデコヒーレンスの影響を考察する最初のものである．

ランダムアクセス符号のタイトな存在性の条件

1999 年に Ambainis, Nayak, Ta-shma, Vazirani によって導入された (n, m, p)-量子ランダムアクセス符号とは，次のような通信システムである．n ビットの情報を持つ送信者はその情報を m キュビットに符号化してそれを受信者に送る．受信者は正作用素値測度によって定義される量子的復号プロセスにより p 以上の確率で正しく元の n ビットの任意の 1 ビットを復号することができる．Ambainis らは (2, 1, 0.85)-量子ランダムアクセス符号の存在を示し，同時に古典的にはそのような符号は不可能であることを示した．Chaung は Ambainis らの符号を (3, 1, 0:79)-量子ランダムアクセス符号に拡張したが，それ以来 $p > 1 = 2$ をみたす $(4, 1, p)$-量子ランダムアクセス符号の存在は未解決であった．本研究では，そのような量子ランダムアクセス符号が存在しないことを示した．また，一般に量子および古典のランダムアクセス符号に関して，タイトな存在条件として以下のことを示した．(1) $(2^{2n}-1, n, > 1/2)$-量子ランダムアクセス符号は存在する．(2) $(2^{2n}, n, > 1/2)$-量子ランダムアクセス符号は存在しない．(3) $(2^n-1, n, > 1/2)$-古典ランダムアクセス符号は存在する．(4) $(2^n, n, > 1/2)$-古典ランダムアクセス符号は存在しない．

以上の研究成果のうち 2 つの項目について，以下でより詳細に述べる．

2 量子文字列封印における情報流出の上下界

2.1 量子文字列封印のモデル

本研究で取り扱う量子文字列封印のモデルを以下のように定める．

Alice は量子レジスタを二つ用意し，入力文字列を符号化して量子レジスタに書き込む．

$$\text{入力文字列 } i\text{:} \quad |0\rangle|0\rangle \longrightarrow \Sigma_j \alpha_j \left|\phi_j^i\right\rangle \left|\psi_j^i\right\rangle .$$

その後，Alice は二つ目のレジスタを公開する．つまり，

$$\rho_i = \Sigma_j |\alpha_j|^2 \left|\psi_j^i\right\rangle \left\langle\psi_j^i\right|$$

が公開された量子状態である．Bob は ρ_i に対して POVM を行い，文字列を復号する．Alice は ρ_i と手元にある一つ目のレジスタの両方に対して POVM を行い，開封確認をする．

上記のような量子文字列封印のモデルに対して，He も指摘している通り [4]，復元可能なビット数に関して，以下に示す自明な下界が存在する．

Lemma 1 復号化率 $1-\varepsilon$ の任意の n ビット量子文字列封印プロトコルに対して，開封確認の検出率が δ 以下で，$\delta \cdot (1-\varepsilon) \cdot n$ ビット復元する手法が存在する．

(証明)
確率 δ で正規の手順に従って復号し，確率 $1-\delta$ で何もしないという復号方法を用いればよい．

2.2 盗聴される情報量の上界

本節では，新しい量子文字列封印プロトコルを示し，復元できるビット数の上界が，補題 1 に一致することを示す．以下にそのプロトコルを示す．

入力 i $(0 \le i \le 2^n-1)$ をランダムに選んだ $X \in \{X_1, \ldots, X_{2^n}\}$ を用いて $\frac{1}{\sqrt{2}}(|i\rangle + |X\rangle)$ と符号化する．ここで，$\{|0\rangle \ldots, |2^n-1\rangle, |X_1\rangle, \ldots, |X_{2^n}\rangle\}$ は互いに直交するものとする． これを全て Bob に対して公開する．

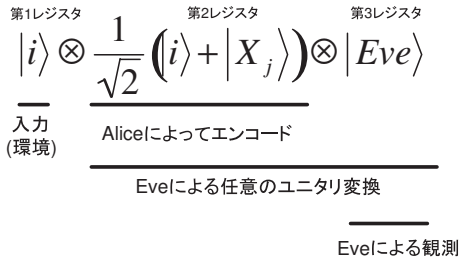


図 2.1: 攻撃のモデル

Bob は $\{|0\rangle, \ldots, |2^n - 1\rangle, |X_1\rangle \ldots, |X_{2^n}\rangle\}$ という基底を用いて観測を行う．よって復号化率は 1/2 である．

このプロトコルに対して，次の定理が成り立つ．

Theorem 1 上記のプロトコルに対して開封確認の検出率が δ 以下であるようなどのような攻撃についても，高々 $O(\delta n)$ ビットしか盗聴されない．

□

定理 1 の証明のために次のような盗聴のモデルを考える．(図 2.1 参照)

入力 $|i\rangle$ は $|0\rangle, \ldots, |2^n - 1\rangle$ の一様な重ね合わせとし，これが第 1 レジスタに入っている．Alice は第 2 レジスタ，第 3 レジスタを使って入力を符号化し，第 3 レジスタを公開する．第 4 レジスタは盗聴者 Eve が使うアンシラとする．Eve は第 3 レジスタ及び第 4 レジスタに対してユニタリ変換 U_E をかけた後，第 4 レジスタを観測する．Alice は第 2, 第 3 レジスタを観測することにより Eve の存在を検出する．

上述のプロトコルでは，Alice は第 2 レジスタを使用しないため，以降第 2 レジスタは $|0\rangle$ と表記する．また，Alice は事前にランダムに $X \in \{X_1, \ldots, X_{2^n}\}$ を選択しておき，符号化の際に全ての i に対して同じ X を使用するものとする．このモデルでは第 1 レジスタが入力の量子的な重ね合わせになっているため実際の状況とは異なる．しかし，第 1 レジスタをトレースアウトすると，実際の状況と等価になり，また，Alice も Bob も第 1 レジスタにアクセスしないため，上記のモデルで安全性を議論して問題ないことに注意されたい．(図 2.2 参照)

上記のモデルでは Eve が観測できるレジスタを第 4 レジスタに制限しているが，この制限をおいても一般性を失わないことを示したのが以下の補題である．

Lemma 2 *Eve* は第 *4* レジスタのみを観測するとして一般性を失わない．

(証明)

Eve は十分多くのアンシラを持っているため，攻撃時に PVM のみを用いるとして一般性を失わない．ここで，Eve は攻撃時に第 3 レジスタを含めて観測を行うとする．この観測に使う射影作用素を $\{P_i\}$ とする．また，観測の直前の第 1 - 第 4 レジスタを $|\Phi\rangle = \Sigma_i \alpha_i |\phi_i\rangle$ と表記することにする．ただし $I \otimes I \otimes P_i |\phi_i\rangle = |\phi_i\rangle$ とする．このとき，アンシラを用意し，$I \otimes I \otimes U |\Phi\rangle |0\rangle = \Sigma_i \alpha_i |\phi_i\rangle |i\rangle$ となるようなユニタリ変換 U (U は第 3，第 4 レジスタにのみ作用するとする．) を施し，アンシラを観測することにより，元の観測をシミュレートできる．シミュレート後の状態からアンシラをトレースアウトしたものは，元の観測によって得られる密度行列に等しい．

上記のモデルにおいて，第 1 レジスタを観測した結果を表す確率変数を X，Eve が観測した結果を表す確率変数を Y とすると，相互情報量 $I(X:Y)$ が Eve が盗聴できる情報量を表している．$I(X:Y)$ の上界を与える補題として，Lo と Chau によって示された以下の補題 [5] がある．

Lemma 3 部分系 A，B からなる任意の純粋状態 $|\phi_{AB}\rangle$ が与えられたとする．A，B に対する任意の観測をそれぞれ X，Y とすると，各部分系のエントロピー $S(\rho_A)$ $(\rho_A = Tr_B |\phi_{AB}\rangle \langle\phi_{AB}|)$ は X と Y の相互情報量の上界を与える．

□

このことから直ちに，以下の系が得られる．

Corollary 1 観測直前の第 *1 - 3* レジスタのみに着目した量子状態を ρ_A，第 *4* レジスタのみに着目した量子状態を ρ_B とする．このとき *Eve* が得られる情報量は $S(\rho_A)$ 以下である．

□

さらに，定理 1 の証明のために，以下の補題を導入する．

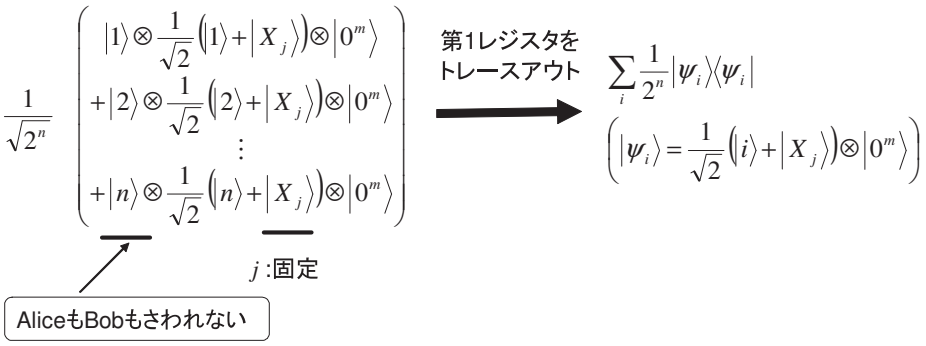


図 2.2: 攻撃モデルと実際の状況

Lemma 4

$$U_E|i\rangle|0\rangle = \Sigma_j a_j |X_j\rangle \left|w_{X_j}\right\rangle + \Sigma_j b_j |j\rangle |w_j\rangle$$

と表す．このとき，$|a_1| = |a_2| = \ldots = |a_{2^n}| (\leq \frac{1}{\sqrt{2^n}})$ として一般性を失わない．

(証明)

符号化時に，$X \in \{X_1, \ldots, X_{2^n}\}$ が一様ランダムに選ばれるため，

$$U_E|i\rangle|0\rangle = \Sigma_j a_j |X_j\rangle \left|w_{X_j}\right\rangle + \Sigma_j b_j |j\rangle |w_j\rangle$$

という攻撃の代わりに，j の置換 π をランダムに用意し，

$$U_E^{\pi}|i\rangle|0\rangle = \Sigma_j a_j \left|X_{\pi(j)}\right\rangle \left|w_{X_{\pi(j)}}\right\rangle + \Sigma_j b_j |j\rangle |w_j\rangle$$

という攻撃を行ったとしても，Eve にとって，検出率，盗める情報量に変化はない．π をランダムに選ぶため，攻撃後の状態は混合状態になるが，Eve に十分なアンシラを用意してこれを純粋化すると，

$$U_E|i\rangle|0\rangle = \Sigma_j a_j |X_j\rangle \left|w_{X_j}\right\rangle + \Sigma_j b_j |j\rangle |w_j\rangle$$

かつ，$|a_1| = |a_2| = \ldots = |a_{2^n}| (\leq \frac{1}{\sqrt{2^n}})$ という攻撃と等価になる．よって，$|a_1| = |a_2| = \ldots = |a_{2^n}| (\leq \frac{1}{\sqrt{2^n}})$ として一般性を失わない．

□

以下に定理 1 の証明を示す．

$$U_E|X\rangle|0\rangle = \alpha_1 |X\rangle|w_\alpha\rangle + \alpha_1' |\psi_{\alpha_1}\rangle|w_\alpha\rangle + \beta_1 |\psi_{\beta_1}\rangle$$

(ここで，任意の $|w\rangle$ に対して $|X\rangle|w\rangle \perp |\psi_{\beta_1}\rangle$，任意の $|\psi\rangle$ に対して $|\psi\rangle|w_\alpha\rangle \perp |\psi_{\beta_1}\rangle$，さらに，$|X\rangle \perp |\psi_{\alpha_1}\rangle$．) と表す．また，

$$U_E\left(\frac{1}{\sqrt{2}}|i\rangle + \frac{1}{\sqrt{2}}|X\rangle\right)|0\rangle = \alpha|\psi_\alpha\rangle|w_\alpha\rangle + \beta|\psi_\beta\rangle$$

と表す．(ここで，任意の $|\psi\rangle$ に対して，$|\psi\rangle|w_\alpha\rangle \perp |\psi_\beta\rangle$) 今，補題 4 より，

$$U_E|i\rangle|0\rangle = \Sigma_j \frac{e^{i\theta_{X_j}} a'}{\sqrt{2^n}} |X_j\rangle \left|w_{X_j}\right\rangle + \Sigma_j b_j |j\rangle |w_j\rangle$$

と書ける．ただし，$a' \leq 1$ である．ここで，

$$\frac{e^{i\theta_X} a'}{\sqrt{2^n}} |X\rangle|w_X\rangle = \frac{a''}{\sqrt{2^n}} |X\rangle|w_\alpha\rangle + \frac{a}{\sqrt{2^n}} |X\rangle \left|w_\alpha^{\perp}\right\rangle$$

とおくと，$|\psi_\beta\rangle$ は次のように書ける．

$$|\psi_\beta\rangle = \frac{a}{\sqrt{2}\sqrt{2^n}} |X\rangle \left|w_\alpha^{\perp}\right\rangle + b|i\rangle|w_i\rangle + c\left|\psi_\beta'\right\rangle$$

(ここで，任意の $|w\rangle$ について $|X\rangle|w\rangle \perp \left|\psi_\beta'\right\rangle$，$|i\rangle|w\rangle \perp \left|\psi_\beta'\right\rangle$，$|a| \leq a' \leq 1, |\frac{a}{\sqrt{2^{n+1}}}|^2 + |b|^2 + |c|^2 = 1$)

ここで，$|\psi_\beta\rangle$ を第 3 レジスタが $(\frac{1}{\sqrt{2}}|i\rangle + \frac{1}{\sqrt{2}}|X\rangle)^{\perp}$ である空間に射影し，その大きさの 2 乗 (p とおく) を考える．これに $|\beta|^2$ をかけたものを d とすると，検出率は少なくとも d である．

以下，p の下界を求める．$c = 0$ かつ $\left|w_\alpha^{\perp}\right\rangle = |w_i\rangle (= |W\rangle)$ としたときが p が最も小さくなる．このとき

$$|\psi_\beta\rangle = \frac{a}{\sqrt{2^{n+1}}} |X\rangle|W\rangle + e^{i\theta}\sqrt{1 - \frac{a^2}{2^{n+1}}} |i\rangle|W\rangle$$

と書ける．このベクトルと，

$$\frac{1}{\sqrt{2}}|X\rangle|W\rangle - \frac{1}{\sqrt{2}}|i\rangle|W\rangle$$

というベクトルの内積の絶対値の 2 乗が p である．よって，

$$\begin{aligned} p &= \left|\frac{a}{\sqrt{2^{n+2}}} - e^{i\theta}\sqrt{\frac{2^{n+1}-a^2}{2^{n+2}}}\right|^2 \\ &\geq \left(\frac{a}{\sqrt{2^{n+2}}} - \sqrt{\frac{2^{n+1}-a^2}{2^{n+2}}}\right)^2 \\ &\geq \left(\frac{1}{\sqrt{2^{n+2}}} - \sqrt{\frac{2^{n+1}-1}{2^{n+2}}}\right)^2 \\ &= \frac{2^{n+1}}{2^{n+2}} - \frac{2\sqrt{2^{n+1}-1}}{2^{n+2}} \\ &\geq \frac{1}{2} - \frac{1}{\sqrt{2^{n+1}}} \end{aligned}$$

検出率が δ なので，$\delta \geq (\frac{1}{2} - \frac{1}{\sqrt{2^{n+1}}}) \cdot |\beta|^2$．よって $|\beta| \leq O(\sqrt{\delta})$.

以上より $|\alpha| \geq \sqrt{1-O(\delta)}$ である．ここで，

$$U_E\left(\frac{1}{\sqrt{2}}|i\rangle + \frac{1}{\sqrt{2}}|X\rangle\right)|0\rangle = \alpha^i|\psi_\alpha^i\rangle|w_\alpha\rangle + \beta^i|\psi_\beta^i\rangle$$

と置き直し，前述の Eve の攻撃モデルを考えると，第 1 レジスタ - 第 4 レジスタまで含めた全体の状態 $|\Psi\rangle$ は，

$$\begin{aligned} |\Psi\rangle &= \frac{1}{\sqrt{2^n}}\Sigma_i|i\rangle|0\rangle\left(\alpha^i|\psi_\alpha^i\rangle|w_\alpha\rangle + \beta^i|\psi_\beta^i\rangle\right) \\ &= A|\Psi_A\rangle|w_\alpha\rangle + B|\Psi_B\rangle \end{aligned}$$

と書ける．ここで，$|A| \geq \sqrt{1-O(\delta)}$ である．よって，第 4 レジスタをトレースアウトすると，

$$\rho_A = |A|^2|\Psi_A\rangle\langle\Psi_A| + |B_1|^2|\Psi_{B_1}\rangle\langle\Psi_{B_1}| + |B_2|^2|\Psi_{B_2}\rangle\langle\Psi_{B_2}| + \ldots$$

と書ける．よって，

$$\begin{aligned} S(\rho_A) &\leq -|A|^2\log|A|^2 + \Sigma_j - B_j\log B_j \\ &\leq -|A|^2\log|A|^2 \\ &\quad +\Sigma_1^{2^{n+1}} - \frac{(1-|A|^2)}{2^{n+1}}\log\frac{(1-|A|^2)}{2^{n+1}} \\ &= H(|A|^2) + (1-|A|^2)\log 2^{n+1} \\ &\leq 1 + O(\delta)(n+1) \end{aligned}$$

以上より，$S(\rho_A) \leq O(\delta n)$ である．系 1 より，Eve が盗聴できる情報量は高々 $O(\delta n)$ である．

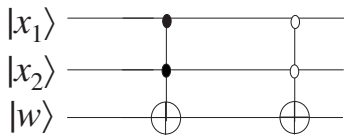


図 2.3: 量子回路 (1)

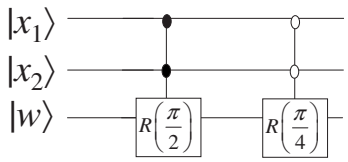


図 2.4: 量子回路 (2)

2.3 むすび

本研究では，量子文字列封印プロトコルを提案し，盗聴できる情報量の上界が自明な下界に一致することを示した．この意味で，本プロトコルは最適な量子文字列封印プロトコルと言える．本結果は，開封確認の検出率と盗聴される情報量のトレードオフを与えるものであり，提案プロトコルにおいて，検出率を δ とすると，盗聴される情報量は $O(\delta n)$ ビットであることが示された．

提案プロトコルの復号化率は 1/2 であるため，正規の復号手順を用いても誤って復号してしまう確率が高い．復号化率を高めた上で，盗聴される情報量の上界が，補題 1 に一致するプロトコルの開発等が今後の課題として挙げられる．

3 量子回路を二分決定グラフ構造から合成する手法

3.1 量子関数と行列関数

組織的な量子回路設計に役立つ概念として，量子関数と行列関数という概念を導入する．

図 2.3の回路は，3 ビット目の量子状態を $|w\rangle$ から $|w \oplus f(x_1,x_2)\rangle$ へ変換する．ここで，$f(x_1,x_2) = x_1 \cdot x_2 + \overline{x_1} \cdot \overline{x_2}$ である．そのため，この回路はブール関数 $f(x_1,x_2) = x_1 \cdot x_2 + \overline{x_1} \cdot \overline{x_2}$ を実現していると考えることができる．この種の量子回路は，有名な Grover Search [3] のオラク

表 2.1: 量子関数の真理値表

x_1, x_2	qf_2
$0, 0$	$R(\frac{1}{4}\pi)\,\|0\rangle$
$0, 1$	$\|0\rangle$
$1, 0$	$\|0\rangle$
$1, 1$	$R(\frac{1}{2}\pi)\,\|0\rangle$

表 2.2: ブール関数の真理値表

x_1, x_2	qf_1
$0, 0$	$\|1\rangle$
$0, 1$	$\|0\rangle$
$1, 0$	$\|0\rangle$
$1, 1$	$\|1\rangle$

ルとして用いることもでき，量子アルゴリズムの一部分としてよく利用される．

一方，図 2.4の量子回路では，3 ビット目の量子状態の出力をブール関数 $f(x_1, x_2)$ を用いて，$|w \oplus f(x_1, x_2)\rangle$ という形で表現することができない．たとえブール関数を実現する量子回路を設計対象としていても，部分的にこのような回路を利用することにより全体の回路規模が小さくなる場合があることが知られている．そのため，そのような量子回路も扱えるように新たに以下の定義を導入する．

Definition 1 n 変数 $x_1, x_2, \cdots, x_n$ 量子関数とは，$\{0, 1\}^n$ から一ビットの量子状態へのマッピングである．

図 2.4の回路の第 3 ビットを用いて説明する．もし，$|w\rangle$ の初期状態が $|0\rangle$ であれば，このビットの最終状態は，表 2.1に示される量子関数 $qf_2(x_1, x_2)$ となる．例えば，$x_1 = 0, x_2 = 0$ の時，最終量子状態は $R(\frac{1}{4}\pi)\,|0\rangle$ となるため，$qf_2(0, 0)$ が $R(\frac{1}{4}\pi)\,|0\rangle$ となっている．

表 2.2に図 2.3の第 3 ビット $|w\rangle$ の初期状態が $|0\rangle$ の時の最終状態を示す．これは，$|0\rangle$ と $|1\rangle$ をそれぞれブール値 0 および 1 と考えれば，ブール関数に対応していることがわかる．そのため，ブール関数は量子関数の特別なケースであることがわかる．

表 2.3: 行列関数の真理値表

x_1, x_2	mf_2
$0, 0$	$R(\frac{1}{4}\pi)$
$0, 1$	I
$1, 0$	I
$1, 1$	$R(\frac{1}{2}\pi)$

表 2.4: 定数行列関数の真理値表

x_1, x_2	$CM(I)$	$CM(R(\frac{1}{2}\pi))$
$0, 0$	I	$R(\frac{1}{2}\pi)$
$0, 1$	I	$R(\frac{1}{2}\pi)$
$1, 0$	I	$R(\frac{1}{2}\pi)$
$1, 1$	I	$R(\frac{1}{2}\pi)$

量子関数 $q(x_1, x_2, \cdots, x_n)$ の出力値は，$mf(x_1, x_2, \cdots, x_n)$ を $\{0, 1\}^n$ から二行二列のユニタリ行列へのマッピングとすると，常に $mf(x_1, x_2, \cdots, x_n)\,|0\rangle$ の形で表すことができるため，議論を容易にするため以下の定義を導入する．

Definition 2 n 個のブール変数 $x_1, x_2, \cdots, x_n$ に関する行列関数 mf とは，$\{0, 1\}^n$ から二行二列のユニタリ行列へのマッピングである．

表 2.1の量子関数 qf_2 に対応する行列関数 $mf(x_1, x_2)$ を表 2.3に示す．

以下の定義も導入する

Definition 3 行列関数 $mf(x_1, x_2, \cdots, x_n)$ は，全ての変数割り当てに対してその出力が同じ行列 M となる場合，定数行列関数と呼び，$CM(M)$ で表す．

表 2.4に，$CM(I)$ と $CM(R(\frac{1}{2}\pi))$ を例として示す．

表 2.3の行列関数 mf_2 を用いれば，図 2.4の回路は，第 3 ビットを $|w\rangle$ から $mf_2(x_1, x_2)\,|w\rangle$ へ変換すると見ることができる．そのため，以降では回路の動作は行列関数で表現することとする．

行列関数に対し，演算子 “$\oplus$” を以下の通り定義する．

表 2.5: 演算子 $\oplus$

x_1, x_2	mf_1	mf_2	$mf_1 \oplus mf_2$
$0, 0$	$R(\frac{1}{2}\pi)$	$R(\frac{1}{2}\pi)$	$R(\pi)$
$0, 1$	I	I	I
$1, 0$	I	$R(\frac{1}{4}\pi)$	$R(\frac{1}{4}\pi)$
$1, 1$	$R(\frac{1}{2}\pi)$	$R(\frac{1}{4}\pi)$	$R(\frac{3}{4}\pi)$

表 2.6: 演算子 $*$

x_1, x_2	mf_1	f_1	$f_1 * mf_1$
$0, 0$	$R(\frac{1}{2}\pi)$	1	$R(\frac{1}{2}\pi)$
$0, 1$	I	0	I
$1, 0$	$R(\pi)$	1	$R(\pi)$
$1, 1$	$R(\pi)$	0	I

Definition 4 $mf_1(x_1, x_2, \cdots, x_n)$ と $mf_2(x_1, x_2, \cdots, x_n)$ を行列関数とすると $mf_1(x_1, x_2, \cdots, x_n) \oplus mf_2(x_1, x_2, \cdots, x_n)$ は，$\cdot$ を通常の行列の乗算演算として，$mf(x_1, x_2, \cdots, x_n) = mf_1(x_1, x_2, \cdots, x_n) \cdot mf_2(x_1, x_2, \cdots, x_n)$ となる行列関数 $mf(x_1, x_2, \cdots, x_n)$ と定義する．

例を表 2.5に示す．

次に演算子 “$*$” を以下の通り定義する．

Definition 5 $mf(x_1, x_2, \cdots, x_n)$ 行列関数，$f(x_1, x_2, \cdots, x_n)$ をブール関数とする．$f(x_1, x_2, \cdots, x_n) * mf(x_1, x_2, \cdots, x_n)$ は，$f(x_1, x_2, \cdots, x_n) = 1$ の時 $mf(x_1, x_2, \cdots, x_n)$，$f(x_1, x_2, \cdots, x_n) = 0$ の時 $CM(I)$ となる行列関数とする．

例を表 2.6に示す．

3.2 行列関数を表現する二分決定グラフ

通常のブール関数と同様 [2] に量子関数も二分決定グラフにより効率よく表現可能である．そのため，我々は以下のような *Decision Diagram for a Matrix Function (DDMF)* と呼ぶ二分決定グラフを導入する．

Definition 6 行列関数を表現する二分決定グラフ（*DDMF: Decision Diagram for a Matrix Function*）は，以下の *3* 種類のノードからなる有向非巡回グラフである．

- 単位行列 I を表現する一つの終端ノード．
- 重み行列 M が付加された入力枝を持つ一つのルートノード．
- 複数の非終端ノード．

非終端ノードおよびルートノードは一つのブール変数 x_i と関連付けられ，別のノード *(1-child node)* につながっている出力枝：*1*-枝 *(*実線）および別のノード *(0-child node)* につながっている出力枝：*0*-枝 *(*点線）を持つ．各枝には重み行列が付加されている．

各ノードは以下の再帰的なルールにより行列関数を表現する．

- 終端ノードが表現する行列関数は $CM(I)$ である．
- 変数 x_i と関連付けられた非終端ノードおよびルートノードが表現する行列関数は，mf_1 と mf_0 を *1-child node* および *0-child node* のあらわす行列関数とし，M_1 と M_0 を *1*-枝および *0*-枝に付加された行列としたときに，$x_i * (CM(M_1) \oplus mf_1) \oplus \overline{x_i} * (CM(M_0) \oplus mf_0)$ となる．図 *2.5*に例を示す．
- ルートノードで表現される行列関数を mf，ルートノードへの入力枝に付加された行列を M とすると，*DDMF* により表現される行列関数は $CM(M) \oplus mf$ となる．

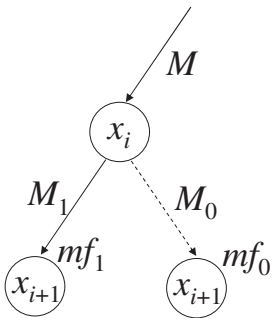


図 2.5: DDMF の非終端ノード

通常の BDD のように，以下の条件により DDMF の標準形を得ることができる．

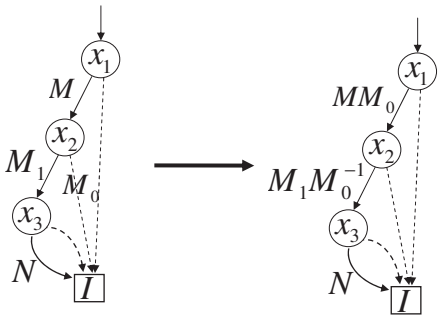


図 2.6: 標準形への変形

Definition 7 変数の順序を固定した *DDMF* は以下の条件を満たすとき，同一の行列関数を表現するものは唯一となり，そのためそれを標準形とする．

- *0*-枝に付加される行列は I.
- *0*-枝と *1*-枝が同一のノードをさし，かつ *1*-枝に付加された行列が I であるようなノードは存在しない．(削除される．)
- 同じ部分グラフは存在しない．(共有される．)

終端ノードからルートノードに向けて順にノードを選択して，そのノードに対して以下の変形を行なえば，任意の DDMF は標準形となる．

変形の対象とするノードへの入力枝，0-枝および 1-枝に付加された行列を M, M_0 および M_1 とする．その時，もし M_0 が I でない場合，以下のように各枝に付加された行列を修正する．

- 入力枝に付加された行列を MM_0 とする．
- 1-枝に付加された行列を $M_1M_0^{-1}$ とする．
- 0-枝に付加された行列を I とする．

例を図 2.6に示す．例では行列 I は省略している．

便宜上 DDMF に対しても行列関数と同じ意味で演算子を次のように用いることにする．

- $mf = mf_1 \oplus mf_2$ の時，(mf を表す DDMF) = (mf_1 を表す DDMF) $\oplus$ (mf_2 を表す DDMF) と表現する．
- $mf = mf_1 * mf_2$ の時，(mf を表す DDMF) = (mf_1 を表す DDMF) $*$ (mf_2 を表す DDMF) と表現する．

3.3 行列関数からの量子回路設計

通常の回路設計と同様に，既に行列関数 mf_1 および mf_2 を実現する量子回路があれば，$mf_1 \oplus mf_2$ および $mf_1 * mf_2$ を実現する量子回路を実現できる．そのため，行列関数 mf を実現したい時には，mf よりも量子回路として実現しやすいような mf_1 および mf_2 により $mf_1 \oplus mf_2$ または $mf_1 * mf_2$ という形に mf を分解すればよいことになる．以下では，この 2 種類の分解に対して量子回路をどのように設計できるかを示す．

分解手法１

$mf_1 \oplus mf_2$ という形に分解される行列関数を実現したい場合には，単純に以下により回路を合成可能である．

Proposition 1 行列関数 mf_1 および mf_2 で表現された変換を行なう量子回路を QC_1 および QC_2 とする．この時，QC_1 と QC_2 を連接して得られる量子回路は，$mf_1 \oplus mf_2$ で表現された変換を行なう量子回路である．

分解手法２

既に行列関数 mf_1 と mf_2 で表現された変換を行なう量子回路が設計済みの時，$mf_1 * mf_2$ で表現される変換を行なう量子回路は以下の手順で合成可能である．

Step. 1 QC_1 を用意する．QC_1 が量子関数を計算するビットを w_1 とする．

Step. 2 QC_2 の各ゲートのコントロールに w_1 を加えた回路を用意し，Step. 1 で用意した回路の後に連接する．

Step. 3 QC_1 のゲートを逆順に並べた回路を用意し，Step. 2 で用意した回路の後に連接する．

mf_1 を実現する QC_1 および mf_2 を実現する QC_2 がそれぞれ図 2.3および図 2.4の時，$mf_1 * mf_2$ で表現される変換を行なう量子回路は図 2.7に示すように合成される．

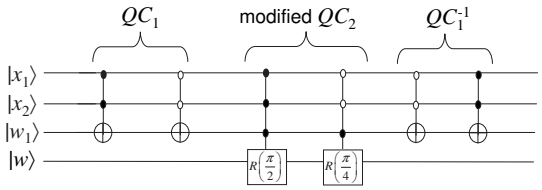


図 2.7: $mf_1 * mf_2$ の量子回路

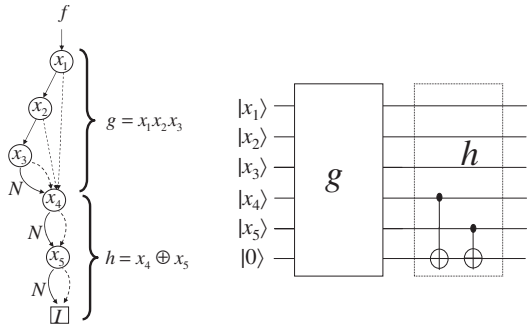


図 2.8: DDMF の分解: 簡単なケース

3.4 DDMF を用いた量子回路設計

DDMF の表現を利用して，制御-NOT ゲート，制御-V ゲートおよび制御-V^{-1} ゲートにより回路を組織的に合成する手法を以下に示す．

簡単なケース１

(f を表す DDMF) = (g を表す DDMF) $\oplus$ (h を表す DDMF) を満たす f に対応する量子回路を設計するには，単純に f と g に対応する量子回路を連接すれば良い．図 2.8に，(DDMF for f) = (DDMF for g) $\oplus$ (DDMF for h) の時に f に対応する量子回路の設計例を示す．

簡単なケース２

Definition 8 *DDMF の全てのノードの 1-枝と 0-枝が同じノードに向かっている時，その DDMF は chain と呼ばれる．*

もし，設計対象の DDMF が *chain* 構造を持つ場合，以下のように対応する量子回路を設計できる．

- 関連付けられた変数が x_i で 1-枝に付加された行列が M_i である各ノードに対して, x_i でコントロールされる制御-M_i ゲートを用意する．
- 上記のゲート全てを連接すれば所望の回路を得る．

図 2.8の h を表す DDMF は chain 構造を持つので，図に示すように量子回路が設計できる．

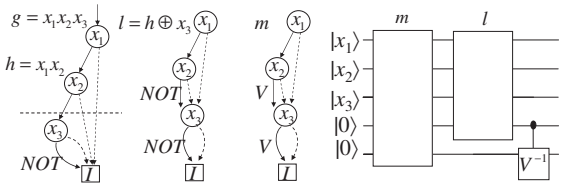


図 2.9: DDMF の分解: 複雑なケース

複雑なケース

もし設計対象の DDMF の下部に chain 構造がなければ，上述した手法を用いることはできない．そのような場合も以下の手法により設計対象の DDMF をより簡単な DDMF に分解することが可能である．

今，設計対象の関数 g を表す DDMF の下部に chain 構造がないとする．そして，その部分の一番上に位置するノードを v_i とそれに関連付けられた変数を x_i とする．この時，以下のように設計対象の DDMF を分解できる．

- ルートノードから v_i に向かう全てのパスに対応するブール関数を h とする．
- $h \oplus x_i$ となるブール関数を l とする．
- l を表す DDMF の全ての枝に付加された行列 NOT を V に変更した DDMF の表現する量子関数を m とする．
- この m を実現する量子回路を用いて，図 2.9 のように所望の回路を設計することができる．

この設計手法では，l と m を表す DDMF は chain 構造をその下部に必ず持つことが保証できる．そのためこれらはより簡単な量子回路として設計できる．従って，上述した手法を再帰的に適用することにより量子回路を組織的に設計することが可能である．

既存の手法 [1] は設計すべき関数の入力数に対して指数的な精度のゲートを利用するので，提案手法のほうがより実用的であると考えられる．

参考文献

[1] A. Abdollahi and M. Pedram: "Analysis and synthesis of quantum circuits by using quantum decision diagrams", Proc. of the Design, Automation and Test in Europe (DATE'06), pp. 317–322 (2006).

[2] R. E. Bryant: "Graph-based algorithm for Boolean function manipulation", IEEE Trans. Comput., **C-35**, 8, pp. 667–691 (1986).

[3] L. K. Grover: "A fast quantum mechanical algorithm for database search", Proceedings of 28th ACM Symposium on Theory of Computing, pp. 212–219 (1996).

[4] G.-P. He, "Secure quantum string seal exists," quant-ph/0602159, 2006.

[5] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," Science, vol. 283, 2050–2056, 1999.

研究業績一覧

学術論文

1. A. Ambainis, K. Iwama, A. Kawachi, R. Raymond, S. Yamashita:
"Improved Algorithms for Quantum Identification of Boolean Oracles", Theoretical Computer Science, (掲載予定).
概要: The oracle identification problem (OIP) was introduced by Ambainis *et al.* It 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 improve the previous algorithms by providing a mostly optimal upper bound of query complexity for this problem: (*i*) For any oracle set S such that $|S| \leq 2^{N^d}$ $(d < 1)$, we design an algorithm whose query complexity is $O(\sqrt{N \log M / \log N})$, matching the known lower bound. (*ii*) Our algorithm also works for the range between 2^{N^d} and $2^{N/\log N}$ (where the bound becomes $O(N)$), but the gap between the upper and lower bounds worsens gradually. (*iii*) Our algorithm is robust, namely, it exhibits the same performance (up to a constant factor) against the noisy oracles as also shown in the literatures for special cases of OIP.

2. T. Suzuki, S. Yamashita, M. Nakanishi, K. Watanabe:
"Robust Quantum Algorithms Computing OR with ϵ-biased Oracles", IEICE transactions on Information and Systems, Vol. E90-D, No.2, pp. 395–402, 2007 年 2 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 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.

3. M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, S. Yamashita:
"(4,1)-Quantum Random Access Coding Does Not Exist—One Qubit Is Not Enough To Recover One of Four Bits", New J. Phys., 8, 129, 2006 年 8 月.
概要: An $(n, 1, p)-$quantum random access (QRA) coding, introduced by Ambainis et al., is the following communication system: the sender which has n-bit information encodes his/her information into one qubit,

which is sent to the receiver. The receiver can recover any one bit of the original n bits correctly with probability at least p, through a certain decoding process based on positive operator-valued measures. Actually, Ambainis et al. shows the existence of a $(2, 1, 0.85)$-QRA coding and also proves the impossibility of its classical counterpart. Chuang immediately extends it to a $(3, 1, 0.79)$-QRA coding and whether or not a $(4, 1, p)$-QRA coding such that $p > 1/2$ exists has been open since then. This paper gives a negative answer to this open question. Moreover, we generalize its negative answer for one-qubit encoding to the case of multiple-qubit encoding

4. M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, S. Yamashita:
"(4,1)-Quantum Random Access Coding Does Not Exist", New J. Phys., Proc. of the 2006 IEEE International Symposium on Information Theory (ISIT2006), pp. 446–450, 2006年7月.
概要: An $(n, 1, p)$-Quantum Random Access (QRA) coding, introduced by Ambainis, Nayak, Ta-shma and Vazirani in ACM Symp. on Theory of Computing 1999, is the following communication system: The sender which has n-bit information encodes his/her information into one qubit, which is sent to the receiver. The receiver can recover any one bit of the original n bits correctly with probability at least p, through a certain decoding process based on positive operator-valued measures. Actually, Ambainis et al. shows the existence of a $(2, 1, 0.85)$- QRA coding and also proves the impossibility of its classical counterpart. Chuang immediately extends it to a $(3, 1, 0.79)$- QRA coding and whether or not a $(4, 1, p)$-QRA coding such that $p > 1/2$ exists has been open since then. This paper gives a negative answer to this open question.

5. A. Ambainis, K. Iwama, A. Kawachi, R. Raymond and S. Yamashita:
"Improved Algorithms for Quantum Identification of Boolean Oracles", Prof. of the 10th Scandinavian Workshop on Algorithm Theory (SWAT 2006), pp. 280–291, 2006年7月.
概要: The oracle identification problem (OIP) was introduced by Ambainis et al. It 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 improve the previous algorithms by providing a mostly optimal upper bound of query complexity for this problem: (i) For any oracle set S such that $|S| \leq 2^{N^d}$ $(d < 1)$, we design an algorithm whose query complexity is $O(\sqrt{N \log M / \log N})$, matching the known lower bound. (ii) Our algorithm also works for the range between 2^{N^d} and $2^{N/\log N}$ (where the bound becomes $O(N)$), but the gap between the upper and lower bounds worsens gradually. (iii) Our algorithm is robust, namely, it exhibits the same performance (up to a constant factor) against the noisy oracles as also shown in the literatures for special cases of OIP.

6. T. Suzuki, S. Yamashita, M. Nakanishi, K. Watanabe:
"Robust Quantum Algorithms with ϵ-biased Oracles", Proc. of 12th Annual International Computing and Combinatorics Conference (COCOON 2006), pp. 116–125, 2006年8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 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. H. Nishiyama, M. Nakanishi, S. Yamashita, Y. Nakashima:
"An Efficient Approximation of SU(d) Using Decomposition", Proc. of Asian Conference on Quantum Information Science 2006 (AQIS 2006), pp. 147–148, 2006 年 9 月.
概要: In this paper, we show the approximation method for n-dimensional unitary matrix using decomposition into the product of the two-level unitary matrices. The computation time for the preparation stage does not depend on d. We show that the length of circuit is asymptotically $O(d^2 \log^{3.97}(1/\varepsilon))$. We also show an exact comparison of the length of the circuit where we can see that our method can even provide smaller circuits than Dawson's method in some cases.

8. Y. Murakami, M. Nakanishi, M. Hagiwara, S. Yamashita, Y. Nakashima:
"Quantum Secure Direct Communication Protocols for Sending a Quantum State", 2006 International Symposium on Information Theory and its Applications (ISITA2006), 2006 年 10 月.
概要: We propose a new quantum secure direct communication protocol, which has an advantage of combining the following features over related works: The protocol allows us to send a quantum state in security; The proper sender and receiver can detect an eavesdropper efficiently; The protocol employs no entanglement resource, and thus it is relatively easy to be experimented in current technology.

9. K. Iwama, H. Nishimura, R. Raymond, S. Yamashita:
"Quantum Random Access Coding using Multiple Qubits", Workshop on Quantum Information Processing 2007, Poster Presentation.
概要: In 1999, Ambainis et al. first proposed the concept of *Quantum Random Access Coding (QRAC)* to show advantages of quantum information beyond the limitation of Holevo Bound. Concerning QRAC, Hayashi et al. show the following: There is no $(2^{2m}, m, p > 1/2)$–QRAC. In other words, for any $(n, m, p > 1/2)$–QRAC, it holds that $m > \frac{\log n}{2}$. However, it was not clear if $(2^{2m} - 1, m, > 1/2)$–QRACs do exist for any $m \geq 1$. This paper show that such QRACs actually exist hence showing the tightness of the above results by Hayashi et al.

10. K. Iwama, H. Nishimura, R. Raymond, S. Yamashita:
"Quantum Network Coding for General Graphs", Workshop on Quantum Information Processing 2007, Poster Presentation.
概要: Network coding is often explained by using a small network model called Butterfly. In this network, there are two flow paths, s_1 to t_1 and s_2 to t_2, which share a single bottleneck channel of capacity one. So, if we consider conventional flow (of liquid, for instance), then the total amount of flow must be at most one in total, say 1/2 for each path. However, if we consider information flow, then we can send two bits (one for each path) at the same time by exploiting two side links, which are of no use for the liquid-type flow, and encoding/decoding operations at each node. This is known as *network coding* and has been quite popular since its introduction by Ahlswede, Cai, Li and Yeung in 2000. In QIP 2006, Hayashi et al showed that *quantum* network coding is possible for Butter-

fly, namely we can send two *qubits* simultaneously with keeping their fidelity strictly greater than 1/2. In this paper, we show that the result can be extended to a large class of general graphs by using a completely different approach. The underlying technique is a new cloning method called *entanglement-free cloning* which does not produce any entanglement at all. This seems interesting on its own and to show its possibility is an even more important purpose of this paper. Combining this new cloning with approximation of general quantum states by a small number of fixed ones, we can design a quantum network coding protocol which "simulates" its classical counterpart for the same graph.

11. Y. Murakami, M. Nakanishi, S. Yamashita, Y. Nakashima:
"A Quantum Secure Direct Communication Protocol for Sending a Quantum State and Its Security Analysis", Workshop on Quantum Information Processing 2007, Poster Presentation.
概要: We propose a new quantum secure direct communication (QSDC) protocol which allows us to (i) carry an arbitrary quantum state; (ii) detect eavesdroppers on a channel efficiently; and (iii) employ no entanglement resource. We also give its security analysis.

12. M. Nakanishi, S. Tani, S. Yamashita:
"Tight Bounds on Information Gains in Quantum Sealing Protocols", Workshop on Quantum Information Processing 2007, Poster Presentation.
概要: This paper investigates the ability of quantum string sealing protocols by giving an optimal quantum sealing protocol when the whole string is not necessarily recovered even for honest players. More specifically, in the followings, we show that the information leaks (i.e. information gains for a cheater) matches a trivial lower bound in our quantum sealing protocol. Thus we give a clear understanding of what we can do by quantum string sealing protocols.

13. M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, S. Yamashita:
"Quantum Network Coding", Proc. of the 24th International Symposium on Theoretical Aspects of Computer Science (STACS 2007), pp. 610–621, 2007年2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. 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. (iv) Several impossibility results including the general upper bound of the fidelity are also given.

研究会等

1. M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, S. Yamashita:
"(4,1)-Quantum Random Access Coding Does Not Exist", 電子情報通信学会コンピュテーション研究会, COMP2006-14, pp.33–38, 2006 年 5 月.
概要: An $(n, 1, p)$-Quantum Random Access (QRA) coding, introduced by Ambainis, Nayak, Ta-shma and Vazirani in ACM Symp. on Theory of Computing 1999, is the following communication system: The sender which has n-bit information encodes his/her information into one qubit, which is sent to the receiver. The receiver can recover any one bit of the original n bits correctly with probability at least p, through a certain decoding process based on positive operator-valued measures. Actually, Ambainis et al. shows the existence of a $(2, 1, 0.85)$- QRA coding and also proves the impossibility of its classical counterpart. Chuang immediately extends it to a $(3, 1, 0.79)$- QRA coding and whether or not a $(4, 1, p)$-QRA coding such that $p > 1/2$ exists has been open since then. This paper gives a negative answer to this open question.

2. 村上ユミコ, 中西正樹, 萩原学, 山下茂, 中島康彦:
"量子状態を送信可能な量子秘密通信プロトコル", 電子情報通信学会 量子情報技術研究会, QIT2006-28, pp. 133–134, 2006 年 5 月.
概要: We propose a new quantum secure direct communication protocol, which has an advantage of combining the following features over related works: The protocol allows us to send a quantum state in security; The proper sender and receiver can detect an eavesdropper efficiently; The protocol employs no entanglement resource, and thus it is relatively easy to be experimented in current technology.

3. 西山寛之, 中西正樹, 山下茂, 中島康彦:
"3 準位量子ゲート設計のためのユニタリ行列近似", 電子情報通信学会 量子情報技術研究会, QIT2006-41, pp. 180–183, 2006 年 5 月.
概要: 近年，量子計算において多準位系を用いる手法が提案されている．本研究では，3 準位系を用いた量子ゲートの設計のためのユニタリ行列の任意精度の近似手法を提案する．本稿ではまず従来の 2 準位系を用いた手法について概観し，その発展として 3 準位でのユニタリ行列の近似法を述べる．そのために，3 準位系の Bloch ベクトルから作られる回転変換を定義し，その回転変換でユニタリ行列を近似する．

4. 竹谷昌敏, 中西正樹, 山下茂, 中島康彦:
"量子封印を用いた量子認証", 電子情報通信学会 量子情報技術研究会, QIT2006-92, pp. 209–212, 2006 年 11 月.
概要: 現在，インターネットを利用する際に暗号技術は欠かせないものである．しかし，量子計算機で因数分解を高速に解ける事がわかったため，現代の数体暗号に換わるあたらしい暗号が必要となった．その中，量子を通信に利用する事により，BB84 等のプロトコルが考案された．その中で量子通信で認証や情報の完全性の保証をその計算量で保証するのではなく，量子の性質を利用し無条件安全なプロトコルの考案が要求された．本稿では現状の技術で実現が容易な量子認証プロトコルを提案する．

5. 山下茂, 中西正樹, 内山智香子, 相原正樹:
"Pure Dephasing を考慮した量子オラクル計算モデル", 電子情報通信学会 量子情報技術研究会, QIT2006-97, pp. 229–232, 2006 年 11 月.
概要: 本稿では，量子オラクルと呼ばれる量子のブラックボックスがデコヒーレンスのエラーを受けた状況を計算科学の視点から考察する．我々の最終的な目標は，計算量（ある計算をするのに必要な量子オラクルの呼び出し回数）とデコヒーレンスのエラーの度合いとの関係を解析することである．その最初

のステップとして，オラクルの出力に pure dephasing のエラーが起こってもそのようなオラクルを複数用いて pure dephasing のエラーを軽減する手法を提案する．これは，古典計算においてエラーのあるオラクルに対処するための最も基本的な手法である多数決による成功確率の増幅に対応する．我々の知る限りでは，我々の問題設定はオラクル計算の枠組みでデコヒーレンスの影響を考察する最初のものである．

6. 中西正樹, 谷誠一郎, 山下茂:
“量子文字列封印における復号化率と検出率のトレードオフについて”, 電子情報通信学会量子情報技術研究会, QIT2006-98, pp. 233–236, 2006 年 11 月.
概要: 量子封印とは，乱数と量子ビットを用いてメッセージを符号化することにより，第三者がそのメッセージを復号すると量子状態が壊れ，メッセージが読まれたことが確認できるというものである．1 ビットの値を封印する量子ビット封印に関しては，安全なプロトコルが存在しないことがすでに知られている．しかし，量子ビット封印が安全でないからと言って量子文字列封印も安全でないとは限らない．そこで，量子文字列封印の可能性について様々な議論がなされている．しかし，今まで盗聴者が盗聴できる情報量と検出率の関係については知られていなかった．本稿では，盗聴される情報量の上界が自明な下界に一致するプロトコルを提案し，盗聴者が盗聴できる情報量と検出率のトレードオフの関係を明らかにする．

7. S. Yamashita, D. Michael Miller:
“Decision Diagram Data Structure to Represent Quantum Circuit”, 電子情報通信学会技術研究報告, VLD2006-58, pp. 41–46, 2006 年 11 月.
概要: In this paper, we propose a systematic design method for quantum circuits that compute Boolean functions. Our synthesis strategy is based on the previous method, but it is much simpler, and also may be more practical since we only use three different types of gates whereas the previous method may use many types of gates including rotation gates with *exponential* (with respect to the number of inputs of the desired function) accuracy. To formulate our synthesis strategy, we introduce and formulate a new concept, *matrix function*, which can describe a quantum circuit's behaviors very well. Then, in order to represent matrix functions efficiently, we naturally introduce decision diagram structures, which we call *(DDMF) Decision Diagram for a Matrix Function*. These formulation may be interesting on their own.

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) 支配集合分割は、公平な資源割り当てが求められるさまざまな応用分野で利用されている主要な概念のひとつである。しかし、参加ノードが動的に変化するネットワーク上で支配集合分割を厳密に維持することはコストの点で不利であることから、「欠陥のある支配集合分割」という新しい概念を提案し、その基本的な性質の解明を行った。

b) ネットワーク上のある頂点集合から別の頂点集合に安全に情報を転送する上で重要な課題のひとつは、転送ルートを冗長化し、故障の影響をできる限り低く抑えることである。この課題に対し、冗長化によるルート長の増加を抑える新しい手法を開発し、その効果をトランスポジショングラフ上のルーティング問題で確かめた。

c) 無線ネットワーク上の通信帯域や電力などの効率的な資源配分方法について検討を行った。具体的には、ランキング問題やリーダ選挙問題について詳細に検討し、最適なアルゴリズムの提案を行った。

d) センサーネットワークの省電力ルーティングを実現するための具体的な手法のひとつとしてグラフの連結支配集合分割問題について検討した。具体的には、キュービックグラフに関する上下限と、交差グラフの一種であるパスグラフに対するアルゴリズムの提案を行った。

以下では、上記各項目の中でも a),b) について、背景と研究の位置づけを含めて、本研究課題で得られた結果の概要を述べる。そのほかの結果の詳細については、業績リスト中の論文を参照されたい。

2　欠陥のある支配集合分割

2.1　諸定義

無向グラフ $G = (V, E)$ を考える。各頂点 $u \in V$ について、u の閉じた近傍を $N[u] \stackrel{\text{def}}{=} \{u\} \cup \{v \in V : \{u, v\} \in E\}$ で定義する。V の部分集合 U は、任意の $u \in V$ について $N[u] \cap U \neq \emptyset$ であるとき G の支配集合であるといい、V の分割 $\mathcal{V} = \{V_1, V_2, \ldots, V_d\}$ は、各 V_i が G の支配集合であるとき G の**支配集合分割** (domatic partition) であるという (ここで $\mathcal{V}$ 中の各要素は、空集合ではないとする)。以下では、グラフ G のサイズ d の支配集合分割を d-DP と呼ぶ。ここで $\mathcal{V}$ が d-DP であるとき、任意の $u \in V$ について $|\{V_i \in \mathcal{V} : N[u] \cap V_i \neq \emptyset\}| = d$ となることに注意しよう。

本節では、**欠陥のある支配集合分割** (defective domatic partition: DDP) という概念を新たに定義し、その基本的な性質を調べる。グラフ G の頂点集合 V の分割 $\mathcal{V}$ は、1) $|\mathcal{V}| =$

d であり、かつ、2) 任意の $u \in V$ について $|\{V_i \in \mathcal{V} : N[u] \cap V_i \neq \emptyset\}| \geq d-k$ のとき、(d,k)-DDP であるという。ここで、欠けている高々k 個の支配集合の種類が頂点ごとに異なっていてもよいことにも注意しておこう。以下では (d,k)-DDP を、頂点あたり高々k 個の欠陥のある支配集合分割と呼ぶ。定義よりあきらかに、グラフ G が (d,k)-DDP をもつとき、任意の $i \geq 1$ について、G が $(d,k+i)$-DDP をもつことに注意されたい。

DDP は、センサーネット上の省電力ルーティングなどのように、支配集合分割によってモデル化されるアプリケーションに対して自然に適用することができる。たとえば $(d,1)$-DDP は、各頂点が (d 個用意された支配集合のうち) 少なくとも $d-1$ 個の部分集合によって支配されていることをあらわしており、時分割でルータノードを切り替えるタイプのルーティング方式のもとでは、そのような分割を用いることで、$(d-1)/d$ の割合でルーティングサービスが提供されることを保証できることになる。

まず以下の補題が成立する：

補題 1 *グラフ G が (d,k)-DDP をもつとき、任意の $1 \leq i \leq |V|-d$ について、G は $(d+i,k+i)$-DDP をもつ。*

したがって、グラフ G の最大支配分割数が $d(G)$ のとき、任意の $1 \leq i \leq |V|-d(G)$ について、G は $(d(G)+i,i)$-DDP をもつことになる。

グラフ G の最大頂点次数を $\Delta(G)$、最小頂点次数を $\delta(G)$ であらわすこととしよう。頂点集合 V を $|V|$ 個の集合に分割すると、各頂点は少なくとも $\delta(G)+1$ 個の異なる頂点集合によって支配されるから、以下のことが言える：

性質 1 *任意のグラフ G は $(|V|, |V|-(\delta(G)+1))$-DDP をもつ。*

また欠陥のない最大の支配集合分割数は $\delta(G)+1$ を超えることはないから、分割数 d が $\delta(G)+2$ 以上のとき、欠陥の数は少なくとも $d-(\delta(G)+1)$ 以上になる。したがって以下のことも直ちに言える：

性質 2 *任意のグラフ G は、任意の $i \geq 0$ に対して、$(\delta(G)+2+i,i)$-DDP をもたない。*

考察の一つの方向は、上記の性質 1 を緩和していくことである。すなわち、すべての頂点に異なるラベルが与えられるという極端な状況から開始し、同じラベルを与えられた頂点がお互いに干渉しないように保ったままで、ラベルの総数をどこまで減少させていけるかを考える (2.2節参照)。もう一つの方向は、k の値を 0 から徐々に増やしていくことで、与えることのできるラベル数をどこまで増やしていけるかを考えていくことである (2.3節参照)。

2.2 ラベル数の上限

グラフ $G=(V,E)$ の平方 G^2 を以下のように定義する：$V(G^2)=V$ かつ、$E(G^2)=\{\{u,v\} \in V \times V : \{u,v\} \in E \text{ or } \exists w \text{ such that } \{u,w\},\{w,v\} \in E\}$. このとき、グラフ G^2 の独立点集合に含まれる任意の 2 頂点は、G において同一頂点の近傍に同時に含まれることはない。したがってこの性質を用いると、性質 1 におけるラベル総数を、d と k のギャップを保ったままで、$|V|$ から $\chi(G^2)$ に減少させることができる (ここで $\chi(G)$ は G の点彩色数)。Brooks の定理より、完全グラフではない任意のグラフ G の点彩色数は G の最大次数以下であることが知られているから、以下の性質が得られる (そのような点彩色は多項式時間で求めることができる)：

補題 2 *G^2 が完全グラフではない頂点数 Δ^2+1 以上の任意のグラフ G は $(\Delta^2, \Delta^2-(\delta+1))$-DDP をもつ。ここで Δ は G の最大次数、δ は G の最小次数である。*

したがってたとえば、頂点数 10 以上の任意のキュービックグラフが $(9,5)$-DDP をもつことを、上記の性質から直ちに導くことができる。

2.3 ラベル数の下限

本節では、正則グラフに対してラベル数の下限を調べる。任意のリングの最大支配集合分割数は 2 以上 3 以下であり、リングが 3-DP を持つための必要十分条件はリング中の頂点数が 3 の倍数になっていることである。以下の補題が成立する：

補題 3 *リングが $(4,1)$-DDP を持つのは、リング中の頂点数が 5 でないときかつそのときに限られる。*

この結果から、任意のリングが $(5,2)$-DDP をもつことが直ちにいえる (サイズ 5 の場合は性質 1 から、それ以外の場合は補題 1と補題 3から)。したがって性質 2とあわせると、リングに関しては、すべての d,k の組合せに関して (d,k)-DDP の存在可能性と存在非可能性が示せたことになる。

次にキュービックグラフについて考える。任意のキュービックグラフ G の最大支配集合分割数 $d(G)$ は、2 以上 4 以下である。また「キュービックグラフ G が 3-DP、すなわち $(3,0)$-DDP をもつかどうか」を問う問題の計算複雑さが NP 困難であることもすでにわかっている (証明には 3 次元マッチングからの帰着を用いる)。

以下の結果が成立する：

- 任意のキュービックグラフ G は、$(4,1)$-DDP をもつ。
- $(5,1)$-DDP をもたないような、ブリッジをもたないキュービックグラフが存在する。

性質 2から、任意のキュービックグラフは $(5,0)$-DDP や $(6,1)$-DDP をもたない。また上記の結果と補題 1から、ブリッジをもたない任意のキュービックグラフは、$(5,2)$-DDP や $(6,3)$-DDP をもつ。したがって、次に考えなくてはならないのは、以下の各項目である：

- キュービックグラフが $(5,1)$-DDP をもつかどうかを問う問題の計算複雑さについて
- キュービックグラフが $(6,2)$-DDP, $(7,3)$-DDP, $(8,4)$-DDP をもつかどうかを問う問題の計算複雑さについて

ちなみにキュービックグラフが (欠陥を許さない)4-DP をもつかどうかを問う問題の NP-困難性は、3-edge-coloring との等価性から示すことができる (つまり $(4,0)$-DDP をもつかどうかを調べる問題は NP 困難)。さきの議論から、任意のキュービックグラフが $(9,5)$-DDP をもつことはわかっているから、ギャップを 4 に保ったままでラベル数を 4 から 9 まであげていくどこかの段階で、計算複雑さが NP 困難から P に変化していることが予想される (ギャップが 3 の場合は、$k=0$ のときのみ NP 困難で、$k \geq 1$ のときはすべて P であることがわかっており、ギャップが 5 の場合は、そのような DDP は存在しない)。

上記の検討課題についてすべて解決したわけではないが、次の結果が得られている：

- $d \leq 7$ のとき、$(d,d-4)$-DDP が存在しないようなインスタンスが存在する。

$(7,3)$-DDP が存在しなければ $(6,2)$-DDP や $(5,1)$-DDP ももちろん存在しない。また $d \geq 4$ のとき、$(d,d-4)$-DDP が存在するようなインスタンスが存在することから (自分と周囲のラベルがすべて異なるような、いわゆる “perfect domination” を考えればよい)、少なくとも $4 \leq d \leq 7$ の範囲においては、与えられたインスタンスが $(d,d-4)$-DDP をもつかどうかという問に対する答えは、YES であるようなインスタンスも NO であるようなインスタンスも存在するという意味で自明ではないことになる ($d=9$ のときは任意のキュービックグラフに対して $(9,5)$-DDP が存在するし、$d=4$ のときの計算複雑さが NP 困難であることもすでにわかっている)。

一方、$d=8$ における十分条件が次のように与えられることがわかっている：

- サイズ 3 の任意のサイクルは、その隣接ノードが $(8,4)$-DDP の条件を満たす範囲でどのようにラベル付けされていたとしても、$(8,4)$-DDP の条件を満たすようにラベル付けすることができる。
- サイズ 4 の任意のサイクルは、その隣接ノードが $(8,4)$-DDP の条件を満たす範囲でどのようにラベル付けされていたとしても、$(8,4)$-DDP の条件を満たすようにラベル付けすることができる。

これらの結果を用いることで、任意のキュービックグラフに対して $(8,4)$-DDP が存在することを証明できると考えている。

3 トランスポジショングラフ上の点素なパスの構成法

本節では、Cayley グラフの一種であるトランスポジショングラフにおいて、与えられたソース頂点と目的頂点集合とを点素なパス集合によって結ぶためのアルゴリズムを示す。このアルゴリズ

ムの実行時間はトランスポジショングラフの次元に関して多項式時間であり、得られるパスの長さは、$n \geq 7$ のとき、各目的頂点までの最短パスの長さに比べて高々14 しか長くならない。この結果はこれまでに知られていた最もよいアルゴリズムの大幅な改良になっている (従来手法では最短パスの長さからの増分は $3n-5$ であり、定数では抑えられない)。

3.1 準備

V_n を記号 $1, 2, \ldots, n$ 上の $n!$ 個の順列の集合とする。順列 $u \in V_n$ の第 i 桁の値を u_i と記す。ジェネレータ $g_{i,j}$ $(1 \leq i < j \leq n)$ とは、与えられた順列の i 桁と j 桁を交換する関数のことであり、与えられた順列が $u = u_1 u_2 \ldots u_n$ $(\in V_n)$ のとき、

$$g_{i,j}(u) \stackrel{\text{def}}{=} u_1 \ldots u_{i-1} \underline{u_j} u_{i+1} \ldots u_{j-1} \underline{u_i} u_{j+1} \ldots u_n$$

のように定義される。

定義 1 (n-TG) n 個のシンボル上のトランスポジショングラフ T_n とは、V_n を頂点集合とし、以下のように定義される E_n を辺集合とするような無向グラフである：$E_n \stackrel{\text{def}}{=} \{\{u, g_{i,j}(u)\} \mid u \in V_n,\ 1 \leq i < j \leq n\}$.

T_n 中の頂点 u の隣接頂点の集合を $N(u) \stackrel{\text{def}}{=} \{v \in V_n \mid \{u, v\} \in E_n\}$ とする。任意の $u \in V_n$ に対して $|N(u)| = n(n-1)/2$ であることに注意しよう。実際、T_4 においては、頂点 1234 は、次の 6 $(= 4 \times 3/2)$ 個の隣接頂点をもつ：$1243, 1324, 1432, 2134, 3241, 4231$。以下では表記を簡単にするため、$f_n \stackrel{\text{def}}{=} n(n-1)/2$ とする。また n-TG の対称性より、$1234...n$ をソース頂点とし、s と D との距離は 2 以上であると仮定する。さらに n-TG が次数 f_n $(= n(n-1)/2)$ の正則グラフであることから、$|D| = f_n$ を仮定する。

3.2 構成法

垂直クラスタリング

提案手法ではまず最初に、T_n を長さ 2 の suffix によって特徴づけられるような T_{n-2} のコピーたちに分割する。suffix ij によって特徴づけられる

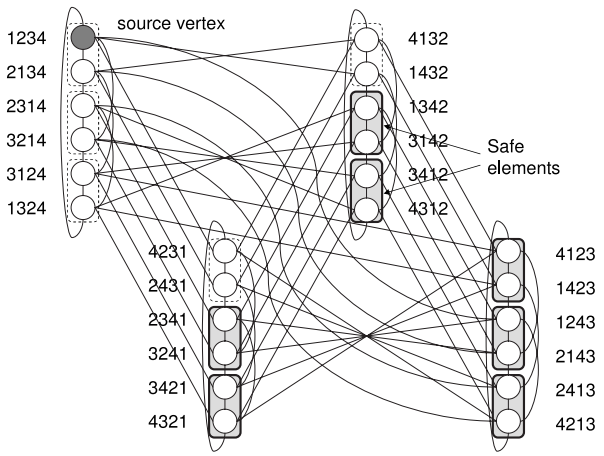


図 2.1: $\mathcal{T}$ 中の垂直クラスタ (ソース頂点は濃いグレーで、安全な垂直クラスタは明るいグレーで示されている).

コピーを $TG(i, j)$ と記し、そのような $n(n-1)$ 個のコピー全体の集合を $\mathcal{T}$ とする (例えばソース $s = 123 \ldots n$ は $TG(n-1, n)$ に属しており、s の f_n 個の隣接頂点のうち f_{n-2} 個は、s と同じコピーに属している)。以下では、$\mathcal{T}$ を V_n の**垂直クラスタリング**と呼び、その各要素を**垂直クラスタ**と呼ぶ。定義より、異なる垂直クラスタが交わりをもたないことに注意しよう。

提案手法の第 1 のアイデアは、D 中の各頂点を $\mathcal{T}$ 中の垂直クラスタに単射によって割り当てることである ($|\mathcal{T}| = 2|D|$ より、$\mathcal{T}$ がそのような単射を実現するのに十分な垂直クラスタを含んでいることに注意しよう)。以下では $i \neq n-1$ かつ $j \neq n$ であるような垂直クラスタ $TG(i, j) \in \mathcal{T}$ をソース頂点 s に関して**安全**なクラスタと呼ぶ。図 2.1は、T_4 における安全な垂直クラスタを示している。任意の安全な垂直クラスタ $TG(i, j)$、$TG(i', j')$ について、s と $TG(i', j')$ 中の任意の頂点を結ぶ最短パスは $TG(i, j)$ と頂点を共有しない。なぜならば、そのようなパスは $(n-1)$ 桁の値が $n-1$ であるか n 桁の値が n であるかによって特徴づけられるからである (つまりそのようなパスのすべての頂点は安全でない垂直クラスタに含まれている)。容易にわかるように、$\mathcal{T}$ は $2n-3$ $(= n-1+n-2)$ 個の安全でない垂直クラスタを含んでおり、その数は $n \geq 2$ のとき $|\mathcal{T}|$ の半数を超えない。

パスの基本設計

提案手法で構成される s と D の各頂点を結ぶパスは、以下の 3 つのパートから成る：

Part 1: 最初のパートは、s と安全な垂直クラスタとを長さ 2 以下の最短パスで結ぶ (パスの長さが 2 のとき、その中間頂点は安全でない垂直クラスタに属している)。

Part 2: 2 番目のパートは、1 番目のパートの端点と 3 番目のパートの端点とを安全な垂直クラスタ内部で結ぶ。

Part 3: 3 番目のパートは D 中の頂点と安全な垂直クラスタの頂点とを結ぶ。

目的頂点の安全な垂直クラスタへの割り当てを厳密に述べるために、以下のような記法を導入する。M を以下のように定義される $n \times n$ 行列とする:

$$M[i,j] \stackrel{\text{def}}{=} |D \cap TG(i,j)| \text{ for each } i,j.$$

行列 M が長さ 2 の suffix に関する目的頂点の初期分布をあらわしていることに注意されたい。$|D| = f_n$ および $D \subset \bigcup_{i,j} TG(i,j)$ より、$\sum_{i,j} M[i,j] = f_n$ が成立する。与えられた行列 M に対し提案手法は、D から $\mathcal{T}$ への単射をあらわす 0,1 行列 M^* を構成する。$d(i,j) \in D$ を行列 M^* のもとで $TG(i,j)$ に対応付けられた頂点とする (ただし $i = j$ の場合や $TG(i,j)$ に何も割り当てられていない場合には、$d(i,j)$ を NULL とする。M^* が $f_n + n$ 個の 0 と f_n 個の 1 を含むことに注意しよう)。提案手法では、行列 M^* は初期分布 M から以下の 3 つの要件を満たすように構成される：

1) $TG(i,j)$ が安全で $M[i,j] = 1$ であるようなペア (i,j) が存在すれば、$D \cap TG(i,j)$ 中の (唯一の) 頂点が、M^* のもとで $TG(i,j)$ に対応する目的頂点として選ばれること。

2) 安全でない任意の垂直クラスタについて $M^*[i,j] = 0$ であること。

3) s と D を結ぶ以下のような点素なパスの集合が存在すること：任意の $(i',j') \neq (i,j)$ について、s と $d(i,j)$ を $TG(i,j)$ を経由して結ぶパスは、s と $d(i',j')$ を $TG(i',j')$ を経由して結ぶパスと点素であること。

水平クラスタリング

目的地までの点素なパスによる配分 (行列 M^* を実現するような点素なパス) は、以下で述べる水平クラスタリングという考え方を用いることで実現される。頂点 $v \in V_n$ は、その長さ $n-2$ の prefix が以下の操作によって c になるとき、クラス c であるという。

- もし v の $(n-1)$ 桁目が n でなければ、v の n 桁目を (必要であれば)n にし、その後で、$(n-1)$ 桁目を (必要であれば)$n-1$ にする。
- もし v の $(n-1)$ 桁目が n であれば、v の $n-1$ 桁目を (必要であれば)$n-1$ にし、その後で、n 桁目を (必要であれば)n にする。

すなわちクラス c は、$TG(n-1,n)$ 中の頂点 "$c\,n-1\,n$" から以下の手順で得られる頂点たちである：

1. 最初に $(n-1)$ 桁目を変更し、そのあとで n 桁目を変更する。
2. 最初に $(n-1)$ 桁目と n 桁目を交換し、その後で n 桁目を変更する。

ここで T_n にはそのようなクラスが $(n-2)!$ 個あり、各クラスは $2f_n$ 個の頂点から成っていることに注意しよう。以下では頂点 $u \in V_n$ の属しているクラスを $c(u)$ であらわし、$(n-2)!$ 個のクラス全体の集合を $\mathcal{C}$ であらわすことにする。

例 1: T_5 中の頂点 14523 はクラス 123 である。なぜならば、この頂点に $g_{3,5}$ と $g_{2,4}$ を順に適用することで頂点 12345 になるからである。同様に、頂点 14352 もクラス 123 に含まれる。なぜならば、この頂点に $g_{2,3}$ と $g_{2,5}$ を順に適用することで頂点 12345 になるからである。図 2.2を参照されたい。ここで、 各クラスの頂点集合が、対応するジェネレータによって誘導される生成木によって特徴づけられることに注意しよう。

ここで注意しなくてはならないのは、異なるクラスに属する 2 つの頂点が与えられたとき、それらの最後の 2 桁 (長さ 2 の suffix) の変化は、安全でない垂直クラスターを経由した点素なパスによって実現されるということである。すなわち、図 2.2 に示すような二次元配列が各クラスごとに用意され、しかもそれらは互いに素になっている。した

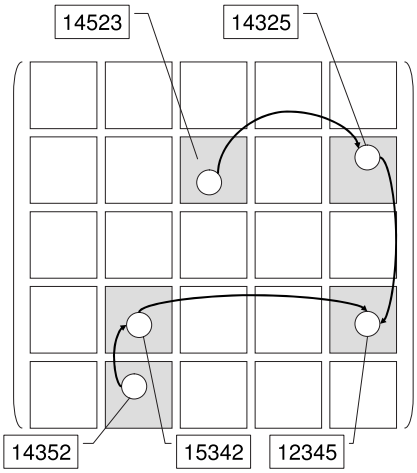


図 2.2: 例 1.

がって、もし D 中の頂点がそれぞれ異なるクラスに属していれば、D 中の各頂点の安全な垂直クラスターへの単射 (割り当て) は、点素なパスによって容易に実現できることになる。具体的には、パスの 3 番目のパートを図に示される生成木に沿ってつくればよい。したがって残る問題は、D 中の頂点にクラスの重複がある場合にどうするか、という点に絞られることになる。

目的頂点のクラス替え

以下では、以下の性質を満たす中間頂点の集合 I ($\subset V_n$) を構成する：1) I 中の各頂点はそれぞれ別のクラスに属していること、2) D と I が互いに素なリンクの集合によって結ばれていること、3) 集合 D が (前節までに述べた)I と s を結ぶパスの集合と共通頂点をもたないこと。これにより、残されていた最後の 1 ホップが実現できる。

D 中の各頂点 u が各垂直クラスタの中で f_{n-2} 個の隣接頂点を持っていたことを思い出そう。そのような隣接頂点の集合を $N'(u)$ とする。頂点 u の隣接頂点から D を除いたものたちの属しているクラスの集合を $C(u)$ とする。すなわち $C(u)$ を

$$C(u) \stackrel{\text{def}}{=} \{c(w) : w \in N'(u) \setminus D\} \cup \{c(u)\}.$$

のように定義する。ここで $N(u) \cap D = \emptyset$ のとき $|C(u)| = f_{n-2}+1$ であることに注意しよう。次に以下のような二部グラフ H を考える：頂点集合が $D \cup \mathcal{C}$ で、頂点 $v \in D$ と頂点 $c \in \mathcal{C}$ は、$c \in C(v)$ のときかつそのときに限り辺で結ばれる。もし H が D 中の頂点をすべて被覆するようなマッチング E を持てば、中間頂点の集合 I を以下のように決定することができる：

- u が $c(u) \in \mathcal{C}$ と E 中の辺で結ばれていれば、u は自分自身を中間頂点とする。
- もし u が $c' \neq c(u)$ と E 中の辺で結ばれていれば、u は $c(v) = c'$ であるような隣接頂点 $v \in N'(u)$ を選び、v を中間頂点とする。

この構成法が上で述べたすべての条件を満たしていることに注意されたい。

以下の定理が得られる。

定理 1 $n \geq 7$ のとき、二部グラフ H が D のすべての頂点を被覆するマッチングをもつか、2つ以上の目的頂点を含むような垂直クラスタが高々 $2n-5$ 個存在するかのいずれか一方が成立する。

証明の基本アイデアは、二部グラフ H が D を被覆するようなマッチングをもつのは、任意の X ($\subseteq D$) に対して X に隣接している頂点数が $|X|$ 以上であるときかつそのときに限られるという、よく知られた性質を利用することである。

マッチングが存在していれば、マッチング中の辺を最後の 1 ホップとして用いることでパスを完成させることができる。一方もしマッチングが存在しなければ、D 中の頂点に対応するクラス数が高々$2n-4$ ($= 2n-5+1$) であり、少なくとも $f_{n-2}+1$ 個の頂点が属しているようなクラス c が存在することから、考慮すべき目的頂点数を f_n から高々$4n-10$ ($= 2(2n-5)$) に削減することができることになる (ちょうどひとつの頂点を含むような垂直クラスタに関しては、クラスの変換を行う必要はない)。

残された頂点のクラス変換は、高々$4n-10$ 個の頂点と $|\mathcal{C}|$ 個の頂点とを結ぶような別の二部グラフ H' をつくることで実現できる。ところが、$n \geq 7$ のとき $f_{n-2}+1 > 2n-4$ であるから、H' 上では、任意の部分集合 X について、X に隣接している頂点数は X 未満ではありえず、したがって、H' には必ずいっぽうの頂点集合を被覆するようなマッチングが存在することになる (つまり、この場合もやはり最後の 1 ホップを何とか実現できることになる)。得られるパスの長さが最短経路よりも高々14 ほど長いことは、構成法から容易に示すことができる。

研究業績一覧

学術論文

1. K. Nakano:
   "An Energy Efficient Ranking Protocol for Radio Networks", IEICE Trans. on Fundamentals, E89-A(5), 1346–1354, 2006 年 5 月
   .
   概要: A radio network (RN for short) is a distributed system with no central arbiter, consisting of n radio transceivers, henceforth referred to as stations. We assume that the stations run on batteries and expends power while broadcasting/receiving a data packet. Thus, the most important measure to evaluate protocols on the radio network is the number of awake time slots, in which a station is broadcasting/receiving a data packet. We also assume that the stations are identical and have no unique ID number, and no station knows the number n of the stations. For given n keys one for each station, the ranking problem asks each station to determine the number of keys in the RN smaller than its own key. The main contribution of this paper is to present an optimal randomized ranking protocol on the k-channel RN. Our protocol solves the ranking problem, with high probability, in $O(\frac{n}{k} + \log n)$ time slots with every station being awake for at most $O(\log n)$ time slots. We also prove that any randomized ranking protocol is required to run in expected $\Omega(\frac{n}{k} + \log n)$ time slots with at least one station being awake for expected $\Omega(\log n)$ time slots. Therefore, our ranking protocol is optimal.

2. J. L. Bordim, Y. Ito, K. Nakano:
   "An Energy Efficient Leader Election Protocol for Radio Network with a Single Tranceiver", IEICE Trans. on Fundamentals, E89-A(5), 1355–1361, 2006 年 5 月.
   概要: In this work we present an energy efficient leader election protocol for anonymous radio network populated with n mobile stations. Previously, Nakano and Olariu have presented a leader election protocol that terminates, with probability exceeding $1 - \frac{1}{f}$ $(f \geq 1)$, in $\log\log n + o(\log\log n) + O(\log f)$ time slots. As the above protocol works under the assumption that every station has the ability to transmit and monitor the channel at the same time, it requires every station to be equipped with two transceivers. This assumption, however, is unrealistic for most mobile stations due to constraints in cost, size, and energy dissipation. Our main contribution is to show that it is possible to elect a leader in an anonymous radio network where each station is equipped with a single transceiver. Quite surprisingly, although every station has only one transceiver, our leader election protocol still runs, with probability exceeding $1 - \frac{1}{f}$ $(f \geq 1)$, in $\log\log n + o(\log\log n) + O(\log f)$ time slots. Moreover, our leader election protocol needs only expected $O(n)$ total awake time slots, while Nakano and Olariu's protocol needs expected $O(n \log\log n)$ total awake time slots. Since every leader election protocol needs at least $\Omega(n)$ awake time slots, our leader election protocol is optimal in terms of the expected awake time slots.

3. J. L. Bordim, T. Hunziker, K. Nakano:
   "Limiting the Effects of Deafness and Hidden Terminal Problems in Directional Communications", Proc. International Symposium on Parallel and Distributed Processing and Application, 195–206, 2006 年 12 月.
   概要: It is known that wireless ad hoc networks employing omnidirectional communications suffer from poor network throughput due to inefficient spatial reuse. Although the use of directional communications is expected to provide significant improvements, the lack of efficient mechanisms

to deal with deafness and hidden terminal problems makes it difficult to fully explore its benefits. The main contribution of this work is to propose a Medium Access Control (MAC) scheme which aims to lessen the effects of deafness and hidden terminal problems in directional communications without precluding spatial reuse. Unlike other proposals that focus on exploring the characteristics of the physical layer, the proposed MAC protocol relies on simple mechanisms that can be easily coupled with a directional antenna without requiring major modifications to the current MAC standard.

4. J. L. Bordim, Y. Ito, K. Nakano:
"Randomized Leader Election Protocols in Noisy Radio Networks with a Single Transceiver", Proc. International Symposium on Parallel and Distributed Processing and Application, 246–256, 2006年12月.

概要: In this work, we present leader election protocols for single-hop, single-channel noisy radio networks that do not have collision detection (CD) capabilities. In most leader election protocols presented so far, it is assumed that every station has the ability to transmit and monitor the channel at the same time, it requires every station to be equipped with two transceivers. This assumption, however, is unrealistic for most mobile stations due to constraints in cost, size, and energy dissipation. Our main contribution is to show that it is possible to elect a leader in an anonymous radio network where each station is equipped with a single transceiver. We first present a leader election protocol for the case the number n of stations is known beforehand. The protocol runs in $O(\log f)$ time slots with probability at least $1 - \frac{1}{f}$ for any $f > 1$. We then present a leader election protocol for the case where n is not known beforehand but an upper bound u of n is known. This protocol runs in $O(\log f \log u)$ time slots with probability at least $1 - \frac{1}{f}$ for any $f > 1$. We also prove that these protocols are optimal. More precisely, we show that any leader election protocol elect a leader with probability at least $1 - \frac{1}{f}$ must run in $\Omega(\log f)$ time slots if n is known. Also, we proved that any leader election protocol elect a leader with probability at least $1 - \frac{1}{f}$ must run in $\Omega(\log f \log u)$ time slots if an upper bound u of n is known.

5. H. Ochi, S. Tagashira, S. Fujita:
"A Localization Scheme for Sensor Networks Based on Wireless Communication with Anchor Groups", IEICE Trans. Inf. & Syst., E89-D(5), 1614–1621, 2006年5月.

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.

6. S. Tagashira, M. Mito, S. Fujita:
"A Generic Solver based on Functional Parallelism for Solving Combinatorial Optimization Problems", IEICE Trans. Inf. & Syst., E89-D(6), 1940–1947, 2006年6月.

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.

7. D. Takemoto, S. Tagashira, S. Fujita:
"A Fault-Tolerant Content Addressable Network", IEICE Trans. Inf. & Syst., E89-D(6), 1923–1930, 2006 年 6 月.
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.

8. 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, J89-A(6), 430–437, 2006 年 6 月.
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、近年新しい展開を見せている。本稿では、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した。

9. S. Fujita:
"Loose Covering by Graphs", 2006 Japan-Korea Joint Workshop on Algorithms and Computation, 9–15, 2006 年 7 月.
概要: This paper introduces a new notion of an embedding of local structure to a global network, defined as a loose covering by graphs. In this paper, we derive several basic properties of the notion including the computational complexity of the problem of finding a loose covering of a given graph by small cycles and paths.

10. H. Kutsuna, S. Tagashira, S. Fujita:
"A Fair and Efficient Congestion Control Scheme Based on Minority Game", Proc. The 14th IEEE International Conference on Networks (ICON '06), 98–103, 2006 年 9 月.
概要: In this paper, we propose a new congestion control scheme for high-speed networks. The basic idea of the scheme is to adopt a game theory called Minority Game (MG) to realize a *selective reduction* of the transmission speed of senders. More concretely, upon detecting a congestion, it plays a game among all senders participating in the communication, and reduces the transmission speed of each sender according to the result of the game. MG is a game that has recently attracted considerable attentions, and it is known to have a remarkable property such that the number of winners converges to a half of the number of players in spite of the selfish behavior of the players. By using such property of MG, we can realize a fair reduction of the transmission speed, which is more efficient than previous schemes in which all senders uniformly reduce their transmission speed. The effect of the proposed scheme is eval-

uated by simulation. The result of simulations indicates that the proposed scheme certainly realizes a selective reduction of the transmission speed, and it is sufficiently fair compared with simple randomized schemes and is sufficiently efficient compared with conventional schemes.

11. K. Kobatake, S. Tagashira, S. Fujita:
"A New Caching Technique to Support Conjunctive Queries in P2P DHT", Proc. IFIP Int'l Conf. on Network and Parallel Computing, 185–190, 2006 年 10 月.
概要: P2P DHT (Peer-to-Peer Distributed Hash Table) is a typical technique to realize an efficient keyword search in pure P2P systems. In this paper, we propose a new caching technique to support conjunctive queries in P2P DHT. The basic idea of the proposed technique is to share a global information on past trials by conducting a local caching of search results for conjunctive queries, and by registering the fact to the global DHT. Such a result caching is expected to significantly reduce the amount of transmitted data compared with conventional schemes. The effect of the proposed method is experimentally evaluated by simulation. The result of experiments indicates that it reduces the amount of transmitted data by 60% compared with conventional P2P DHT.

12. S. Fujita:
"Vertex-Disjoint Paths in Transposition Graphs", Proc. the 18th IASTED Int'l Conf. on Parallel and Distributed Computing and Systems, 490–494, 2006 年 11 月.
概要: A transposition graph is a Cayley graph in which vertices correspond to permutations and edges are placed between permutations that differ by exactly one transposition. In this paper, we propose an algorithm to find a collection of vertex-disjoint paths connecting a given source vertex s and a given set of destination vertices D. The running time of the algorithm is polynomial to the number of destination vertices, and the resultant path connecting s and each destination is longer than the length of a shortest path connecting those vertices by at most fourteen.

13. K. Kobatake, S. Tagashira, S. Fujita:
"Efficient Support of Conjunctive Queries in P2P DHT by using Bloom Filter", Proc. the 18th IASTED Int'l Conf. on Parallel and Distributed Computing and Systems, 202–207, 2006 年 11 月.
概要: P2P DHT (Peer-to-Peer Distributed Hash Table) is a typical technique to realize an efficient keyword search in pure P2P systems. In this paper, we propose a new method to support conjunctive queries in P2P DHT. The basic idea of the proposed method is to cache the result of conjunctive queries to each peer, and to register the fact to the DHT. In addition, in order to reduce the number of meaningless queries to DHT, it registers cached conjunctions to Bloom filter, and circulates it among all peers. The effect of the proposed method is experimentally evaluated by simulation. The result of experiments indicates that by using the proposed method, the amount of returned data reduces to 40%, and the number of queries reduces to 66%, compared with conventional P2P DHT.

14. K. Yasuda, S. Tagashira, S. Fujita:
"Adaptive MAC Scheme for Wireless LAN based on Dynamic Group Constructions", Proc. Int'l Conf. on Parallel and Distributed Computing, Applications and Technologies, 300–305, 2006 年 12 月.
概要: In wireless LAN, several terminals could share a single communication channel by using an appropriate media access control (MAC) mechanism. However, existing MAC schemes for wireless LAN

have serious drawbacks such that it significantly degrades the throughput if it frequently occurs a collision of frames or a useless assignment of communication bandwidth. In this paper, we propose a new MAC scheme for wireless LAN to realize an efficient utilization of the communication bandwidth while suppressing the probability of frame collisions. The basic idea of the scheme is to conduct a channel assignment for each group which is dynamically constructed based on the unique identifier that is assigned to each terminal beforehand. The scheme could be customized by appropriately tuning parameters according to the given communication environment. The effect of the scheme is estimated by simulation. By the result of simulations, it is confirmed that the proposed scheme could achieve a stable performance for any access frequency.

15. M. Yamane, S. Tagashira, S. Fujita:
"An Efficient Assignment of Transmission Opportunity in QoS Guaranteed Wireless LAN", Proc. Int'l Conf. on Parallel and Distributed Computing, Applications and Technologies, 105–108, 2006年12月.
概要: IEEE802.11e standard adopts several important techniques to guarantee the quality of service (QoS) of multimedia communications in wireless LAN. A key technique introduced in the standard is an efficient media access control based on Hybrid Coordination Function (HCF), in which each flow is assigned an appropriate transmission opportunity (TXOP) to satisfy several requirements on the flow such as the delay bound and the communication bandwidth. Although it could provide an efficient tool to guarantee the QoS in wireless LAN, HCF has a serious drawback such that a useless bandwidth assignment frequently occurs, which is primarily due to the limitation of the scheme such that all flows share the same service interval (SI). In this paper, we propose a new scheduling scheme that associates each flow with its own SI according to the hardness of the delay bound. The effect of the scheme is experimentally evaluated by simulation. The result of simulations indicates that the number of admitted flows and the data transmission rate certainly increase by the proposed scheme.

16. A. Ohtsubo, S. Tagashira, S. Fujita:
"A Content Addressable Small-World Network", Proc. Parallel and Distributed Computing and Networks, 551-111, 2007年2月.
概要: In this paper, we study the effect of shortcut links in overlay networks for distributed systems. In particular, we exam ine the effect of shortcuts in Content Addressable Network (CAN) which is known as a typical pure P2P network based on the notion of Distributed Hash Table (DHT). The pro posed scheme is an extension of Kleinberg's method which was originally proposed for the study of small-world net works. The result of simulations indicates that the proposed shortcutting scheme significantly reduces the average num ber of hopcounts in a greedy routing, and the rate of im provement increases as increasing the number of nodes.

17. K. Maruyama, S. Tagashira, S. Fujita :
"A P2P Information Monitoring System Supporting Conjunctive Continual Queries", Proc. Parallel and Distributed Computing and Networks, 551-109, 2007年2月.
概要: In this paper, we propose a P2P information monitoring system to support the processing of conjunctive queries. The proposed system is an extension of PeerCQ, and our main contribution in this paper is the following three points: 1) we provide a detailed speci?cation of Conjunc tive Con-

tinual Queries (CCQs) that is an agent to check the satisfaction of a given conjunction, 2) we propose a map ping of CCQs to peers by considering the similarity of the referred data items, and 3) we improve the utility function used in PeerCQ in such a way that the trade-off between the load of each peer and the overall load of the system can be explicitly controlled. The effect of the proposed method is evaluated by simulation.

研究会等

1. 田頭 茂明, 忽那 寛, 藤田 聡:
“Minority Game を利用した輻輳制御手法の評価”, 情報処理学会システム評価研究会, Vol.2006 No.66, 1–6, 2006 年 6 月.
概要: 本論文では，Minority Game というゲーム理論を転送速度の調節に利用する新しい輻輳制御手法の提案をおこなう．Minority Game は，複雑系などの分野で注目されているゲームのひとつであり，利己的に振舞う参加者間で協調的行動が発現するという特性をもつ．したがって輻輳制御に Minority Game を利用することで，利己的に振舞う送信者間で協調的行動が発現し，効率的なパケット通信が実現されるのではないかと期待される．シミュレーションの結果，提案手法は，従来手法に比べて，公平で高効率な帯域の利用を可能にすることが明らかとなった.

2. 田頭 茂明, 齋藤 美幸, 藤田 聡:
“パッシブ型 RFID を用いた方向検出システム”, 電子情報通信学会モバイルマルチメディア通信研究会, Vol.106, No.161, 25–30, 2006 年 7 月.
概要: 本稿では，リーダの読み取り方向を検出できるパッシブ型 RFID を用いた方向検出システムを提案する．方向の検出には，リーダとタグとの角度が通信範囲に影響を与えるという電磁誘導方式の特性を利用している．具体的には，この電磁誘導方式の特性を利用して，リーダの読めるタグが識別可能な各方向で異なるように複数枚のタグを配置する．方向の検出時には，リーダが読むことができたタグから，リーダの読み取り方向を推定する．提案する方向検出システムのプロトタイプシステムを周波数 13.56MHz 帯のパッシブ型 RFID を用いて実際に作成し，提案方式の性能評価を行った．実験の結果から，提案システムを用いて 8 方向の検出を 9cm 以内で安定してできることがわかった.

3. 徳永 達也, 田頭 茂明, 藤田 聡:
“DART を用いたアドホックネットワークのアドレス空間均等化手法”, 情報処理学会システムソフトウェアとオペレーティング・システム研究会, Vol.2006, No.86, 17–24, 2006 年 7 月.
概要: 本稿では, 大規模アドホックネットワーク向けに設計されたルーティングプロトコル DART（Dynamic Address RouTing）において，アドレス空間の均等化手法を提案する．DART は，動的な階層型アドレッシング手法とシンプルなルーティング手法を提供することにより，大規模ネットワークに対しても効率の良いルーティングを実現している．しかしながら，各ノードがアドレス空間を自律的に割り当てるために，ノード間で割り当てられるアドレス空間に偏りが発生する問題がある．そこで，アドレス空間の偏りを判断し，アドレスの再割り当てをおこなうことでアドレス空間を均等化する手法を提案する．提案手法をシミュレーションにより評価した．その結果，均等化の効果により，提案手法では従来手法よりも経路長を約 10%短くでき，また，経路表のサイズも減少することができた.

4. 圓山 康太, 田頭 茂明, 藤田 聡:
“PeerCQ における効率的な条件付き情報監視手法”, 情報処理学会システムソフトウェアとオペレーティング・システム研究会, Vol.2006, No.86, 1–8, 2006 年 7 月.
概要: 本稿では，PeerCQ に基づいた新しい P2P 型の情報監視システムを提案する．提案システムでは，AND 条件をサポートする情報監視に着目し，そのような情報監視を効率的に実現する枠組みを提供する．具体的には，

AND 条件をサポートするために，PeerCQ に以下の拡張を行った．1) 与えられた AND 条件の成立を確認するエージェントとして，Conjunctive Continual Query(CCQ) を導入し，その詳細な仕様を提供した．2) 監視するデータ項目の類似性を考慮した CCQ のビアへの割り当て手法を提案した，3) 各ビアの負荷とシステム全体の負荷との間のトレードオフを制御できるように，PeerCQ において使われるユーティリティ関数を改良したい提案手法の効果をシミュレーションにより評価した．シミュレーションの結果，提案するユーティリティ関数によりシステムの性能は向上し，性能のトレードオフはパラメータを調整することにより制御できることを示した．

5. XiaoRan Wang, 田頭 茂明, 藤田 聡:
“ノードの Free Degree に基づいた MANET のための適応的ルーティングプロトコルの評価”, 情報処理学会システム評価研究会, Vol.2006 No.89, 9–14, 2006 年 8 月.
概要: 本稿では，リアクティブ型のプロトコルである Dynamic Source Routing (DSR) に着目し，ノードの“ Free Degree ”(FD) の概念に基づいた Free Degree Adaptive Routing (FDAR) プロトコルを提案する．FDAR は，ネットワークの負荷を分散させて，パケットを低遅延で転送するために，ルーティングメトリックとして FD を採用し，混雑している経路を迂回するようにパケットをルーティングする．また，ネットワークトポロジの変更時に必要な経路変更フェーズの過剰な実行を避けるために，寛容な経路変更ポリシーを確立した．FDAR の有効性をシミュレーションにより評価した．評価の結果，FDAR はパケットの転送遅延およびスループットにおいて，DSR より良い性能を示すことを確認した．

6. 田頭 茂明, 小畠 功士, 藤田 聡:
“分散ハッシュテーブル型 P2P システムにおけるブルームフィルタを用いた高速連言検索手法の評価”, 情報処理学会システム評価研究会, Vol.2006 No.89, 15–22, 2006 年 8 月.
概要: 分散ハッシュテーブル型 P2P システム (P2P DHT) は，分散ネットワーク上に存在する共有資源の管理とキーワード検索とをピア・ツー・ピア (P2P) で効率よく実現するための代表的な手法の一つである．本稿では，P2P DHT 上で AND 検索を効率よくサポートするための新しい手法の提案と評価を行う．提案手法では，ブルームフィルタ (Bloom filter) を用いて，各ピアがローカルにキャッシュする過去の検索結果の情報を伝搬し，ピア間でそれらのキャッシュを効果的に共有する．提案手法の有効性を，シミュレーションにより実験的に評価した．実験の結果，システムに対する問合せ回数で約 66%改良できることを確認した．

7. 山内 亮, 田頭 茂明, 藤田 聡:
“ベンディング法を用いたセンサネットワークのためのナビゲーション手法”, 電子情報通信学会情報ネットワーク研究会, Vol.106, No.420, 79–84, 2006 年 12 月.
概要: センサネットワークにおいて，センサが危険を検知した場合，ユーザをそれらの危険から回避させつつ安全な目的地へできるだけ早く導くことができるようなパスを発見するナビゲーションシステムを提案する．これまでに提案されているおもな経路発見アルゴリズムは，折り返し探索法と網羅的な探索法とに大別される．しかしいずれの手法も，危険領域の大きさや形状によっては，得られるパスの長さや通信コストの点で，その性能が大きく劣化する可能性がある．本稿では折り返し法と網羅探索法の長所を併せ持った新しい経路探索アルゴリズムを提案する．提案手法の基本アイデアは，センサで覆われた領域内に複数のチェックポイントを系統的に配置し，それぞれのチェックポイントを通過する経路を並行して探索することである．提案手法の効果はシミュレーションにより実験的に評価される．実験の結果，提案手法は，非常に少ない通信コストで，網羅探索に匹敵するよさのパスを発見することがわかった．

8. 土井 賢治, 田頭 茂明, 藤田 聡:
“ノードの近接性を考慮した P2P DHT の構築手法”, 電子情報通信学会情報ネットワー

ク研究会, Vol.106, No.420, 139–144, 2006 年 12 月.
概要: 分散ハッシュテーブル (Distributed Hash Table: DHT) は，P2P システムにおいてネットワーク上に遍在する資源に対して効率的なアクセスを実現する手法のひとつとして高い注目を集めている．しかし，DHT には P2P オーバーレイネットワーク上のピア間の隣接関係が物理ネットワークにおけるノードの近接性には無関係に決められているという問題がある．本稿では，ピアが DHT に参加する際の手続きにおいて物理ネットワークにおけるノード間の近接性の全体的な関係を考慮できる手法を用いることで，ノードの近接性を考慮した P2P DHT の構築手法を提案する．提案手法の有効性はシミュレーションにより評価される．

9. 田頭 茂明, 安田 健一, 藤田 聡:
"グループの動的形成に基づく無線 LAN のための適応的メディアアクセス制御手法", 電子情報通信学会モバイルマルチメディア通信研究会, Vol.106, No.498, 25–30, 2007 年 1 月.
概要: 無線 LAN においてメディアアクセス制御機構 (MAC) を用いることで，単一の無線通信チャネルを複数の端末間で共有することができる．しかしながら，既存の MAC 手法では，フレーム衝突の発生や不必要な通信帯域の割り当てが問題となり，通信帯域を有効に利用できない状況がある．本稿では，フレームの衝突確率を抑えながら，通信帯域を効率的に利用する無線 LAN のための新しい MAC 手法を提案する．基本的なアイデアは，事前に端末に割り当てた識別子からグループを動的に形成し，各グループに対してチャネルを割り当てていくことである．提案手法は，パラメータを適切に調節することにより，通信環境に応じたチャネル割り当てを行うことができる．シミュレーションの結果から提案手法は安定した性能を達成できることを確認できた．

10. A. Boulenouar, A. Regidor, S. Fujita:
"On Some Computational Aspect of Point Configurations in the Enclidean Space", 情報処理学会アルゴリズム研究会, Vol.2007 No.5, 63–70, 2007 年 1 月.
概要: Given a finite set $S \subset R^m$ in general position and a point $p \in R^m$, we devise an algorithm that checks if $S \cup \{p\}$ is also in general position, and if it is not, given a real number $\epsilon > 0$, finds another point p' within ϵ-distance from p so that $S \cup \{p_1\}$ is in general position. The worst-case running time of our algorithm is $O(n^{m-1} \log n)$, where n is the number of points in S, hence extending [l]'s result in dimension 2 and 3 to higher dimensions

11. W. Liu, S. Tagashira, S. Fujita:
"SwRED: A Robust Active Queue Management Scheme based on Load Level Prediction", 電子情報通信学会情報ネットワーク研究会, 2007 年 3 月.
概要: Active queue management (AQM) is a novel technique to realize a smooth congestion control in communication networks, which is expected to work effectively by combining it with end-to-end congestion control schemes such as the window control adopted in TCP. Although it has been proposed a lot of AQM schemes in the literature, an appropriate tuning of parameters used in those schemes is recoginzed as a challenging problem to be overcome. In this paper, we proposed a new AQM scheme based on a load level prediction of bottleneck links, and on a combination of queue-based and rate-based AQM schemes in multiple time scales. Different from most of conventional AQM schemes, the propoesed scheme, called Switch-RED (SwRED), employs a new packet drop strategy based on a macroscopic analysis of the queue dynamics. The performance of the resultant scheme is evaluated by simulation. The result of simulations indicates that SwRED realizes a more stable queue behavior compared with previous schemes, i.e., it realizes a low queuing delay and a low packet loss

rate while keeping a high link utilization.

12. 杉本 あい, 田頭 茂明, 藤田 聡:
“BitTorrent 型並列ダウンロードシステムにおける効率的なマッチメーキング手法の提案”, 電子情報通信学会情報ネットワーク研究会, 2007 年 3 月.
概要: 本稿では，P2P ネットワークにおいて BitTorrent に基づいた並列ダウンロード手法を提案する．提案手法では，従来手法と同程度のダウンロード性能を維持しながらピース情報の交換コストを削減することを試みる．提案手法の基本的なアイデアは，従来手法におけるピース選択アルゴリズムをローカルなピース情報だけを用いて実現するように改良することである．また，改良によって起こりうるダウンロード時間の増加は，トラッカーで実行されるマッチメーキング手法を新たに導入することで抑制する．

A09: 非明示的表現に対するアルゴリズムの開発

篠原　歩 †　石野　明 †　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,ishino}@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　はじめに

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．

本年度は，まず，XML テキストの高速処理に関する技法に関する技法についての研究を行った．XML は，あらゆるデータをタグ付きのテキスト文字列として行うことによって可搬性と機械可読性を備えた汎用フォーマットとして，広範囲に活用されている．本研究では，与えられた XML テキストを，パストライとバイナリ XML データの対に変換することによって，領域効率と実行速度を向上させることに成功した．また，圧縮されデータを陽に展開することなく，そのままパターン照合を行う，圧縮文字列照合の研究に関して，形式文法に基づく圧縮法に対する効率のよいアルゴリズムを与えた．さらに，文字列中に共通に現れる共通部分文字列を新たな記号に置き換える作業を繰り返す事による圧縮法に関して，線形時間の圧縮アルゴリズムを与えた．一方，文字列に対する索引構造に関して，単語単位の接尾辞木 (suffix tree) や有向文字列グラフ (DAWG), 圧縮有向文字列グラフ (CDAWG) をそれぞれ線形時間で構築する，簡潔なアルゴリズムを開発した．また，種々の文字列処理アルゴリズムに対して，最悪実行時間の解析に活用されることの多いフィボナッチ文字列について，その繰り返し構造に関する組み合わせ的性質を解析した．

2　XML 文書フィルタリングのための軽量な高速化技法

インターネット上のニュース記事や広告等のメディア，日々観測されるセンサー情報や株価表示器など，膨大な量の情報が絶え間なく生成されている．これらの情報を有効に活用するための技術が強く求められている．SDI (Selective Dissemination of Information) は，そのようなサービスの一つであり，日々生成される大量の機械可読文書を購読者が選択的に，かつ，リアルタイムに取得することができる．このような publish/subscribe 型のデータ配送システムは，従来，キーワードや “bag-of-words” に基づくフィルタリングによる比較的単純なものであった．

しかし近年，XML (eXtensible Markup Language) の台頭により，XPath を用いたより高度なフィルタリングが可能となった．XPath は，W3C の勧告による，XML 文書の特定の部分 (要素，属性，テキストなど) を指定するための言語で，事実上の標準となっている．

XML データストリームのフィルタリングに関する研究の初期段階では，DOM 木を用いた手法が主流であった．しかし，DOM 木の構築に多大な時間と主記憶領域を要するため，このような手法では，50–200MB 程度の XML データになると事実上適用不可能である．そこで，近年はストリーム処理に基づくフィルタリング手法が主流になっているストリーム処理とは，XML データを一方向に走査することによって出力を得る方式を指し，DOM 木を用いた方式に比べある一定サイズのバッファしか必要とせず，次々と生成されるデータに

対して即座に対応可能といった特徴をもつ．

代表的な XML データストリーム処理器である YFilter や XMLTK は，非常に高速に XPath を処理できるが，扱う軸は順方向軸 (forward axes) のみと限定している．これに対して，最近では先祖軸 (ancestor axes), 兄弟軸 (sibling axes) にも対応したストリーム処理手法が提案されているが，順方向軸のみに限定した手法に比べ規模耐性，処理速度等を犠牲にしている．本研究で提案する手法は，扱う軸は順方向軸のみで，オートマトンを用いて XML データを走査する点では YFilter や XMLTK と同様であるが，XML データに前処理を施すことによって高速化・軽量化を可能とした点で異なる．

YFilter は，XFilter のパス照合処理を改良したもので，質問式毎に非決定性有限オートマトン (NFA) を構築するのではなく，質問式全体の共通接頭辞パスを共通の状態として束ねたもので，XFilter よりも質問数に関して規模耐性があり，高速に動作する．しかしながら，NFA は同時に複数の状態遷移を処理しなければならないため，決定性オートマトン (DFA) と比較して照合速度は遅い．NFA を等価な DFA に変換すると，一般に状態数が指数的に増大する．そこで，XMLTK では，XML データ走査中に必要に応じて NFA を部分的に DFA に変換する *Lazy-DFA* と呼ばれる手法を採用している．XMLTK は，質問数に関して規模耐性があり高速であるが，一方，DFA の状態数が増大し大量のメモリを必要とするという欠点がある．

本研究では，配信する XML データにあらかじめ簡単な前処理を施しておくことにより，さらなる規模耐性と高速化・省メモリ化を達成する．ここで提案する前処理手法は，XML データをパストライとバイナリ XML データの対に変換する．パストライは，XML データ中の根から葉へ向かうパスに沿って現れるタグ名の列全体を表すトライ構造である．また，バイナリ XML データは，XML データ中の開始タグと終了タグを各々特殊コードで置き換えたもので，開始タグを表すコードの直後に，タグ名を表す番号ではなく，対応するパストライ節点を識別するための番号（以下，パストライ節点番号）を埋め込んでいる．データ送信サーバは，このパストライとバイナリ XML データを対として送信する．データ受信側では，まず，パストライを対象にパス照合を行い，その結果をパストライの節点に付加する．これにより，バイナリ XML データの走査時にはもはやパス照合の必要はなく，バイナリ XML データ中に埋め込まれたパストライ節点番号を頼りにパス照合の結果を参照することが可能となる．通常，パストライは XML データ全体の木に比べて十分小さいため，処理速度は劇的に向上する．この前処理で行うデータの変換は，以下の望ましい性質を有する．

1. 変換に要する時間が極めて小さい．
2. 変換して得られたデータの大きさは，もとの XML データ以下に抑えられる．

さらに，この手法を SIX と併用することで，さらなる高速化が達成できる．

2.1 パストライを用いた高速なフィルタ処理

本研究では，XQuery の部分族をパスプルーニングと DFA を用いて効率的に処理する手法において，入力となる XML データを事前に調べてパストライを得るが，パスパターン照合をデータ走査時に実行するのではなく，質問式を得た段階で完了させておくことによってより高速なフィルタ処理を実現することに成功した．

以下では用語を定義したあと，フィルタ処理に必要な問題を定式化し，本手法のアルゴリズムを紹介する．

定義

Σ を文字の有限集合とし，$\mathcal{N}$ をタグ名から成る集合とする．*XML* **木**とは，$\mathcal{N}$ のタグ名を内部節点のラベルとし，Σ 上の文字列を葉 (テキスト節点) のラベルとするようなラベル付き順序木をいう．

単純パスパターンとは $\mathcal{N}$ のタグ名と特殊な記号 “*” から成る記号列をいい，各々の記号は “/” または “//” で区切られているものとする．ここで，“/” と “//” は，それぞれ，親子関係，先祖-子孫関係に対応する．単純パスパターン π が XML

木のパスに**マッチする**とは，“∗” を任意のタグ名にマッチするワイルドカード，“//” を任意のタグ名列にマッチする可変長ワイルドカードとみなした際に，π がそのパスに沿ったタグ名の列に合致するときをいう．

パスパターンとは単純パスパターン π_1，π_2 の順序対であり，$\pi_1[\pi_2]$ と表す．XML 木の任意の節点 x とその子孫 y（$x = y$ の場合も含む）に対し，パスパターン $\pi_1[\pi_2]$ が**位置** (x, y) **に出現する**とは，π_1，π_2 が，それぞれ，根から x へのパスと x' から y へのパスにマッチするときをいう．ここで，x' は，根から y へ向かうパスに沿った x の子節点である．

$e = e(w_1, \ldots, w_m)$ を，Σ 上の空でない文字列 $w_1, \ldots, w_m$ の生起の有無に関する論理式であるとする．Σ 上のテキスト d が論理式 e を**充足する**とは，d におけるキーワード $w_1, \ldots, w_m$ の生起に対応した真偽値割り当て (truth assignment) のもとで e が真となるときをいう．

XPattern とは，パスパターン $\pi_1[\pi_2]$ と論理式 e の組をいい，$\pi_1[\pi_2 : e]$ と表す．XPattern $\pi_1[\pi_2 : e]$ が XML 木の**節点** x **に出現する**とは，x の子孫 y が存在して，パスパターン $\pi_1[\pi_2]$ が位置 (x, y) に出現し，かつ，y の子であるテキスト節点の少なくとも一つが e を充足するときをいう．この定義より，パスパターン $\pi_1[\pi_2]$ は，XPattern $\pi_1[\pi_2 : \mathbf{true}]$ と見なすことができる．図 2.1に，XPattern $\pi_1[\pi_2 : e]$ とその生起位置 (x, y) との関係を図示した．

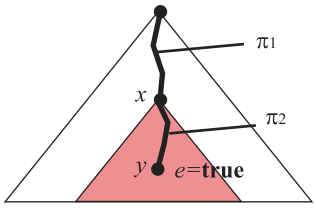


図 2.1: XML 木の位置 (x, y) における XPattern $\pi_1[\pi_2 : e]$ の生起．

本研究では，以下の問題に取り組む．

定義 1
Given: *XML* データ T.
Query: *XPattern* $P_1, \ldots, P_\ell$.
Answer: 各 $i = 1, \ldots, \ell$ に対し，T に対応する *XML* 木において P_i が生起する節点 x を返せ．

ここで，入力として与えられる XML データ T は，複数の XML 文書の系列（XML 木の系列）となっていることを仮定している．なお，フィルタリング問題では，該当の XML 文書が質問に合致するかどうかだけを考えればよいため，上の定義で節点 x を求める必要はないように見える．しかし，複数の XPattern を組み合わせた複雑な質問を処理するためには，このような節点 x を求めることが必要である．

パストライとバイナリデータ

本手法では XML データに対して一度だけ前処理を行い，パストライと，バイナリ XML ファイルを作成する．XML データと前処理によって作成されるパストライ及びバイナリ XML データとの関係を図 2.2に示す．

この前処理に要する時間は $O(n \log |\mathcal{N}| + |T|)$ であり，表 2.2に示すとおり高速な処理が可能である．ここで，n は XML データ T 中の開始タグの個数を表し，$|\mathcal{N}|$ はタグ集合の要素数を，$|T|$ は XML データのサイズを表す．また，XML データと生成されるデータサイズの関係を表 2.1, 2.2 に示す．このことから，パストライは，XML 木に対して十分に小さく，バイナリ XML データに関しても入力ファイルサイズの 76%と小さくなっていることが分かる．

バイナリ XML データについては，開始タグを表す特殊記号の直後に，タグを表す番号ではなく，根からのパスに沿ったラベルの列を表すパストライ節点番号を埋め込むことに注意されたい．このことによって，パスパターン照合はパストライを対象としたパターン照合を行うだけで良く，パストライが XML データに比べ非常に小さいため，高速に処理を完了することが可能となる．

表 2.1: DBLP と xmlgen によってランダムに生成された入力 XML データの大きさ．

	XML データ		
	サイズ (MB)	節点数	タグ数
DBLP	352	8,632,812	35
random	111	1,666,310	74

表 2.2: 前処理で構築されるバイナリ XML データとパストライのサイズ及びその構築時間.

	バイナリ XML ファイル	パストライ	CPU 時間
	サイズ (MB)	節点数	(sec)
DBLP	208	138	100.41
random	84	515	73.26

パスパターンの照合

本研究では，XML 木に対するパスパターン照合の問題を，パストライに対するパスパターン照合に置き換える．

図 2.2で示した XML データを例にとり，XML 木中，および，パストライ中におけるパスパターン $P = \mathrm{a//b[//d]}$ の生起の様子を図 2.3に示した．この例では，パスパターン $P_1 = \mathrm{a//b[//d]}$ は XML 木中の位置 $(x, y) = (4, 5), (6, 8), (6, 10), (9, 10)$ で生起している．一方，パストライ中においては，生起位置は $(x, y) = (2, 5), (2, 7), (6, 7), (2, 4)$ である．そこで，パストライ中の生起位置 (x, y) の節点 y にパスパターンの番号と節点 x, y の深さの差の情報を付加する．すると，XML 木中の生起位置は，パストライに付加された情報から得ることができる．

次に，パストライに対するパスパターン照合の手法について述べる．質問式に含まれる各パスパターンに対し，パストライ中の出現位置 (x, y) をすべて求めなければならない．このために，各パスパターンから非決定有限オートマトン (NFA) をそれぞれ作成し，それらをパストライ中を深さ優先で巡回させることにより照合を行う．NFA の実装にはビット並列化手法を用いる．多くの場合，各 NFA の状態数がワード長である 32（あるいは 64）以内に収まるため，非決定的な状態遷移を並列に高速に処理することが可能となる．また NFA の構築も極めて高速である．これら二つの NFA を用いて，パストライ中を深さ優先で巡回し，パスパターン $P_i = \pi_1[\pi_2]$ の出現位置 (x, y) をすべて求める．出現位置 (x, y) がみつかる度に，節点 y に出力 $\langle P_i, d\rangle$ を付加する．ここに，d は節点 x, y の深さの差である．

本手法を用いることで，バイナリ XML データ走査時のパスパターン照合処理は不要となり，XML データ走査時にパスパターンの照合を行っている YFilter や XMLTK と比べ，処理時間を大幅に短縮することができる．

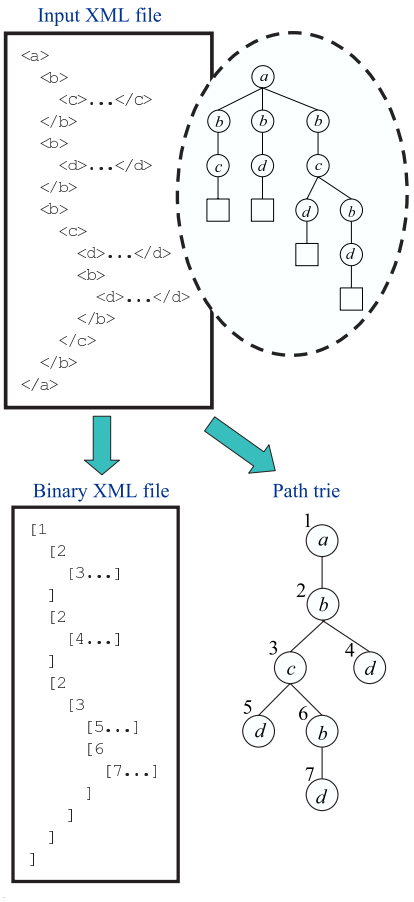


図 2.2: XML データに対して行う前処理の様子を図示した．XML データと対応する XML 木を上側に示した．正方形はテキスト節点を表す．この XML データから作成されるバイナリ XML データとパストライを，それぞれ，左下と右下に示した．パストライの節点の傍にある数は，その節点の ID である．バイナリ XML データにおいて，開始タグと終了タグは，それぞれ，特殊記号 “[” と “]” に置き換えられ，“[” の直後にはパストライの節点 ID が埋め込まれていることに注意しよう．

キーワード照合

パスパターン照合は，フィルタリング問題の一部に過ぎない．XPath の仕様から明らかなように，述語はパス以外に，テキストデータや属性，ポジションを含むことができる．このうち，テキストデータや属性は，/a/b[@month=December], /a/b[containts(name, “mickey”)] などのように記

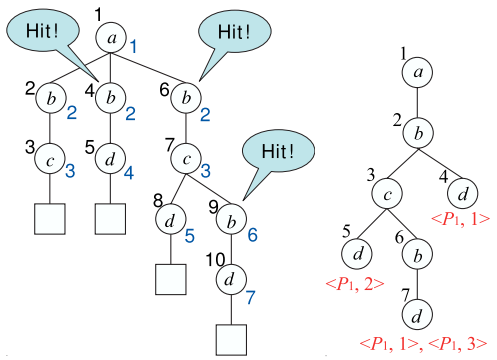


図 2.3: パスパターン P_1 = a//b[//d] は図左の XML 木の位置 (x, y) = $(4,5),(6,8),(6,10),(9,10)$ に生起している．これらの位置は，図右に示したパストライの節点に付加された情報から得ることができる．たとえば，XML 木中の位置 $(6,8)$ における P_1 の生起は，パストライの節点 5 のもつ出力 $\langle P_1, 2\rangle$ から得ることができる．すなわち，バイナリ XML データ中において，XML 木の節点 $y = 8$ に対応する箇所にはパストライ節点番号 5 が埋め込まれており，パストライの節点 5 に付加された情報 $\langle P_1, 2\rangle$ によって，y から 2 つ上の先祖である節点 $x = 6$ が得られる．

述され，前者はパス/a/b の属性値が December であること，後者は/a/b/name のテキスト節点に，キーワード “mickey” があることを調べるときに用いられる．

フィルタリングにおいてこのような問い合わせの処理を考えるとき，XML データ中のすべてのテキスト節点における複数キーワードの出現を求める問題として捉えることができる．著者らは，この問題に対して古典的手法である Aho-Corasick(AC) 法を用いた．AC 法は同時に複数キーワードの照合を行うことができ，キーワード数の増加に伴うテキスト走査速度の低下は特にない．また，索引を用いる方法では，キーワード毎に出現するテキストの番号のリストを求め，ブール式に応じた集合演算を行うが，AC 法で複数のキーワードを同時に照合する場合には，テキスト節点毎にブール演算を行えばよいため，集合演算のために領域・時間を消費しないという利点もある．フィルタリングにおいては，大量の質問式から集めたキーワードの総数は膨大なものになり得るため，これらの利点のもつ意義は大きい．

バイナリ XML データ走査アルゴリズム

バイナリ XML データを走査してキーワード照合を行い，その結果とパスパターン照合の結果を結合して質問処理を行うアルゴリズムの概略を以下に示す．

与えられた XPattern $P_1, \ldots, P_\ell$ の論理式 e 中に含まれるキーワードからなる集合を $W = w_1, \ldots, w_m$ とする．W から AC 機械 M を構築する．バイナリ XML ファイル先頭からの位置を表す変数 $depth$ と，入力を XML 木として見たときの節点の深さを表す変数 $depth$ を用意する．ブール値を格納する 2 次元配列 Occ と Q を用意する．配列 Occ は，現在巡回している深さ d の節点の子であるテキスト節点にキーワード w_i が生起するときに $Occ[d][i]$ の値が真となるというものであり，配列 Q は，現在巡回している深さ d の節点に XPattern P_q が出現するときに $Q[d][q]$ の値が真となる．本アルゴリズムは，バイナリ XML ファイルを 1 バイトずつ走査し，読み込んだバイト c に対して以下を実行する．

- c が開始タグを表す特殊記号 “[” であるとき．パストライ節点番号 v を読み込み，$(v, depth)$ をスタック S にプッシュする．$depth$ を 1 インクリメントする．$Occ[depth][1 \ldots m]$ と $Q[depth][1 \ldots l]$ を偽に初期化する．M の状態を初期状態に設定する．
- c が終了タグを表す特殊記号 “]” であるとき．スタック S より $(v, depth)$ をポップする．もしパストライのノード v が出力をもっていたら，それぞれの $\langle q, d\rangle$ に対して，XPattern P_q の論理式 e を，$Occ[depth][1 \ldots m]$ の値に基づいて計算し，もし e が真ならば，$Q[depth - d][q]$ を真と設定する．$depth$ を 1 デクリメントする．M の状態を初期状態に戻す．
- c がそれ以外のバイトコードであるとき．M を文字 c で状態遷移させる．もし遷移先の状態が出力をもつならば生起したキーワードに対応して $Occ[depth][1 \ldots m]$ を更新する．

実験の詳細については，本報告からは割愛するが，パストライがフィルタ処理の高速化に寄与することを示し，本手法が YFilter や XMLTK と比較して高い性能を有することわかった．

3　文字列の繰り返し構造の解析

隣接 2 項の漸化式で定義される**フィボナッチ数列**は，

$$\Phi_0 = 1, \quad \Phi_1 = 2,$$
$$\Phi_m = \Phi_{m-1} + \Phi_{m-2} \quad (m \geq 2)$$

である．漸化式 $\Phi_m = \Phi_{m-1} + \Phi_{m-2}$ から導かれる特性方程式 $x^2 = x+1$ の正の実数解 $(1+\sqrt{5})/2$ は**黄金比**として知られており，ϕ と表記される．また，これは**フィボナッチ定数**とも呼ばれ，フィボナッチ数の隣接 2 項の比の極限がこの値と等しくなる．

フィボナッチ数列は隣接 2 項の数の和で生成されるが，これを文字に置き換え，次のように隣接 2 項の文字列の連結として生成される文字列がフィボナッチ文字列 F_m である．

$$F_0 = \mathtt{a}, \quad F_1 = \mathtt{ab}, \quad F_m = F_{m-1}F_{m-2} \quad (m \geq 2).$$

よって，任意の $m \geq 0$ について $|F_m| = \Phi_m$ となる．フィボナッチ文字列の初めの数項は次のようになる．

$$F_2 = \mathtt{aba},$$
$$F_3 = \mathtt{abaab},$$
$$F_4 = \mathtt{abaababa}.$$

また，文字列 w における部分文字列 u の繰り返し（連続出現），および繰り返し数を次のように定義する．文字列 u，v，w が

$$w = uu...uv = u^k v \quad (v \text{ は } u \text{ の接頭辞})$$

であり，$k \geq 2$ であるとき，文字列 w は u の繰り返しであるといい，

$$e = \frac{|w|}{|u|} = k + \frac{|v|}{|u|}$$

を文字列 u の繰り返し数という．

フィボナッチ数は自然現象のあらゆるところに出現し，面白い性質を示すことが知られている．フィボナッチ文字列も部分文字列のグラフ化問題や組み合わせ問題等においてさまざまな性質を持つことが知られている．そのひとつとして，Knuth-Morris-Pratt アルゴリズムや Boyer-Moore アルゴリズム，Aho-Corasick アルゴリズムといった文字列のパターンマッチングアルゴリズムにおいて最悪の入力インスタンスとなることが知られている．特に，Knuth-Morris-Pratt アルゴリズムでは，マッチングに失敗したときにキーワードの何文字目と照合すればよいかという情報を用いて再照合を行うが，キーワードの長さを z としたとき，この再照合の回数が高々$\log_\phi z + 1$ 回であることが証明されている．

Mignosi と Pirillo は無限フィボナッチ文字列中における m 番目の有限フィボナッチ文字列の最大繰り返し数について，無限フィボナッチ文字列中に $2+\phi \approx 3.618$ 回を超える部分文字列の繰り返し出現はないことを証明した [1]．

本研究では，隣接 n 項の文字列を連結したものとして定義される n-ボナッチ文字列と n-ボナッチ定数 $\phi^{(n)}$ との関連を明らかにした．フィボナッチ文字列の場合 $n = 2$ となり，その最大繰り返し数の極限は $2 + \phi^{(2)}$ である．では，$n > 2$ における一般的な最大繰り返し数の極限はどのように表現されるだろうかが興味の対象となる．フィボナッチ文字列の場合ではフィボナッチ定数 $\phi^{(2)}$ がそのままの形で現れたので，直感的には $2 + \phi^{(n)}$ となりそうであるが，実際には $2 + 1/(\phi^{(n)} - 1)$ となることを本研究で示した．特に $n = 2$ のとき，$\phi^{(2)} = 1/(\phi^{(2)} - 1)$ であり，これは Mignosi と Pirillo の結果と一致する．

ϵ を空文字とする．文字列 u_0， u_1， u_2， ... の連結を，整数 i， j を用いて次のように表現する．

$$u_{[i\nearrow j]} = \begin{cases} u_i u_{i+1} u_{i+2} ... u_{j-1} u_j & (i \leq j) \\ \epsilon & (i > j), \end{cases}$$

$$u_{[i\searrow j]} = \begin{cases} u_i u_{i-1} u_{i-2} ... u_{j+1} u_j & (i \geq j) \\ \epsilon & (i < j). \end{cases}$$

さらに，$u_i u_{i+1} u_{i+2} ...$ のように文字列を無限に連結してできる文字列を $u_{[i\nearrow\infty]}$ と表す．

n-ボナッチ数は次のように定義される．

$$\Phi_0^{(n)} = 1,$$

$$\Phi_m^{(n)} = \begin{cases} \sum_{i=0}^{m-1} \Phi_i^{(n)} + 1 = 2^m & (1 \le m < n), \\ \sum_{i=m-i}^{m-1} \Phi_i^{(n)} & (m \ge n). \end{cases}$$

これを元に，n-ボナッチ文字列を次のように定義する．

定義 2 n を 2 以上の整数とし，アルファベット $\Sigma = \{\sigma_1,\ \sigma_2,\ \sigma_3,\ \ldots,\ \sigma_n\}$ とする．次の漸化式で定義される文字列を **n-ボナッチ文字列**という．

$$F_0^{(n)} = \sigma_1,$$

$$F_m^{(n)} = \begin{cases} \epsilon & (n < 0), \\ F^{(n)}_{[m-1 \searrow 0]} \sigma_{m+1} & (0 < m < n), \\ F^{(n)}_{[m-1 \searrow m-n]} & (m \ge n). \end{cases} \tag{2.2}$$

例 1 $n = 3$ のとき，アルファベット $\Sigma = \{\mathtt{a},\ \mathtt{b},\ \mathtt{c}\}$ とすると，

$$F_0^{(3)} = \mathtt{a},$$
$$F_1^{(3)} = F_0^{(3)}\mathtt{b} = \mathtt{ab},$$
$$F_2^{(3)} = F_1^{(3)}F_0^{(3)}\mathtt{c} = \mathtt{abac},$$
$$F_m^{(3)} = F_{m-1}^{(3)}F_{m-2}^{(3)}F_{m-3}^{(3)} \quad (m \ge 3).$$

となる．また，初めの数項は以下のようになる．

$$F_3^{(3)} = \mathtt{abacaba},$$
$$F_4^{(3)} = \mathtt{abacabaabacab},$$
$$F_5^{(3)} = \mathtt{abacabaabacababacabaabac}.$$

これはトリボナッチ文字列とも呼ばれる． ■

n-ボナッチ数と n-ボナッチ文字列には，$\left|F_m^{(n)}\right| = \Phi_m^{(n)}$ という関係がある．また，無限 n-ボナッチ文字列 $F_\infty^{(n)}$ も定義でき，全ての有限 n-ボナッチ文字列を接頭辞として持っている．

例 2 $n = 3$ のとき，無限トリボナッチ文字列は次のようになる．

$$F_\infty^{(3)} = \mathtt{abacabaabacababacabaabacabacabaab}\ldots$$

■

定理 1 $m - k \ge n + 1$ および $n \ge 2$ を満たす任意の m，n，k において，$F_m^{(n)}$ 中に出現する $F_k^{(n)}$ の最長の連続出現は $F_k^{(n)}F_k^{(n)}F_k^{(n)}G_{k-n+1}^{(n)}$ である．

定理 2 $m - k \ge n + 1$ および $n \ge 2$ を満たす任意の m，n，k において，$F_m^{(n)}$ 中の $F_k^{(n)}$ の最大繰り返し数の極限は $2 + 1/(\phi^{(n)} - 1)$ である．

定理 3 整数 n，$k \to \infty$ のとき，n-ボナッチ文字列 $F_k^{(n)}$ の最大繰り返し数はちょうど *3* に近づく．

参考文献

[1] F. Mignosi and G. Pirillo. Repetitions in the Fibonacci infinite word. *RAIRO Theoret. Inform. Appl.*, 26:199–204, 1992.

研究業績一覧

学術論文

1. Shunsuke Inenaga and Masayuki Takeda: “On-line Linear-time Construction of Word Suffix Trees”, Proc. 17th Annual Symposium on Combinatorial Pattern Matching (CPM’06), LNCS 4009, 60–71, 2007 年 7 月.

概要: Suffix trees are the key data structure for text string matching, and are used in wide application areas such as bioinformatics and data compression. Sparse suffix trees are kind of suffix trees that represent only a subset of suffixes of the input string. In this paper we study word suffix trees, which are one variation of sparse suffix trees. Let D be a dictionary of words and w be a string in D^+, namely, w is a sequence $w_1 \ldots w_k$ of k words in D. The word suffix tree of w w.r.t. D is a path-compressed trie that represents only the k suffixes in the form of $w_i \ldots w_k$. A typical example of its application is word- and phrase-level search on natural language documents. Andersson et al. proposed an algorithm to build word suffix trees in $O(n)$

expected time with $O(k)$ space. In this paper we present a new word suffix tree construction algorithm with $O(n)$ running time and $O(k)$ space in the worst cases. Our algorithm is on-line, which means that it can sequentially process the characters in the input, each by each, from left to right.

2. Shunsuke Inenaga and Masayuki Takeda:
"Sparse Compact Directed Acyclic Word Graphs", Proc. Prague Stringology Conference 2006, 195–211, 2006 年 8 月.
概要: The suffix tree of string w represents all suffixes of w, and thus it supports full indexing of w for exact pattern matching. On the other hand, a sparse suffix tree of w represents only a subset of the suffixes of w, and therefore it supports sparse indexing of w. There has been a wide range of applications of sparse suffix trees, e.g., natural language processing and biological sequence analysis. Word suffix trees are a variant of sparse suffix trees that are defined for strings that contain a special word delimiter #. Namely, the word suffix tree of string $w = w_1 w_2 \dots w_k$, consisting of k words each ending with #, represents only the k suffixes of w of the form $w_i \dots w_k$. Recently, we presented an algorithm which builds word suffix trees in $O(n)$ time with $O(k)$ space, where n is the length of w. In addition, we proposed sparse directed acyclic word graphs (SDAWGs) and an on-line algorithm for constructing them, working in $O(n)$ time and space. As a further achievement of this research direction, this paper introduces yet a new text indexing structure named sparse compact directed acyclic word graphs (SCDAWGs). We show that the size of SCDAWGs is smaller than that of word suffix trees and SDAWGs, and present an SCDAWG construction algorithm that works in $O(n)$ time with $O(k)$ space and in an on-line manner.

3. Yasuto Higa, Hideo Bannai, Shunsuke Inenaga, and Masayuki Takeda:
"Reachability on Suffix Tree Graphs.", Proc. Prague Stringology Conference 2006, 212-225, 2006 年 8 月.
概要: We analyze the complexity of graph reachability queries on ST-graphs, defined as directed acyclic graphs (DAGs) obtained by merging the suffix tree of a given string and its suffix links. Using a simplified reachability labeling algorithm presented by Agrawal et al. (1989), we show that for a random string of length n, its ST-graph can be preprocessed in $O(n \log n)$ expected time and space to answer reachability queries in $O(logn)$ time. Furthermore, we present a series of strings that require $\Theta(n\sqrt{n})$ time and space to answer reachability queries in $O(\log n)$ time for the same algorithm. Exhaustive computational calculations for strings of length $n \leq 33$ have revealed that the same strings are also the worst case instances of the algorithm. We therefore conjecture that reachability queries can be answered in $O(\log n)$ time with a worst case time and space preprocessing complexity of $\Theta(n\sqrt{n})$.

4. Shunsuke Inenaga and Masayuki Takeda:
"Sparse Directed Acyclic Word Graphs", Proc. 13th International Symposium on String Processing and Information Retrieval (SPIRE'06), LNCS 4209, 61–73, 2006 年 10 月.
概要: The suffix tree of string w is a text indexing structure that represents all suffixes of w. A sparse suffix tree of w represents only a subset of suffixes of w. An application to sparse suffix trees is composite pattern discovery from biological sequences. In this paper, we introduce a new data structure named sparse directed acyclic word graphs (SDAWGs), which are a sparse text indexing version of directed acyclic word graphs (DAWGs) of Blumer et

al.We show that the size of SDAWGs is linear in the length of w, and present an online linear-time construction algorithm for SDAWGs.

5. Yasuto Higa, Shunsuke Inenaga, Hideo Bannai, and Masayuki Takeda:
"A New Family of String Classifiers Based on Local Relatedness", Proc. 9th International Conference on Discovery Science (DS'06), LNAI 4265, 114–124, 2006 年 10 月.
概要: This paper introduces a new family of string classifiers based on local relatedness. We use three types of local relatedness measurements, namely, longest common substrings (LCStr's), longest common subsequences (LCSeq's), and window-accumulated longest common subsequences (wLCSeq's). We show that finding the optimal classier for given two sets of strings (the positive set and the negative set), is NP-hard for all of the above measurements. In order to achieve practically efficient algorithms for finding the best classifier, we investigate pruning heuristics and fast string matching techniques based on the properties of the local relatedness measurements.

6. Shirou Maruyama1 , Hiromitsu Miyagawa1 and Hiroshi Sakamoto:
"Improving Time and Space Complexity for Compressed Pattern Matching", Proc. of The 17th International Symposium on Algorithms and Computation (ISAAC 2006), LNCS 4288, 484–493, 2006 年 12 月.
概要: The compressed pattern matching problem is to find all occurrences of a given pattern in a compressed text. In this paper an efficient grammar-based compression algorithm is presented for the compressed pattern matching. The algorithm achieves the worst-case approximation ratio $O(g_* \log g_* \log n)$ for the optimum grammar size g_* with an input text of length n. This upper bound improves the complexity of the compressed pattern matching problem to $O(g_* \log g_* \log m + \frac{n}{m} + m^2 + r)$ time and $O(g_* \log g_* \log m + m^2)$ space for any pattern shorter than m and the number r of pattern occurrences.

7. Ryosuke Nakamura, Hideo Bannai, Shunsuke Inenaga, and Masayuki Takeda:
"Simple Linear-Time Off-Line Text Compression by Longest-First Substitution", Data Compression Conference '07, 123–132, 2007 年 3 月.
概要: We consider grammar based text compression with longest first substitution, where non-overlapping occurrences of a longest repeating substring of the input text are replaced by a new non-terminal symbol. We present a new text compression algorithm by simplifying the algorithm presented in {S. Inenaga, T. Funamoto, M. Takeda, and A. Shinohara, Linear-time off-line text compression by longestfirst substitution, Proc. SPIRE'03}. We give a new formulation of the correctness proof introducing the sparse lazy suffix tree data structure. We also present another type of longest first substitution strategy that allows better compression. We show results of preliminary experiments comparing grammar sizes of the two versions of the longest first strategy and the most frequent strategy.

8. Hayato Kobayashi, Tsugutoyo Osaki, Eric Williams, Akira Ishino, and Ayumi Shinohara:
"Autonomous Learning of Ball Trapping in the Four-legged Robot League", RoboCup 2006: Robot Soccer World Cup X, 掲載予定.
概要: This paper describes an autonomous learning method used with real robots in order to acquire ball trapping skills in the four-legged robot league. These skills in-

volve stopping and controlling an oncoming ball and are essential to passing a ball to each other. We first prepare some training equipment and then experiment with only one robot. The robot can use our method to acquire these necessary skills on its own, much in the same way that a human practicing against a wall can learn the proper movements and actions of soccer on his/her own. We also experiment with two robots, and our findings suggest that robots communicating between each other can learn more rapidly than those without any communication.

研究会等

1. 御手洗秀一，石野　明，竹田　正幸:
“XML 文書フィルタリングのための軽量な高速化技法”, 電子情報通信学会データ工学ワークショップ論文集, L5-4, 2007 年 3 月.
概要: XML データに極めて単純な前処理を施すことで，質問数の増大に頑健な XML フィルタリング方式を開発した．その手法は，データ配信側で XML データを事前に走査し，根から葉へ向かうパスに沿ったタグ名の列全体を表すパストライと，XML 文書中の開始タグと終了タグを特殊な記号で置き換えたバイナリ XML データを作成する．開始タグを表すコードの直後には，タグを表す番号ではなく，対応するパストライ節点の番号を埋め込む．データ受信側では，このパストライとバイナリ XML データを受け取るものとする．質問式に現れるパスパターンの照合は，パストライを対象として行う．パストライは XML データに比べ非常に小さいため，高速に処理を完了することが可能である．パスパターンの照合結果はバイナリ XML データ走査時に参照することができ，これをテキスト節点を対象としたキーワード照合の結果と結合させることで質問処理は完了する．代表的なストリーム型 XML プロセッサである XMLTK との比較において，実行速度で 4〜6 倍高速であり，メモリ使用量は 1/6 程度であることが判明した．

2. 奥山　哲郎，Masayoshi Sugimoto，大崎　嗣豊，石野　明，篠原　歩:
“ロボカップ４足サッカーロボットのためのファジィ論理を用いた意思決定エンジン”, 人工知能基本問題研究会, SIG-FPAI-65, 65–70, 2007 年 3 月.
概要: In this paper, we introduce a decision engine for autonomous robots in RoboCup fourlegged robot league. The whole system is a platform which can be used for all programs which need a decision process between numerical entries and a set of actions. Robots are particularly appropriate to use a decision process because they have to choose a motion accordingly to their environment. We have implemented the decision engine in agent players. The rules for the decision engine are quite simple and rapid to construct compared to our previous if-then-rule-based system. In this way, each developer can create and improve behaviors solely.

学会大会等

1. 畑瀬　卓司，大橋　健士郎，下薗　真一:
“幾何点列近似照合を用いたタンパク質二次構造近似検索の実現”, 火の国情報シンポジウム 2007, B-2-4, 2007 年 3 月.

2. 里中　政儀，下薗　真一:
“SQL による評価関数の外部定義が可能な最適時間割作成システム”, 火の国情報シンポジウム 2007, C-2-5, 2007 年 3 月.

3. ミュラ アーノルド，下薗 真一，篠原 武:
“空間索引を用いたバイナリプログラムの高速照合”, 火の国情報シンポジウム 2007, C-5-3, 2007 年 3 月.

4. 今村 安，伸市来亮，二宮大輔，下薗　真一，篠原　武:
“文字列編集距離の成分分解を用いた類似文

字列検索辞書の実現”, 火の国情報シンポジ
ウム 2007, C-5-4, 2007 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，移動系における経路最適化問題，オンライン環境における経路最適化問題，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，グラフ有向化の頂点出次数最適化問題，時間割作成最適化問題に関して，それぞれの最適化モデルとしての定式化，結果概要について述べる．

2 移動系における経路最適化問題

概要． 巡回セールスパーソン問題 (TSP) は，計算機科学の分野で古くから知られる問題の一つである．行商人は入力として与えられる都市をすべて巡回して出発位置に戻ってこなければならないが，その時通った道のりの総和をできるだけ小さくしたい．TSP については多くの研究成果が知られておりいまだに活発な研究対象である．本研究課題では，TSP を動的な環境へ拡張した，すなわち巡回対象が都市のように静止しておらず移動している問題である移動物体回収問題を扱っている．これまでに得られた研究成果については，電子情報通信学会・2007 年 3 月号において解説記事として掲載された (学術論文 [8]).

2.1 はじめに

以下のジョブ・スケジューリング問題を考える．ジョブの集合を $J_1, \ldots, J_n$ とする．ここで, ジョブ

J_i の実行にかかるコスト $c_i(t,j)$ は実行開始時刻 t と J_i の直前にスケジュールされるジョブ J_j から決まるものとする．任意の i,j,t に対して $c_i(t,j) = c_j(t,i) = d_{ij}$ (d_{ij} は正の定数) とすると，実行にかかる総コストを最小化する問題は有名な NP-困難問題の一つである巡回セールスパーソン問題 (TSP) である．コスト $c_i(t,j)$ が i と j だけでなく実行開始時刻 t にも依存する場合は，都市の位置が時刻に依存して変わる TSP 問題に対応し，Moving TSP と呼ばれている．

Moving TSP でモデル化される事例をいくつか見てみよう．自然な例としては配送経路を最適化する問題がある．ただし，経路の混み具合は時刻に依存して変化するので (配送時間のような) コストは時刻に依存する．例えば，工場内に複数のベルトコンベアがあり，その上を製品が流れているとしよう．欠陥のある製品を発見したときに，ベルトコンベアを止めずにロボットを用いて欠陥製品を回収することにした．このとき，与えられた欠陥製品の集合を最小時間で回収する問題は Moving TSP でモデル化できる．壮大な事例が好きならば，宇宙ステーション間を宇宙船で行商する行商人を考えることもできる．

Moving TSP ではコストは有限であると仮定されている．しかし，時刻に依存してコストが無限大になるような事例も考えられるだろう．たとえば，デッドラインが決まっている場合である．このような場合には，すべてのジョブを実行するための総コストを最適化する問題と共に (以前に)，有限コストで実行可能なジョブ数を最大化する問題が重要になってくる．このような問題の一つに本研究課題で扱っている移動物体回収問題がある．

移動物体回収問題を詳しく説明する．n 個の移動物体が座標平面上に存在し，それぞれの経路と速さは事前に与えられる．移動ロボット R によりこれらの物体を回収する．ここで，R と物体 b が同じ時刻に同じ点に存在したら R が b を回収したと考える．物体がすべて停止しており，かつ R は全方向に移動可能という条件下では TSP と同じ問題になる．つまり，移動物体回収問題は TSP を拡張した問題であり一見して難しそうである．

先に述べたようにデッドラインが決まっている場合や，R の速さが物体よりも遅い場合には，すべての物体を回収できないかもしれない．そのため，R の移動能力や物体の経路の条件により 2 種類の問題設定がある：(i) できるだけ早くすべての物体を回収 (総コストを最小化) することが目的の時間最小化と，(ii) できるだけ多くの物体を回収することが目的の回収数最大化．(i) は TSP に対する単純かつ自然な拡張であるが，(ii) は R の移動能力に対する制約を設けることで，問題の本質が大きく異った状況になる．以降では，本研究課題で得られた (ii) に関する研究成果 (学術論文 [5]，[9]) を簡単にまとめる．(i) については例えば文献 [1, 2, 3] を参照されたい．

2.2 アルゴリズムの性能評価

移動物体回収問題を解くアルゴリズムは，移動物体の初期配置，経路，速さの情報を用いて R の行程 (まずどの点に移動して，次はどの点に移動して…というスケジュール) を決定する．R の行程を求めることを，単に「解く」と言うことにする．計算機で実行することを想定しているので，アルゴリズムの性能評価のための指標の一つは，物体の個数 n に対してどの程度の時間で R の行程を決定できるか (実行時間と呼ぶ) である．いい加減に説明すると「ほぼ n^2 に比例する時間で決定できる」ということを 「$O(n^2)$ 時間で実行できる」などと言う．注意して欲しいのは，アルゴリズムの実行時間とは R の行程を計算機で求めるために必要な時間であり，R の回収作業自体にかかる時間ではない点である．

上で「指標の一つ」と断った理由を述べる．例えば，TSP に対して理論的に最良な行程を得るのは非常に困難である．専門的には「NP 困難である」と言うが，NP 困難な問題に対しては n の多項式程度の時間 (多項式時間) で解く方法が知られていない．例えば 2^n 程度の指数時間かければ解けたりするのだが，そのようなアルゴリズムを計算機上に実装すると，n が数百程度になると非現実的な時間がかかってしまうことになる．

アルゴリズムの性能評価のためのもう一つの指標について説明する．NP 困難な問題に対する一つのアプローチとして近似アルゴリズムがある．これは，最良の行程は求められないかもしれないが，多項式時間で実行できる．もちろん，余りにも悪い行程を求めてもしょうがないので，近似度

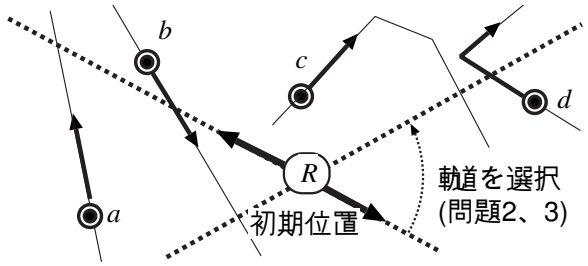


図 2.1: (問題 1) ロボット R は直線軌道上を移動し，物体 (a, b) も直線上を移動．(問題 2) R の軌道を選択．(問題 3) 1 個回収するたびに R は初期位置に戻り軌道を再選択．(問題 4) 物体 (c, d) が折れ線上を移動．

による性能保証がついていることが多い：理論的に最良な行程の値を OPT，アルゴリズムが出力した行程の値を A としたときに，OPT/A が常に r 以下であるとき，このアルゴリズムは近似度 r であるという．ここで行程の値とは回収した物体の個数になる．例えば近似度 2 のアルゴリズムは，回収できる物体数の理論的最大値の半分以上を回収できる行程を出力する．

2.3 回収数最大化

回収数最大化を目的とする，4 つの問題設定とそれぞれに関する研究成果について紹介する．問題 1 と 2 については学術論文 [5]，問題 3 と 4 については学術論文 [9] による．それぞれの問題設定を図 1 に簡単に図示する．

問題 1: R は 1 本の固定された直線 (軌道) 上を往復し，物体はそれぞれ別の直線上を一定の速さで移動する．

結果：すべての物体を回収するには，軌道を通過する時刻の小さい順に物体を整列し，その通過位置に R が随時移動すればよい．軌道が直線に制限されているため全部を回収できないかもしれないが，全部回収できるかを判断し，可能な場合にはその行程を求めるアルゴリズムは $O(n \log n)$ 時間で実行できる．すべての物体を回収できない時は，物体間の関係をうまくモデル化することで最大個数回収する行程を求めるアルゴリズムを構築でき，その実行時間は $O(n^2)$ である．また工夫により，$O(n \log n)$ 時間で実行できるアルゴリズムも構築できる．

問題 2: 問題 1 では固定されていた軌道を R は自由に選ぶことができる．軌道を決めれば，その軌道を用いて最大個数回収する行程は問題 1 の方法で得られるので，できるだけ多くの物体を回収できる軌道を求めたい．

結果：R の初期位置を通る直線すべてが軌道の候補になり無限に存在しそうである．しかし実は，n^2 個程度の直線を調べれば最大個数を回収できる軌道を発見でき，結果として R の行程を $O(n^3 \log n)$ 時間 ($n^2 \times n \log n$ 程度) で求めることができる．さらに工夫することで，$O(n^2 \log n)$ 時間で実行できるアルゴリズムも構築できる．

問題 3：R は物体を 1 個回収するたびに初期位置に戻る必要がある．ただし，先の 2 つの問題と異り，初期位置に戻るたびに R は軌道を回転できる．R の速さは物体よりも遅く，物体の経路は問題 1，2 と同様に直線とする．

結果：初期位置に戻ってくる時刻に関する貪欲法，すなわち未回収物体中で最も早く原点に戻ってこれるものから順に回収するアルゴリズムで最大個数の回収ができる．その実行時間は単純な実現方法だと $O(n^2)$ であるが，工夫により $O(n \log n)$ に減らすことができる．

問題 4：物体の経路として直線ではなく折れ線を考える．それ以外は問題 3 と同様．

結果：直感的には直線の場合よりも，折れ線の方が難しそうに思える．本当に難しいのかが興味の 1 つであるが，各物体が 1 回以上曲がると NP 困難になる．問題 3 で説明した貪欲法と同じ方針のアルゴリズムが近似度 2 であり，その実行時間は $O(mn^2)$ である．ここで m は最もたくさん曲がる物体の，その曲がる回数である．

文献

[1] P. Chalasani, R. Motowani, and A. Rao, “Approximation algorithms for robot grasp and delivery,” Proc. International Workshop on Algorithmic Foundations of Robotics, pp.347-362, 1996.

[2] M. Hammar and B.J. Nilsson, “Approximation results for kinetic variants of TSP,” Lecture Notes in Computer Science, vol.1644, pp. 392-401, 1999.

[3] C.S. Helvig, G.Robins, and A.Zelikovsky, “The moving-target traveling salesperson problem,” J. Algorithms, vol.49, no.1, pp.153-174, 2003.

3 オンライン環境における経路最適化問題

概要． オンライン環境における経路最適化問題とは，探索者が未知のグラフの全ての頂点を訪問することによりグラフ構造を調査する問題である．探索者は辺の存在とその長さをその端点を訪れるまで判らないとする．探索者は，できるだけ短い経路を通ることにより全ての頂点と辺を調査して，出発点まで戻って来なければならない．本研究課題では，このオンライン環境における経路最適化問題に対するオンラインアルゴリズムの設計とその競合比解析を行い，得られた研究成果については，第 33 回 Conference on Current Trends in Theory and Practice of Informatics (SOFSEM 2007) において公表を行った (学術論文 [6]).

3.1 はじめに

TSP は，オペレーションズ・リサーチや組合せ最適化の分野において最も有名な問題の一つである．TSP では，頂点数，辺の長さ，頂点の隣接関係・ネットワーク構造などの入力例題の完全な環境・情報が予め与えられており，それらを TSP の巡回者が巡回経路を決定するときに利用することができる．巡回者の目標は，それらの完全情報を利用して，移動距離を最短にするような経路を発見することである．しかし，このような**オフラインモデル** では実世界の問題を表現できない場合がある．すなわち，多くの経路選択問題やスケジューリング問題では，経路決定を行うための環境に関する全体情報が前もっては与えられずに，不完全な一部の情報のみが**オンライン**に与えられる場合がある．

上のような未知の環境で最適解を求めるオンライン経路選択問題は，**探索問題** (exploration problem) や**地図作成問題** (map construction) として知られている [1]．本稿では，次のようなグラフ上での地図作成問題を考える．本問題は，文献 [3] において，Kalyanasundaram と Pruhs によって定式化された問題である．探索者 (他の応用においては巡回者，ロボット，またはエージェントと呼ばれることがある) ができるだけ短い経路を移動することにより，未知の環境の完全な地図を構成することを考える．多くの場合に，この未知の環境は重み付きグラフ G で形式化することができる．探索者はある特定の出発点から地図作成を始める．探索者が頂点 v を訪問するとき，v を端点とする辺とその辺によって隣接する頂点までの距離情報を得る．頂点の個数や頂点間の隣接関係を知らないため，環境全体を調べるためには，探索者はすべての頂点を少なくとも一度は訪れなければならない．探索者は十分に多くの情報を記憶することができると仮定する．これにより，既に訪問した頂点やその頂点を端点とする辺を再び調べたときには，既に訪問済みであることが判るとする．従って，すべての頂点を訪問したことを知ることができ，探索者は最後に出発点に戻って来る．オンラインアルゴリズムの評価には**競合比**を用いる [2]．競合比は，すべての頂点を訪問し最後に出発点に戻って来る巡回経路の中で最短の経路の移動距離と，オンラインアルゴリズムが出力する出発点まで戻って来る巡回経路の移動距離の比の最大値である．

オンラインアルゴリズムの最初には，出発点のみが訪問済みであり，他の頂点は未訪問である．次のステップでは，出発点に隣接する頂点の中から 1 つの頂点が選ばれ，探索者は選択した頂点に移動する．アルゴリズムが進むに従って，既知となるグラフ構造が大きくなっていく．すなわち，アルゴリズムのあるステップで実行しなければならないことは，それまでに得られた知識を利用することによって，訪問済みの領域に隣接する未訪問頂点の中から，どの新しい頂点に移動すべきであるかを決定することである．最も単純な戦略の 1 つは，最近傍アルゴリズム (NN) である．NN は常に探索者の現在の位置から最も近い頂点を選択する．ただし，頂点の数を n とすると平面グ

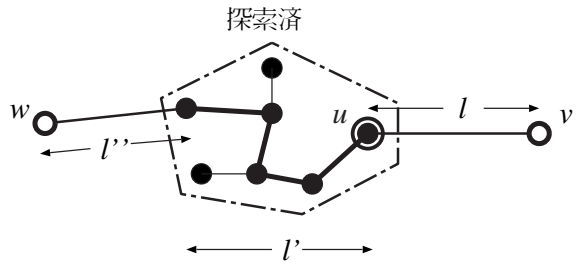


図 2.2: 重み付き最近傍アルゴリズム

ラフにおいて競合比は $\Omega(\log n)$ まで大きくなることが知られている [4]．他の戦略としては，深さ優先アルゴリズムが有名であるが，サイクルグラフに対してさえ競合比が非常に大きくなってしまう．本問題に対する最初の競合アルゴリズムは，Kalyanasundaram と Pruhs により提案された [3]．彼らは，*ShortCut* と呼ばれる重み付き最近傍アルゴリズム (WNN) を提案し，平面グラフに対して ShortCut アルゴリズムの競合比が 16 になることを示した．

WNN は固有の正定数 Δ の値に従って動作する．すなわち，WNN は Δ を用いた重み付き距離を用いて，次に訪問すべき頂点を決定する．図 2.2を用いてアイデアを説明する．探索者が，ある時点で，頂点 u にいるとする．また，頂点 v は，長さが ℓ であるような辺 (u, v) により頂点 u に隣接していると仮定する．さらに，他にまだ訪問していない新しい頂点 w を訪れるために，既に通ったことのある長さ ℓ' の経路と頂点 w を端点とする長さが ℓ'' の辺を通らなければならないと仮定する．重み付き最近傍戦略に従って動作するとき，探索者は $\Delta\ell \leq \ell' + \ell''$ ならば頂点 v を訪れ，そうでなければ，頂点 w を訪れる．上述の平面グラフに対する 16 競合比は，$\Delta = 3$ とすることによって得られる．すなわち，平面グラフの場合には，目前の新しい未訪問の頂点に貪欲的に進むよりも，以前通った経路を逆戻りして新しい未訪問頂点に行くことを優先するという戦略により，良い競合比を得られるということを意味している．

3.2 結果

入力グラフ G がもし木であるならば深さ優先アルゴリズムによって最適な経路を得ることができることは容易に分かる．しかし，もし入力がサイクルを持つグラフであるならば，この問題は単純ではなくなる．本稿では，WNN をサイクルグラフに適用することにより，WNN の能力を調べることを目的とする．本稿の結果は以下である．

- NN (すなわち，$\Delta = 1$ とした WNN) は 1.5 競合アルゴリズムである．
- NN の競合比が 1.5 となるようなサイクルグラフが存在し，我々の 1.5 競合比の解析は厳密である．
- WNN の中で，重みを $\Delta = 1$ とおくことが最適である．すなわち，Δ の値を $\Delta > 1$ または $0 < \Delta < 1$ とすると，WNN の競合比は少なくとも 1.5 となる．
- 任意の決定性オンラインアルゴリズムは，1.25 よりも小さい競合比を持たない．

文献

[1] P. Berman. On-line searching and navigation. In *Online Algorithms: The State of the Art* (Fiat and Woeginger Ed., Springer), pp.232–241 (1998)

[2] A. Fiat and G.J. Woeginger. Competitive analysis of algorithms. In *Online Algorithms: The State of the Art* (Fiat and Woeginger Ed., Springer), pp.1–12 (1998)

[3] B. Kalyanasundaram and K.R. Pruhs. Constructing competitive tours from local information. *Theoretical Computer Science* **130**, pp.125–138 (1994)

[4] D.J. Rosenkrantz, R.E. Stearns, P.M. Lewis. An analysis of several heuristics for the traveling salesman problem. *SIAM J. Computing* **6** (3), pp.563–581 (1997)

4 データ分類におけるバンプハンティング

概要． 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．本研究課題で得られた研究成果については，第 3 回 International Conference on Cybernetics and Information Technologies (学術論文 [2])，IEICE Transactions on Information and Systems (学術論文 [3])，第 6 回 Hawaii International Conference on Statistics, Mathematics and Related Fields (学術論文 [7]) で公表を行った．

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

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．

さらに，上で述べた方法により得られた結果の精度について詳しく調べた．ここでは，テストサンプル法とブートストラップ法のメリットを併せ持つ方法を提案することができた．

5 ブロック転送問題に対するオフライン計算モデル

概要． 本研究課題では次のようなグラフのレイアウト問題の一種を考える．入力として有向非巡回グラフ (DAG) が与えられたとき，DAG 上の根から葉までのすべての道を見て，その外部有向辺数の最大値を最小にするように，それぞれのノードをサイズが高々B であるブロックに分割することを目標とする．ここで，外部有向辺とは異なるブロックに属すノード間の有向辺とする．本問題は一般的には NP 困難となり，B の値が 2 で DAG の高さが 3 の場合にも NP 困難のままであることを示すことができる．本研究課題では，$B = 2$ で DAG の高さが 2 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た．この多項式時間アルゴリズムを利用することにより，DAG の高さが一般のときに，$B = 2$ の場合には，$\frac{3}{2}$ 近似アルゴリズムが存在し，近似精度保証の観点からこの $\frac{3}{2}$ の近似率は最適であることを示した．これまでに知られた近似率は 2 であった．また，$B \geq 3$ の場合にも，$P \neq NP$ と仮定すると，任意の正数 ε に対して，$\frac{3}{2} - \varepsilon$ 近似アルゴリズムが存在しないことを示した．さらに，$B = 3$ の場合，入力グラフを階層グラフに限定すると，2 近似アルゴリズムが存在することを示した．これらの研究成果については，第 6 回 International Conference on Algorithms and Complexity (CIAC 2006) において公表を行った (学術論文 [1])．

6 グラフ有向化の頂点出次数最適化問題

概要． 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 [1]．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 [2]．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．

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．

以下の研究成果は，International Journal of Foundation of Computer Science に掲載されることが決まっている (学術論文 [10])．

- 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．

文献

[1] H.E. Robbins, “A theorem on graphs with an application to a problem of traffic control,”

[2] V. Chvátal and C. Thomassen, “Distances in orientation of graphs,” *J. Combinatorial Theory, series B* **24** (1978) 61–75.

7　時間割作成最適化問題

概要．本稿で取り扱う問題は，大学における時間割作成問題 (timetabling problem) の一つで，試問予定表作成問題と呼ぶ．本問題では，発表する学生 1 人に付き 3 人の先生が発表を審査している状況を考える．それぞれの先生は複数の学生の審査をするように予め担当学生が決められている．例年は，1 つの会場で論文発表を行っていたが，昨年度は，論文発表を行う学生数が増えたため，2 つの会場で行う必要があった．このときに，審査を行う先生が 2 つの会場を移動することが無いようにスケジュールする必要が出て来た．そのため，先生がなるべく会場を移動せずに発表の採点がスムーズに出来るようにしたい．このような背景から試問予定表作成問題が生まれた．現実に扱われる問題をモデルにしているため，実用性の高い問題である．

試問予定表作成問題に対して試問スケジュールを作成する際には，いずれの先生も同時刻に審査を担当する学生が割り当てられることが無いようにする必要があり，この条件を満たす試問スケジュールを正当なスケジュールと呼ぶことにする．試問予定表作成問題は，学生の試問会場の割り当てに対して，試問する先生の会場移動回数を最小化するような正当なスケジュールを求めることを目的としたコスト最小化問題である．

ここで，先生の移動回数を考慮しなければ，正当なスケジュールを求めること自体は簡単であることに注意しておく．すなわち，正当なスケジュールが存在するならば，それを求めるのは多項式時間で計算可能である．これは，頂点を学生として，その学生を審査する先生が異なるような学生に対応した頂点の間に辺を張ったグラフを考え，このグラフの最大マッチングを求めれば良い．最大マッチングは多項式時間で求めることが可能であり，得られたマッチングが完全マッチング (ただし，頂点数は偶数の場合) であれば，それが一つの正当なスケジュールになっている．

本稿で考える試問予定表作成問題では，先生の移動回数を尺度とした最適化問題を考え，本問題の計算複雑さの解明を目標とする．試問予定表作成問題を考える第一ステップとして，2 つの制約条件を与える．一つ目は，学生の発表時刻は入力

のスケジュールから変わらず，同時刻に割り当てられた 2 人の学生の発表会場の交換のみを行うという制約である．この制約により定義された問題を，Room 問題と呼ぶ．2 つ目は，会場の交換は行わず，発表時刻のみを入れ替える制約である．このとき，入力スケジュールでの同時刻の学生ペアは，出力スケジュールでも同時刻でペアにならなければならない．この制約により定義された問題を，Order 問題と呼ぶ．いずれの問題においても，ある先生が，同時刻に異なる部屋において異なる学生を審査するようなことが無いような正当な初期入力割り当てが与えられた場合には，スケジュールの正当性を考慮する必要はない．

本稿では，Room 問題と Order 問題の計算複雑さについて考える．まず，それぞれの先生が担当する学生の数は s 以下であり，それぞれの学生を担当する先生の数は t 以下であると仮定する．このように制限した Room 問題を Room(s,t) 問題とする．Order(s,t) 問題についても同様の制限を加えた問題であるとする．

Room$(1,t)$ と Order$(1,t)$ は各先生の担当する学生が 1 人のみであるので，多項式時間で解くことが出来るのは明らかである．本研究課題の主要な研究成果は以下であり，第 6 回 International Conference on the Practice and Theory of Automated Timetabling (PATAT 2006) において公表を行った (学術論文 [4]).

- Room$(2,1)$ は，クラス $\mathcal{P}$ に属する．
- Room$(2,2)$ は $\mathcal{NP}$ 困難である．よって，$s \geq 2$ かつ $t \geq 2$ について Room(s,t) も $\mathcal{NP}$ 困難となる．
- $s \leq 2$ かつ $t \geq 1$ について Order(s,t) はクラス $\mathcal{P}$ に属する．
- Order$(3,1)$ もクラス $\mathcal{P}$ に属する．

最適化問題の一つにスケジューリング問題がある．スケジューリングとは，複数の仕事があるときに，どういう順番で仕事を進めればもっとも早く仕事が終了するか，あるいは都合が良いかなど，その最適な仕事を行う順番を求める問題のことを言う．スケジューリング問題は，最適解を見つけるようなプログラムを作っても膨大な計算時間を必要とするため，一般的に難しい問題に分類される．また，スケジューリング問題の中で特に実際の場面で頻繁に見られる問題として，授業の時間割を決める問題や，従業員の勤務表作成問題などの時間割作成問題がある．時間割作成問題は，教育機関や，医療施設，交通機関，スポーツの試合など，応用範囲は幅広い．

教育機関における時間割作成は，学校の授業時間割作成，大学のコースや試験の日程や時間割決定などにおいて用いられている [4]．例えば，De Werra は学校の時間割作成問題の枠組みを与え [1]， Junginger は，ドイツにおける時間割作成問題の研究について報告している [2]．また，Petrovic や Burke らによって，大学の講義や試験の予定表作成問題が調査されている [3]．このような多くの時間割作成問題では，担当教員や教室配置といった，多くのスケジュールや制約条件を考慮しなければならないため，非常に困難な問題であり，大学における時間割作成問題は，40 年以上も研究され続けている重要な研究課題である．

文献

[1] D. deWerra, “ An introduction to timetabling, ” European J. Operational Research, Vol.19, No.2, pp.151.162, 1985.

[2] W. Junginger, “ Timetabling in Germany - a survey, ”Interfaces, Vol.16, pp.66.74, 1986.

[3] S. Petrovic and E. Burke. “ University Timetabling, ”Handbook of Scheduling: Algorithms, Models, and Performance Analysis. Josepy Y-T.Leung(Ed.), Chapman and Hall/CRC, 2004.

[4] A. Schaerf, “ A survey of automated timetabling, ”Artificial Intelligence Review, Vol.13, No.2, pp.87.127, 1999.

研究業績一覧

著書

1. 牛島和夫編著，相利民，朝廣雄一著:
“離散数学 (コンピュータサイエンス教科書シリーズ)”, コロナ社, 2006 年 8 月.
概要: 本書は，計算機科学・情報工学の基礎である離散数学を扱った教科書であり，学部生対象の講義での利用を目的としている．教科書本体は概念・定義や定理そのものの説明に重点をおいており，定理の証明や演習問題の解答は付録 CD- ROM にて提供されている．本書は全 4 章構成であり，各章の内容は次の通りである: 第 1 章：集合論，第 2 章：代数系，第 3 章：数理論理，第 4 章：グラフ理論.

学術論文

1. 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, Vol.3998, pp.272–283, 2006 年 5 月.
概要: The paper studies the following variant of clustering or laying out problems of graphs: Given a directed acyclic graph (DAG for short), 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 generally, and to remain intractable even if $B = 2$ and the height of DAGs is three. In this paper we provide a $\frac{3}{2}$ factor linear time approximation algorithm for $B = 2$, and prove that the $\frac{3}{2}$ ratio is optimal in terms of approximation guarantee. 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 restricted to a set of layered graphs.

2. Hideo Hirose, Takahiro Yukizane, Eiji Miyano:
“Boundary Detection for Bumps Using the Gini’s Index in Messy Classificatin Problems”, Proceedings of the 3rd International Conference on Cybernetics and Information Technologies, Systems and Applications, pp.293–297, 2006 年 7 月.
概要: Suppose that we are interested in classifying the points into two groups giving 0-1 responses in z-dimensional space which corresponds to z explanation variables. So far a lot of classification tools which adopt the misclassification rate to evaluate how well the discrimination be achieved have been proposed and played a key role in the field of statistical learning or data mining. In the real world, however, we often encounter the cases that the misclassification rate remains considerably high no matter how carefully we search for the discriminating boundaries if we want to capture the points to some extent with rather simpler rules. In such a messy case, the optimization criterion in classification goes to obtaining the larger number of points of response 1, we are interested in, with a specified pureness rate. Such a region is called to be a bump or a hotspot. Our primary objective is to find the bumps. To use the information of the boundaries of the bumps with ease, it would be beneficial that the bumps have much simpler shapes of their boundaries such as the z-dimensional box located parallel to some explanation variable axes. The problem raised is, however, how to find such a boundary for some bump. The decision tree algorithms find the splitting point for an ex-

planation variable to construct much purer sub-regions using the entropy or the Gini's index criterion, from the top node to the bottom leafs step by step. Regarding that to produce the purer regions is just the same as to exclude those regions, this splitting criterion may also be applicable to produce the denser region for response 1 including response 0 points to some extent. This paper deals with this point. Mimicking the real data case in a customer database of a correspondence course in Japan, we investigate the fundamental data cases such that the marginal distributions for response 1 are rather simple shaped, such as monotonic or unimodal, and those for response 0 is almost uniformly distributed. The unimodal and monotonic cases are studied by using the normal distributions located at the center of and on the corner of the uniform distributions, respectively. Under such restricted conditions, we have found that the Gini's index can detect the boundaries for the bumps as if eyes of human beings do so.

3. Takahiro Yukizane, Shin-ya Ohi, Eiji Miyano, Hideo Hirose:
"The Bump Hunting Method Using the Genetic Algorithm with the Extreme-Value Statistics", IEICE Transactions on Information and Systems, Invited Papers from New Horizons in Computing, Vol.E89-D, No.8, pp.2332–2339, 2006年8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 under a specified ratio of the number of the 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 a 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 also guarantees the accuracy of the semi-optimal solution with the simple descriptive rules. This combined method of genetic algorithm search and extreme-value statistics use is new. We apply this method to some artificial messy data case which mimics the real customer database, showing a successful result. The reliability of the solution is discussed.

4. Yuuki Kiyonari, Eiji Miyano, Shuichi Miyazaki:
"Computational Complexity Issues in University Interview Timetabling", Proceedings of the 6th International Conference on the Practice and Theory of Automated Timetabling, pp.448–453, 2006年8月.
概要: This paper introduces a new timetabling problem on universities, called interview timetabling. In this problem, some constant number, say, three, of referees are assigned to each of $2n$ graduate students. It requires to assign these students to an $n \times 2$ array, consisting of n timeslots and two rooms, so that two students sharing the same referee must be assigned to different timeslots. Furthermore, we want to mini-

mize the total number of movements of all referees between two rooms. This is a problem actually having arisen in the interview timetabling in Kyoto University. We propose two restricted models of this problem, and investigate their time complexities.

5. Yuichi Asahiro, Takashi Horiyama, Kazuhisa Makino, Hirotaka Ono, Toshinori Sakuma, Masafumi Yamashita:
"How to Collect Balls Moving in the Euclidean Plane", Discrete Applied Mathematics, Vol.154, No.16, pp.2247–2262, 2006年11月.
概要: In this paper, we study how to collect n balls moving with a fixed constant velocity 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; (iii) minimizing the number of the robots to collect all n balls. The situations considered in this paper 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.

6. Yuichi Asahiro, Eiji Miyano, Shuichi Miyazaki, Takuro Yoshimuta:
"Weighted Nearest Neighbor Algorithms for the Graph Exploration Problem on Cycles", Proceedings of the 33rd Conference on Current Trends in Theory and Practice of Informatics, Lecture Notes in Computer Science, Vol.4362, pp.164–175, 2007年1月.
概要: In the graph exploration problem, a searcher explores the whole set of nodes of an unknown graph. The searcher is not aware of the existence of an edge until he/she visits one of its endpoints. The searcher's task is to visit all the nodes and go back to the starting node by traveling as a short tour as possible. One of the simplest strategies is the nearest neighbor algorithm (NN), which always chooses the unvisited node nearest to the searcher's current position. The weighted NN (WNN) is an extension of NN, which chooses the next node to visit by using the weighted distance. It is known that WNN with weight 3 is 16-competitive for planar graphs. In this paper we prove that NN achieves the competitive ratio of 1.5 for cycles. In addition, we show that the analysis for the competitive ratio of NN is tight by providing an instance for which the bound of 1.5 is attained, and NN is the best for cycles among WNN with all possible weights. Furthermore, we prove that no online algorithm is better than 1.25-competitive.

7. Hideo Hirose, Shin-ya Ohi, Takahiro Yukizane:
"Assessment of the Prediction Accuracy in the Bump Hunting Procedure", Proceedings of the 6th Hawaii International Conference on Statistics, Mathematics and Related Fields, pp.1–23, 2007年1月.
概要: In a series of the previous study (Hirose 2005a, Hirose 2005b, Hirose et. al. 2006a, Yikizane et. al. 2006), we have developed a bump hunting method using probabilistic and statistical methods, where we are interested in finding denser regions for response 1 among regions for responses 0 and 1 mixed under a condition that the pureness rate is pre-specified; the pureness rate is the ratio of the number of response 1 to the number of responses 0 and 1 in the target region. A global maximum capture rate is estimated by using lo-

cally obtained maximum captured response 1 points, where the capture rate is the ratio of the number of response 1 to the number of responses 0 and 1 in the region defined. The accuracy of the estimated maximum capture rate was assessed by using the simple bootstrap method without correction formula. We have not thought seriously of the bias and the variance to the predicted estimate. However, we are now aware of that we should treat the value of the predicted estimate very carefully. In the previous study, we have dealt with all the data as the training data or the learning data. As is well-known in machine learning world, the best fitted model using the training data would not necessarily be accurate when the test data are used. A typical research in assessing the misclassification error in classification problems is reported by Kohavi (1995), and a more general explanation is found in the literature (Hastie, et. al. 2001), where the test sample method, the cross-validation, and the bootstrap method are often used to assess the accuracy of the predicted estimate and the model. It is recommended to take into account this kind of assessment to our problem too. However, difficulties lie on the bump hunting method that we have proposed because we are interested in not only estimating the maximum capture rate but also in finding the corresponding (binary decision) rule to capture the points of response 1. Since we consider that the rule should also capture a large amount of response 1 points to the future data, a combination of the maximum capture rate and the corresponding rule becomes important. In the example in the previous study, however, we have found that the optimized rule to capture the maximum points for response 1 to the training data did not necessarily capture a large amount of response 1 points to the test data. In this paper, we show first how badly the optimality collapses to the test data. We then discuss how to circumvent this kind of difficulty.

8. 朝廣雄一，小野廣隆，宮野英次，山下雅史:
“移動物体回収問題”，電子情報通信学会誌, Vol.90, No.3, pp.245–247, 2007 年 3 月.
概要: 巡回行商人問題 (TSP) は，計算機科学の分野で古くから知られる問題の一つである．行商人は入力として与えられる都市をすべて巡回して出発位置に戻ってこなければならないが，その時通った道のりの総和をできるだけ小さくしたい．TSP については多くの研究成果が知られておりいまだに活発な研究対象である．本記事では，TSP を動的な環境へ拡張した，すなわち巡回対象が都市のように静止しておらず移動している場合を扱う，移動物体回収問題についての理論的な研究成果を紹介する．

9. Yuichi Asahiro, Eiji Miyano, Shinichi Shimoirisa:
“Grasp and Delivery for Moving Objects on Broken Lines”, Theory of Computing Systems, (掲載予定).
概要: This paper studies the following variant of the Vehicle Routing Problem that we call the *Grasp and Delivery for Moving Objects (GDMO)* 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 one product and then delivers it to the depot. 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 GDMO is MAXSNP-hard, and (ii) it can be approximated with ratio 2. However, (iii) if we impose the “straight line without bend” re-

striction on the motion of every product, then the GDMO becomes tractable.

10. Yuichi Asahiro, Eiji Miyano, Hirotaka Ono, Kouhei Zenmyo:
"Graph Orientation Algorithms to Minimize the Maximum Outdegree", International Journal of Foundation of Computer Science, (掲載予定).
概要: This paper studies the problem of orienting all 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, and (ii) the input graph is a tree. Then, by using those algorithms as subprocedures, 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.

11. Yuichi Asahiro, Jesper Jansson, Eiji Miyano, Hirotaka Ono, Kouhei Zenmyo:
"Approximation Algorithms for the Graph Orientation Minimizing the Maximum Weighted Outdegree", Proceedings of the 3rd International Conference on Algorithmic Aspects in Information and Management, (掲載予定).
概要: Given an undirected graph $G = (V, E)$ and a weight function $w : E \to \mathbb{Z}^+$, we consider the problem of orienting all edges in E so that the maximum weighted outdegree among all vertices is minimized. In this paper (1) we prove that the problem is strongly NP-hard if all edge weights belong to the set $\{1, k\}$, where k is any integer greater than or equal to 2, and that there exists no pseudo-polynomial time approximation algorithm for this problem whose approximation ratio is smaller than $(1 + 1/k)$ unless P=NP; (2) we present a polynomial time algorithm that approximates the general version of the problem within a factor of $(2 - 1/k)$, where k is the maximum weight of an edge in G; (3) we show how to approximate the special case in which all edge weights belong to $\{1, k\}$ within a factor of $3/2$ for $k = 2$ (note that this matches the inapproximability bound above), and $(2 - 2/(k + 1))$ for any $k \geq 3$, respectively, in polynomial time.

12. Kazuo Iwama, Eiji Miyano, Hirotaka Ono:
"Drawing Borders Efficiently", Proceedings of the 4th International Conference on Fun with Algorithms, (掲載予定).
概要: A spreadsheet, especially MS Excel, is probably one of the most popular software applications for personal-computer users and gives us convenient and user-friendly tools for drawing tables. In practical situations, we often wish to draw several vertical and horizontal black lines on selective gridlines to enhance the readability of our spreadsheet. Such situations we frequently encounter are formulated as the Border Drawing Problem (BDP). Given a layout of black line segments, we study how to draw it efficiently from an algorithmic view point, by using a set of border styles and investigate its complexity. (i) We first give a formal model based on MS Excel, and then (ii) show that the problem is $\mathcal{NP}$-hard for the set of the Excel border styles and for any reasonable subset of the styles. Moreover, in order to provide potentially more efficient drawing, (iii) we propose a new compact set of border styles and show a necessary and sufficient condition of its drawability.

研究会等

1. 清成悠貴，宮野英次，宮崎修一:
“試問予定表作成問題の計算複雑さ”，電子情報通信学会技術研究報告, 106 巻・128 号, pp.7–14, 2006 年 6 月.
概要: 本稿では，試問予定表作成問題と呼ばれる大学における時間割表作成問題を考える．この問題では，m 人の審査員の集合，$2n$ 人の学生の集合，各学生について審査する複数の審査員の担当割当 (例えば各学生を 3 人ずつの審査員が担当) が与えられる．審査は n 人ずつ 2 つの部屋で同時に行われるため，学生と担当審査員の組は，n 個の時刻と 2 つの部屋から成る $n \times 2$ 行列に割り当てられる必要がある．ここで，同じ審査員が担当する異なる 2 人の学生は異なる時刻に割り当てられなければならない．さらに，すべての審査員が 2 つの部屋を移動する回数の合計をできるだけ少なくしたい．本問題は，実際に京都大学の試問予定表作成時に起きた問題を形式化したものである．この問題について 2 つの制約付きモデルを提案し，それらの計算複雑さについて調査する．

2. Yuichi Asahiro, Jesper Jansson, Eiji Miyano, Hirotaka Ono, Kouhei Zenmyo:
“(In)approximability of Graph Orientation to Minimize the Maximum Weighted Outdegree”, 情報処理学会アルゴリズム研究会情処研報, 2006 巻・71 号, pp.21–28, 2006 年 7 月.
概要: Given an undirected graph $G = (V, E)$ and a weight function $w : E \to \mathbb{Z}^+$, we consider the problem of orienting all edges in E so that the maximum weighted outdegree among all vertices is minimized. It has previously been shown that the unweighted version of the problem is polynomially solvable while the weighted version is (weakly) NP-hard. In this paper, we strengthen these results as follows: (1) We prove that the weighted version is strongly NP-hard even if all edge weights belong to the set $\{1, k\}$, where k is any integer greater than or equal to 2, and that there exists no pseudo-polynomial time approximation algorithm for this problem whose approximation ratio is smaller than $(1 + 1/k)$ unless P=NP; (2) we present a new polynomial-time algorithm that approximates the general version of the problem within a factor of $(2 - 1/k)$, where k is the maximum weight of an edge in G; (3) we show how to approximate the special case in which all edge weights belong to $\{1, k\}$ within a factor of $3/2$ for $k = 2$ (note that this matches the inapproximability bound above), and $(2 - 2/(k + 1))$ for any $k \geq 3$, respectively, in polynomial time.

3. 朝廣 雄一，宮野 英次，宮崎 修一，吉牟田 拓朗:
“サイクルグラフ上での地図作成問題に対する重み付き最近傍アルゴリズム”, 電子情報通信学会技術研究報告, 106 巻・405 号, pp.15–22, 2006 年 12 月.
概要: グラフ上での地図作成問題とは，探索者が未知のグラフの全ての頂点を訪問することによりグラフ構造を調査する問題である．探索者は辺の存在とその長さをその端点を訪れるまで判らないとする．探索者は，できるだけ短い経路を通ることにより全ての頂点と辺を調査して，出発点まで戻って来なければならない．本問題に対する最も単純な方法の一つは，最近傍アルゴリズム (NN) であり，まだ訪れていない頂点の中で探索者の現在の場所から最も近い場所に移動する戦略である．重み付き最近傍アルゴリズム (WNN) は，NN の拡張であり，ある重み付きの距離により次の移動場所を決める．平面グラフにおいては，重み 3 である WNN が 16 競合であることが知られている．本稿ではサイクルグラフについては，NN の競合比が 1.5 となること，その解析が厳密であることを示す．また，サイクルグラフに対しては WNN の中で NN が最適であることを示す．さらに，本問題に対しては，1.25 競合よりも良いアルゴリズムが存在しないことを示す．

4. 行實隆広，廣瀬英雄，大井伸哉，宮野英次: “バンプ探索における解の精度”, 情報処理学会数理モデル化と問題解決研究会, 2006 巻・135 号, pp.13–16, 2006 年 12 月.
   概要:　多次元空間内に特徴量を持ち 2 値 (0/1) 反応をとる N 個の中から反応 1 を示す点が他に比べて密な領域 (バンプ，ホットスポット) を探索する問題を考える．これまに，探索結果を予測に使いやすくするためには決定木を用いたバンプ探索法が有効であり，また最適値を求めるためには確率的探索法 (GA) に加え，極致統計法を用いる方法を新しく提案した．しかし，得られた結果がどのような精度を持っているかはまだ分かっていなかった．ここでは，学習データとテストデータを使うことで，この問題がいかに深刻であるかを指摘し，次に最適に探索された結果の精度について述べる．テストサンプル法とブートストラップのメリットを併せ持つ方法も提案する．

学会大会等

1. 大井伸哉，行實隆広，宮野英次，廣瀬英雄: “最適 tree 探索の確率的一方法”，電気関係学会九州支部第 59 回連合大会, pp.12-2A-05, 2006 年 9 月.

2. 朝廣雄一，古川哲也，池上佳一，宮野英次: “サイズ 3 の最小ブロック転送問題の近似困難性”, 電気関係学会九州支部第 59 回連合大会, pp.10-2A-08, 2006 年 9 月.

3. 吉牟田拓朗，宮野英次，宮崎修一: “オンライン TSP アルゴリズムに対する下限について”, 電気関係学会九州支部第 59 回連合大会, pp.10-2A-07, 2006 年 9 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) 線形符号の双対距離と共通鍵暗号への応用に関する研究;

(2) QoS アルゴリズムに関する研究;

(3) VLSI 計算に関する研究;

(4) 可逆計算に関する研究;

(5) 量子計算に関する研究,

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 線形符号の双対距離と共通鍵暗号への応用に関する研究

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．さらに，計算機実験により，これらの上界・下界の良好性を確認した．

1.2 QoS アルゴリズムに関する研究

QoS アルゴリズムの競合比の解析について考察した．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るパケット破棄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，これまで知られていた下界を改善した．

1.3 VLSI 計算に関する研究

3 次元集積回路設計における基本的な問題である 3 次元チャネル配線とまたその特別な場合である 3 次元単層配線について考察した．3 次元チャネル配線問題に関しては，それが $\mathcal{NP}$ 困難であることの簡便な証明を与え，さらに配線のベント数を詳細に検討することによりその $\mathcal{NP}$ 完全性を明らかにした．一方，3 次元単層配線に関しては，既存の結果を改良し，n 個のネットが $5\sqrt{n}/2$ 層の 3 次元チャネル内で単層配線可能である多項式時間アルゴリズムを示すことにより構成的上界を明らかにした．

1.4 可逆計算に関する研究

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，可逆論理回路の全て配線上の縮退故障を検出する最小完全テスト集合生成問題が $\mathcal{NP}$ 困難であることを示し，可逆論理回路の故障検出問題の計算複雑度を明らかにした．

1.5 量子計算に関する研究

グラフの最小全域木問題や最短路問題などに対しては, 古典的アルゴリズムよりも高速である量子アルゴリズムが知られている．本研究では, 全点対間最短路問題の量子計算量の非自明な下界 $\Omega(\sqrt{m^3/n^2})$ を導出し，特に $m = \omega(n^{3/2})$ であるときには，この下界が既存の下界の改良となっていることを明らかにした．

2 線形符号の双対距離と共通鍵暗号への応用に関する研究

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，以下の条件を満たすような線形符号 $\mathcal{C}$ 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 $d^\perp$.

これまでに本研究では，任意の整数 $d, d^\perp$ に対して，代数的手法などにより，以下に示す $N(d, d^\perp)$ の上界・下界を導出している．

定理 2.1 ([$N(d, d^\perp)$**の上界**]) 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．

$$\frac{2^m - 1}{2^n - 1} \sum_{i=1}^{d-1} \binom{n}{i} + \frac{2^{n-m} - 1}{2^n - 1} \sum_{i=1}^{d^\perp - 1} \binom{n}{i} < 1.$$

定理 2.2 ([$N(d, d^\perp)$**の下界**]) 任意の整数 $d, d^\perp$ が与えられたとき，以下が成り立つ．

$$\begin{aligned} & N(d, d^\perp) \\ & \quad \geq \quad \min\{n : n \geq \lg \ell(n, d) + \lg \ell(n, d^\perp)\}, \end{aligned}$$

ただし，任意の整数 $n \geq d$ に対して

$$\ell(n, d) = \begin{cases} \displaystyle\sum_{i=0}^{(d-1)/2} \binom{n}{i} & d \text{ は奇数;} \\ \displaystyle\sum_{i=0}^{d/2-1} \binom{n}{i} + \binom{n-1}{\frac{d}{2}-1} & d \text{ は偶数.} \end{cases}$$

そこで，本研究では，新たに以下に示すような $N(d, d^\perp)$ に対する下界を導出した．

定理 2.3 ([$N(d, d^\perp)$**の下界**]) 任意の整数 $d, d^\perp$ が与えられたとき，以下が成り立つ．

$$\begin{aligned} & N(d, d^\perp) \\ & \quad \geq \quad \min \Bigg[n : 2n \geq d + d^\perp \\ & \qquad + \min_{1 \leq m \leq n-1} \left\{ \sum_{i=1}^{m-1} \left\lceil \frac{d}{2^i} \right\rceil + \sum_{i=1}^{n-m-1} \left\lceil \frac{d^\perp}{2^i} \right\rceil \right\} \Bigg]. \end{aligned}$$

定理 2.4 ([$N(d, d^\perp)$**の下界**]) 任意の整数 $d, d^\perp$ が与えられたとき $N(d, d^\perp) \geq n$，ただし n は以下を満たす最小の整数とする．

$$\begin{aligned} A_i & \geq 0 && d \leq i \leq n; \\ \sum_{i=d}^{n} A_i P_w(i) & = -\binom{n}{w} && 1 \leq w \leq d^\perp - 1; \\ \sum_{i=d}^{n} A_i P_w(i) & = -\binom{n}{w} && d^\perp \leq w \leq n; \end{aligned}$$

(1) d が偶数の場合*:* 以下のどちらか.

$$\begin{cases} \displaystyle\sum_{i:\ \text{偶数}} A_i = \sum_{i:\ \text{奇数}} A_i; \\ A'_n = 0. \end{cases}$$

$$\begin{cases} A_i = 0 & i:\ \text{奇数}; \\ \displaystyle 4\sum_{i:4|i} A_i \geq \sum_{i=0}^{n} A_i; \\ A'_n = 1; \\ A'_i = A'_{n-i} & 0 \leq i \leq n-1. \end{cases}$$

表 2.1: $N(d, d^\perp)$ の上界・下界

d	$d^\perp$	$N(d,d^\perp)$	上界	下　界			
		実験結果	定理 2.1	定理 2.2	定理 2.3	定理 2.4	定理 2.5
3	3	6	17	6	5	6	6
4	3	7	21	7	6	7	7
4	4	8	25	8	7	8	8
5	3	11	24	9	7	11	8
5	4	13	29	11	8	13	9
5	5	16	34	14	11	14	10
6	3	12	28	10	8	12	9
6	4	14	33	12	9	14	10
6	5	17	38	15	12	17	11
6	6	18	42	16	13	18	10
7	3	14	31	12	9	14	10
7	4	15	37	14	10	15	11
8	3	15	35	14	10	15	11
8	4	16	40	15	11	16	12

(2) d が偶数の場合*:*

$$\begin{cases} \sum_{i:\ \text{偶数}} A_i &= \sum_{i:\ \text{奇数}} A_i; \\ A'_n &= 0. \end{cases}$$

(3) $d^\perp$ が偶数の場合*:* 以下のどちらか.

$$\begin{cases} \sum_{i:\ \text{偶数}} A'_i &= \sum_{i:\ \text{奇数}} A'_i; \\ A_n &= 0. \end{cases}$$

$$\begin{cases} A'_i &= 0 \qquad i:\ \text{奇数}; \\ 4\sum_{i:4\mid i} A'_i &\geq \sum_{i=0}^{n} A'_i; \\ A_n &= 1; \\ A_i &= A'_{n-i} \qquad 0 \leq i \leq n-1. \end{cases}$$

(4) $d^\perp$ が偶数の場合*:*

$$\begin{cases} \sum_{i:\ \text{偶数}} A'_i &= \sum_{i:\ \text{奇数}} A'_i; \\ A_n &= 0. \end{cases}$$

ただし，任意の線形符号 $\mathcal{C}$ とその双対符号 $\mathcal{C}^\perp$ に対して，$A_w, A'_w, P_w(i)$ は以下で与えられる.

$$\begin{aligned} A_w &= |\{c \in \mathcal{C} : w(c) = w\}|; \\ A'_w &= |\{c \in \mathcal{C}^\perp : w(c) = w\}|; \\ P_w(i) &= \sum_{j=0}^{w} (-1)^j \binom{i}{j}\binom{n-i}{w-j}. \end{aligned}$$

定理 2.5 ([$N(d, d^\perp)$の下界]) 任意の整数 $d, d^\perp$ が与えられたとき，以下が成り立つ.

$$N(d, d^\perp) \geq \begin{cases} d + d^\perp - 2 & d, d^\perp \geq 1; \\ d + d^\perp & d, d^\perp \geq 3. \end{cases}$$

また，計算機実験により上記の上界・下界を検証し，表 2.1のような結果を得た．表 2.1より明らかに，上界 (定理 2.1) は実際の $N(d, d^\perp)$ と大きな隔たりがあるものの，下界 (定理 2.3・定理 2.5) は実際の $N(d, d^\perp)$ を良好に評価している.

今後の課題として実際の $N(d, d^\perp)$ を良好に評価する上界の導出が挙げられる.

3　QoS アルゴリズムに関する研究

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

$$\frac{\mathrm{OPT}(\sigma)}{\mathrm{ALG}(\sigma)} \leq c$$

が成り立つことを言う．ただし $\mathrm{ALG}(\sigma)$ 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 $\mathrm{OPT}(\sigma)$ 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．また，各パケットの優先度が β 以上 α 以下に制限されたパケット列集合を $\Pi_{[\beta,\alpha]}$ と表すものとする．

一般に QoS アルゴリズムは，

- **パケット破棄可能モデル:** 新たなパケットが到来した際に，既にキューに格納されているパケットの破棄を許すポリシー
- **パケット破棄不可能モデル:** 新たなパケットが到来した際に，既にキューに格納されているパケットの破棄を許さないポリシー

に大別される．本研究では，パケット破棄可能 QoS 問題に関して，その競合比の上界と下界の解析を行い，以下の結果を導出した．

定理 3.1 任意の $\alpha \geq 1$ に対する *QoS* 問題 $\Pi_{[1,\alpha]}$ に関して，パケット破棄可能モデル *QoS* アルゴリズム TLH は $(3-1/\alpha)$-競合的である：任意のパケット列 $\sigma \in \Pi_{[1,\alpha]}$ に対して，

$$\frac{\mathrm{OPT}(\sigma)}{\mathrm{ALG}(\sigma)} \leq 3 - \frac{1}{\alpha}.$$

定理 3.2 任意の $\alpha \geq 1$ に対して，以下を満たすパケット列 $\sigma_\alpha \in \Pi_{[1,\alpha]}$ が存在する*:*

$$\frac{\mathrm{OPT}(\sigma_\alpha)}{\mathrm{TLH}(\sigma_\alpha)} \geq \frac{3 - 1/m}{1 + 1/B + 1/\alpha},$$

ただし，m はキューの数，$B = B_1 + B_2 + \cdots + B_m$ で B_i は各キューのパケット格納可能数とする．

定理 3.1は，既知の結果 — QoS 問題 $\Pi_{[0,\alpha]}$ に対するパケット破棄可能 QoS アルゴリズム TLH が 3-競合的である — を改善するものである．また，定理 3.2は，十分大きな α, m, B に対して，パケット破棄可能 QoS アルゴリズム TLH の競合比 $3-1/\alpha$ が良好な評価であることを保証するものである．

定理 3.3 任意の $\alpha \geq 1$ と任意のパケット破棄可能 *QoS* アルゴリズム ALG に対して，以下を満たすパケット列 $\sigma_\alpha \in \Pi_{[0,\alpha]}$ が存在する*:*

$$\frac{\mathrm{OPT}(\sigma_\alpha)}{\mathrm{ALG}(\sigma_\alpha)} \geq 1.514 - \Theta(0.559^m).$$

定理 3.3は，既知の結果 — QoS 問題 $\Pi_{[0,\alpha]}$ に対する競合比の下界は 1.419 である — を改善するものである．

4 VLSI 計算に関する研究

VLSI 計算に関する研究では，グラフの直交描画，3 次元配線，及び 3 次元レイアウトについて考察している．グラフの直交描画に関する研究については昨年度にすでに詳細に報告しているので，今年度は 3 次元配線と 3 次元レイアウトに関する研究について詳細に報告する．

4.1 3 次元配線に関する研究

3 次元配線に関する研究では，3 次元チャネル配線と 3 次元単層配線について考察している．

4.1.1 3 次元チャネル配線に関する研究

3 次元チャネル配線においては，端子は最上層あるいは最下層に存在している．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．

昨年度報告したように，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，すべての端子が偶数座標上に存在する場合には，n 個の 2 端子ネットは $3\sqrt{n}$ 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．層数の上界は，多項式時間の 3 次元チャネル配線アルゴリズムを示して，構成的に証明されている．

さらに，3 次元チャネル配線問題は $\mathcal{NP}$ 困難であることも昨年度報告している．この $\mathcal{NP}$ 困難性の証明は，2 次元マンハッタンチャネル配線問題の $\mathcal{NP}$ 困難性の証明を 3 次元に自然に一般化したものであるが，複雑で見通しの悪いものであった．

そこで今年度は，3 次元チャネル配線問題の $\mathcal{NP}$ 困難性の簡明な証明を与えると共に，この問題が $\mathcal{NP}$ に属すことを示すことにより，この問題が $\mathcal{NP}$ 完全であることを初めて示している．$\mathcal{NP}$ 困難性は，すでに $\mathcal{NP}$ 完全であることが知られている “(n^2-1) パズル” に付随する判定問題から 3 次元チャネル配線問題への多項式時間還元を示して証明している．この多項式時間還元は自然なものであり，大変見通しのよい証明であるといえる．3 次元チャネル配線問題が $\mathcal{NP}$ に属することは自明ではなく，配線のベンド数に関する詳細な検討に基づいて証明されている．

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．

4.1.2 3 次元単層配線に関する研究

3 次元単層配線においては，すべての端子が同一の (最上あるいは最下) 層上に存在している．したがって，3 次元単層配線は 3 次元チャネル配線の特別な場合である．すでに，

- すべての端子が偶数座標上に存在する場合には，n 個のネットは $6\sqrt{n}$ 層の 3 次元チャネル内で単層配線できること
- 単層配線するためには $\sqrt{n}/4$ 層の 3 次元チャネルを必要とするような n 個のネットの組が存在すること

などが知られている．

本研究では既存の結果を改良し

- すべての端子が偶数座標上に存在する場合には，n 個のネットは $5\sqrt{n}/2$ 層の 3 次元チャネル内で単層配線できること

を明らかにしている．この上界は，多項式時間の単層配線アルゴリズムを示すことにより，構成的に証明されている．この多項式時間単層配線アルゴリズムは，**4.1.1** 節で述べた多項式時間 3 次元チャネル配線アルゴリズムを修正して設計されている．

一方，3 次元単層配線問題の計算複雑度は未解決であり，今後の課題ある．

4.2 3 次元レイアウトに関する研究

ハイパーキューブは並列計算機の相互結合網としてよく用いられている．N 点から成るハイパーキューブ Q_N の 2 次元レイアウトに関しては，$\mathrm{A}(Q_N)$ を Q_N の 2 次元レイアウトの最小面積としたときに，

$$\mathrm{A}(Q_N) = \Theta(N^2)$$

であることがよく知られている．

一方，Q_N の 3 次元レイアウトに関しては，$\mathrm{vol}(Q_N)$ を Q_N の 3 次元レイアウトの最小体積としたときに，

$$\mathrm{vol}(Q_N) = \Omega(N^{3/2})$$

であることが知られていが，$\mathrm{vol}(Q_N)$ の上界を明示的に考察している文献は見当たらない．

そこで本研究では，Q_N の具体的な 3 次元レイアウトを初めて示すことにより，

$$\mathrm{vol}(Q_N) = O(N^{3/2})$$

であることを証明し，

$$\mathrm{vol}(Q_N) = \Theta(N^{3/2})$$

であることを明らかにしている．Q_N の 3 次元レイアウトは，Q_N のよく知られている最適な 2 次元レイアウトの自然な一般化になっている．すなわち，Q_N を $N^{2/3}$ 個の $Q_{N^{1/3}}$ に分解し，これらの $Q_{N^{1/3}}$ の 3 次元線形レイアウトを組み合わせて Q_N の 3 次元レイアウトを構成している．

5　可逆計算に関する研究

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．

全単射である論理関数を計算する論理ゲートを可逆であるという．可逆ゲートをファンアウトあるいはフィードバックを用いずに結合して得られる論理回路を可逆であるという．可逆論理回路 C のすべての配線上の（単一及び多重）縮退故障を検出できるテストの集合を C に対する完全テスト集合という．C に対する完全テスト集合のテストの数の最小値を $\tau(C)$ で表す．

k-CNOT ゲートは $k+1$ 入力の可逆ゲートである．制御ビットとよばれる k 個の入力は値が変化することなく出力される．ターゲットビットとよばれる残りの 1 個の入力の値は，制御ビットの入力値がすべて 1 であるときに反転して出力される．0-CNOT ゲートは古典的な NOT ゲートである．CNOT ゲートだけで構成される可逆論理回路を CNOT 回路という．2-CNOT ゲートで NAND 関数を実現できるので，任意の論理関数は CNOT 回路で実現できることが分かる．

任意の可逆回路 C に対して，m を C の配線の数とすると，

- $\tau(C) = O(\log m)$ であること
- n 入力 CNOT 回路 C が 0-CNOT ゲートも 1-CNOT ゲートも含まないならば，$\tau(C) \leq n$ であること

が知られている．

昨年度報告したように，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った．

今年度は，可逆論理回路 C に対して $\tau(C)$ を計算する問題は $\mathcal{NP}$ 困難であることを示して，可逆論理回路の故障検出問題の計算複雑度を初めて明らかにしている．$\mathcal{NP}$ 困難性は，3SAT から CNOT 回路 C に対する $\tau(C)$ の判定問題への多項式時間還元を示して証明されている．

6　量子計算に関する研究

グラフの最小全域木問題や最短路問題などに対しては，古典的アルゴリズムよりも高速である量子アルゴリズムが知られている．実際，単一始点最短路問題の古典的時間計算量は

$$\Theta(m + n \log n)$$

であるが，量子クエリ計算量は

$$O(\sqrt{mn} \log^2 n)$$

及び

$$\Omega(\sqrt{mn})$$

であることが知られている．ここで，m と n はそれぞれグラフの辺数と点数である．

一方，全点対間最短路問題の古典的時間計算量は

$$O(mn + n^2 \log \log n)$$

及び

$$\Omega(mn)$$

であることが知られているが，量子クエリ計算量に関しては，単一始点最短路問題の下界から得られる自明な下界

$$\Omega(\sqrt{mn})$$

しか知られていない．

そこで，本研究では, 全点対間最短路問題の量子計算量の非自明な下界

$$\Omega(\sqrt{m^3/n^2})$$

を示している．この下界は，$m = \omega(n^{3/2})$ であるときには，自明な下界よりも真に大きいことが分かる．

$m = O(n^{3/2})$ であるときの非自明な下界の導出と古典的アルゴリズムよりも高速である量子アルゴリズムの設計は今後の課題である.

研究業績一覧

学術論文

1. Ryutaroh Matsumoto, Kaoru Kurosawa, Toshiya Itoh, Toshimitsu Konno, and Tomohiko Uematsu:
"Primal-Dual Bounds of Linear Codes with Application to Cryptography", IEEE Transactions on Information Theory, Vol.52, No.9, pp.4251-4256, September 2006.
概要: Let $N(d, d^{\perp})$ be the minimum code length n of a linear code $\mathcal{C}$ with d and $d^{\perp}$, where d is the minimum Hamming distance of the code $\mathcal{C}$ and $d^{\perp}$ is the minimum Hamming distance of its dual code $\mathcal{C}^{\perp}$. In this paper, we show several lower bounds and an upper bound on $N(d, d^{\perp})$. Futhermore, for small values of d and $d^{\perp}$, we determine $N(d, d^{\perp})$ and give a generator matrix of the optimal linear code. This problem is directly related to the design method of cryptograpic Boolean functions suggested by Kurosawa, et al.

2. Toshiya Itoh and Noriyuki Takahashi:
"Competitive Analysis of Multi-Queue Preemptive QoS Algorithms for General Priorities", IEICE Transactions on Fundamentals, Vol.E89-A, No.5, pp.1186-1197, May 2006.
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 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 to each packet. In this paper, we first derive the upper bounds for the competitive ratio of multi-queue preemptive QoS problem with priority between $1/\alpha$ and 1, i.e., for any $\alpha \geq 1$, the algorithm TLH is $(3 - 1/\alpha)$-competitive. This is a generalization of known results—for the case that packets have only priority 1 ($\alpha = 1$), the algorithm GREEDY (or TLH) is 2-competitive; for the case that packets have priorities between 0 and 1 ($\alpha = \infty$), the algorithm TLH is 3-competitive. Then we consider the lower bounds for the competitive ratio of multi-queue preemptive QoS problem with priority between 0 and 1, and show that the competitive ratio of any multi-queue preemptive QoS algorithm is at least 1.514.

3. Satoshi Tayu, Kumiko Nomura, and Shuichi Ueno:
"On the Two-Dimensional Orthogonal Drawing of Series-Parallel Graphs", Proceedings of the 2006 IEEE International Symposium on Circuits and Systems, pp.1796-1799, 2006.
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.

研究会等

1. Satoshi Tayu and Shuichi Ueno:
   "The Complexity of Three-Dimensional Channel Routing", IEICE Technical Report, Vol.106, No.366, pp.37-41, 2006.
   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 objective of the 3-D channel routing problem is to connect the terminals in each net with a Steiner 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 the problem is intractable.

学会大会等

1. Fuwei Cai, Satoshi Tayu, and Shuichi Ueno:
   "On the Quantum Query Complexity of All-Pairs Shortest Paths", Proceedings of the 2007 IEICE General Conference, p.20, 2007.

2. Yohei Arai, Satoshi Tayu, and Shuichi Ueno:
   "A Note on the Three-Dimensional Single-Active Layer Routing", Proceedings of the 2007 IEICE General Conference, p.21, 2007.

3. Shigeru Ito, Satoshi Tayu, and Shuichi Ueno:
   "The Complexity of Fault Testing for Reversible Circuits", Proceedings of the 2006 IEICE Society Conference, pp.S-1 - S-2, 2006.

4. Satoshi Tayu and Shuichi Ueno:
   "Three-Dimensional Channel Routeing is in $\mathcal{NP}$", Proceedings of the 2006 IEICE Society Conference, pp.S-5 - S-6, 2006.

5. Toshihiro Kubo, Satoshi Tayu: and Shuichi Ueno:
   "On the Three-Dimensional Layout of Hypercubes", Proceedings of the 2006 IEICE Society Conference, pp.S-7 - S-8, 2006.

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，コーダルグラフの自己同型群と同型性判定のためのアルゴリズムに

関する研究を行った.

目的 2 に関しては，渡辺が，アドバイス列へのランダムアクセスを与えられた状況での計算モデルの考察，および，具体的な計算問題に対するアルゴリズムの planted solution model での解析を行った．河内が，計算量理論に基づいた量子暗号系の安全性についての考察を行った.

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 3 月 2，3 日に電気通信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 コーダルグラフの自己同型群と同型性判定のためのアルゴリズム

戸田はまず，IEICE Technical Report, COMP2005-24，および，IEICE Transactions on Information and Systems, August 2006 において，コーダルグラフの自己同型群を求めるためのアルゴリズムを設計し，それを利用することによって同型性も判定できることを示した.

しかし，そこでは群論的手法を多用しており，複雑で時間量の解析も困難であった．さらに，自己同型群のもとで不変な木表現 (s-木) が構成可能であるといった事実以外には，コーダルグラフに関する様々な性質をまったく利用していないものになっていた (注: これは群論的手法を多用しているためである)．そこで，コーダルグラフの性質をうまく利用することによって，より単純なアルゴリズムを設計できるのではないかということが素直な疑問として残されていた．そこで戸田はこの疑問をに答えるために，アルゴリズム設計のための指針についての考察も行った．このなかで，アルゴリズムがうまくいかない場合の具体例についても考察した。

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 アドバイス列へのランダムアクセスを与えられた状況での Turing 機械

渡辺は，Turing 機械がアドバイス列へのランダムアクセスを与えられた状況での計算モデルを提案した．ランダムアクセスがあると，指数的長さの advice string は多項式時間計算クラスに影響を及ぼす．本モデルにおける計算クラスの比較を行った結果，新しいモデルは相対化による通常の計算モデルよりも厳密な概念を与えることがわかった．さらに，このランダムアクセスが可能なモデルにおいて，多項式時間階層およびパリティ多項式時間のクラスが共に P に落ち込むことを証明した.

この新しい相対化の概念 (より厳密な相対化) により，計算量クラスを研究するための新しいアプローチが開かれた．これに基づき，渡辺は厳密な相対化のもとでの計算量クラスの関係の落ち込みについて，その意味と影響について議論を行った.

3.2 planted solution model における MAX-2SAT

渡辺は，MAX-2SAT 問題の平均時の計算量を議論するための “planted solution model” とよばれるモデルを提案した．ここでは、広い範囲のパラメータにおいて，planted solution (正確には，一つの planted solution pair) が，高い確率で生成された問題例に対する最適解となることを証明した．さらに，メッセージパッシング法に基づいた単純な線形時間アルゴリズムを提案し，そのアルゴリズムが planted solution model において，高い確率で MAX-2SAT 問題を解くことを示した.

3.3 planted solution model におけるグラフ二分割問題

渡辺は，グラフ二分割問題およびそれに関連する問題に対して，単純で決定的なメッセージパッシングアルゴリズムを提案した．主なアルゴリズムの実行時間は頂点および辺の数の線形時間で

ある．ここでは，平均時の正当性を評価するために，planted solution model が使われている．確率パラメータが p および r の標準的な planted solution model のもとでのグラフ二分割問題に対して，もし $p-r=\Omega(n^{-1/2}\log(n/\delta))$ ならば，提案アルゴリズムは $1-\delta$ の確率で planted solution を求めることを証明した．

3.4 計算量理論に基づいた量子暗号系の安全性

河内は，計算量理論に基づいた量子暗号系の安全性証明の新たなテクニックとして，誤り訂正符号に対する量子リスト復号法を導入し，ハードコア関数の新たな一般的構成方法を与えた．更に今回の結果を応用することで 1988 年に提案されて以来，未解決であった Dangaard の擬似乱数生成器の安全性を量子一方向性関数に基づいて証明することができた．リスト復号法とは，与えられた符号語に誤りが多すぎて一意的に元々の符号化された情報が復元できないような状況でも符号化された情報の候補を比較的短いリストとして与えてくれるような復号法である．元来，リスト復号法は符号理論で考案された概念であったが，近年，リスト復号法が現代暗号理論や計算量理論で応用できることが判明し，急速に研究が進んでいる．またハードコア関数は一方向性関数に対して定義される暗号理論における非常に基本的な道具であり，例えばハードコア関数を利用して擬似乱数生成器やビットコミットメントプロトコルが構成できることが知られている．今回の結果はリスト復号法の量子計算版の有用性を示しており，元々のリスト復号法と同様に量子リスト復号法も量子計算における暗号理論や量子計算量理論において今後幅広い応用を持つことが期待できる．

オラクルへの質問計算量は計算量理論・暗号理論のともに非常に重要な概念である．というのも例えば暗号理論における安全性証明ではオラクルへの質問回数がそのまま安全性の高さと直結している．この基礎付けの研究としてオラクル同定問題と呼ばれる問題における量子計算的な質問計算量についても研究を行った．オラクル同定問題とは M 個のブール関数集合 $\{f_i:\{0,...,N-1\}\to\{0,1\}\,(i=0,...,M-1)\}$ に属するある関数が与えられたときに，その関数の値を何回質問することで同定できるか，という問題である．この問題は量子計算で頻繁に扱われる探索問題の一般化として既に Ambainis らによって 2003 年に定式化され，$M\leq N$ の場合には最適な量子アルゴリズムが与えられていた．しかしそれよりさらに一般の場合については未解決であった．今回の研究の結果，任意の M に対する量子アルゴリズムを与えることができ，更に非常に広い範囲の M でこのアルゴリズムが最適であることも証明できた．

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 複数ユーザーを考慮したトークンつき公開鍵暗号

トークンつき公開鍵暗号とは，Baek, Safavi-Naini, Susilo によって提案された概念である．

トークンつき公開鍵暗号では，暗号化を行う際，暗号文とともにトークンと呼ばれる補助情報を生成する．このとき，暗号文だけでは，秘密鍵をもっている人ですら復号を行うことができない．しかしながら，ひとたびトークンが公開されれば，秘密鍵をもっている人のみがその暗号文を復号することができる．このとき，秘密鍵をもっていない人は，暗号文とトークンの両方を手に入れても復号することができないようになっている．

つまり，トークンつき公開鍵暗号は，暗号文を事前に生成してそのデータを配布しておき，暗号文を復号させたいと思った時点でトークンを公開し，秘密鍵をもっている人だけに復号させるといった状況に適している．

トークンつき公開鍵暗号の安全性として，Baek らは 3 つの安全性を定式化した．これらは大きく 2 つに分けられる．ひとつは，秘密鍵をもっていてもトークンなしでは暗号文を復号できないという安全性 (IS-CPA) であり，もうひとつは，秘密鍵をもっていない人は（トークンが公開されても）暗号文を復号できないという安全性 (T1-CCA, T2-CCA) である．その後，Galindo, Herranz は，あ

る暗号文とトークンのペアに対して，そのトークンを別のものに置き換えることで，それがはじめに意図したものと異なる平文に復号されてしまうことがないという安全性 (SETUF) を定式化している．すなわち，この安全性はトークンつき公開鍵暗号に対する改ざん不可能性をとらえている．

トークンつき公開鍵暗号の利用例としては，前に述べたように，暗号文を事前に生成してそのデータを配布しておき，暗号文を復号させたいと思った時点でトークンを公開し，秘密鍵をもっている人だけに復号させるといったものが考えられる．このような利用を考えた場合，トークンつき公開鍵暗号は，同じトークンを複数ユーザーで使えることが望ましい．すなわち，同じトークンを用いて複数ユーザーに複数の暗号文を送信し，あとでそのトークンを公開するといった使い方ができれば，使用するトークンがひとつだけですむため，効率の向上が期待できる．しかしながら，その場合の安全性については，現在の安全性の定式化ではとらえられておらず，新たに定式化を行う必要がある．

これをふまえて，我々はまず，複数ユーザーを考慮したトークンつき公開鍵暗号の安全性を提案した．安全性は 4 種類あり，M-IS-CPA, M-T1-CCA, M-T2-CCA, M-SETUF と呼ばれ，それぞれが Baek らおよび Galindo らが提案した安全性の複数ユーザー版となっている．これらの安全性は，単に複数ユーザーに拡張しただけではなく，Boldyreva, Micali のアイディアを用いて，より強力な攻撃者を考慮したものとなっている．すなわち，単に複数ユーザーに拡張したものに比べてより強い安全性を定式化したことになる．

次に，我々が提案した 4 つの複数ユーザー版の安全性と，過去に提案された単一ユーザー版の安全性の関係の一部を証明した．その結果は図 2.1 に示されている．この図からわかるように，M-T2-CCA と M-SETUF については，対応する単一ユーザー版の安全性を証明すれば十分である．一方で，M-IS-CPA および M-T1-CCA については，対応する単一ユーザー版の安全性だけで十分であるかはわからない．

さらに，我々は，過去に提案されている Galindo, Herranz の方式が，提案した複数ユーザー版の安全性をみたすことを証明した．

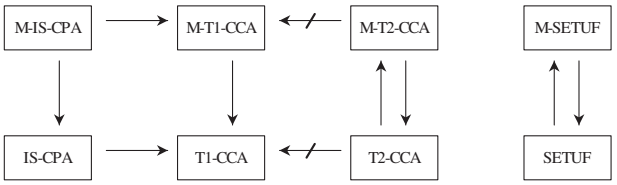


図 2.1: 安全性の関係．上段が複数ユーザーでの安全性，下段が単一ユーザーでの安全性を表す．

Galindo らは，彼らの方式が IS-CPA, T2-CCA, SETUF をみたすことを証明している．よって，我々が示した安全性間の関係（図 2.1）より，あとは M-IS-CPA を証明すれば，複数ユーザー版の全ての安全性をみたすことがわかる．我々は Galindo らの方式がランダムオラクルモデルにおいて M-IS-CPA をみたすことを証明した．なお，M-IS-CPA を証明するときの仮定は，Galindo らが IS-CPA を証明したときと変わっていない．

4.2 格子問題に基づく認証方式と署名方式

格子問題に基づく暗号方式が注目を集めている．その理由は, 暗号方式の安全性を格子問題の最悪時の困難性から保証できることにある．また今のところ格子問題を解く量子アルゴリズムが知られていないことにもある．現在, 公開鍵暗号とハッシュ関数については安全性を格子問題の最悪時の困難性から保証できるものが知られている．

格子問題に基づく署名方式として GGH 署名と NTRU 署名が知られている．しかし, 両者とも安全性証明が付けられておらず, 様々な攻撃を受けてきた．2006 年には NTRU 署名の一モードと GGH 署名について, Nguyen と Regev が公開鍵と数万個の署名から確率的に秘密鍵を求める攻撃を提案している．

次に, 格子問題に関する認証方式について述べる．Micciancio と Vadhan は 2003 年に GapCVP と呼ばれる問題の近似版について統計的なゼロ知識証明を提案している．また林と多田は BNELVP と呼ばれる問題について証拠秘匿性を持つ認証プロトコルを提案している．しかしこれらのプロトコルの安全性は格子問題の平均時の困難性に基づいて証明されている．

以上から分かるように, 認証方式と署名方式に

ついては, 安全性を格子問題の最悪時から保証できるものが知られていない. そこで, 我々は安全性の根拠を格子問題の最悪時とする認証方式と署名方式について研究を行った.

まず我々はRegev05暗号の鍵生成アルゴリズムを変形した. 変形したRegev05暗号の安全性がある学習問題の最悪時の困難性から保証できる. 鍵生成アルゴリズムの変形により, 公開鍵がq進符号のパリティ検査行列とシンドロームに, 秘密鍵がエラー付の符号語に対応する. 一方, Sternが二進符号のパリティ検査行列とシンドロームからハミング重みが固定されたエラー付符号語を求める問題に関するゼロ知識アーギュメントを提案している. 我々は, Sternのゼロ知識証明をq進版に拡張し, 公開鍵認証方式を得た. またFiat-Shamir変換を施すことで署名方式も得た.

さらに格子問題に基づくハッシュ関数も, ハッシュ関数のインデックスをq進符号のパリティ検査行列に, ハッシュ値をシンドロームに, ハッシュされる文書をエラー付の符号語に対応させることができる. ハッシュされる文書に少し制限を加えることで, 拡張したゼロ知識アーギュメントの枠組みに乗せることができる. したがって, ハッシュ関数のインデックスとハッシュ値を公開鍵に, ハッシュされる文書を秘密鍵とすることで, 公開鍵認証方式を得た. 先と同様に, Fiat-Shamir変換を施すことで署名方式も得た.

認証方式の安全性については以下である. 認証方式のなりすましに成功する敵が存在すると仮定する. このとき, 敵を上手く使うことで, 公開鍵から秘密鍵を得ることができる. 変形されたRegev05暗号を用いた認証方式では, 秘密鍵を得ることで暗号文の解読ができるので, なりすましに成功することは暗号の安全性が破れることを意味する. 暗号の安全性は, ある学習問題の最悪時に基づいているので, 認証方式の安全性も同じ問題の最悪時の困難性に基づいていることが言える. 一方, ハッシュ関数を用いた認証方式では, 秘密鍵を得ることで, ハッシュ関数の一方向性を破っている. ハッシュ関数の一方向性は格子問題の最悪時に基づいているので, 認証方式の安全性も同じ問題の最悪時に基づいている.

Fiat-Shamir変換を施して得られた署名方式のランダムオラクルモデルでの安全性は, 認証方式の安全性に基づくことがすでに知られている. したがって, 署名方式の安全性はランダムオラクルモデルでは格子問題または学習問題の最悪時に基づいている.

4.3 格子問題に基づく暗号方式の平文知識証明

平文知識証明とは, 公開鍵と暗号文を共通入力としたときに, 証明者が暗号文に対応する平文を知っていることを証明するゼロ知識証明のことである. 数論の問題に基づく暗号方式ではすでに多くの平文知識証明プロトコルが知られている. その暗号方式と平文知識証明を組み合わせることでより強い安全性を持つ暗号方式を得ることができる. また, 他のプロトコルに暗号方式を組み込む際にも使われるなど, 平文知識証明の応用は広い.

格子暗号の分野では, GoldwasserとKharchenkoが, Ajtai-Dwork暗号の暗号文に関する平文知識証明のプロトコルを2005年に提案している. 格子暗号にはAjtai-Dwork暗号以外にもRegev04暗号, Regev05暗号, GGH暗号, NTRU暗号等が知られているが, 平文知識証明プロトコルが提案されているのは, Ajtai-Dwork暗号のみである. そこで, 我々は彼らのプロトコルを応用し，Regev04暗号とRegev05暗号の暗号文に関する平文知識証明を提案した.

GoldwasserとKharchenkoのプロトコルでは, 共通入力である暗号文と公開鍵から, あるベクトルと格子の基底を生成する. 彼らはNguyenとSternがAjtai-Dwork暗号の攻撃に用いた基底の生成方法を採用し, 暗号文から得たベクトルと公開鍵から得た格子の関係を基底の生成方法に基づいて証明している. 具体的には, 基底の生成方法から, 0の暗号文から得たベクトルは公開鍵から得られた格子に近く, 1に復号される暗号文から得たベクトルは公開鍵から得られた格子から遠いということが言える. これと認証方式の関連研究で述べたMicciancioとVadhanのGapCVPに関するゼロ知識証明と疑似準同型性を用いることで, 全体のプロトコルを構成している.

そこで我々はRegev04暗号とRegev05暗号の公開鍵の特性に基づいて, 格子の基底の生成方法を考案し, 同様に暗号文から得たベクトルと公開鍵

から得た基底で張られる格子の関係について証明を行った．さらに全体のプロトコルも Goldwasser と Kharchenko と同様に構成し, 証明を行った．証明の都合上, Regev04 暗号と Regev05 暗号の安全性の基となる問題の安全性パラメータが悪くなることが分かった．全体の安全性は格子暗号の安全性の基となる問題の最悪時の困難性から保証することができる．

我々の結果には別の意味もある． Nguyen と Stern は格子の基底の生成方法を考案することにより, Ajtai-Dwork 暗号の暗号文を識別する問題が GapCVP の問題に関係することを示している．Nguyen と Stern は暗号の安全性パラメータ (格子の次元) が小さければヒューリスティックに 0 と 1 の暗号文を識別することが出来ることを示した．我々は, Regev04 暗号と Regev05 暗号について, 格子の基底の生成方法を考案し, 暗号文を識別する問題が GapCVP の問題に関係することを本研究中で示した．したがって, Nguyen と Stern の攻撃方法と同様に, 安全性が低い場合の Regev04 暗号と Regev05 暗号も, 安全性パラメータが小さければヒューリスティックに 0 と 1 の暗号文を識別することが出来ることになる．

4.4 Pseudo-Free Group の変形について

公開鍵暗号の安全性は，ある種の計算問題が効率的に解くことができないという仮定に依存している．よく知られた問題としては RSA 問題や離散対数問題などがある．これらの問題が効率的に解くことができないということを仮定して安全性が証明できる具体的な暗号方式としては，前者は RSA 暗号系や RSA-OAEP，後者は ElGamal 暗号系や Cramer-Shoup 暗号系などがある．

2004 年に Rivest は多くの暗号的な計算問題が効率的に解けないことが証明できる Pseudo-Free Group と呼ばれる群を提案した．具体的に Pseudo-Free Group においては，上述の RSA 問題や離散対数問題は効率的に解くことができない．この群は，Free Group の方程式に着目して定義されたものである．Free Group は多くの暗号的な問題が解くことができないことが知られている．しかしながら，この群は原始的過ぎて暗号で用いるには使い物にならない．よって，擬似的な Free Group を定義することは暗号学的に有用である．

Pseudo-Free Group は先に述べたように，多くの計算問題が効率的に解くことができないということから，暗号学的にみて強い仮定だと言える．それゆえに，様々な安全性の証明が簡単になると同時に，証明の新しいフレームワークになることが期待できる．さらには，この強い仮定を利用して新たなアプリケーションが構築できるのではないかとも期待できる．

Rivest が Pseudo-Free Group の定義する以前に，Hohenberger によって簡単に概念が提示されていた．そこでは Pseudo-Free Group をさらに強くすることで，Micali と Rivest によって提案された Directed Transitive Signature と呼ばれる特殊な署名方式の構築の十分条件が与えられていた．

Rivest は Pseudo-Free Group のいくつかの性質を述べたのではあるが，肝心な Pseudo-Free Group であるような群が実際にあるかどうかはわかっていなかった．2005 年に Micciancio は RSA 暗号系などで用いられる群 $(\mathbb{Z}/n\mathbb{Z})^{\times}$ が Strong RSA 仮定の下で Pseudo-Free であることを示した．ただし，n は Strong Prime と呼ばれる特殊な 2 つの素数の積である．

今回我々は，Rivest の論文中の証明についての問題点の指摘と，Pseudo-Free Group の変形についてのいくつかの性質を示した．

前者については Pseudo-Free Group において，RSA 問題のような暗号的な計算問題が効率的に解くことはできないということを先に述べたが，このことが疑わしいことがわかった．その理由は Rivest が与えた Pseudo-Free Group の方程式に問題があったためである．具体的には指数部分に変数を持つことが許されないということである．離散対数問題等の多くの暗号的な計算問題は方程式からの立場から述べると，指数の部分に (整数) 変数を持つことが多々ある．それにも関わらず Rivest は許されない方程式の形を使って，離散対数問題等の問題が Pseudo-Free Group では効率的に解けないと述べた．

それゆえ我々は，Rivest が同じ論文中で提案した Pseudo-Free Group の変形である Pseudo-Free Group with Generalized Exponential Expression と，発表で使われたプレゼンテーション資料に記されていた Weakly Pseudo-Free Group という二

つの変形を用いて，Pseudo-Free Group の議論を行うことにした．

特に Pseudo-Free Group with Generalized Exponential Expression については紹介程度にとどまっており，我々は定式化を行い，さらにはそのことを用いて，先ほどの Pseudo-Free Group では成り立つことが疑わしい問題も解決することができた．

次に後者であるが，これは Pseudo-Free Group with Generalized Exponential Expression と Weakly Pseudo-Free Group の関係を中心にいくつか性質を示した．

特に，一つの元 g で生成される群 $\langle g \rangle$ を Pseudo-Free Group with Generalized Exponential Expression としたとき，適当に選んだ元 h を加えた二つの元で生成される群 $\langle g, h \rangle$ は Weakly Pseudo-Free Group となることを示した．一般的には，$\langle g \rangle$ の暗号的な強さが $\langle g, h \rangle$ になると弱まってしまう場合があることが知られている．この定理は，例えば $\langle g \rangle$ を使って離散対数問題ベースの暗号系を構成したときに，群を $\langle g \rangle$ のように拡張しても安全性が保証できることを述べてもいる．このことは，Pseudo-Free Group with Generalized Exponential Expression と Weakly Pseudo-Free Group においてどちらの群ともに離散対数問題が効率的に解くことができないことから言える．

5 ミニ研究集会 (暗号理論)

昨年度，総括班の櫻井の呼びかけをきっかけに開催した研究集会に続き，今年度も特定領域研究「新世代の計算限界」暗号関係ミニ研究集会を開催した．本研究集会は，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開催された．電気通信大学の國廣が会場世話人とプログラムのとりまとめを行った．

昨年度は函館での開催，期間は 1 日であったが，今年度は東京での開催，期間は 2 日だった．参加者は，昨年度は約 20 名だったが，今年度は 1 日目が約 40 名，2 日目が約 30 名と増加した．また昨年度と異なり，企業の研究所からも多くの参加者がいた．

講演は下記の概要の通りであるが，1，10 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り，残りの講演は各自の研究成果に関する内容が中心であった．

参加者は少なくなかったものの自由に質問できる雰囲気が常にあった．実際に，講演の最中にも質問がでたり，講演直後の決められた時間以外にも活発な討論がされたりと，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．

研究集会 1 日目の後の懇親会では，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や，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が多く聞かれた．他にも研究集会に関して具体的に，一件あたりの発表および質疑応答の時間をもっと長くとりたい，チュートリアル講演を主体としたスクール的な研究集会をもちたいなどといった意見も聞かれた．

次年度も継続して，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予定である．

日時 2007 年 3 月 2 日 (金) 13:30–17:30, 3 日 (土) 9:30–15:45

場所 電気通信大学 総合研究棟 601 会議室 (〒182-8585 東京都調布市調布ヶ丘 1-5-1)

プログラム

1. 3 月 2 日 (金) 13:30–14:30
   証明可能安全性理論に向けて
   太田 和夫 (電気通信大学)

2. 14:45–15:15
   耐タンパ性を備えたユニークデバイスに基づく暗号認証基盤の検討
   今本 健二 (九州大学) (発表者: 蘇 春華 (九州大学))

3. 15:15–16:00
   ペアリング暗号の安全な高速実装について
   高木 剛 (はこだて未来大学)

4. 16:15–16:45
   指定検証者署名の定式化，および，送信者と受信者の匿名性について
   大山 千尋 (東京工業大学)

5. 16:45–17:30
   Concurrently Secure Password-based Authenticated Key Exchange without Random Oracles or Setup Assumptions
   米山 一樹 (電気通信大学)

6. 3 月 3 日 (土) 9:30–10:30
   スタンダードモデル PA の基礎に関して
   寺西 勇 (NEC)

7. 10:45–11:30
   Non-Malleability Definitions Reconsidered
   宮川 聡 (電気通信大学)

8. 11:30–12:15
   Collusion-resistant Private Association Rules Mining in Distributed Environment
   蘇 春華 (九州大学)

9. 13:30–14:15
   Revisiting Zero-Knowledgeness of an On the Fly Authentication Scheme
   Bagus Santoso (電気通信大学)

10. 14:15–15:45
    格子問題をベースとした暗号について
    草川 恵太 (東京工業大学)

各発表の概要

1. 証明可能安全性理論に向けて
   太田 和夫 (電気通信大学)
   概要: 実用的な暗号技術として，安全性が理論的に証明できる（証明可能安全な）方式が期待されている．公開鍵暗号の発明後しばらくの間『ある攻撃に対して安全な方式は，別の攻撃に対しては安全性証明がつかない』と信じられていた (Folklore)．本解説では,「folklore」の呪縛から逃れ,「安全性証明」への道筋を示した Goldwasser, Micali, Rivest による記念碑的な論文を紹介することで，本研究集会の導入とする．安全性定理に込められた「ココロ」，呪縛からの解放の「アイデア」などを解説した．

2. 耐タンパ性を備えたユニークデバイスに基づく暗号認証基盤の検討
   今本 健二 (九州大学)
   概要：従来，公開鍵証明書を用いた公開鍵基盤（PKI）や ID ベース暗号を利用した暗号化システムにおいては，数学アルゴリズムや第三者機関の利用など，様々な仮定に基づいた設計が行われている．本論文では，深谷らが提案したデバイス固有値を用いた対称暗号技術による ID ベース暗号化方式（IST 方式）に基づいた手法を検討し，本方式を用いることで認証を行う方式（3way 認証方式）を提案し，既存の認証方式との比較を行う．

3. ペアリング暗号の安全な高速実装について
   高木 剛 (公立はこだて未来大学)
   概要：ペアリング暗号の安全な高速実装について考察を行う．高速実装するにあたっては，ペアリングに関する演算の理論的改良，ペアリングをプログラミングコードで実装する際の種々の工夫を行っている．理論的改良については，３乗根を求めることなく EtaT ペアリングを演算する方法，および，トーラスを用いた最終的な結果を得るための指数演算の方法の２つを主に提案した．プログラミングコードで実装する際の種々の工夫に関しては，Java, C, BREW, FPGA の４つのコードにおいて高速実装を行った．さらには，ペアリングに関するサイドチャネル攻撃についても考察した．

4. 指定検証者署名の定式化，および，送信者と受信者の匿名性について大山 千尋 (東京工業大学)
   概要：本研究では，指定検証者署名における「受信者（指定検証者）の匿名性」という新しい安全性の概念を提案する．指定検証者署名を用いると，署名者が，特定の人にだけ検証が可能であるような署名を生成することができる．受信者の匿名性とは，攻撃者が署名を

盗聴しても，その署名がだれに向けて指定されたのかが判別できないという性質である．我々は，この受信者の匿名性という概念を定式化するとともに，この性質をみたす方式を2つ提案する．

5. Concurrently Secure Password-based Authenticated Key Exchange without Random Oracles or Setup Assumptions
米山 一樹 (電気通信大学)
概要：本発表では，plain model におけるパスワード認証つき鍵交換の一般的な構成法を提案する．ここで plain model とは，その方式がランダムオラクル，あるいは，trusted setup assumption を必要としないという意味である．さらに，我々の方式は複数のインスタンスが同時にプロトコルを実行したとしても（concurrent でも）安全である．我々の方式は plain model で concurrent な安全性を達成する初めての方式である．

6. スタンダードモデル PA の基礎に関して
寺西 勇 (NEC)
概要：plaintext awareness という安全性の概念についての考察を行った．plaintext awareness とは，公開鍵暗号の安全性についての概念であり，暗号文を作れる人はいうその平文を知っているはずであるという性質である．plaintext awareness は，もともとはランダムオラクルモデルという強い仮定の下で定義されていたが，近年はスタンダードモデルでの定義も提案されている．本発表では，現在の定義の問題点などを指摘するとともに，他の安全性の概念との関連性を示した．

7. Non-Malleability Definitions Reconsidered
宮川 聡 (電気通信大学)
概要：公開鍵暗号方式が 頑健性 (NM) を満たすとは，攻撃者が，暗号文から，対応する平文を改ざんした新たな暗号文を作成できないことをいう．この NM の概念を定式化するためには，攻撃者が作成すべき「新たな暗号文」に条件を付加する必要がある． この条件は2種類にわけられ，攻撃者は新たな暗号文に不正な暗号文を含めることはできないといった定義 (定義 1) と，攻撃者は新たな暗号文に不正な暗号文を含めることはできるが，含めた場合には実験に失敗するといった定義 (定義 2) がある．本研究では，NM に関する3種類の定義 (SNM, CNM, IND-P) について，SNM および CNM においては，定義 1 と定義 2 の間には攻撃者の能力の観点からすると差がないことを示した．また，IND-P においては，定義 2 のような方法では条件を付加することは不可能であることも示した．

8. Collusion-resistant Private Association Rules Mining in Distributed Environment
蘇 春華 (九州大学)
概要：相関ルールマイニングはデータベースに蓄積された大量のデータから，頻繁に同時に生起する事象同士を相関の強い事象の関係，すなわち相関ルールとして抽出する技術である．本論文では，相関ルールのプライバシー保護問題に着目し，結託を防止した安全なプライベート相関ルールマイニング手法を提案した．従来の提案では準同型性暗号の暗号を用いており，鍵の管理と生成，計算量と通信量はかなり大きいものだった．今回の我々のの提案では，分散ネットワークにおける n 個のパーティーがデータベースのプラバシーを保ったままで，共同の相関ルールマイニングを算出するシナリオを想定する．我々は，Han による Apriori algorithm の効率を大きく改善するアルゴリズムを使って，結託を防止できる効率のよい手法を提案した．

9. Revisiting Zero-Knowledgeness of an On the Fly Authentication Scheme
Bagus Santoso (電気通信大学)
概要：on-the-fly の認証方式である GPS のなりすましに対する安全性は，ゼロ知識性に依存して証明されているが，実際に使用した場合の安全性についての詳細な考察は行われていなかった．我々は，GPS に対して，正当な証明者と検証者の間での通信履歴を集めるだけで，秘密鍵の先頭ビットを計算することができることを示した．

10. 格子問題をベースとした暗号について
草川 恵太 (東京工業大学)

概要：格子問題に基づく暗号方式が注目を集めている．その理由は, 暗号方式の安全性を格子問題の最悪時の困難性から保証できることにある．また今のところ格子問題を解く量子アルゴリズムが知られていないことも格子問題に基づく暗号方式が注目を集める理由のひとつである．現在, 公開鍵暗号とハッシュ関数については安全性を格子問題の最悪時の困難性から保証できるものが知られている．本発表では，ハッシュ関数を攻撃することが，組合せ問題の最悪時の困難性と結びつくことを詳細に解説した．さらに，未解決問題についても解説を行った．

研究業績一覧

著書

1. 金森敬文，畑埜晃平，渡辺治:
“ブースティング — 学習アルゴリズムの設計技法”, 森北出版, 2006 年.
概要: ブースティング技法について，その入門的な解説を述べ，著者らが行ってきた理論的な研究を紹介した本．ブースティング技法の背景にある PAC 学習の話から始め，ブースティングによる学習アルゴリズムの基礎を解説する．その後で，著者らの研究の中で，とくにブースティングを応用してみたい人が直面するだろう疑問点に対し，我々が理論的に見出した解決法を紹介する形で解説した．

学術論文

1. S. Balaji, H.M. Mahmoud, and O. Watanabe:
“Distributions in the Ehrenfest process”, tatistics and Probability Letters, Vol. 76, 666-674, 2006.
概要: We introduce a tenable class of urns that generalize the classical Ehrenfest model, and analyze the Ehrenfest process obtained by embedding the discrete evolution in real time. We show that lurking under the Ehrenfest process is a limiting binomial distribution, whose number of trials is an integer invariant property of the process.

2. J.Y. Cai and O. Watanabe:
“Random access to advice strings and collapsing result”, Algorithmica, Vol. 45, 43-57, 2006.
概要: We propose a model of computation where a Turing machine is given random access to an advice string. With random access, an advice string of exponential length becomes meaningful for polynomially bounded complexity classes. We compare the power of complexity classes under this model. It gives a more stringent notion than the usual model of computation with relativization. Under this model of random access, we prove that there exist advice strings such that the Polynomial-time Hierarchy PH and Parity Polynomial-time all collapse to P.

3. 河内亮周:
“量子計算における整数格子問題へのアプローチ”, IEICE 論文誌特集号「量子情報処理」招待解説論文, (掲載予定)．
概要: 今まで計算困難と思われていた素因数分解・離散対数問題が量子計算機を使うと効率良く解けるというのは今となっては良く知られた事実である．一方，多くの研究者は NP 困難問題はさすがに量子計算でも効率良く解くことはできない，と予想しているようである．それでは，素因数分解・離散対数問題以外（特に数論的な問題以外）で，NP 困難ではなさそうで P（あるいは BPP）に入ることも知られていない問題に対して量子計算は有効であるのか？というのは自然な疑問であろう．本稿ではその代表として整数格子にまつわるいくつかの問題に関して量子計算の分野でどのような進展があるのか，アルゴリズム，暗号，計算量理論の観点から解説したい．

4. Akinori Kawachi and Takeshi Koshiba:
“Progress in Quantum Computational Cryptography”, Journal of Universal Com-

puter Science, Vol. 12, No. 6, 691-709, 2006.

概要: Shor's algorithms can be regarded as a negative effect of the quantum mechanism on public-key cryptography. From the computational point of view, his algorithms illustrate that quantum computation could be more powerful. It is natural to consider that the power of quantum computation could be exploited to withstand even quantum adversary. Over the last decade, quantum cryptography has been discussed and developed even from the complexity-theoretic point of view. In this paper, we will survey the investigation on quantum computational cryptography.

研究会等

1. Ryotaro Hayashi and Keisuke Tanaka:
"PA in the Two-Key Setting and a Generic Conversion for Encryption with Anonymity", Information Security and Privacy - 11th Australasian Conference, ACISP 2006, Lecture Notes in Computer Science 4058, 271-282, July, 2006.

概要: We propose the notion of plaintext awareness in the two-key setting, called PATK. We also prove that if a public-key encryption scheme is secure in the sense of PATK, 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 PATK than to prove directly that it is secure in the sense of IK-CCA, the notion of PATK 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 public-key encryption scheme derived from the Fujisaki-Okamoto conversion scheme, where the 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.

2. Naoyuki Yamashita and Keisuke Tanaka:
"Secret Handshake with Multiple Groups", In Information Security Applications: 7th International Workshop, WISA 2006, Lecture Notes in Computer Science 4298, 339-348, August, 2007.

概要: 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 themselves secretly to the other whether they belong to a same group or not, in the sense that each party reveals his affiliation to the other only if the other party is also a same group member. The previous works focus on the models where each participant authenticates himself as a member of one group. In this paper, we consider a secret handshake model with multiple groups. In our model, two users authenticate themselves to the other if and only if each one's memberships of multiple groups are equal. We call this model secret handshake with multiple groups. We also construct its concrete scheme. Our scheme can easily deal with the change of memberships. Even if a member is added to a new group, or deleted from the one that he belongs to, it is not necessary to change the memberships for the other groups that he belongs to.

3. Akinori Kawachi, Keisuke Tanaka, and Keita Xagawa:
"Multi-Bit Cryptosystems Based on Lattice Problems", 10th International Workshop on Theory and Practice in Public Key Cryptography, PKC 2007, Lecture Notes in Computer Science 4450, 315-329, April, 2007.

概要: We propose multi-bit versions of several single-bit cryptosystems based on lattice problems, the error-free version of

the Ajtai-Dwork cryptosystem by Goldreich, Goldwasser, and Halevi [CRYPTO '97], the Regev cryptosystems [JACM 2004 and STOC 2005], and the Ajtai cryptosystem [STOC 2005]. We develop a universal technique derived from a general structure behind them for constructing their multi-bit versions without increase in the size of ciphertexts. By evaluating the trade-off between the decryption errors and the hardness of underlying lattice problems, it is shown that our multi-bit versions 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. Our technique also reveals an algebraic property, named *pseudo-homomorphism*, of the lattice-based cryptosystems.

4. Akinori Kawachi and Tomoyuki Yamakami:
"Quantum Hardcore Functions by Complexity-Theoretical Quantum List Decoding", 33rd International Colloquium on Automata, Languages and Programming (ICALP 2006), Lecture Notes in Computer Science 4052, 216-227, 2006.
概要: We present three new quantum hardcore functions for any quantum one-way function. We also give a quantum solution to Damgaard's question (CRYPTO'88) on his pseudorandom generator by proving the quantum hardcore property of his generator, which has been unknown to have the classical hardcore property. Our technical tool is quantum list-decoding of "classical" error-correcting codes (rather than "quantum" error-correcting codes), which is defined on the platform of computational complexity theory and cryptography (rather than information theory). In particular, we give a simple but powerful criterion that makes a polynomial-time computable code (seen as a function) a quantum hardcore for any quantum one-way function. On their own interest, we also give quantum list-decoding algorithms for codes whose associated quantum states (called codeword states) are nearly orthogonal using the technique of pretty good measurement.

5. Andris Ambainis, Kazuo Iwama, Akinori Kawachi, Rudy Raymond, and Shigeru Yamashita:
"Improved Algorithms for Quantum Identification of Boolean Oracles", 10th Scandinavian Workshop on Algorithm Theory (SWAT 2006), Lecture Notes in Computer Science 4059, 280-291, 2006.
概要: The oracle identification problem (OIP) was introduced by Ambainis et al. It 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 improve the algorithms of Ambainis et al. by providing a mostly optimal upper bound of query complexity for this problem: (i) For any oracle set S such that $|S| \leq 2^{N^d}$ ($d < 1$), we design an algorithm whose query complexity is $O(\sqrt{N \log M / \log N})$, matching the lower bound proved in 2004. (ii) Our algorithm also works for the range between 2^{N^d} and $2^{N/\log N}$ (where the bound becomes $O(N)$), but the gap between the upper and lower bounds worsens gradually. (iii) Our algorithm is robust, namely, it exhibits the same performance (up to a constant factor) against the noisy oracles as also shown in the literatures for special cases of OIP.

6. 作本紘一, 田中圭介:
"Key-Substitution Attacks on Group Signature", 2007年 暗号と情報セキュリティシンポジウム (SCIS2007), 1B1-4, 2007年1月.
概要: Group signatures were introduced by Chaum and Van Heyst, and many se-

curity requirements for group signatures have been proposed. Bellare, Micciancio, and Warinschi showed that satisfying full-anonymity and full-traceability is sufficient, in the sence that all the above-mentioned requirements are implied by them. Wilson and Menezes introduced a considerable attack against standard signatures, key substitution attack. In this paper, we propose security conditions of group signatures against this attack and show that the security requirements are not sufficient regarding the attack. We also propose a group signature scheme that is secure against key substitution attack, fully-anonymous, and fully-traceable.

7. 草川恵太, 河内亮周, 田中圭介:
"A Lattice-Based Cryptosystem and Proof of Knowledge on Its Secret Key", 2007 年 暗号と情報セキュリティシンポジウム (SCIS2007), 1C1-1, 2007 年 1 月.
概要: We propose a lattice-based cryptosystem by modifying the Regev05 cryptosystem (STOC 2005), and design a proof of secret-key knowledge. Lattice-based public-key identification schemes have already been proposed, however, it is not known that their public keys can be used for the public keys of encryption schemes. Our modification admits the proof of knowledge on its secret key, however, we need a stronger assumption than that required by the original cryptosystem.

8. 草川恵太, 河内亮周, 田中圭介:
"Proof of Plaintext Knowledge for the Regev Cryptosystems", 2007 年 暗号と情報セキュリティシンポジウム (SCIS2007), 1C1-2, 2007 年 1 月.
概要: Goldwasser and Kharchenko (TCC 2006) showed a proof of plaintext knowledge for the Ajtai- Dwork cryptosystem and left the open problem designing a proof of plaintext knowledge for the Regev04 cryptosystem (JACM 2004). In this paper, we show a proof of plaintext knowledge for the Regev04 cryptosystem (JACM 2004) using their technique. Furthermore, we show that it can be applied to the Regev05 cryptosystem (STOC 2005). The key idea is to analyze tradeoffs between the hardness of the underlying lattice problem and the variance of ciphertexts, which given by Kawachi, Tanaka, and Xagawa (SCIS 2006).

9. 林良太郎, 田中圭介:
"The Security with the Randomness Revealed for Public-Key Encryption", 2007 年 暗号と情報セキュリティシンポジウム (SCIS2007), 2C1-4, 2007 年 1 月.
概要: We consider the situation for public-key encryption that the adversary knows the randomness which was used to compute the ciphertext. In some practical scenarios, there is a possibility that the randomness is revealed. For example, the randomness used to make a ciphertext may be stored in insecure memory, or the pseudo-random generator may be corrupted. We first formalize the security notion on this situation as "the one-wayness with the randomness revealed." In addition to the formalization, we focus on two schemes, the generic chosen-ciphertext secure encryption method (GEM) and 3-round OAEP, and prove that these two schemes satisfy our security notions.

10. 竹部裕俊, 田中圭介:
"Steganographic Signature", 2007 年 暗号と情報セキュリティシンポジウム (SCIS2007), 2B2-6, 2007 年 1 月.
概要: Steganography is the science of sending messages hidden in harmless communications over a public channel so that an adversary eavesdropping on the channel even detect the presence of the hidden messages. In this paper, we formalize and propose steganographic signature.

We define the security of steganographic signature, steganographic security and unforgeability. We construct a steganographic signature scheme, and we show that our proposed steganographic signature scheme with the extended Schnorr signature scheme is steganographically secure and unforgeable.

11. 八代正俊, 田中圭介:
"Private Approximation of the Set Cover Problem", 2007 年 暗号と情報セキュリティシンポジウム (SCIS2007), 2D2-1, 2007 年 1 月.
概要: Private approximation, introduced by Feigenbaum, Ishai, Malkin, Nissim, Strauss, and Wright, allows us to find approximate solutions with disclosing as little information as possible. In STOC 2006, Beimel, Carmi, Nissim, andWeinreb studied the private approximation for both the vertex cover and the max exact 3SAT problems. In this paper, we consider the set cover problem where the costs of all sets are polynomially bounded. We show that there exists neither a deterministic nor a randomized private approximation. We also consider the case that the frequencies of all elements are equal. We show that in this case there exist no deterministic private approximation.

12. 平野貴人, 田中圭介:
"Variations on Pseudo-Free Groups", 2007 年 暗号と情報セキュリティシンポジウム (SCIS2007), 2D2-2, 2007 年 1 月.
概要: The notion of the pseudo-free group was informally introduced by Hohenberger [Hoh03], and was formalized by Rivest. Rivest showed that many cryptographic assumptions (e.g. the RSA assumption, the strong RSA assumption, the discrete logarithm problem and so on) hold in pseudo-free groups. In this paper, we point out the fact that in the definition by Rivest, many cryptographic assumptions except for the RSA assumption do not hold. The reason is that the equation in pseudo-free groups contains no integer-valued exponent variables. Rivest probably supposed that we may not need the notion of exponent variables since the adversary can choose himself equations. In this paper, we also study some of the variations introduced by Rivest. Using these variations, we show several properties for pseudo-free groups. In particular, we describe the subgroup of pseudo-free groups.

13. 井上大輔, 田中圭介:
"Constructions for Conditional Oblivious/Converge Transfer/Cast", 2007 年 暗号と情報セキュリティシンポジウム (SCIS2007), 2D4-1, 2007 年 1 月.
概要: In this paper, we introduce a new notion of conditional converge cast (CCC), such that we append the conditional property to converge cast. Additionally, we generalize the three primitives with conditional property, conditional oblivious transfer (COT), conditional oblivious cast (COC), and CCC. CCC is a three-party protocol which involves two sender S_0 and S_1 and a receiver R. S_0 owns a secret x and a message m_0, and S_1 y and m_1. In a CCC protocol for the predicate Q (Q-CCC), S_0 and S_1 send their messages to R in a masked form. R obtains the message depending on the value of $Q(x, y)$, i.e. R obtains m_0 if $Q(x, y) = 0$ and m_1 otherwise. Besides, the secrets x and y cannot be revealed to R or the other sender. We propose a CCC protocol for "equality" predicate with an additively homomorphic encryption scheme. Additionally, we extend 1-out-of-2 COT/COC/CCC to 1-out-of-n COT/COC/CCC. In 1-out-of-2 protocols, a sender or senders send two messages to a receiver or receivers. In 1-out-of-n protocols, a sender or senders

send n messages, where $n = 2l$ for some l. We provide the consecutive definitions and the concrete protocols for 1-out-of-n COT/COC/CCC protocols. We prove that our protocols are secure under the security of 1-out-of-2 protocols.

14. 林良太郎, 田中圭介:
"Token-Controlled Public-Key Encryption in the Multi-User Setting", 2007 年 暗号と情報セキュリティシンポジウム (SCIS2007), 3C2-4, 2007 年 1 月.
概要: In this paper, we formalize the security notions for token-controlled public-key encryption in the multi-user setting, by not simply modifying the previous security notions in the single-user setting proposed by Baek, Safavi-Naini, and Susilo, but employing the idea to formalize the attacks in the multi-user setting proposed by Bellare, Boldyreva, and Micali. Our security notions capture the possibility of an adversary seeing encryptions of related messages under the same token and different keys when the choice of the relation can be made by the adversary. We also show that the Galindo.Herranz scheme is secure in the multi-user setting.

15. 大山千尋, 田中圭介:
"Privacy of Verifier's Identity on Designated-Verifier Signature", 2007 年 暗号と情報セキュリティシンポジウム (SCIS2007), 3C4-5, 2007 年 1 月.
概要: In this paper, we propose a new notion of the designated-verifier 's anonymity on designatedverifier signature (DVS), called " the privacy of verifier 's identity ". In DVS schemes, a signer can designate a signature to an intended verifier, that is, a signature generated via a DVS scheme can convince only one intended recipient of the validity or the invalidity of the signature. The privacy of verifier 's identity explains that an eavesdropper who obtains a designated-verifier signature cannot tell to whom the signature was designated, which means that the recipient is anonymous. We define the privacy of verifier 's identity, provide two concrete schemes which satisfies the property, and prove their security.

16. 山下直之, 田中圭介:
"An ID-based Combined Scheme with Encryption and Signature", 2007 年 暗号と情報セキュリティシンポジウム (SCIS2007), 4C2-5, 2007 年 1 月.
概要: The cryptographic protocol known as the combined scheme allows users to decrypt ciphertexts and create signatures using the same key. In this paper, we model ID-based combined schemes. Many ID-based encryption schemes and ID-based signature schemes are proposed. Most of them are based on bilinear maps. Although it seems possible to combine these schemes, there is no security definition for the combination. We propose a model for this combinations, and define the security condition. As an additional property, a definition for the key privacy of encryption schemes is proposed. In the combined scheme, the same private key is used for the decryption and the signing. To protect the owner ' s privacy, both the encryption scheme and the signature scheme must satisfy the key privacy condition. When combining them, the encryption scheme should not degrade the key privacy of the signature scheme, and vice versa. We propose a key privacy condition for ID-based signature schemes. We then modify this notion to ID-based combined schemes. We construct a concrete scheme and prove that this scheme satisfies these security requirements.

17. J. Cai and O. Watanabe:
"Stringent relativization: a new approach for studying complexity classes", SIGACT

News, Vol. 37, Dec. Issue (#140), 2006.
概要: A new notion of relativization—stringent relativization—has been proposed recently for discussing collapsing relations of complexity classes, with which we hope to open a new approach for studying complexity classes. Starting with the motivation of this notion, we discuss the meaning and implication of collapsing relations under the stringent relativization.

18. O. Watanabe and M. Yamamoto:
"Average-case analysis for the MAX-2SAT problem", 9th International Conference on Theorem and Application of Satisfiability Testing (SAT'06), Lecture Notes in Computer Science 4142, 277-282, 2006.
概要: We propose a "planted solution model" for discussing the average-case complexity of the MAX-2SAT problem. We show that for a large range of parameters, the planted solution (more precisely, one of the planted solution pair) is the optimal solution for the generated instance with high probability. We then give a simple linear time algorithm based on a message passing method, and we prove that it solves the MAX-2SAT problem with high probability under our planted solution model.

19. M. Onsjoe and O. Watanabe:
"A simple message passing algorithm for graph partition problem", 17th International Symposium on Algorithms and Computation (ISAAC'06), Lecture Notes in Computer Science 4288, 507-516, 2006.
概要: Motivated by the belief propagation, we propose a simple and deterministic message passing algorithm for the Graph Bisection problem and related problems. The running time of the main algorithm is linear w.r.t. the number of vertices and edges. For evaluating its average-case correctness, planted solution models are used. For the Graph Bisection problem under the standard planted solution model with probability parameters p and r, we prove that our algorithm yields a planted solution with probability $1-\delta$ if $p-r=\Omega(n^{-1/2}\log(n/\delta))$.

20. 戸田誠之助:
"コーダルグラフに関する同型性判定のための単純なアルゴリズム", コンピュテーション研究会, 信学技報, vol. 106, no. 29, COMP2006-8, 57-62, 2006 年 4 月.
概要: 筆者による以前の研究 (IEICE Technical Report, COMP2005-24; IEICE Transactions on Information and Systems, August 2006) において, コーダルグラフの自己同型群を求めるためのアルゴリズムを設計し, それを利用することによって同型性も判定できることを示した. しかし, そこでは群論的手法を多用しており, 複雑で時間量の解析も困難であった. さらに, 自己同型群のもとで不変な木表現 (s-木) が構成可能であるといった事実以外には, コーダルグラフに関する様々な性質をまったく利用していないものになっていた (注: これは群論的手法を多用しているためである). そこで, コーダルグラフの性質をうまく利用することによって, より単純なアルゴリズムを設計できるのではないかということが素直な疑問として残されていた. 本研究では, この疑問に答えるために, アルゴリズム設計のための指針を与える.

21. Akinori Kawachi, Hirotada Koabashi and Masahito Hayashi:
"Quantum Measurements for Hidden Subgroup Problems with Optimal Sample Complexity", preprint, quant-ph/06041724, 2006.
概要: One of the central issues in the hidden subgroup problem is to bound the sample complexity, i.e., the number of identical samples of coset states sufficient and necessary to solve the problem. In this paper, we present general bounds for the sample complexity of the identification and decision versions of the hidden subgroup problem. As a consequence of the bounds, we

show that the sample complexity for both of the decision and identification versions is $\Theta(\log|\mathcal{H}|/\log p)$ for a candidate set $\mathcal{H}$ of hidden subgroups in the case that the candidate subgroups have the same prime order p, which implies that the decision version is at least as hard as the identification version in this case. In particular, it does so for the important instances such as the dihedral and the symmetric hidden subgroup problems. Moreover, the upper bound of the identification is attained by the pretty good measurement, which shows that the pretty good measurements can identify any hidden subgroup of an arbitrary group with at most $O(\log|\mathcal{H}|)$ samples.

22. 河内亮周, Christopher Portmann:
"Quantum Asymmetric-Key Cryptosystem Secure Against A Computationally Unbounded Adversary", 2007 年 暗号と情報セキュリティシンポジウム (SCIS2007), 4C1-5, 2007 年 1 月.
概要: In this paper we propose a quantum asymmetric-key cryptosystem, which does not rely on a computationally hard problem for security, but on uncertainty principles of quantum mechanics, thus obtaining security against a computationally unbounded adversary. We first propose a universally composable security criteria for quantum asymmetrickey cryptosystems by adapting the universally composable security of quantum key distribution by Mayers et al. to the context of quantum asymmetric-key encryption. We then give a specific implementation using this security notion, which improves the quantum asymmetric-key cryptosystem of Kawachi et al. in the sense of information-theoretic security. We prove that the information leak on the decryption key from the multiple copies of the encryption keys released in our scheme is exponentially smaller than that of Kawachi et al., which allows Alice to produce exponentially more encryption keys.

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 東京都調布市調布ヶ丘 1-5-1
{nishino,tarui,ota,kunihiro}@ice.uec.ac.jp

1　はじめに

1985 年に D. Deutsch が，量子力学に基づく新たな計算モデルとして量子 Turing 機械を提案し，量子計算機のモデル化を行って以来，量子計算に関する研究が活発に行われてきた．例えば，1994 年に P. W. Shor は，整数の因数分解を多項式時間内に高い成功確率で行う量子アルゴリズムを示した．さらに，1996 年には L.K.Grover が，効率的量子探索アルゴリズムを提案した．このように，量子計算は本質的に古典計算よりも強力である可能性がある．

また，一方，幾何学的手法を用いた量子論理回路のサイズの下界に関する研究や，補助量子ビットが回路計算量に及ぼす影響を明らかにする研究が行われている．これらの研究により，通常の計算量理論に，何らかの貢献ができるのではないかと期待されている．

量子計算機の物理的実装の実現には，多くの困難が存在する．例えば，量子もつれ合いを保つことができる時間が短いことや，複雑な量子操作を行なうことは難しい等である．これらの問題の解決のためにも，量子回路サイズは重要である．本研究では，量子回路サイズを評価するよい方法を検討する．特に，C-NOT ゲートに着目し，量子回路計算量と C-NOT ゲート数の関係について，幾つかの定理を示す．

量子コンピュータは従来のコンピュータに比べて本質的に計算能力の高い、未来のコンピュータとして期待されている．現在、その物理的実現が盛んに研究されているが、量子コンピュータの実現には多くの困難が伴う．

そのうちの一つとして、量子コンピュータは量子重ね合わせ状態という量子力学的にデリケートな状態をとる、ということが挙げられる。そのためサイズの大きい量子コンピュータの複雑な量子重ね合わせ状態を長時間維持することは非常に困難となる．

それに加えて，量子コンピュータは扱えるビット数が大きくなるほど実現が困難であることが知られている．すなわち，同じアルゴリズムを実行する場合，量子コンピュータにおいては特に，時間計算量および領域計算量を縮小することが本質的に重要な問題となる．

本研究では，量子回路のゲート数とビット数の関係についても考察する．具体的には，あるアルゴリズムを実行する量子回路に対して，それに補助量子ビットを付加し，回路を再構成することで，ゲートの総数をさらに縮小できるかどうかを検証する．

我々は古典コンピュータを用いてアルゴリズムを実行するときに，計算時間の短縮のために計算の途中で，その計算結果の一部をメモリの別の場所に一時的に保管することをよく行う．量子コンピュータの回路設計においても，補助量子ビットはそのようなワークビットとしてたびたび用いられるが，そこで使われる補助量子ビットは厳密に定義されているわけではない．本研究ではどのような種類の補助量子ビットにゲート数縮小の効果があるのかを検証するために，補助量子ビットの分類，定式化を目指す．

2　量子回路

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．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 や Yao 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．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 $x_1, x_2, ..., x_n$ 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 $y_1, y_2, ..., y_m$ 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，$n \ge 3$ 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．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．

量子コンピュータが行う計算は，ユニタリ変換によって定められる．そこでユニタリ変換 U を持つ量子コンピュータを，$\boldsymbol{x}$ を入力としてとり，$U\boldsymbol{x}$ を出力する**量子回路**とみなす．

量子回路を表現するダイアグラムでは，平行した k 本のワイヤはベクトル空間 $\underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{k}$ を表す．k 本のワイヤに入力される情報は古典コンピュータの k ビット に相当するので，k 本のワイヤで扱える情報を **k 量子ビット**とよぶ．また，k 本のワイヤを **k 量子ビット レジスタ**とよぶ．

任意の量子回路は以降に述べる 2 種類の**量子ゲート**を組み合わせて構成できる．そのため，これらの量子ゲートは**基本ゲート**と呼ばれる．

本研究では量子回路を構成する基本ゲートの数を，量子コンピュータのサイズと考える．

3 補助量子ビットの分類

補助量子ビットには，それを付加する元の回路の入力に無関係な値が入力される．また回路内部では補助量子ビットに自由に値を書き込むことが出来る．すなわち，作業域として使われる．

補助量子ビット問題とは、既存の回路に内部で作業域として利用できる余分な量子ビットレジスタを加えて再構成したとき、その回路の最小サイズが小さくなることがあるか、という問題である。

次に述べる 2 種類が，現在までに厳密に定式化できた補助量子ビットである．

単純補助量子ビット

論理変数 $|x\rangle$ を入力し論理変数 $|x\rangle$ を出力するような補助量子ビットを単純補助量子ビットと呼ぶ。

定数補助量子ビット

論理定数 $|0\rangle$ を入力し、それぞれ $|0\rangle$ を出力するような補助量子ビットを定数補助量子ビットと呼ぶ。

定数補助量子ビットは、実際の回路設計において、ワークビットとしてゲート数削減のために用いられている。

この補助量子ビットの入出力は以下のように書き直すことが出来る．

論理変数 $|a\rangle$ を入力し，$a = 0$ のときに $|a\rangle \otimes U|x\rangle$ を出力し，$a = 1$ のときに $|a\rangle \otimes *|x\rangle$ を出力する．ただし，$*$ は任意のユニタリ変換とする．

ここで、$U \oplus U = I \otimes U$ より、単純補助量子ビット問題は、定数補助量子ビット問題の限定的な場合であることがわかる。

その他の補助量子ビット

このほかにも，論理入力に対して，任意の論理値を出力するような補助量子ビットや，重ね合わせや絡み合い状態を出力して観測結果を確率的にするような補助量子ビットが考えられる．

4　単純補助量子ビットの効果の検証

単純補助量子ビットの効果を検証するに当たって，問題をわかりやすくするために分割回路の概念を導入する．

分割回路

二つの回路を縦に接続し，新たな回路を作ることを考える．得られた回路について，もし元の二つの回路がそれぞれ用いていた量子ビットの間をまたぐ量子ゲートが存在しなければ，その回路を**分割回路**とよぶ．

また，二つの回路が実現するユニタリ変換について，それぞれをテンソル積で結んだ変換を**分割変換**と呼ぶ．

命題 4.1 分割変換

ある分割変換 $U \otimes V$ に対して，それを実現する分割回路が存在する．

証明 自明である．

□

命題 4.2 分割回路

複数の，ワイヤの数が等しい分割回路を横に接続して作られる回路に対して，その回路に等価な分割回路が存在する．

証明

複数の分割回路を接続した回路が実現する変換は，

$$\prod_i (U_i \otimes V_i) \tag{4.3}$$

と書くことが出来る．この式を変形すると，

$$\prod_i (U_i \otimes V_i) = \left(\prod_i U_i\right) \otimes \left(\prod_i V_i\right) \tag{4.4}$$

となり，分割変換であることが分かる．

よって命題 1 より，この分割変換を実現する分割回路が存在する．

□

2 つの回路をまたぐ C-NOT ゲートが 1 個のときの解析

単純補助量子ビットを 1 つ用いて，回路を最適化するに当たって，補助量子ビットにまたがる C-NOT ゲートが 1 つの回路に最適化することは出来ない，ということを証明した．

補題 4.1 *C-NOT* ゲートと等価な分割回路は存在しない．

補題 4.2 *2* つの部分回路をまたぐ *C-NOT* ゲートがただ *1* つの回路は，分割回路でない．

定理 1 $U \otimes V$ を実現する最小サイズの回路が，*2* つの部分回路をまたぐ *C-NOT* ゲートをただ *1* つしか含まないとき，そのような回路は U, V を実現する二つの回路は接続することで最適化できない．

定理 1 で，$V = I$ とすると，単純補助量子ビットを用いて，元の回路と補助量子ビットをまたぐ C-NOT ゲートが一つの回路に，最適化することは出来ない，ということが分かる．

補助量子ビットの分類について，単純補助量子ビットと定数補助量子ビットの 2 種類について定式化を行い，定数補助量子ビットは単純補助量子ビットの一般化であることを示した．

さらに，単純補助量子ビットを回路に加えたときに，補助量子ビットにまたがる C-NOT ゲートが 1 つの回路に再構成することはできない，ということを証明した．

今後は，さらに補助量子ビットの分類を進めその効果を検証する．

5 量子回路のサイズとC-NOTゲート数の関係

本節では，量子回路のサイズと C-NOT ゲート数の関係について考察する．

あるユニタリ作用素 U を実現するにあたり，回路サイズが最小になる回路のゲート数を $m_{\mathcal{G}}(U)$ と，また，C-NOT ゲート数が最小となる回路の C-NOT ゲート数を $m_{\mathcal{C}}(U)$ と表記する．

定理 2 $m_{\mathcal{C}}(U) = \Omega(n)$ のとき，次の関係が成立する．

$$m_{\mathcal{G}}(U) = \Theta\left(m_{\mathcal{C}}(U)\right)$$

証明

1. $m_{\mathcal{G}}(U) = \Omega\left(m_{\mathcal{C}}(U)\right)$ の証明
   回路サイズが最小となる回路の C-NOT ゲート数を c'，1 qubit ゲートの数を s' とすると，

   $$m_{\mathcal{G}}(U) = c' + s'$$

   が成立する．あきらかに $m_{\mathcal{C}}(U) \leq c'$, $s' \geq 0$ なので，

   $$m_{\mathcal{C}}(U) \leq m_{\mathcal{G}}(U)$$

   が成り立つ．したがって，

   $$m_{\mathcal{G}}(U) = \Omega\left(m_{\mathcal{C}}(U)\right) \tag{5.5}$$

   となる．

2. $m_{\mathcal{G}}(U) = O\left(m_{\mathcal{C}}(U)\right)$ の証明
   C-NOT ゲート数が最小になる回路の回路サイズ g を

   $$g = m_{\mathcal{C}}(U) + s$$

   とする．ここで，s は 1 量子ビットゲートの個数である．同じワイヤー上で隣接する 1 量子ビットゲートは，ひとつの 1 量子ビットゲートにまとめることができる．したがって，量子回路に含まれる 1 量子ビットゲートは，C-NOT ゲートのすぐ右隣に 2 つと，n 本ある各ワイヤーの最も左に 1 つずつあれば十分である．よって，

   $$g \leq 3m_{\mathcal{C}}(U) + n$$

   が成立する．あきらかに，$m_{\mathcal{G}}(U) \leq g$ なので

   $$m_{\mathcal{G}}(U) \leq 3m_{\mathcal{C}}(U) + n$$

   が成り立つ．よって，$m_{\mathcal{C}}(U) \geq O(n)$ のとき

   $$m_{\mathcal{G}}(U) = O\left(m_{\mathcal{C}}(U)\right) \tag{5.6}$$

   となる．

式 (5.5),(5.6) より $m_{\mathcal{C}}(U) = \Theta\left(m_{\mathcal{G}}(U)\right))$ を得る．□

6 ゲートの種類を制限した場合

本節では，使用するゲートの種類を制限した場合における回路サイズについて，考察を行なう．

定理 3 C-NOT ゲートのみから構成される量子ビット数 n の量子回路のサイズは，高々 $O(n^2)$ である．

証明 C-NOT ゲートのみを利用した回路においては，第 1 番目から第 n 番目までの，各々のワイヤーから出力される値は，入力 x_i の排他的論理和となる．各ワイヤーからの出力が x_i の排他的論理和の形で与えられたとき，C-NOT ゲートのみを使用した回路を構成するアルゴリズムを示すことで，定理の証明を行なう．

第 i 番目のワイヤーからの出力を $|z_{i,1}x_1 \oplus z_{i,2}x_2 \oplus ... \oplus z_{i,n}x_n\rangle$, $z_{i,j} \in \{0,1\}$ としたとき，すべてのワイヤーからの出力をまとめて，

$$Z = \begin{pmatrix} z_{1,1} & z_{1,2} & \cdots & z_{1,n} \\ z_{2,1} & z_{2,2} & & z_{2,n} \\ \vdots & & & \vdots \\ z_{n,1} & z_{n,2} & \cdots & z_{n,n} \end{pmatrix}$$

のように表現する．行列 Z のランクが n で無い場合，その回路は C-NOT ゲートのみで構成することはできない．

回路構成アルゴリズム
入力：Z
出力：$C-NOT$ ゲートのみを使用した回路
アルゴリズム：

1. ゲートが1つもない（つまりワイヤーのみの）量子回路を書く．

2. 2a から 2b を $i=1$ から n まで繰り返す．

   (a) もし，$z_{i,i}=0$ ならば，$z_{j,i}=1$ である列 j を1つ探し出し，$z_{i,k} := z_{i,k} \oplus z_{j,k}, k \in \{1,...,n\}$ とする．
   すなわち，第 i 行目と第 j 行目の，それぞれの要素の排他的論理和を，新たな第 i 行目の要素とする．
   第 j 番目のワイヤーを制御ビット，第 i 番目のワイヤーを目標ビットとした C-NOT ゲートを，量子回路の一番左側に置く．

   (b) $j=1$ から n（ただし $j=i$ は除く）に対して，以下を繰り返す．

      i. $z_{j,i}=1$ ならば，
      $z_{j,k} := z_{i,k} \oplus z_{j,k}$, $k \in \{1,...,n\}$
      とする．
      すなわち，第 i 行目と第 j 行目の，それぞれの要素の排他的論理和を，新たな第 j 行目の要素とする．
      第 i 番目のワイヤーを制御ビット，第 j 番目のワイヤーを目標ビットとした C-NOT ゲートを，量子回路の一番左側に置く．

      ii. $z_{j,i}=0$ ならば，何もしない．

ステップ 2aにおいて，C-NOT ゲートは高々 1個，ステップ 2bにおいて，C-NOT ゲートは高々 $n-1$ 個記入される．また，ステップ 2aから 2bは，n 回繰り返されるので，全体として，書き込まれる C-NOT ゲートの個数は，高々 n^2 個である．

定理 4 C-NOT ゲートと NOT ゲートのみから構成される量子ビット数 n の量子回路のサイズは，高々 $O(n^2)$ である．

また，C-NOT ゲートと NOT ゲートのみで構成された回路が出力できるパターン数は，C-NOT ゲートのみで構成された回路が出力できるパターン数の，高々 2^n 倍である．

証明

C-NOT ゲートと NOT ゲートのみから構成される回路においては，それぞれのワイヤーからの出力は，リテラルの排他的論理和と否定のみで構成された式となる．

また，排他的論理和と否定のみで構成された式においては，

$$\overline{x \oplus y} = \overline{x} \oplus y = x \oplus \overline{y}$$

が成り立つ．つまり，1つのリテラルの否定は全体の否定と等価である．リテラルが 3 つ以上含まれる場合でも，1 つのリテラルの否定は全体の否定と等価である．したがって，リテラルの排他的論理和と否定のみで構成可能な式は，排他的論理和のみで構成される形の式と，排他的論理和のみの式全体を否定した形の式の，2 パターンしかない．

これらのことより，出力に対応する排他的論理和の式中に否定が含まれていた場合，その回路の最後の層に NOT ゲートを置くことで，その層の直前においては，排他的論理和のみの式とすることができる．

排他的論理和のみの式を計算するのに必要な回路サイズは，$O(n^2)$ であり，また，この回路に含まれる NOT ゲートの数は，高々 n 個である．したがって，C-NOT ゲートと NOT ゲートのみを使用して量子回路を組む場合，必要なゲート数は高々 $O(n^2)$ である．

C-NOT ゲートと NOT ゲートのみによって構成される回路は，C-NOT ゲートのみによって構成される回路と比べ，それぞれのワイヤーの最後の層に，NOT ゲートが有るか否かの差しかない．そのため，C-NOT ゲートと NOT ゲートしか使用しない回路が出力できるパターン数は，C-NOT のみの回路が出力できるパターン数の高々 2^n 倍となる．

□

7 おわりに

今年度の本研究では，量子回路計算量と制御 NOT ゲート数の関係について議論を行なった．

これらの議論より，量子回路計算量の評価においては，C-NOT ゲート数が本質的であることがわかったが，一方，C-NOT ゲートや NOT ゲートのみでは，単純な回路しか構成できないことも判明した．

今後の課題としては，C-NOT ゲートとある特定の 1 量子ビットゲートのみからなる回路のサイズを評価することなどがあげられる．

参考文献

[1] 上坂吉則: 「量子コンピュータの基礎数理」，コロナ社, 2000.

[2] A. Barenco, *et al.*: "Elementary gates for quantum computation", *Physical Review*, Vol. A 52 pp. 3457-3467, 1995.

[3] A. Nielsen: "A geometric approach to quantum circuit lower bounds", quant-ph/0502070, 2005.

研究業績一覧

学術論文

1. J. Tarui:
"On the Minimum Number of Completely 3-Scrambling Permutations", Discrete Mathematics, （to appear）.
概要: 集合 $[n] = \{1, ..., n\}$ の置換の族 P は次の条件を満たすとき k-completely scrambling [Spencer 1972; Furedi 1996] と呼ばれる：任意の異なる $x_1, ..., x_k \in [n]$ に対して、置換 $\pi \in P$ により $\pi(x_1), ..., \pi(x_k)$ に関する $k!$ 個すべての順序が作られる。このような族の最小サイズを $N(n, k)$ とする。本論文では $k = 3$ にフォーカスする。シンプルな構成的方法により次の上界を与える： $N(n, 3) \leq (2 + o(1))log_2 n$. さらに $lim_{n\to\infty} N(n, 3)/(log_2 n) = c_3$ が存在することを示す。c_3 の値を決定することと $k \geq 4$ について $limN(n, k)/(log_2 n) = c_k$ の存在を示すことは未解決問題として残る。

2. 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 $O(n^3 logn)$, respectively. The number of qubits used in the circuit is less than that in any other quantum circuit ever construted 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.

3. Yuichi Komano and Kazuo Ohta:
"Taxonomical Security Consideration of OAEP Variants", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E89-A, No.5, pp.1233-1245, 2006.
概要: We first model the variants of OAEP and SAEP by changing a construction and position of a redundancy, and establish a universal proof technique in the random oracle model, the comprehensive event dividing tree. We then make a taxonomical security consideration of the variants of OAEP and SAEP, based on the assumptions of one- wayness and partial-domain one-wayness of the encryption permutation, by applying the tree. Furthermore, we demonstrate the concrete attack procedures against all insecure schemes; we insist that the security proof failure leads to some attacks. From the security consideration, we find that one of the variants leads to a scheme without the redundancy; the scheme is not PA (plaintext aware) but IND-CCA2 secure. Finally, we conclude that some of them are practical in terms of security tightness and short bandwidth.

4. Mitsugu Iwamoto, Lei Wang, Kazuki Yoneyama, Noboru Kunihiro and Kazuo Ohta:
"Visual Secret Sharing Schemes for Mul-

tiple Secret Images Allowing the Rotation of Shares", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E89-A, No.5, pp.1382-1395, 2006.
概要: In this paper, a method is proposed to construct a visual secret sharing (VSS) scheme for multiple secret images in which each share can be rotated with 180 degrees in decryption. The proposed VSS scheme can encrypt more number of secret images compared with the normal VSS schemes. Furthermore, the proposed technique can be applied to the VSS scheme that allows to turn over some shares in decryption. From the theoretical point of view, it is interesting to note that such VSS schemes cannot be obtained from so-called basis matrices straightforwardly.

5. N. Kunihiro W. Abe and K. Ohta:
"Maurer-Yacobi ID based Key Distribution Revisited", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E89-A, No.5, pp.1421-1424, 2006.
概要: Maurer and Yacobi proposed an ID-Based key distribution scheme in 1991. In this scheme, the private key for each user is generated by solving discrete logarithm problem. We examine the realizability of this scheme. We show that this scheme can be practical by appropriate parameter setting.

6. 伊豆哲也，國廣昇，太田和夫，武仲正彦:
"双線形写像を用いた墨塗り署名方式の安全性について", 情報処理学会論文誌, Vol. 47, No. 7, pp.2409-2416, 2006.
概要: 部分情報がマスキング（墨塗り）された電子文書において，開示部分の完全性と非開示部分の秘匿を両立させる暗号要素技術として墨塗り署名が注目を集めている．2005 年 1 月に宮崎・花岡・今井が提案した双線形写像を用いた墨塗り署名方式（本稿では SUMI-6 と呼ぶ）は上の性質に加え，墨塗り箇所数の秘匿と墨塗り者による開示条件のコントロールが可能という特徴を持っている．しかしアルゴリズムや技術が不十分であったり，条件の妥当性の議論に欠けたりするという問題があった．本稿はさらなる安全性解析を目的として SUMI-6 を詳細検討し，条件によっては可能となるいくつかの問題点を指摘する．また SUMI-6 の改良墨塗り署名方式 SUMI-6' を提案し，その安全性を議論する．さらに，宮崎らが別に提案した墨塗り署名方式 SUMI-5 に対して，双線形写像を用いて改良を施した墨塗り署名方式 SUMI-5' の提案・検討を行う．

7. Yu SASAKI, Yusuke NAITO, Noboru KUNIHIRO and Kazuo OHTA:
"Improved Collision Attacks on MD4 and MD5", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E90-A, No.1, pp.36-47, 2007.
概要: At Eurocrypt'05, Wang et al. presented efficient collision attacks on MD5 and MD4 hash functions. They found a collision of MD5 with a complexity of less than $2^{3}7$ MD5 hash operations, and a collision of MD4 with complexity less than 28 MD4 hash operations. In their attack, the procedure to generate a collision is divided into 4 steps. First, they determine the message differential and output differentials of chaining variables in each step, which generates a collision with small complexity. Second, they construct sufficient conditions that guarantee that the desired differential is always calculated. Third, they find a message modification that can satisfy the sufficient conditions with high probability. Finally, they search for a message that satisfies all sufficient conditions. In this paper, we focus on the message modification of MD5 and MD4, and propose a new message modification. Using our message modification, a collision of MD5 can be found with

complexity less than 229 MD5 hash operations, and a collision of MD4 can be found with complexity less than 3 MD4 hash operations. To improve the complexity from previous attacks, we mainly use two ideas. The first idea is to use message modification that can satisfy more sufficient conditions in the second round than in previous attacks. The second idea is to use message modification that can enable us to search for a collision starting from an intermediate step.

8. Yuichi KOMANO, Kazuo OHTA, Atsushi SHIMBO and Shinichi KAWAMURA:
"Toward the Fair Anonymous Signatures: Deniable Ring Signatures", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E90-A, No.1, pp.54-64, 2007.
概要: Ring signature scheme enables a signer to sign a message anonymously. In the ring signature scheme, the signer who wants to sign a document anonymously first chooses some public keys of entities (signers) and then generates a signature which ensures that one of the signer or entities signs the document. In some situations, however, the ring signature scheme allows the signer to shift the blame to victims because of the anonymity. The group signature scheme may be a solution for the problem; however, it needs an electronic big brother, called a group manager, who can violate the signer anonymity by himself, and a complicated key setting. This paper introduces a new notion of a signature scheme with signer anonymity, a deniable ring signature scheme (DRS), in which no group manager exists, and the signer should be involved in opening the signer anonymity. We also propose a concrete scheme proven to be secure under the assumption of the DDH (decision Diffie Hellman) problem in the random oracle model.

9. Haruki OTA, Kazuki YONEYAMA, Shinsaku KIYOMOTO, Toshiaki TANAKA and Kazuo OHTA:
"Universally Composable Hierarchical Hybrid Authenticated Key Exchange", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E90-A, No.1, pp. 139-151, 2007.
概要: Password-based authenticated key exchange protocols are more convenient and practical, since users employ human-memorable passwords that are simpler to remember than cryptographic secret keys or public/private keys. Abdalla, Fouque, and Pointcheval proposed the password-based authenticated key exchange protocol in a 3-party model (GPAKE) in which clients trying to establish a secret do not share a password between themselves but only with a trusted server. On the other hand, Canetti presented a general framework, which is called universally composable (UC) framework, for representing cryptographic protocols and analyzing their security. In this framework, the security of protocols is maintained under a general protocol composition operation called universal composition. Canetti also proved a UC composition theorem, which states that the definition of UC-security achieves the goal of concurrent general composition. A server must manage all the passwords of clients when the 3-party password-based authenticated key exchange protocols are realized in large-scale networks. In order to resolve this problem, we propose a hierarchical hybrid authenticated key exchange protocol (H2AKE). In H2AKE, forwarding servers are located between each client and a distribution server, and the distribution server sends the client an authentication key via the forwarding servers. In H2AKE, public/private keys are used between servers, while passwords are also used between clients and

forwarding servers. Thus, in H2AKE, the load on the distribution server can be distributed to the forwarding servers concerning password management. In this paper, we define hierarchical hybrid authenticated key exchange functionality. H2AKE is the universal form of the hierarchical (hybrid) authenticated key exchange protocol, which includes a 3-party model, and it has the characteristic that the construction of the protocol can flexibly change according to the situation. We also prove that H2AKE is secure in the UC framework with the security-preserving composition property.

10. Yasuhiro Takahashi, Noboru Kunihiro, and Kazuo Ohta:
"The Quantum Fourier Transform on a Linear Nearest Neighbor Architecture", Quantum Information and Computation, Vol.7 No.4, pp.383-391, 2007.
概要: We show how to construct an efficient quantum circuit for computing a good approximation of the quantum Fourier transform on a linear nearest neighbor architecture. The constructed circuit uses no ancillary qubits and its depth and size are $O(n)$ and $O(nlogn)$, respectively, where n is the length of the input. The circuit is useful for decreasing the size of Fowler et al.'s quantum circuit for Shor's factoring algorithm on a linear nearest neighbor architecture.

11. Yoshikazu Hanatani, Yuichi Komano, Kazuo Ohta and Noboru Kunihiro:
"Provably Secure Untraceable Electronic Cash against Insider Attacks", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E90-A, No.5, (2007, to appear).
概要: Although a great deal of research has been done on electronic cash schemes with blind multisignatures to prevent an insider attack, there is no discussion of a formal security model in the literature. Firstly we discussed the security model of ecash schemes based on the blind multisignature scheme against a (restricted) attack model and proposed a concrete scheme proven to be secure in the model [1]; however, this attack model disallows an attacker from corrupting an issuing bank and shops in the forgery game. In this paper, first, we reconsider the security model to remove the restriction of the attack model. Second, we propose a new untraceable e-cash scheme with a blind multisignature scheme and prove that the proposed scheme is secure against the (non-restricted) attacks under the DDH assumption in the random oracle model.

12. Takashi Nishide and Kazuo Ohta:
"Constant-Round Multiparty Computation for Interval Test, Equality Test, and Comparison", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E90-A, No.5, (2007, to appear).
概要: We propose constant-round protocols for interval tests, equality tests, and comparisons where shared secret inputs are not given bitwise. In [9]. Damgard et al. presented a novel protocol called the bit-decomposition, which can convert a polynomial sharing of an element in prime field Z_p into sharings of bits. Though, by using the bit-decomposition protocol, those protocols can be constructed with constant round complexities theoretically, it involves expensive computation, leading to relatively high round and communication complexities. In this paper, we construct more efficient protocols for those protocols without relying on the bit-decomposition protocol. In the interval test protocol, checking whether a shared secret exists in the known interval is reduced to checking whether a bitwiseshared random secret exists in the

appropriate interval. In the comparison protocol, comparing two shared secrets is reduced to comparing the two secrets via $p/2$ indirectly where p is an odd prime for an underlying linear secret sharing scheme. In the equality test protocol, checking whether two shared secrets are equal is reduced to checking whether the difference of the two secrets is zero and furthermore checking whether the difference is a zero is reduced to checking quadratice residuosity of a random secret in a probabilistic way.

研究会等

1. Seiya Okubo and Tetsuro Nishino:
"NMR Quantum Algorithms and Information Security", International Symposium on Advanced ICT (AICT) 2006, pp.289-297, August, 2006.
概要: In this paper, we propose the bulk quantum Turing machine (BQTM for short) which is a mathematical model of the NMR (Nuclear Magnetic Resonance) quantum computer (NMRQC for short) and two efficient quantum algorithms on BQTM to solve some problems which are closely related to some security problems. Namely, we discuss the computational complexity of the searching problem and the minimum finding problem on NMR quantum computers with the measurement accuracy ε. Since our proposed algorithm is more efficient than ordinary quantum algorithms on ordinary quantum computers, we can conclude that NMRQCs are more effective to security problems.

2. Shin-ichi Hashiba, Seiya Okubo and Tetsuro Nishino:
"Efficient Quantum Algorithms for Algebraic Problems", International Conference on Computer & Communication Engineering (ICCCE '06), pp.567-572, May 9-11, 2006.
概要: In this paper, we deal with so called counting problems. For these problems efficient classical or quantum algorithms are not known. But, these problems are very important in some practical applications. So, in this paper, we show how to efficiently compute the permanent of a matrix by using NMR quantum computation.

3. J. Tarui:
"Finding a Duplicate and a Missing Item in a Stream", TAMC07-LNCS: Lecture Notes in Computer Science: Proceedings of TAMC07: The 4th Annual Conference on Theory and Applications of Models of Computation, May 22-25, 2007, (to appear).
概要: 次のストリーム計算問題を考える. 入力は $a = \langle a_1, ..., a_m \rangle$, ただし各 $a_i \in \{1, ..., n\}$ で $m > n$. 入力の中の duplicate, すなわち, ある $d = a_i = a_l, i < l$ を s ビットのメモリーと r 回のパスによって見つけたい. アルゴリズムは1回のパスで入力を $a_1, ..., a_m$ の順に読む. 鳩の巣原理により duplicate は存在する. 次の下界を示す：$s = O(logn)$ であれば $r = \Omega(logn/loglogn)$.

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}@j.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」

- 築地は，唯一最短格子ベクトル問題を解く量子アルゴリズムの設計と解析を行った．
- Chen は，築地と共同して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複雑さの研究，ならびに近似アルゴリズムの設計と解析を行った．
- 松浦は，有限オートマトンの等価変換と状態数解析を行った．また，六角盤面上の一般三並べの先手必勝問題を研究した．

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）．

3 唯一最短格子ベクトル問題を解く量子アルゴリズムの設計と解析

唯一最短格子ベクトル問題を，多項式の大きさ指数をもつ多次元整数環上のサイモン問題に帰着させた．このように一般化されたサイモン問題を線型計画問題に帰着させて，既知のアルゴリズムにより，多項式時間でとけることを確認した（投稿準備中）．

4 相関グラフから遺伝系統図を構築する問題の計算複雑さ，ならびにその近似アルゴリズムの設計と解析について

与えられたグラフが非連結の場合でも，遺伝系統図の次数が有限であれば，ダイナミックプログラミングの手法が適用できて，線形時間アルゴリズムが適用されることを確認した．また，遺伝系統図の次数が有限で，かつデータが誤差を含むとき，最適化問題の解法がＮＰ困難であることを証明した

5 有限オートマトンの等価変換と状態数解析

有限オートマトンとしては, 入力記号に応じて遷移状態が一意に決定される決定性オートマトン (DFA), 複数の遷移状態を持つ非決定性オートマトン (NFA) 等が代表的なものとして知られる. NFA を等価極小な DFA に変換すると, 一般に状態数が指数オーダーに増加する．これまで, 入力記号が状態数に比例する程度である場合には, $0 \leq \alpha \leq 2^n - n$ を満たす任意の整数 α に対して, n 状態 NFA で, それと等価な DFA が $2^n - \alpha$ 状態有するものが知られている (G. Jirásková, Proc. of MFCS 2001), また, 入力記号が一種類, すなわち unary の場合は, 無数の α に対し, そのような NFA は存在しないことが示されている (V. Geffert, Proc. of MFCS 2006). 入力記号が $\{0,1\}$ である場合は, これまで $0 \leq \alpha \leq 2n-2$ の範囲にある α に対してしか, そのような NFA の存在は知られていない.

本研究においては, 入力記号が $\{0,1\}$ で, かつ n が奇数である場合に, $\alpha \leq 3n-3$ の範囲で上記の条件を満たす n 状態 NFA が存在することを示した. 証明においては, α の値が $3n-3$ 以下のそれぞれの場合に, 実際に $2^n - \alpha$ 状態の DFA と等価となる n 状態の NFA を構成する. ちょうど $2^n - \alpha$ 状態となることを示すために, 到達不可能な状態については, 列挙して到達不可能性を示し, 到達可能な状態については, 状態サイズが小さいものから順次到達可能であることを帰納的に示す．この NFA の族を拡張することにより, α の値が $4n-4$ 以下の場合にも, α が 4 の倍数でない限り, 所望の NFA が存在することを示した. 本結果は, 現在投稿準備中である.

6 六角盤面上の一般三並べの先手必勝問題

一般化三並べとは, 指定されたサイズの盤面上に 2 人で交互に石を置いていき, 指定された図形 (生物) を先に作ることを競うゲームである．その単純な問題設定にも関わらず, 単純な探索では計算量が指数爆発を起こしてしまうため, その組合せ構造を解析する研究が数多く行われている. 本ゲームにおいては, 先に着手した一手が不利に働く事はなく, 後手に必勝手順があると仮定すると先手はそれを利用して必勝手順を作ることができるため, 後手に必勝手順はない．つまり，両者が最適な手を打つ限り, 先手が勝つか引き分けとなる．先手が勝つ図形を勝ち型, 引き分けとなる図形を負け型と呼ぶ.

本研究では, 用いる盤面を通常の正方盤面から正六角形盤面に変更し, 指定された図形の先手必勝問題を考察した．これまで, 4 つまでのタイルから成る全ての図形に関して, 全てのサイズの盤面 ($m \times m \times m$) に対して, 負け型である場合, および, 勝ち型である場合は手順の最小性を示した. また, 5 つのタイルから成る 22 種類の図形に関しては, 16 種類が勝ち型であること, 2 種類が負け型であることを示した. 残りの 4 種類は未解決で現在調査中である.

研究業績一覧

学術論文

1. Zhi-Zhong Chen, Tatsuie Tsukiji:
"Computing Bounded-Degree Phylogenetic Roots of Disconnected Graphs", Journal of Algrithms, 59(2), pp. 125-148, 2006.
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.

2. Tatsuie Tsukiji, Zhi-Zhong Chen:
"Computing Phylogenetic Roots with Bounded Degrees and Errors Is Hard", Theoretical Computer Science, 363(1), pp. 43-59, 2006.
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.

3. Zhi-Zhong Chen, Michelangelo Grigni, Christos H. Papadimitriou:
"Recognizing Hole-Free 4-Map Graphs in Cubic Time", Algorithmica, 45(2), pp. 227-262, 2006.
概要: We present a cubic-time algorithm for the following problem: Given a simple graph, decide whether it is realized by adjacencies of countries in a map without holes, in which at most four countries meet at any point. Key words. planar graphs, maps, map graphs, cliques, graph algorithms.

4. Zhi-Zhong Chen:
"New Bounds on the Number of Edges in a k-Map Graph", Journal of Graph Theory, (掲載予定).
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 $k \geq \frac{140}{41\epsilon}$, 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.

5. Zhi-Zhong Chen:
"Approximation Algorithms for Bounded Degree Phylogenetic Roots", Algorithmica, (掲載予定).
概要: The Degree-Δ Closest Phylogenetic kth Root Problem (ΔCPR$_k$) 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 in 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, i.e., $|E \oplus \{\{u, v\} : u, v$ are leaves of T and $d_T(u, v) \leq k\}|$, is minimized, where $d_T(u, v)$ denotes the distance between u and v in tree T. This problem arises from theoretical studies in evolutionary biology and generalizes several important combinatorial optimization problems such as the maximum matching problem. Unfortunately, it is known to be NP-hard for all fixed constants Δ, k such that either both $\Delta \geq 3$ and $k \geq 3$, or $\Delta > 3$ and $k = 2$. This paper presents a polynomial-time 8-approximation algorithm for ΔCPR$_2$ for any fixed $\Delta > 3$, a quadratic-time 12-approximation algorithm for 3CPR$_3$, and a polynomial-time approximation scheme for the maximization version of ΔCPR$_k$ for any fixed Δ and k.

6. Zhi-Zhong Chen, Takayuki Nagoya:
"Improved Approximation Algorithms for Metric Max TSP", Journal of Combinatorial Optimization, (掲載予定).
概要: We present two polynomial-time approximation algorithms for the metric case of the maximum traveling salesman problem. One of them is for directed graphs and its approximation ration is $\frac{27}{25}$. The other is for undirected graphs and its approximatin ratio is $\frac{7}{8} - o(1)$. Both algorithms improve on the previous bests.

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: 本報告では，平成 18 年度の B05 班の研究活動に関係する成果を報告する．特に, 動的な木構造ネットワークにおけるフロー問題に対する高速アルゴリズム，ならびに，正モジュラシステムの最小横断に対する成果に重点を置き説明する．

キーワード: 計算効率，アルゴリズム，正モジュラシステム，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．本年度は，

1. 動的な木構造ネットワークにおけるフロー問題に関する成果 [7].
2. 正モジュラシステムの最小横断に関する成果 [9].
3. 最小枝ランキング全域木に関する成果 [5].
4. 2 次元平面上を動くロボットのスケジューリング問題に関する成果 [2].

の 4 つ挙げられる．以下の章では，2. 3. の動的な木構造ネットワークにおけるフロー問題に関する成果と正モジュラシステムの最小横断に関する成果に重点を置き報告する．

1.1 動的ネットワーク中の避難施設配置問題

点集合が V, 枝集合が A である（有向）グラフを $G = (V, A)$ と記す．ここで，$n = |V|$，$m = |A|$ とする．$c : A \to \mathbb{R}_+$ $c : A \to \mathbb{R}_+$ は各枝に非負の実数を与える容量関数，$\tau : A \to \mathbb{Z}_+$ は各枝始点から終点への輸送時間を与える非負整数値関数である とする．このようにグラフ G の枝に容量関数 c と輸送時間 τ が付与されたものを動的ネットワーク（dynamic network）と呼び, $\mathcal{N} = (G = (V, A), c, \tau)$ と表す.

いま，動的ネットワークの各点に供給量 $b : V \to \mathbf{R}_+$ が与えられているとする．このとき全ての点 v の供給量 $b(v)$ を最速で送り届けられるような出口 $t \in V$ を 求める問題を動的ネットワーク上における施設配置問題と呼ぶ．より正確には，$V \setminus \{t\}$ からの供給量を t へ流す動的フローを考えたときに，その全てのフローが t に到着する時間を最小にする出口 t を求める施設配置問題である． この問題は，交通ネットワークにおいて，すべての人が 最速に避難できるような避難施設をネットワーク中に 1ヵ所求めるという問題であり，静的ネットワーク・フローに基づくソース/シンク配置問題 [1, 10, 11] の動的版，あるいは，1-センター問題 [8] の動的フロー版としてとらえることができる．

以下では，離散時間動的フローの定義を与える．任意の枝 $(u, v) \in A$, $\theta \in \{0, 1, \cdots, \tau(u, v)\}$, $k \in \mathbf{Z}_+$ に対して，$f_k((u, v), \theta)$ を時刻 k に枝 (u, v) の第 θ 部を流れるフロー量とする．ただし，$f_0((u, v), \theta) = 0$ $(1 \le \theta \le \tau(u, v))$ と定義する．これは，時刻 0 において，枝の始点以外の部分を流れるフローがないことを表す．この $f_k((u, v), \theta)$ $((u, v) \in A,\ \theta \in \{0, 1, \cdots, \tau(u, v)\},\ k \in \mathbf{Z}_+)$ が以下に示す (a)，(b)，(c) の条件を満足するとき，ネットワーク $\mathcal{N}$ 上の出口 t に対する動的フローと呼ぶ．

(a) 容量条件 (Capacity constraints): 任意の $(u, v) \in A$, $\theta \in \{0, 1, \cdots, \tau(u, v)\}$, $k \in \mathbf{Z}_+$ に 対して，

$$0 \le f_k((u, v), \theta) \le c(u, v) \tag{2.7}$$

が成立する．

(b) フロー移動条件 (Flow transition): 任意の $(u, v) \in A$, $\theta \in \{0, 1, \cdots, \tau(u, v) - 1\}$, $k \in \mathbf{Z}_+$ に対して，

$$f_k((u, v), \theta) = f_{k+1}((u, v), \theta + 1) \tag{2.8}$$

が成立する．

(c) 流量保存則 (Flow conservation): 任意の $v \in V \setminus \{t\}$，$k \in \mathbf{Z}_+$ に対して，

$$\sum_{u:(u,v)\in A} f_k((u, v), \tau(u, v)) + h_{k-1}(v) = \sum_{w:(v,w)\in A} f_k((v, w), 0) + h_k(v) \tag{2.9}$$

$$h_{-1}(v) = b(v), \quad h_k(v) \ge 0 \quad (k = 0, 1, \cdots) \tag{2.10}$$

が成立する．ただし，$f_k((v, w), 0)$ は，時刻 k において w に向かい v を離れたフロー量，$h_k(v)$ は，時刻 k において点 v に留まるフロー量を表す．すなわち，各点でフローの滞留を許すモデルである．

この定式化において，条件（a）は，どの時刻どの地点においてもフロー量が容量条件をみたすことを意味している．条件（b）は，枝 (u, v) の第 θ 部を流れるフローは，1 単位時間で枝 (u, v) の第 $\theta + 1$ 部に移動することを示している．また，条件（c）は，出口 t 以外の点 v では，各時刻 k に v に到達するフロー量と時刻 $k - 1$ に v で滞留したフロー量との総和が各時刻 k に v を去るフロー量と時刻 k に v で滞留したフロー量との総和と等しいことを示している．

我々が扱う施設配置問題においては，(c) に示すように各点でのフローの滞留を許すモデルを用いているが，許さないモデルでも最適解等は不変である（この性質は，例えば，[3, 4] で議論されている）．

一般に動的フローに関する問題は，与えられた動的ネットワークに対する時間展開ネットワーク上での静的フローを扱うことにより解かれる [3]. 動的ネットワーク $\mathcal{N} = (G = (V, A), c, \tau)$ と時間区間 T に対する時間展開ネッ トワーク (time-expanded network) $\mathcal{N}(T)$ とは，容量関数 $c : A \to \mathbb{R}_+$ 付き有向グラフ $G(T) = (V(T), A(T))$ のことである．ここで，$V(T)$ は，元の動的ネットワークの各点 $v \in V$ に対して，$(T + 1)$ 個のコピー $v(0), \cdots, v(T)$ を作り，それらの全体としたもの，すなわち，

$$V(T) \quad = \quad \{v(0), \cdots, v(T) \mid v \in V\}$$

であり，$A(T)$ は，元の動的ネットワークの各枝 $(u, v) \in A$ に対して，$(u(\theta), v(\theta + \tau(u, v)))$ $(\theta =$

$0, 1, \cdots, T - \tau(u, v))$ というように，u と v を $\tau(u, v)$ 分ずらし結んだ $(T-\tau(u, v)+1)$ 個のコピーと，各点 $v \in V$ に対する T 本の残留枝 (holdover arc) $(v(\theta), v(\theta + 1))$ $(\theta = 0, 1, \cdots, T - 1)$ を要素とするものである．

$$A(T) = \{(u(\theta), v(\theta + \tau(u, v))) \mid (u, v) \in A, \theta = 0, 1, \cdots, T - \tau(u, v)\} \cup \{(v(\theta), v(\theta + 1)) \mid v \in V, \theta = 0, 1, \cdots, T - 1\}.$$

枝の容量は，コピー枝 $(u(\theta), v(\theta + \tau(u, v))$ には元の枝の容量 $c(u, v)$，残留枝には無限大を与えるものとする．定義から明らかに，時刻 T までの動的フロー f は，$\mathcal{N}(T)$ 中の静的フローとして表現される。

本研究で扱う避難施設配置問題は，入口 $v \in V \setminus \{t\}$，出口 t とする多始点 1 終点の最速動的フロー問題を n 回（出口 t を取り替えることにより）解くことにより最適な出口 $t \in V$ を求めることができる．すなわち，時間展開ネットワークを用い，最速時間 T を求めること（例えば，2 分探索を行う）により解くことはできるが，一般に時間展開ネットワークのサイズは入力の多項式サイズではなく，多項式時間解法ではない．Hoppe–Tardos [4] は，多始点多終点の最速動的フロー問題をこのような時間展開ネットワークを用いない強多項式時間アルゴリズムを開発した．従って，動的ネットワーク上の施設配置問題も強多項式時間で解けることが分かる．しかしながら，Hoppe–Tardos のアルゴリズムは，高次多項式時間アルゴリズムであり，必ずしも，実用的であるとは言えない．次節では，ネットワークが木構造であるとき，施設配置問題が高速に解けることを示す．

木構造動的ネットワーク中の避難施設配置問題

$G = (V, A)$ の枝を無向化することによって得られるグラフが木（tree）になるとき，動的ネットワーク $\mathcal{N} = (G = (V, A), c, \tau)$ が木構造であると言う．本節では，木構造動的ネットワーク $\mathcal{N} = (G = (V, A), c, \tau)$ における施設配置問題のアルゴリズムを与える．

交通ネットワークにおいて，すべての人がある避難施設 t に退避する状況を考えよう．このとき，ある点 v にいる人 α さんと β さんが，異なった避難路で施設 t に避難誘導されたとすると，避難誘導が混乱し，また，α さんと β さんの間に不公平が生じる．1 つの解決策として，同じ点 v にいる人は，すべて同じ経路で避難するという方法が考えられる．したがって，本研究では，一般の動的ネットワーク中の施設配置問題を以下に示すように 2 つのステップに分けて解くことを提案する．

(i) ネットワーク中で全域木を作る．

(ii) (i) で求めた全域木の中で最適な施設配置問題を解く．

もちろん，(i)(ii) まとめて，最速に退避できるような全域木とそれに基づく避難施設配置点 t を同時に求めることが望ましい．しかしながら，このような問題は，計算量の観点から難しいので，本研究では，(i),(ii) を別にして，(i) では，供給量 b，移動時間 τ，容量 c，グラフの形状（例えば，次数 (degree) や直径 (diameter) など）を考慮して，退避時間が小さくなるように全域木を求め，(ii) で，それに基づく配置点 t を求めることとする．(i) の基準として，例えば，枝コスト τ/c を最小にする全域木などが考えられる．本節では，上記の (ii) を多項式時間で行うアルゴリズムを紹介する．

以下での説明を簡単にするため，$G = (V, A)$ は，（無向）木 $T = (V, E)$ の枝を有向化したグラフ，すなわち，$A = \vec{E}$ $(= \{(u, v), (v, u) \mid \{u, v\} \in E\})$ であると仮定する．

提案するアルゴリズムは，各点 $v \in V$ が到着テーブル（Arriving Table）A_v と送出テーブル（Sending table）S_v という 2 つのテーブルを用いる．到着，送出テーブルともに時刻 k の関数であり，到着テーブルは，時刻 k に点 v に到着するフロー量

$$\sum_{u:(u,v)\in\vec{E}} f_k((u, v), \tau(u, v)) + \eta_k(v) \qquad (2.11)$$

を表し（ただし，$\eta_0(v) = b(v)$ and $\eta_k(v) = 0$ $(k = 1, 2, \cdots)$），送出テーブルは，時刻 k に点 v からその親 v' に向う (与えられた出口 t を根としたとき) 送出されるフロー量

$$f_k((v, v'), 0) \qquad (2.12)$$

を表す．図2.1では，到着，送出テーブルの例を示す．

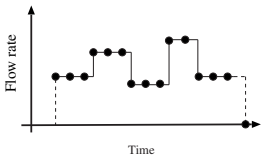


図 2.1: An example of table.

このようなテーブルを葉から順に構成する２つのフェイズから成る $O(n^2)$ 時間アルゴリズムが提案されていた [6]．本研究では，高速なアルゴリズムを開発するために，まず，１つのフェイズから成るアルゴリズムを構成し，次に，そのアルゴリズムにデータ構造として，動的に構造変更が可能な平衡２分木を用いる．このことにより，$O(n \log^2 n)$ 時間アルゴリズムを構成する．平衡２分木を用いたデータ構造の説明は，非常に技巧的，かつ，複雑であるので，本報告では，省略して，１つのフェイズから成るシンプルなアルゴリズムを紹介する．なお．このアルゴリズムは，素直なデータ構造を用いると $O(n^2)$ 時間必要となり，単にこのアルゴリズムを用いるだけでは，計算時間の改善はない．しかし，このアルゴリズムがシンプルであるため，上記の平衡２分木をうまく用いることがてきるため，結果として計算時間が改善される．

下記のシングルフェイズアルゴリズムは，直感的に，まず全ての葉のテーブルを作る．次に，作ったテーブルを利用することで，最適出口にはならない葉 v^*（より正確には，自分以外に最適出口が存在するような葉 v^*）を見つけ，その点を木 T から除く．v^* を除くことにより新たに葉となった点があれば，その点のテーブルを作る．ここで新たに葉となりうる点は高々一つであることに注意されたい．上記の作業を繰り返し行い，最終的に一点となったとき，その点を最適出口として出力するというものである．

アルゴリズム シングルフェイズ

入力: 木構造動的ネットワーク $\mathcal{N} = (T = (V, E), c, \tau, b)$.

出力: 最小輸送完了時間 $C(t)$ と，それを与える出口 t.

ステップ 0: $W := V, T$ の葉の集合 を L とする．各 $v \in W$ に対して到着テーブル A_v をつくる．

ステップ 1: L に含まれる全ての点 v に対して，A_v に基づき v から $p(v)$ への送出テーブル S_v を作り，v から $p(v)$ へのフローの最終到着時刻 $Time(v)$ を求める．

ステップ 2: $\min_{v^* \in L} Time(v^*) = Time(v)$ である $v^* \in L$ に対して，$W := W \setminus \{v^*\}, L := L \setminus \{v^*\}$.
もし，$T[W]$ の葉でかつ，L に属さない点 v があれば，$L := L \cup \{v\}$ とする．さらに W に属さず v に隣接する点の送出テーブルに基づき v の到着テーブル A_v を作る．

ステップ 3: $|W| = 1$ であれば，そ の点を t として出力する．また，t の到着テーブルを作ることにより，最小輸送完了時間 $C(t)$ も出力する．
そうでなければ，ステップ２へ．
□

このアルゴリズムの各反復において，ステップ２終了時には，L が絶えず $T[W]$ の葉 集合であることに注意されたい．

補題 1 シングルフェイズアルゴリズムは最適出口 t を出力する．

証明 点 t 以外の点 u が最適解であると仮定する．このとき，t と u を結ぶパス上で，t に隣接する頂点を w とする．いま，枝 (t, w) を除くことによりできる２つの連結成分で t 側のものを U_1 とする．また，$U_2 = U_1 \cup \{w\}$，$U_3 = (V - U_1) \cup \{t\}$ とする．木 $T[U_1]$ において出口を t としたときの最小輸送完了時間を k_1，木 $T[U_2]$ において出口を w としたときの最小輸送完了時間を k_2，木 $T[U_3]$ において出口を t としたときの最小輸送完了時間を k_3 とする．定義より明らかに

$$k_1 \leq k_2, \quad C(t) = max\{k_1, k_3\}, \quad C(u) \geq k_2 \tag{2.13}$$

また，k_3 はアルゴリズムのステップ1で計算され，ステップ2で，$Time(w) = min_{v \in L}\, Time(v)$ をみたすことにより，w が W, L から除かれているので，$k_3 \leq k_2$．さらに式 (2.13) より，$C(t) \leq C(u)$ が成立する．したがって，$C(t) = C(u)$ を得る．すなわち．アルゴリズムから出力された点 t も最適出口である． □

上記に説明したようにこのアルゴリズムにおいて，各テーブルを平衡2分木を用いて，間接的に表現することで高速化することができる．

定理 1 動的ネットワークが木構造であるとき，施設配置問題が $O(n \log^2 n)$ 時間で解くことができる．

2 正モジュラシステムの最小横断

最小横断問題とは，有限集合 V と $f(\emptyset) \geq d(\emptyset)$ を満たす2つの集合関数 $f : 2^V \to \mathbf{R}$, $d : 2^V \to \mathbb{R}$ から成るシステム (V, f, d) が与えられたとき，すべての $X \subseteq V - R$ に対して $f(X) \geq d(X)$ を満たす最小サイズの $R \subseteq V$ を求める問題である [9].

$$\begin{array}{ll} \text{Minimize} & |R| \\ \text{subject to} & f(X) \geq d(X) \text{ for all } X \subseteq V - R \\ & R \subseteq V. \end{array}$$

ここで， $f(\emptyset) \geq d(\emptyset)$ を仮定する．定義から明らかに，f，d が一般の集合関数のときは，効率に解くことができない．我々は，f が正モジュラ，劣モジュラ関数，d が模調関数であるときの最小横断問題を考察した．ここで，集合関数 $f : 2^V \to \mathbb{R}$ が劣モジュラであるとは，任意の V の部分集合 X, Y に対して，

$$f(X) + f(Y) \geq f(X \cup Y) + f(X \cap Y) \quad (2.14)$$

が成立することであり，正モジュラ関数であるとは，任意の V の部分集合 X, Y に対して，

$$f(X) + f(Y) \geq f(X - Y) + f(Y - X) \quad (2.15)$$

が成立することである．また，$d : 2^V \to \mathbb{R}$ が，すべての非空な $X \subseteq V$ が下記の条件を満たす $v \in X$ をもつとき， 模調であるといわれる．

$$d(Y) \geq d(X) \text{ for all } Y \subseteq X \text{ containing } v.$$

この問題は，ネットワーク設計問題として重要なソース配置問題や外部ネットワーク問題などの一般化とみなすことができる．ソース入り問題とは，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，近年盛んに研究されている．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．より正確には，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 $p : V \to \mathbb{R}_+$ 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．

$$\begin{array}{ll} \text{Minimize} & |S| \\ \text{subject to} & \lambda_{\mathcal{N}}(S, v) \geq p(v) \text{ for all } v \in V \\ & S \subseteq V, \end{array}$$

ただし，$\lambda_{\mathcal{N}}(S, v)$ は，ネットワーク $\mathcal{N}$ 中の S-v 間の最大フロー量を示す．このソース配置問題は，最大フロー最小カット定理を用いることで，f が正モジュラ，劣モジュラ関数，d が模調関数である最小横断問題であることが分かる．

我々は，正モジュラ f があり，d が模調であるならば，極小な不足集合族が木ハイパーグラフとなることを示した．逆に，任意の木ハイパーグラフは，正モジュラ関数 f と 模調関数 d に対する最小横断問題の極小な不足集合族として表現可能であることも示した．

さらに，この構造的な特徴付けを用いることで，f が正，かつ劣モジュラ関数であり，d がある $p : V \to \mathbf{R}_+$ に対して，

$$d(X) = \max\{p(v) \mid v \in X\}$$

となるとき，あるいは，ある $r : V^2 \to \mathbf{R}_+$ に対して，

$$d(X) = \max\{r(v, w) \mid v \in X, w \in V - X\}$$

となるときに, 最小横断問題に対する多項式時間アルゴリズムを開発した. また, このアルゴリズムを用いることで無向ネットワークにおける外部ネットワーク問題も効率的に解けることを示した.

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] 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*, 154 (2006) 2247-2262.

[3] L. R. Ford, Jr. and D. R. Fulkerson, *Flows in Networks*, Princeton University Press, Princeton, NJ, 1962.

[4] B. Hoppe and É. Tardos, The quickest transshipment problem, *Mathematics of Operations Research*, 25 (2000) 36–62.

[5] K. Makino, U. Uno, T. Ibaraki, Minimum Edge Ranking Spanning Trees of Split Graphs, *Discrete Applied Mathematics*, 154 (2006) 2373-2386.

[6] S. Mamada, K. Makino and S. Fujishige: Optimal sink location problem for dynamic flows in a tree network, *IEICE Trans. Fundamentals*, E85-A (2002) 1020–1025.

[7] S. Mamada, T. Uno, K. Makino, and S. Fujishige, An $O(n \log^2 n)$ algorithm for the optimal sink location problem in dynamic tree networks, *Discrete Applied Mathematics*, 154 (2006) 2387-2401.

[8] P. B. Mirchandani and R. L. Francis: *Discrete Location Theory* (John Wile & Sons, Inc., 1989).

[9] M. Sakashita, K. Makino, H. Nagamochi, and S. Fujishige, Minimum Transversals in Posi-modular Systems, *ESA 2006, Lecture Notes in Computer Science*, 4168 (2006) 576-587.

[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, H. Nagamochi, S. Fujishige:
   "Minimum Transversals in Posi-modular Systems", ESA 2006, Lecture Notes in Computer Science, 4168, 576-587, 2006.
   概要: Given a system (V, f, d) on a finite set V consisting of two set functions $f : 2^V \to \mathbb{R}$ and $d : 2^V \to \mathbb{R}$, we consider the problem of finding a set $R \subseteq V$ of the minimum cardinality such that $f(X) \geq d(X)$ for all $X \subseteq V - R$, where the problem can be regarded as a natural generalization of the source location problems and the external network problems in (undirected) graphs and hypergraphs. We give a structural characterization of minimal deficient sets of (V, f, d) under certain conditions. We show that all such sets form a tree hypergraph if f is posi-modular and d is modulotone (i.e., each nonempty subset X of V has an element $v \in X$ such that $d(Y) \geq d(X)$ for all subsets Y of X that contain v), and that conversely any tree hypergraph can be represented by minimal deficient sets of (V, f, d) for a posi-modular function f and a modulotone function d.

By using this characterization, we present a polynomial-time algorithm if, in addition, f is submodular and d is given by either $d(X) = \max\{p(v) \mid v \in X\}$ for a function $p : V \to \mathbb{R}_+$ or $d(X) = \max\{r(v, w) \mid v \in X, w \in V - X\}$ for a function $r : V^2 \to \mathbb{R}_+$. Our result provides first polynomial-time algorithms for the source location problem in hypergraphs and the external network problems in graphs and hypergraphs. We also show that the problem is intractable, even if f is submodular and $d \equiv \mathbf{0}$.

2. S. Mamada, T. Uno, K. Makino, S. Fujishige:
"An $O(n \log^2 n)$ algorithm for the optimal sink location problem in dynamic tree networks", Discrete Applied Mathematics, 154, 2387-2401, 2006.
概要: In this paper, we consider a sink location in a dynamic network which consists of a graph with capacities and transit times on its arcs. Given a dynamic network with initial supplies at vertices, the problem is to find a vertex v as a sink in the network such that we can send all the initial supplies to v as quickly as possible. We present an $\mathrm{O}(n \log^2 n)$ time algorithm for the sink location problem, in a dynamic network of tree structure where n is the number of vertices in the network. This improves upon the existing $\mathrm{O}(n^2)$-time bound [6]. As a corollary, we also show that the quickest transshipment problem can be solved in $\mathrm{O}(n \log^2 n)$ time if a given network is a tree and has a single sink. Our results are based on data structures for representing tables (i.e., sets of intervals with their height), which may be of independent interest.

3. K. Makino, U. Uno, T. Ibaraki:
"Minimum Edge Ranking Spanning Trees of Split Graphs", Discrete Applied Mathematics, 154, 2373-2386, 2006.
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, 154, 2247-2262, 2006.
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.

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 ¶[1]

† 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
〒 819-0395 福岡市西区元岡 744 番地
sakurai@csce.kyushu-u.ac.jp

1 Introduction

Development of information security technology has advanced the popularization of many services using the Internet such as electronic money, e-commerce and so on. Such a trend has provided not only convenient situations but also security issues because a lot of attackers called cracker or phisher attempt to steal the property of users. Thus, most services require privacy protection and authentication.

Because of the above reason, we need a system which achieves that contents of any transferred message are concealed (only a legitimate receiver can understand it) and a receiver can confirm who sent a message. The former property is called confidentiality, and the latter is called authentication. As one solution for achieving such a system, several public key infrastructures (PKI) using certificate have been designed so far. A certificate authority (CA) issues certificates that certify the relationship between a public key and the owner of its private key. By encrypting a message by a public key certified by the intended receiver's certificate, it is guaranteed that only the legitimate receiver can decrypt the message.

Although many commercial and government PKI systems are based on the above approach there exists one disadvantage that is to require an additional procedure for obtaining a certificate. To solve this problem, Shamir introduced ID-based encryption[12]. This is an encryption system that uses identity information (e.g. name, mail address) as public key. Thus, compared with certificate-based PKI, it is easy to retrieve an intended user's public key.

After [12], several approaches that realize similar functionality have been proposed under various settings[2, 4, 5, 10]. This paper compares them and clarifies the differences. After the analysis, we design a PKI system for device authentication and enhance the security of linear scheme to solve key escrow problem. The constructions of the proposed protocols are based on unique device.

2 Related Work

In this paper, a system that enables encryption and/or authentication by using ID information is called ID-based cryptosystem. This section introduces some methods proposed by Matsumoto et al.[10], Desmedt et al.[4], and Boneh

[1] Our Main results of this report was appeared in "Cryptographic Infrastructures based on a Unique Device with Tamper-Resistant", 1st International Conference on Information Security and Computer Forensics, ISCF2006, pp, 41-47, India, with authored by Kenji Imamoto, Hiromi Fukaya, and Kouichi Sakurai, which is related to an implementation and application of tamper-free cryptographic device.

et al.[2] as existing ID-based cryptosystems.

E' and D' (E" and D") used in figures shown in this paper denote encryption and decryption functions respectively. Let k mean secret (symmetric) key, and s mean master key chosen by a trusted third party called private key generator (PKG). It is assumed that each user is assigned a unique ID information.

2.1 Key Predistributionb System (KPS)

Key Predistributionb System (KPS) [10] is a system that establishes a common key among arbitrary group without any additional communication. This system consists of two steps: initial setting and key generation phase. In the initial setting, PKG chooses an algorithm that computes secret keys for any party (called center algorithm). Then, PKG derive a secret algorithm for each party by using the center algorithm, and distribute it securely. After the initial setting, the key generation phase is available. In the phase, a user can generate a common key by entering ID information of intended party(s) into its secret algorithm (See Fig.2.1[1]).

By using KPS, a user can start encrypted communication with any party. To achieve the above functionality, some functions are required that realize the following properties.

- $S_i = f(s, ID_i)$
- $K_{ij} = g(S_i, ID_j) = g(S_j, ID_i)$
  $= f(s, ID_j, ID_i) = f(s, ID_i, ID_j)$

Here, s denotes the master key chosen by PKG. S_i is a secret key assigned to a user, U_i, and K_{ij} is a common key shared by U_i and U_j. ID_i and ID_j mean ID information of U_i and U_j respectively. By letting $g()$ be a publicly known function, each user can generate any common key shared with arbitrary partner.

As a practical implementation, Matsumoto et al. propose linear scheme in [10]. In this scheme, PKG generates a $(\omega + 1) \times (\omega + 1)$ symmetric matrix, A, and distributes a secret algorithm, $S_i = v_i A$, to U_i. v_i is a $\omega + 1$ row vector that is determined from ID_i. The master key, A, is not derivable without obtaining ω users' secrets. U_i who holds S_i derives K_{ij} by computing as follows.

- $K_{ij} = S_i \cdot^t v_j$

The above protocol is a scheme for two party key establishement, but it is easy to construct schemes for more than three party. Various KPSs that consider the trade-off of efficiency and security have been proposed so far [11].

2.2 ID-based encryption

After Shamir proposed the concept of ID-based encryption[12], many ID-based encryption and signature schemes have been proposed. The initial setup of this approach is as follows (See Fig.2.2). At first, PKG chooses a master key and some system parameters. PKG generates users' secret key by using the master key and the parameters then distributes them securely. After the initial setup, each user can encrypt/decrypt a message. A sender enters a receiver's ID and a plaintext into an encryption algorithm and obtains the corresponding ciphertext. Upon receipt of the ciphertext, the receiver enters its secret key and the ciphertext into a decryption algorithm.

One different property from KPS is that a sender cannot know the decryption key. This property is important to construct a signature scheme because no party but signer should know the signature key (certificate-based PKI also has this property). This approach enables to eliminate some procedure for certifying the

[1] KPS is a procedure for generating a common key and it does not refer the purpose of the key. However, in order to compare with other methods, Fig.2.1 shows the case that it is used for encryption.

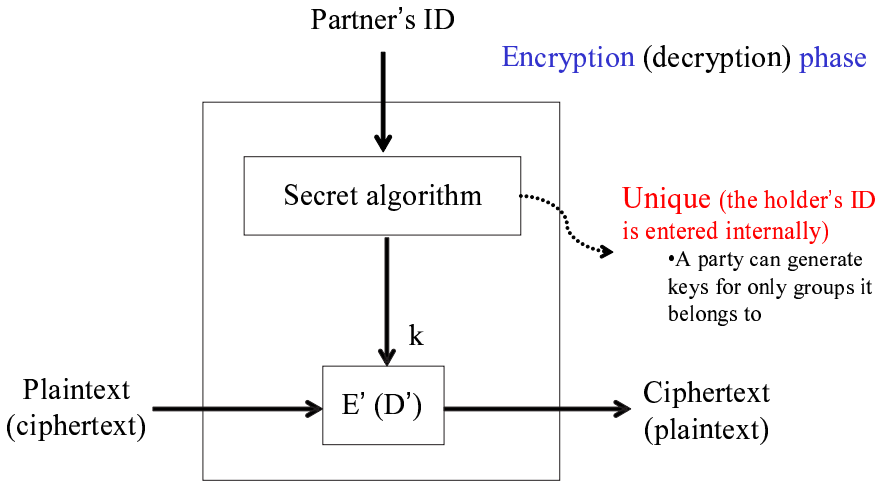


図 2.1: Key Predistributionb System (KPS)

correctness of public key, which is required in certificate-based PKI.

By using pairing over elliptic curve, Boneh and Franklin firstly designed a practical implementation of ID-base encryption[2]. The security of the scheme is based on Bilinear Diffie-Hellman (BDH) problem. After the proposal, many schemes based on the same idea have been designed so far[3]. Moreover, some papers discuss the effectiveness on Maurer-Yacobi ID-based encryption that is based on the difficulty of factoring and discrete logarithm problems[1].

2.3 PKI systems using Tamper-resistant Device

Desmedt et al. propose two ID-based cryptosystems using tamper-resistant device [4]. Tamper-resistant device is a device that ffers physical protection to the keys residing inside them, thereby providing some assurance that these keys have not been maliciously read or modified. As well as KPS, it also assumes a trusted party (PKG) and secure symmetric-key based encryption/decryption function (e.g. AES) Because of the assumption on device, any information inside the gray-colored domains in Fig.2.3 and Fig.2.4 cannot be revealed. In other words, it is assumed that a holder of the device can choose any input value and obtain its output but cannot know any value under calculation.

In the schemes given in [4], each party's secret key is generated by decrypting the party's ID information with a master key chosen by PKG, and then deployed to the party. In case of the first scheme of [4] (we call it DQ1 in this paper), a sender enter its receiver's ID and a plaintext into the device. Then, the receiver's ID is entered into the decryption function with the master key and the receiver's secret key is generated internally. The plaintext is encrypted with the secret key and outputted from the device. The receiver can obtain the plaintext by decrypting the ciphertext with the secret key distributed by PKG. Fig.2.3 shows the above procedure.

The constraction of the second scheme (called DQ2) is different from DQ1. In this scheme, some information on a sender can be entered in case of encryption and decryption. This means that a sender may enter its secret key in addition to a plaintext and its receiver's ID. The receiver's ID is entered into a decryption function with the master key and its output is exclusive ORed with the sender's secret key. The exclusive ORed value is used as the encryption key of the plaintext. In case of the decryption step,

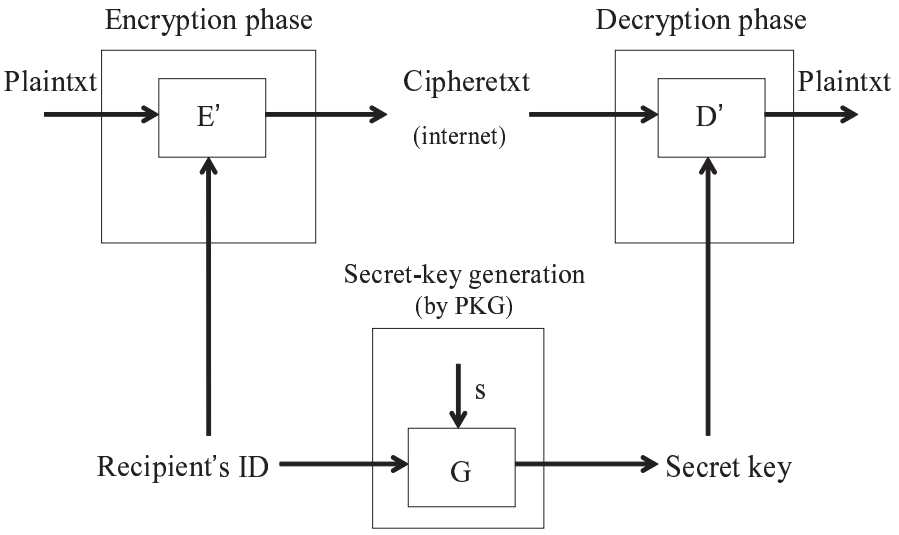


図 2.2: ID-based encryption

the receiver enters the sender's ID in addition to the ciphertext and own secret. The sender's ID is decrypted with the master key internally and exclusive ORed with the receiver's secret key. Then the exclusive ORed value is used as the decryption key of the ciphertext.

DQ1 uses the master key inside the device but it accepts no information on the sender. Only the receiver can decrypt the ciphertext (even the sender cannot decrypt it because the encryption key is generated under the device). Because anyone can encrypt a message and only one particular user can decrypt it, this system is regarded as ID-based encryption. That is, it provides some similar functionality to certificate-based PKI such as digital signature. On the other hand, DQ2 can use peculiar information (e.g. ID or secret key) on both a sender and receiver and establish a common key. Thus this system is regarded as an implementation of KPS. However, if a user may not input information on the sender in encrypting, it can also provide ID-based encryption. So, we can say that the concept of DQ2 implies that of DQ1.

2.4 ID-based encryption scheme based on symmetric-key technique with a trusted device (IST)

Fukaya et al. proposed ID-based encryption scheme based on a unique device that has an unforgeable area with unique value[5]. It is assumed that cloning of the device is impossible. The purpose of this system is to acheive device authentication, which is a second layer of authentication ensuring that only a specific authorized device operated by specific authorized users can access some sensitive resource. As well as KPS, by entering a plaintext and partner's ID into the device, a common key only the partner can generate is produced.

IST consists of a tamper-resistant device as well as the schemes proposed by Desmedt et al. However the device used in IST is different from the device used in DQ1 and DQ2. It is assumed that no information stored in the device of DQ1 and DQ2 is readable and modifiable while the unique ID stored in the device of IST is not modifiable but readable. We call such a device with unique value unique device.

Although the description on how to generate a common key is not concretely given in

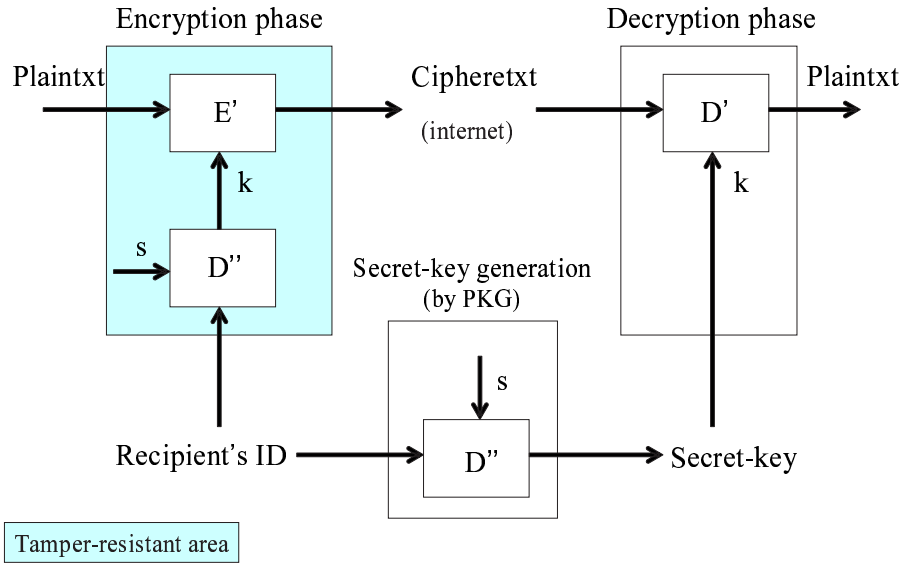


図 2.3: Desmedt-Quisquater scheme (DQ1)

[5], the abstract is as follows (See Fig.2.5 [2]). At first, a device generator (DG) distributes tamper-resistant devices with unique ID. When a sender sends a message, it enters the receiver's ID and a plaintext into the device. Then the device generates a common key and encrypts the plaintext by using the key internally. The device provides only the ciphertext and the sender cannot know the common key. Each device has a secret algorithm that generates any common key from ID information for a group including the holder. Upon receipt of the ciphertext, the receiver enters the sender's ID and the ciphertext into its device. As well as the encryption step, the decryption key for the ciphertext is generated internally and the receiver obtains no information except for the plaintext.

Because no user knows its secret algorithm stored in the device the procedure for generating a common key is not available without the legitimate device. Therefore IST can realize device authentication, which can realize various applications such as digital right management (DRM) [6].

[2]The original protocol shown in [5] provides authentication, but we omit the step to easily understand the concept

3 Comparison

In Section 2, we introduce some existing ID-based cryptosystems[2, 4, 5, 10]. After the feature of each technique is enumerated, correlation of them is clarified in this section. Especially, each feature is examined from the required condition, I/O information in the encryption and the decryption by each method, and the viewpoint of the role of the third party organization.

3.1 I/O information

To analyze the difference of the algorithms, we consider I/O information of the existing ID-based cryptosystems given in Section 2. The output information of every schemes in encryption/decryption step is ciphertext/plaintext. So, we clarify the input information. Table.2.1 shows input information of the schemes at encryption and decryption.

When encrypting a message in every schemes, a sender inputs a receiver's ID and plaintext (in case of certificate-based PKI, a receiver's certificate is input as ID information). As for a sender's secret key, it is input inside a tamper-resistant device in IST and secret algorithm in

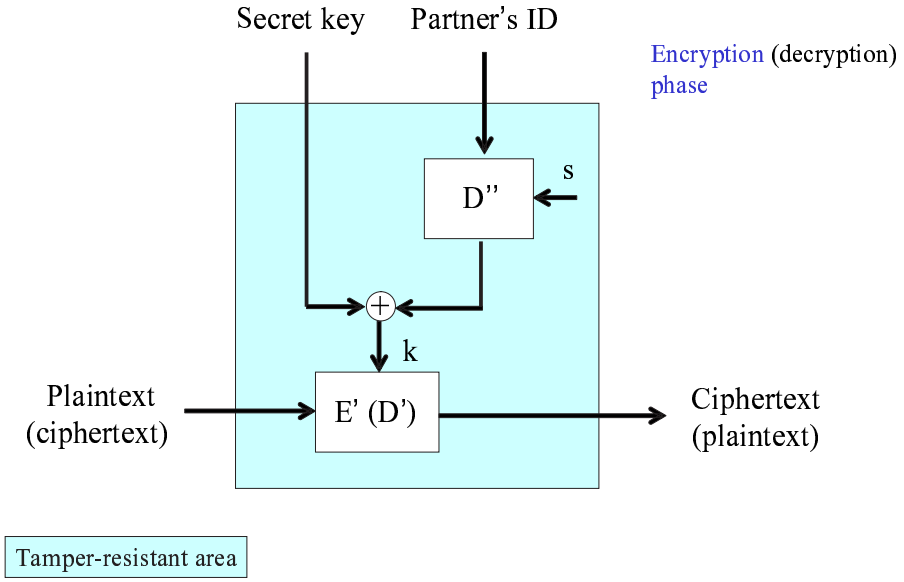


図 2.4: Desmedt-Quisquater scheme (DQ2)

表 2.1: Input information of existing ID-baesd cryptosystems

Methods	Encryption			Decryption		
	Secret key	ID	Plaintext	Secret key	ID	Ciphertext
Certificate-based PKI	-	√*	√	√	-	√
KPS [10]	Internal	√	√	Internal	√	√
DQ1 [4]	-	√	√	√	-	√
DQ2 [4]	√	√	√	√	√	√
ID-based encryption[2, 12]	-	√	√	√	-	√
IST [5]	Internal	√	√	Internal	√	√

KPS. Since it is an internal input, no user can change the value. In case of DQ2, the sender's secret key is input from outside of the device. Further, the construction of DQ2 allows a user to choose whether it enters the sender's information or not.

A ciphertext and a receiver's secret key are input in the decryption step. Especially, the receiver's secret key is input internally in KPS and IST as well as the encryption step. The sender's ID is input in KPS, ID-based encryption, DQ2 and IST. If the sender's secret key is not input in the encryption step of DQ2, the receiver does not input the sender's ID.

From the above discussion, the relationship between the schemes is as Fig.2.6. That is, ID-based cryptosystems can be divided into two types: systems with and without input of sender's information. Certificate-based PKI, DQ1 and ID-based encryption are the former, and KPS and IST are the latter one. DQ2 contains both types. From the viewpoint of information each user can obtain, both a sender and a receiver generate a common key in the former while a sender cannot know the decryption key in the latter.

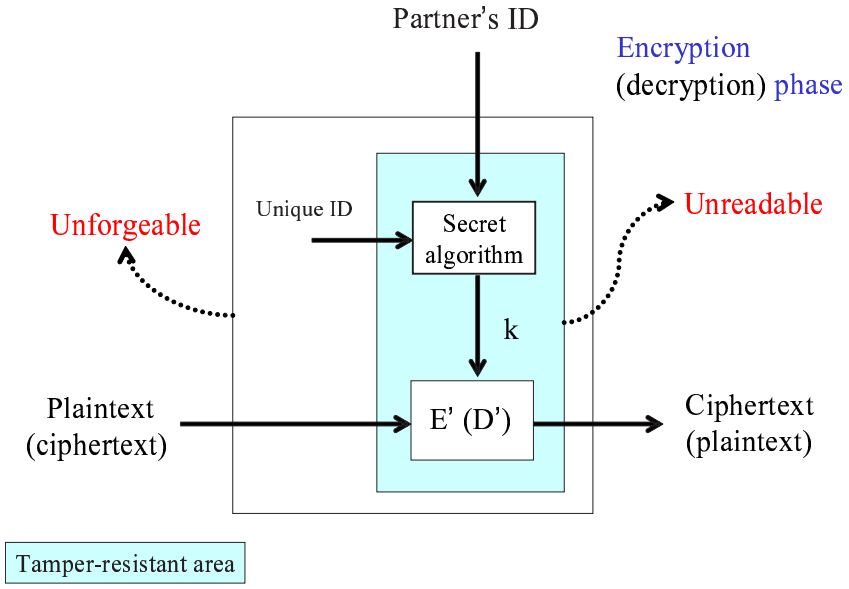


図 2.5: ID-based encryption scheme based on symmetric-key technique with a trusted device (IST)

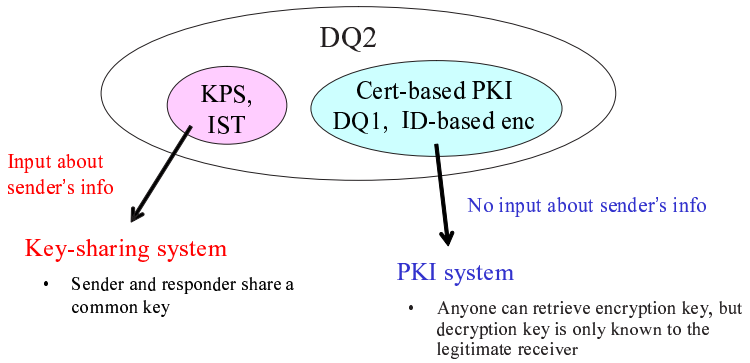


図 2.6: Relationship between ID-based cryptosystems (from the viewpoint of input)

3.2 Assumption

Each system requires some assumption for secure implementation. Table.2.2 shows required condition and a party that generates a secret key in each system. In addition to the condition shown in the table, systems using PKG requires a condition on secrecy of the master key (i.e. PKG does not compromise the security of users' secret key).

The security of ID-based cryptosystems explained in Section 2 are based on the assumption that PKG is trusted. If PKG is malicious, any ciphertext is decrypted by PKG. When using a certificate, the security of the system is based on the correctness of public key certified by CA's certificate. Thus if CA is malicious the security of the system is compromised. The security of DQ1, DQ2 and IST depends on the condition on the device. Even if only one device used in DQ1 and DQ2 is tampered, the security of whole system is compromised because every device stores the master key.

3.3 Role of third party

In certificate-based PKI, generation and distribution of certificate of public key are the third

表 2.2: Assumption

	Secret key generator	Condition
Certificate-based PKI	Depends on scheme	Confidence on certificate
Linear scheme [10]	PKG	Conspiracy below threshold
DQ1, DQ2 [4]	PKG	Tamper-resistant device
Boneh et al.'s system [2]	PKG	BDH problem
IST [5]	PKG	Unique device

party's tasks. To generate a certificate is performed by CA. Distribution of certificate means that any certificate is published at public directory to make any user retrieve any public key. This can be done by any party including user itself.

In IST, DQ1 and DQ2, a third party generates tamper-resistant device and writes a secret key into the device. A master key is the most important information because its revelation can cause the compromise of the whole system. So, to choose and write a secret key should be done by PKG. It can be a task of another party to generate a device. That is, PKG may be a different party from DG.

At last, we consider a key revocation procedure that is required when a secret key is revoked. For certificate-based PKI several solutions have been proposed such as certificate revocation list (CRL) and online certificate status protocol (OCSP) [9]. ID-based encryption, [2] proposes one approach that is to add the expiration date of the key to ID information (e.g. `alice@yahoo.com||December.2006`). This solution can be applied to the other ID-based cryptosystems. When tamper-resistant device is used, it is necessary to consider the loss of the device and the reissue when breaking down.

4 ID-based Cryptosystems using Unique Device

As explained in the previous section, there exists various kinds of ID-based cryptosystems. Based on unique device, we design two systems for device authentication in this section. Since IST is designed for establishing a common key, the first proposed system is a PKI (i.e. the former type described in Section 3.1). Next, we construct a system based on linear scheme [10] to enhance the security of the original scheme by using unique device.

4.1 PKI using unique device

Based on IST, we construct a PKI-type system like ID-based encryption and DQ1. The abstract of the system is shown in Fig.2.7. The encryption phase of the proposed system is based on the construction of KPS/DQ1. When a sender encrypts a message, it chooses a receiver's ID, which is equal to unique ID stored in the receiver's device. The sender's secret key is input inside the device (internal input). The detail of key generation is same as the original scheme. In case that the receiver decrypts the ciphertext, the procedure is same as the decryption phase of IST. The detail of the decryption phase depends on the encryption one.

The ciphertext can be decrypted by only the holder who owns a device with the unique ID chosen by the sender because unique ID is a fixed unique value that is assigned to each device. As well as DQ1, it is possible to modify the above scheme to achieve a digital signature scheme by entering the plaintext in decryption phase (the output can be used as a signature of the plaintext).

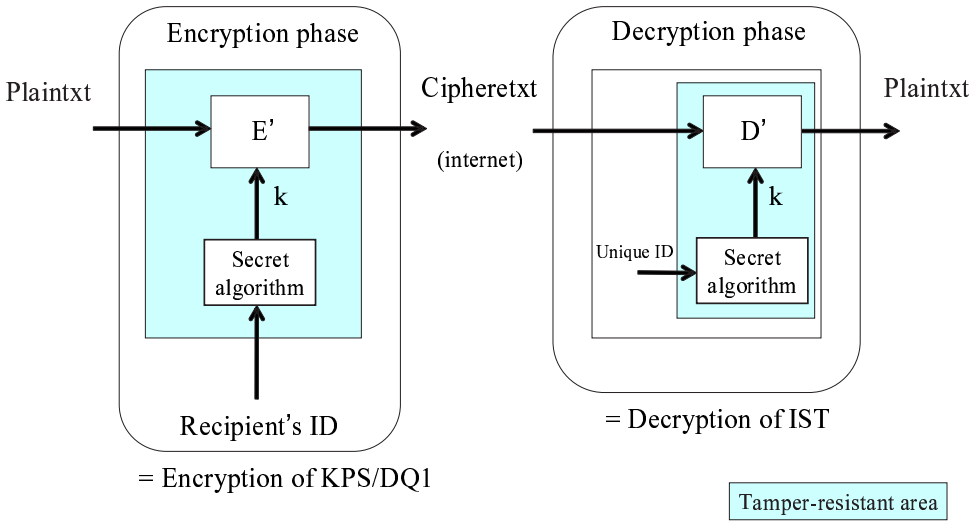


図 2.7: Proposed PKI using unique device

As shown in Fig.2.7, the construction of the proposed protocol is simple but it is very important how to design a secret algorithm stored in the device because the security of the protocol completely depends on the algorithm. For example, to tamper a device used in DQ1 (i.e. revelation of the master key) results in a compromise of the security of the whole system. In Section 4.2, we design a system that restrict the damage of tampering a device.

4.2 Security-enhanced linear scheme

Any ID-based cryptosystems explained in Section 2 have one important problem called key-escrow problem. This problem results from the fact that PKG computes private keys for users. Thus, PKG inevitably has users' secret keys and users' privacy can be compromised. In this section, we design a security-enhanced protocol that solves the key-escrow problem of linear scheme [10].

ID information is translated deterministically into a specific $\omega + 1$ row vector, v_i, in linear scheme by using a public function, h, as follows: $v_i = h(ID_i)$. In the proposed protocol, DG chooses the function, h, and stores it secretly in each tamper-resistant device. Therefore, even if PKG has malice, it can compute no secret key without tampering a device. v_i is also stored in the device as U_i's unique ID because it is required when U_i asks PKG to issue its secret key in the initial step (Note that the function, h, is not known to any user). The construction of the proposed protocol is given in Fig.2.8.

At the initial setting, DG chooses h and stores some functions, g, h and a symmetric-key encryption/decryption function. g is a public function that computes a common key, $K_{ij} = g(S_i, v_j) = S_i \cdot^t v_j$. Then, DG distributes a device with v_i to U_i. Next, U_i asks PKG to compute S_i from the master key chosen by PKG. S_i is stored into the tamper-resistant area of the device to make it unknown to any party including legitimate users. In computing the secret key, a multi-party protocol[3] [7] is used to conceal v_i and S_i from PKG and A from users. Since U_i does not know v_j $(i \neq j)$ it can obtain only its secret key, S_i, that is computed from v_i assigned to its device.

In the encryption/decryption steps, each user enters the partner's ID (ID_j) and a plaintext/ciphertext into its device. The device

[3] By using a multi-party protocol, while keeping each participant's information secret, everyone can learn the result of a function.

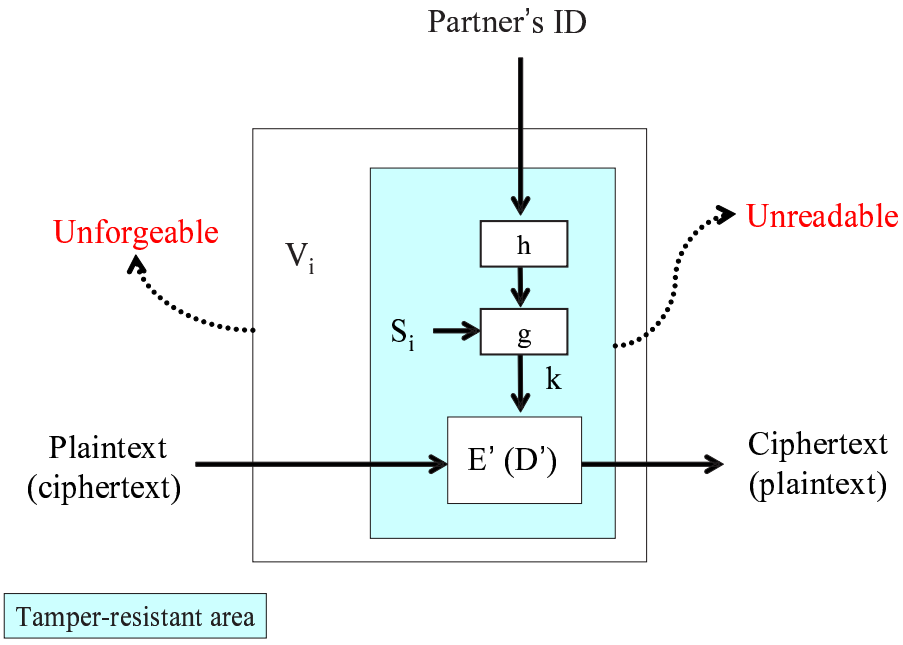


図 2.8: Security enhanced linear scheme

translates ID_j into a row vector ($v_j = h(ID_j)$), and computes a common key, $K_{ij} = S_i \cdot^t v_j$, by entering S_i and v_j into g. Encryption or decryption is done inside the device and the device outputs the result.

No user can generate any common key because it does not know own secret key, so device authentication is available in this system. Moreover, using tamper-resistant device makes it difficult to derive the master key, A, because an attacker needs to tamper at least ω devices. Reducing the number of ω can reduce the computational cost of generating secret key. One interesting feature of the proposed protocol is that DG's work is completely independent from that of PKG. Hence, even if a master key is revealed, new master key should be chosen but it is not necessary to renew any device. Similarly, if a device is tampered, any device should be renewed but the master key can use without renewal.

5 Conclusion

This paper clarifies the relationship between several ID-based cryptosystems such as KPS [10], Desmedt et al.'s schemes [4], ID-based encryption [2, 12] and IST [5]. And based on unique-device, we design a PKI system for device authentication and enhance the security of linear scheme to solve key escrow problem.

As our future work, we are going to try to design of secret algorithm in order to control/reduce the damage of whole system when device is broken. Moreover, it is also necessary to investigate the limitation of system using unique-device

参考文献

[1] W. Abe, N. Kunihiro, K. Ohta, "Maurer-Yacobi ID-Based Encryption Scheme Revisited", SCIS 2005, 2005.

[2] D. Boneh, M. Franklin, "Identity Based Encryption from the Weil Pairing", Crypto 2001.

[3] C. Cocks, “An Identity Based Encryption Scheme Based on Quadratic Residues”,

8th IMA International Conference on Cryptography and Coding, 2001.

[4] Y. Desmedt, J. Quisquater, “Public-Key Systems Based on the Difficulty of

Tampering (Is There a Difference Between DES and RSA?), Crypto 1986.

[5] H. Fukaya, K. Sakurai, “Realization of the ID-based encryption scheme based on

symmetric-key technique with Device characteristic value”, ISEC, 2006.

[6] H. Fukaya, K. Sakurai, “A Design of DRM systems with hardware-based authentication”,

ISEC, 2006.

[7] O. Goldreich, S. Micali, A. Wigderson, “How to play any mental game –

a completeness theorem for protocols with honest majority”,

19th ACM Symposium on the Theory of Computing (STOC), 1987.

[8] M. Joye, “An overview of cryptographic techniques based on identity and

implementation on smart cards”, Identech 2005.

[9] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, “X.509 Internet Public Key

Infrastructure Online Certificate Status Protocol - OCSP”, RFC2560, 1999.

[10] T. Matsumoto, H. Imai, “On the key predistribution systems: A practical solution to the key distribution problem”,

in Advances in Cryptology - Crypto 1987.

[11] M. Ramkumar, “I-HARPS: An Efficient Key Pre-distribution Scheme”, Cryptology ePrint Archive

2005/138.

[12] A. Shamir, “Identity-based cryptosystems and signature schemes”, Advances in cryptology, Crypto 1984.

研究業績一覧

学術論文

1. Yufeng Wang, Yoshiaki Hori, Kouichi SAKURAI:
“Economic-inspired truthful reputation feedback mechanism in P2P network”, The IEEE 11th International Workshop on Future Trends of Distributed Computing Systems, IEEE Computer Society, 2007 Mar..
概要: Recently, cross-disciplinary efforts involving economics and computer security have proliferated. And Peer-to-Peer (P2P) reputation systems are essential to evaluate the trustworthiness of participating peers and to combat the selfish, dishonest and malicious peer behaviors. But reputation feedback is special kind of information, and it is not free. Based on those above consideration, in this paper, VCG-like reputation remuneration scheme inspired by economic model is proposed to stimulate rational peers not only to provide reputation feedback, but truthfully offer feedback.

2. Jeong Ok Kwon, Kouichi Sakurai, Dong Hoon Lee:
“Efficient Password-Authenticated Key Exchange for Three-Party Secure Against Undetectable On-Line Dictionary Attacks”, The sixth International Conference on Computational Science (ICCS 2006), Volume 1, Spriger LNCS Volume 3991, pp. 977–980, 2006. Nov.
概要:

3. Kenji Imamoto, Kouichi Sakurai,:
"Enhanced Privacy in Key-Exchange Protocols by One-time ID", The Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2006), IEEE Computer Society, pp. 63–68, 2006.
概要: This paper considers how two parties communicate securely over an adversary-controlled network. We especially focus on the problem of ID protection because of the recently rapid development of mobile network where any transferred message is easily eavesdoropped on. We analyze several existing key exchange protocols and point out their problems: e.g. imcompleteness of ID protection and vulnerability to DoS attacks. Then we model the notion of ID protection and construct a protocol with provable security. Key-words: Key-exchange protocol, SK-security, ID protection, One-time ID, DoS attacks.

4. Kenji Imamoto, Hiromi Fukaya, Kouichi Sakurai:
"Cryptographic Infrastructures based on a Unique Device with Tamper-Resistant", 1st International Conference on Information Security and Computer Forensics, ISCF2006, pp. 41–47, 2006.
概要: Public key infrastructures (PKI) that use certificate of public key and identity-based encryption systems have been designed so far by introducing some assumptions such as computational difficult problems and participation of trusted third party. This paper considers how to construct PKI based on tamper-resistant hardware. Especially, we study an ID-based encryption scheme based on symmetric-key technique with a trusted device (IST) proposed by Fukaya et al. and compare with several existing schemes. Based on unique device, we design a PKI system for device authentication and enhance the security of linear scheme to solve key escrow problem.

5. Yufeng Wang, Wendong Wang, Kouichi SAKURAI, Yoshiaki Hori:
"On studying P2P topology construction based on virtual region and its effect on search performance", The Third International Conference on Ubiquitous Intelligence and Computing (UIC 2006), Springer, LNCS Volume 4159, pp.1008–1018, 2006.
概要: The virtual region-based P2P architecture was provided in this paper, which extended the proximity concept in overlay network. By virtual region it meant various related factors should be integrated into the design of P2P topology, such as peer interest, peer locality, and heterogeneity in peer capacity etc. But, the shared contents in P2P are vast and miscellaneous, it is very difficult to recognize the interest similarity among peers, dynamically form the interest region and direct peer to appropriate interest region. In this paper, the Jensen-Shannon Divergence (JSD) was used to characterize interest/semantic similarity among peers, and the interest region formation and location mechanism based on Dynamic Interest Landmark (DIL) was offered to facilitate to dynamically guide peers to join the appropriate interest region corresponding to peers ' content semantic. Considering that interest region is composed of geographically sporadic peers, each interest region was organized according to peer proximity in underlying infrastructure. The theoretical and simulated results illustrated that our architecture can significantly reduce the query overhead, and improve the search performance.

6. Zhan Wang, Yoshiaki Hori, and Kouichi Sakurai:
"Application and evaluation of Bayesian filter for Chinese spam", The SKLOIS confer-

ence on information security and cryptology, Springer-Verlag, LNCS 4318, pp. 253–263, 2006.

概要: Recently, a statistical filtering based on Bayes theory, so-called Bayesian filtering gain attention when it was described in the paper " A Plan for Spam " by Paul Graham, and has become a popular mechanism to distinguish spam email from legitimate email. Many modern mail programs make use of Bayesian spam filtering techniques. The implementation of the Bayesian filtering corresponding to the email written in English and Japanese has already been developed. On the other hand, few work is conducted on the implementation of the Bayesian spam corresponding to Chinese email. In this paper, firstly, we adopted a statistical filtering called as bsfilter and modified it to filter out Chinese email. When we targeted Chinese emails for experiment, we analyzed the relation between the parameter and the spam judgement accuracy of the filtering, and also considered the optimal parameter values.

7. Jeong Ok Kwon, Kouichi Sakurai, Dong Hoon Lee:
"One-Round Protocol for Two-Party Verifier-Based Password-Authenticated Key Exchange", The tenth IFIP TC-6 TC-11 International Conference on Communications and Multimedia Security (CMS 2006), Springer LNCS Volume 4237, pp. 87–96, 2006.

概要: Password-authenticated key exchange (PAKE) for two-party allows a client and a server communicating over a public network to share a session key using a human-memorable password only. PAKE protocols can be served as basic building blocks for constructing secure, complex, and higher-level protocols which were initially built upon the Transport Layer Security (TLS) protocol. In this paper, we propose a provably-secure verifier-based PAKE protocol well suited with the TLS protocol which requires only a single round. The protocol is secure against attacks using compromised server 's password file and known-key attacks, and provides forward secrecy, which is analyzed in the ideal hash model. This scheme matches the most efficient verifier-based PAKE protocol among those found in the literature. It is the first provably-secure one-round protocol for verifier-based PAKE in the two-party setting.

8. Jong-Phil Yang, Kyung Hyune Rhee, Kouichi Sakurai:
"A Proactive Secret Sharing for Server Assisted Threshold Signatures", The Second International Conference on High Performance Computing and Communications (HPCC 2006), Springer LNCS Volume 4208, pp. 250–259, 2006.

概要: Threshold signature schemes distribute secret information to several servers and make the whole system that maintains the secret information fault-tolerant. Since threshold signature schemes typically assume that the shared signing function can only be activated by a quorum number of servers. If anyone has a power to activate the signing function of servers, he can easily compute valid signatures for a specific organization without knowing the private key. S. Xu et al. proposed a general construction to build threshold signature schemes (called as server assisted threshold signatures) which provide an organization (e.g., a user) with controllability for activating his private signing function in a certain enhanced way. In this paper, we newly propose proactive secret sharing schemes which are suitable for server-assisted threshold signatures.

9. Satoshi Hada, Kouichi Sakurai:

"Ciphertext-Auditable Public Key Encryption", The First International Workshop on Security (IWSEC 2006), Springer LNCS Volume 4266, pp. 308–321, 2006.

概要: Loss of backup tapes containing personal information (PI) is a potential breach of privacy and encryption is the typical way to prevent the breach. This paper considers an attack scenario where an adversary who encrypts the PI for backup purpose tries to hide the plain PI in a valid-looking ciphertext without being detected. We show that the standard security notion IND-CCA2 does not capture such a scenario. For example, the Cramer-Shoup scheme is vulnerable to such an attack. To capture such a scenario, we define a new notion of " ciphertext-auditability " as a new property of public key encryption schemes (PKESs). It requires that, given a public key and a ciphertext, anyone should be able to verify whether the ciphertext was actually generated using the public key. Also, it requires that, given a public key and a plaintext, no adversary should be able to generate a valid-looking ciphertext so that the verification passes, but nevertheless the plaintext can be recovered from the ciphertext without the corresponding secret key. We propose a general construction of such PKESs based on standard cryptographic primitives in the random oracle model.

10. Tae Hyun Kim, Tsuyoshi Takagi, Dong-Guk Han, Ho Won Kim, Jongin Lim:
"Side Channel Attacks and Countermeasures on Pairing Based Cryptosystems over Binary Fields", 5th International Conference on Cryptology and Network Security, CANS 2006, LNCS volume 4301, pp. 168–181, 2006.

概要: Pairings on elliptic curves have been used as cryptographic primitives for the development of new applications such as identity based schemes. For the practical applications, it is crucial to provide efficient and secure implementations of the pairings. There have been several works on efficient implementations of the pairings. However, the research for secure implementations of the pairings has not been thoroughly investigated. In this paper, we investigate vulnerability of the pairing used in some pairing based protocols against side channel attacks. We propose an efficient algorithm secure against such side channel attacks of the eta pairing using randomized projective coordinate systems for the pairing computation.

11. Katsuyuki Okeya, Tsuyoshi Takagi:
"Security Analysis of CRT-Based Cryptosystems", International Journal of Information Security, IJIS, Vol.5, No.3, pp. 177–185, 2006.

概要: A side channel attack (SCA) is a serious attack on the implementation of cryptosystems, which can break the secret key using side channel information such as timing, power consumption, etc. Recently, Boneh et al. showed that SSL is vulnerable to SCA if the attacker gets access to the local network of the server. Therefore, public-key infrastructure eventually becomes a target of SCA. In this paper, we investigate the security of RSA cryptosystem using the Chinese remainder theorem (CRT) in the sense of SCA. Novak first proposed a simple power analysis (SPA) against the CRT part using the difference of message modulo p and modulo q. In this paper, we apply Novak 's attack to the other CRT-based cryptosystems, namely Multi-Prime RSA, Multi-Exponent RSA, Rabin cryptosystem, and HIME(R) cryptosystem. Novak-type attack strictly depends on how to implement the CRT. We examine the operations related to CRT of these cryptosystems, and show that an extended Novak-type attack is effective on them. Moreover, we present

a novel attack called zero-multiplication attack. The attacker tries to guess the secret prime by producing ciphertexts that cause a multiplication with zero during the decryption, which is easily detected by power analysis. Our experimental result shows that the timing with the zero multiplication is reduced about 10% from the standard one. Finally, we propose countermeasures against these attacks. The proposed countermeasures are based on the ciphertext blinding, but they require no inversion operation. The overhead of the proposed scheme is only about 1–5

12. Camille Vuillaume, Katsuyuki Okeya, Tsuyoshi Takagi:
"Defeating Simple Power Analysis on Koblitz Curves", IEICE Transactions, Vol. E89-A, No. 5, pp. 1362–1369, 2006.
概要: Koblitz curves belong to a special class of binary curves on which the scalar multiplication can be computed very efficiently. For this reason, they are suitable candidates for implementations on low-end processors. However, such devices are often vulnerable to side channel attacks. In this paper, we propose two countermeasures against side channel attacks on Koblitz curves. Both of them utilize a fixed-pattern recoding to defeat simple power analysis. Our first technique extends a known countermeasure to the special case of Koblitz curves. In our second technique, the scalar is recoded from left to right, and can be easily stored or even randomly generated.

13. Toru Akishita, Tsuyoshi Takagi:
"Power Analysis to ECC Using Differential Power between Multiplication and Squaring", Seventh Smart Card Research and Advanced Application, CARDIS 2006, LNCS 3928, pp. 151–164, 2006.
概要: Power analysis is a serious attack to implementation of elliptic curve cryptosystems (ECC) on smart cards. For ECC, many power analysis attacks and countermeasures have been proposed. In this paper, we propose a novel power analysis attack using differential power between modular multiplication and modular squaring. We show how this difference occurs in CMOS circuits by counting the expectation of signal transition frequency, and present a simulation result on our ECC coprocessor. The proposed attack is applicable to two efficient power analysis countermeasures based on unified addition formulae and elliptic curves with Montgomery form.

14. Dong-Guk Han, Tsuyoshi Takagi, Jongin Lim:
"Further Security Analysis of XTR", The 2nd Information Security Practice and Experience Conference, ISPEC 2006, LNCS 3903, pp. 33–44, 2006.
概要: In Crypto 2000 and 2003, Lenstra-Verheul and Rubin- Silverberg proposed XTR public key system and torus based public key cryptosystem CEILIDH, respectively. The common main idea of XTR and CEILIDH is to shorten the bandwidth of transmission data. Due to the contribution of Granger et al., that is the comparison result of the performance of CEILIDH and XTR, XTR is an excellent alternative to either RSA or ECC in some applications, where computational power and memory capacity are both very limited, such as smart-cards. Among the family of XTR algorithm, Improved XTR Single Exponentiation (XTR-ISE) is the most efficient one, which computes single exponentiation. However, there are few papers investigating the side channel attacks of XTR-ISE, even though the memory constraint devices suffer most from vulnerability to side channel attacks. Chung-Hasan and Page-Stam tried to analyze XTR-ISE with the

known simple power analysis, but unfortunately their approach were not practically feasible. Recently, Han et al. proposed new collision attack on it with analysis complexity $O(2^{40})$ when the key size is 160-bit. In this paper we analyze XTR-ISE from other point of view, namely differential power analysis (DPA). One straightforward result is that XTR-ISE can be free from the original DPA. However, a non-trivial result is that an enhancing DPA proposed in this paper threatens XTR-ISE. Furthermore, we show several weak points of the structure of XTR-ISE. From our simulation results, we show the proposed attack requires about 584 times queries to DPA_{Oracle} to detect the whole 160-bit secret value. This result shows that XTR-ISE is vulnerable to the proposed enhancing DPA.

研究会等

1. Chunhua Su, Jianying Zhou, Feng Bao and Kouichi Sakurai,:
   "Distributed Privacy-preserving Document Clustering", 情報セキュリティ研究会 (ISEC), 岡山大学, pp.123-130, 2006年7月.
   概要: Many government organizations and companies want to share their documents in a similar theme to get the joint benefits. Textual document clustering is a powerful data mining technique to analyze the large amount of documents and structure large sets of text or hypertext documents. While doing the document clustering in the distributed environment, it may involve the users' privacy of their own document. In this paper, we propose a framework to do the privacy-preserving text mining among the users under the distributed environment: multiple parties. each having their private documents, want to collaboratively execute agglomerative document clustering without disclosing their private contents to any other parties

2. 蘇 春華, 鮑 豊, 周 建英, 櫻井 幸一,:
   "乱数摂動よるデータクラスタリングのプライバシー保護手法", 2006年 コンピュータセキュリティシンポジウム CSS2006 (Computer Security Symposium 2006), 京都, 7B-1, 2006年10月.
   概要: The random data perturbation (RDP) method is widely used for preserving the privacy of individual records in a statistical database. In this paper, we propose a distributed data clustering scheme using the Random Data Perturbation. We proposed a new distributed clustering algorithm based on non-parametric kernel density estimation, which takes into account the issues of privacy and communication costs that arise in a distributed environment.

3. Chunhua Su, Feng Bao, Jianying Zhou, Kouichi Sakurai:
   "Private Data Clustering based on Secure Approximation", 第29回情報理論とその応用シンポジウム,SITA2007, 函館, pp. 839–842, 2006年12月.
   概要: K-means clustering is a powerful and frequently used technique of data mining. And rapid growth of Internet provides oppurtunity for coperation between individual or companies. However, the direct use of k-means clustering in coperation can cause privacy breach problems. No idividual or companes want to release their sensitive information. In this paper, we consider a scenario in which two parties have their confidential databases and wish to run a k-means clustering algorithm on the union of their databases. We show that 4 exsiting cryptography-based schemes have some security or accuracy problem and we present a scheme which based on secure approximation. we show our scheme is more secure and efficient.

4. 蘇春華, 鮑峰, 周剣英, 高木剛, 櫻井幸一,:

“Collusion-resistant Private Association Rules Mining Protocol”, 2007年 暗号と情報セキュリティシンポジウム, SCIS 2007, 3B4-4, 2007, 1月.

概要: Association rule mining finds interesting associations and correlation relationships among large set of data items that occur frequently together. In the association rules mining over multi-client's dataset, there are some serious concerns on privacy and security. In this paper, we propose a secure multi-party protocol which can do association rule mining of multi-client's dataset while strictly respecting their privacy with maintaining the accuracy of the results. We also show that our protocol is collusion resistant, which means that even if all dishonest respondents collude with a dishonest data minerin an attempt to learn the associations between honest respondents and their responses, they will be unable to do so.

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 § 伊藤 健洋 †

† 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,takehiro}@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

§ 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
asano@j.dendai.ac.jp

1 はじめに

本研究課題の本年度の研究成果の概要は以下の通りである.

(1) **平面グラフの凸描画**
平面グラフ G が凸描画を持つために必要な外凸多角形の頂点の最小個数は，G から新しく構成されるグラフの 3 連結成分分解木の葉の個数に等しいことを示すとともに，G の外頂点数最小の凸描画が線形時間で求まることを示した.

(2) **平面グラフの内部矩形描画**
平面グラフ G が内部矩形描画を持つための必要十分条件を与えた．更に，G とその外面の概形が与えられたとき，G の内部矩形描画を求める多項式時間アルゴリズムを与えた.

(3) **4 連結平面グラフの格子凸描画**
4 連結平面グラフ G が外周上に 4 つ以上の点を持つならば，面積が $n^2/4$ 以下の平面格子に格子凸描画できることを証明した．更に，G のそのような格子凸描画を求める線形時間アルゴリズムを与えた．ここで n は G の点数である.

(4) **平面グラフの格子凸描画**
平面グラフ G が内部 3 連結であり，3 連結成分分解木に葉がちょうど 4 個あるならば，G を多項式サイズの整数格子内に格子凸描画できることを示した．また，そのような描画を線形時間で求めるアルゴリズムを与えた.

(5) **平面グラフの開矩形勢力描画**
内部三角化平面グラフ G が開矩形勢力描画できるための十分条件を与えるとともに，与えられたグラフの開矩形勢力描画を求める多項式時間アルゴリズムを与えた.

(6) **Web 情報検索**
Web ページのスコアリングアルゴリズムとして有名なものに HITS があり，その改良法も複数提案されている．しかし，近年の Web の急速な発展に伴い，HITS とその改良法の精度は実用に供せないほど低くなってしまった．リンクファームへの対策と TrustRank の考え方を応用して，現在の Web 上でも十分な精度を達成する新たな改良法を提案した.

(7) **グラフの均一分割問題**
グラフの均一分割問題は選挙区割問題等に応用できる．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.

(8) **グラフの最大分割の近似**
需要点と供給点があるグラフの最大分割問題は電力供給問題をモデル化しており，一般には強 NP 困難であることが知られている．この問題の近似可能性について研究した．また，直並列グラフや部分 k-木に対して完全近似スキーム (FPTAS) と呼ばれる近似アルゴリズムを提案した.

(9) **端子シュタイナー木問題**
グラフの端子シュタイナー木を求める問題は VLSI の配線問題に応用できる．この問題が固定パラメータ容易（Fixed Parametor Tractable）であることを示した．

(10) **リスト全彩色**
リスト全彩色では，グラフの隣接する点や辺が異なる色になるように, 点や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．直並列グラフがリスト全彩色を持つための十分条件を色候補リストのサイズを用いて与えた．

以下，各節において，上の (1)–(10) の各成果について述べる．

2　平面グラフの凸描画

平面グラフ G の各辺が互いに交わることのない直線分となり，各内面が凸多角形となるような描画を G の**凸描画**という．G の外閉路に対応する多角形を**外凸多角形**という．例えば図 2.1(a) の平面グラフ G は，外凸多角形が頂点を 4 つ以上持つならば図 2.1(b) のように凸描画を持つが，外凸多角形が三角形ならば図 2.1(c) のように凸描画を持たない．

平面グラフ G が凸描画を持つための必要十分条件は千葉らおよび Thomassen によりそれぞれ与えられており，G の凸描画を線形時間で求めるアルゴリズムも知られている．近年，三浦らは外凸多角形が三角形である凸描画を G が持つための必要十分条件を与えた．しかし，G の凸描画の外凸多角形が何個の頂点を持たねばならないかは知られていなかった．

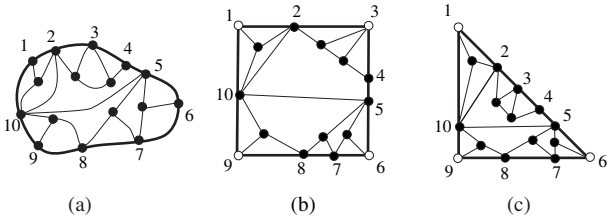


図 2.1: (a) 平面グラフ G, (b) G の凸描画, (c) 凸描画ではない G の描画.

本研究では，G が凸描画を持つために必要な外凸多角形の頂点の最小個数が，G から新しく構成されるグラフの “3 連結成分分解木” の葉の個数に等しいことを示すとともに，G の外頂点数最小の凸描画が線形時間で求まることを示した．図 2.2 に平面グラフ G，G を縮約して新しく構成されるグラフ G'，G' の 3 連結成分, G' の 3 連結成分分解木, G' の凸描画および G の凸描画の例をそれぞれ示す．

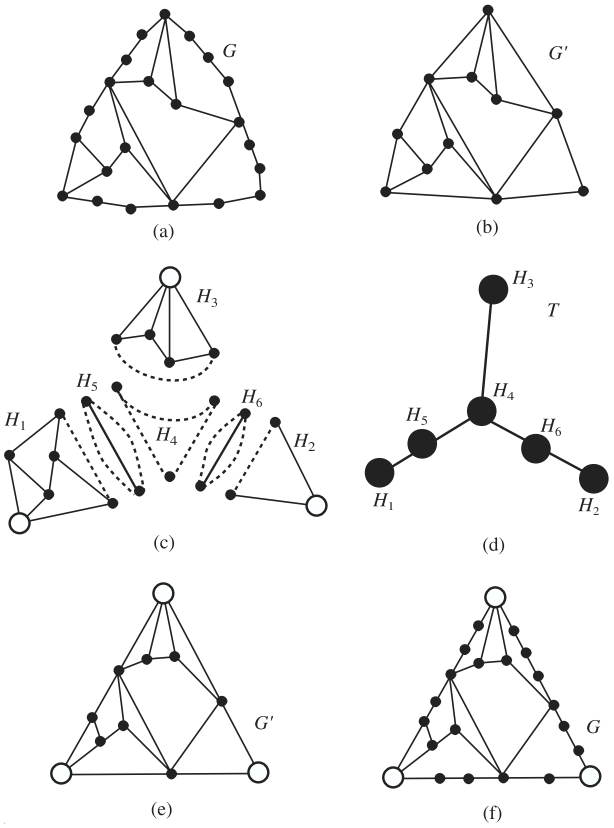


図 2.2: (a) 平面グラフ G, (b) G を縮約して新しく構成されるグラフ G', (c) G' の 3 連結成分, (d) G' の 3 連結成分分解木, (e) G' の凸描画, (f) G の凸描画.

3　平面グラフの内部矩形描画

平面グラフ G の**矩形描画**では，G の各面が矩形になるように各辺は水平線分あるいは垂直線分で描かれる．むろん G の外面も矩形である．矩形描画は VLSI のフロアプランに応用される．VLSI 回路の外面は矩形とは限らず L 字形や T 字形，X

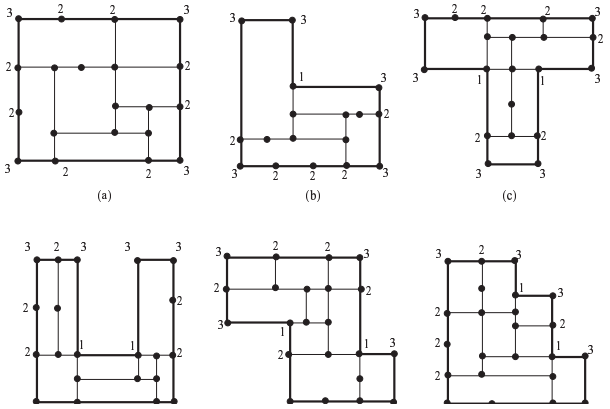


図 2.3: (a) 矩形描画, および (b)–(f) 内部矩形描画の例 (b) 外面が L 字形, (c) 外面が T 字形, (d) 外面が U 字形, (e) 外面が Z 字形, (f) 外面が階段形.

字形等の軸平行多角形になるように描画したいことが多い．したがって，軸平行多角形の内部に，各 “ モジュール” が矩形となるような VLSI 回路のフロアプランを見つけたい．外面が矩形，L 字形，T 字形，U 字形，Z 字形，階段形の VLSI フロアプランの例を図 2.3に示す．このように G の外面を軸平行多角形で描き，内面を矩形で描いたものを，G の**内部矩形描画**と呼ぶ．本文ではグラフ G の最大次数を Δ と書くことにする．$\Delta \leq 3$ なる平面グラフ G が矩形描画を持つための必要十分条件は Thomassen により与えられており，矩形描画を求める線形時間アルゴリズムも知られている．しかし，$\Delta \leq 3$ とは限らない一般の平面グラフ G が矩形描画あるいは内部矩形描画を持つための必要十分条件は知られていなかった．むろん，平面グラフ G が矩形描画や内部矩形描画を持つならば，$\Delta \leq 4$ である．

本研究では，平面グラフ G が内部矩形描画を持つための必要十分条件は G から新しく作られる二部グラフ G_d が完全マッチングを持つことであることを示した．更に，G とその外面の概形が与えられたとき，G の内部矩形描画 D を $O(n^{1.5}/\log n)$ 時間で求めるアルゴリズムを与えた．ここで n は G の点数である．図 2.4に平面グラフ G，G_d および内部矩形描画 D の例を示す.

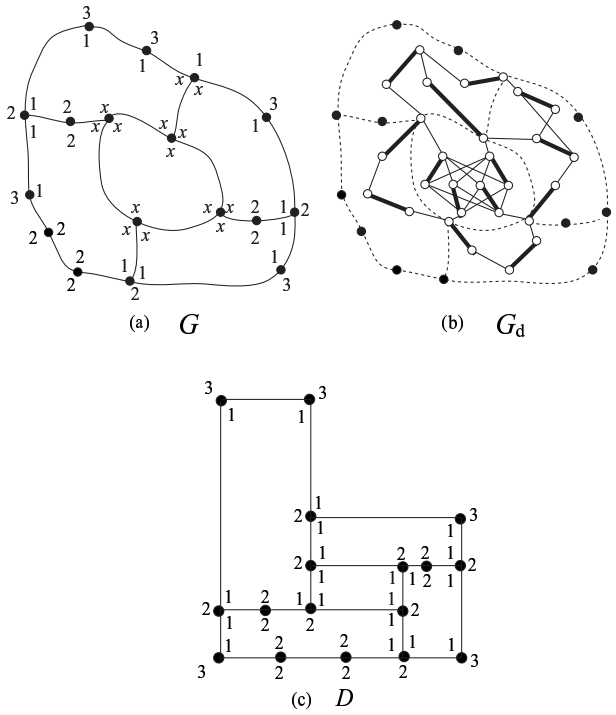


図 2.4: (a) 平面グラフ G, (b) 二部グラフ G_d, (c) G の内部矩形描画 D.

4　4 連結平面グラフの格子凸描画

平面グラフ G の各点を整数格子点上に配置し，各辺が互いに交わることのない直線分となり，各内面が凸多角形となるような描画を G の**格子凸描画**という.

任意の 3 連結平面グラフは $(n-2)\times(n-2)$ の大きさの整数格子に線形時間で格子凸描画できることが Chrobak らによって知られていた．グラフの制約を 3 連結から 4 連結により厳しくすれば，格子凸描画に必要な整数格子の大きさはさらに小さくできると予想されるが，どの程度小さくできるかは知られていなかった.

本研究では，4 連結平面グラフで外周上に 4 つ以上の点があるものは，$W+H \leq n-1$ なる整数格子に格子凸描画できることを証明し，そのような格子凸描画を求める線形時間アルゴリズムを与えた．ここで W は平面格子の幅であり，H は高さである．$W+H \leq n-1$ なので，必要な整数格子の面積は高々$W \cdot H \leq \lceil (n-1)/2 \rceil \cdot \lfloor (n-1)/2 \rfloor$ である．また，$\lceil (n-1)/2 \rceil \cdot \lfloor (n-1)/2 \rfloor$ 以上の面積の整数格子が必要な 4 連結平面グラフが無限個

存在するので，整数格子の面積に関する結果は最適である．図 2.5に 4 連結平面グラフとその格子凸描画の例を示す．

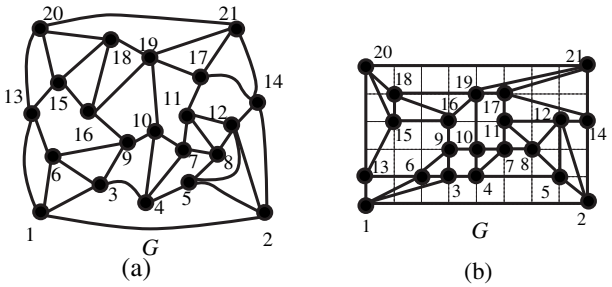


図 2.5: (a) 4 連結平面グラフ G, (b) G の格子凸描画.

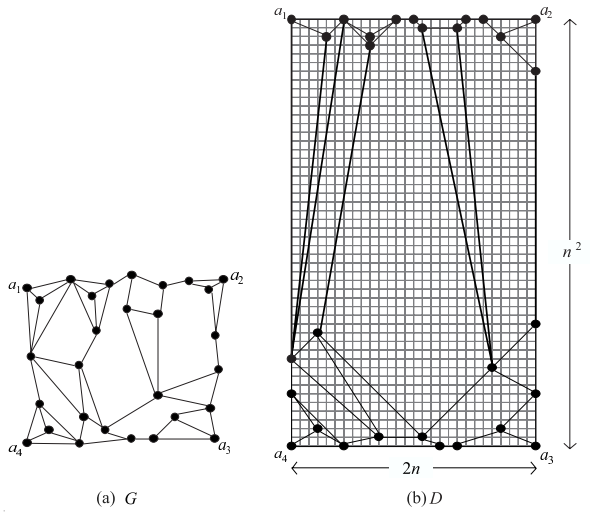


図 2.6: (a) 平面グラフ G, (b) G の格子凸描画 D.

5　平面グラフの格子凸描画

図 2.6(a) の平面グラフの格子凸描画の一例を図 2.6(b) に示す．このように平面グラフの凸描画においては，全ての辺は交差しない直線分で描かれ，全ての面は凸多角形で描かれる．格子凸描画においては，全ての点は整数格子点上に配置しなければならない．平面グラフ G は，内部 3 連結のとき，かつそのときに限り凸描画を持つ．また内部 3 連結平面グラフ G が 3 連結であるか，あるいは G の 3 連結成分分解木 $T(G)$ に葉が 2 個あるいは 3 個しかないならば，G は大きさ $n \times n$ の整数格子内に格子凸描画できる．

本研究では，内部 3 連結平面グラフ G の分解木 $T(G)$ に葉がちょうど 4 個あるならば，G を大きさ $2n \times n^2$ の整数格子内に格子凸描画できることを示した．また，そのような描画を線形時間で求めるアルゴリズムを与えた．

図 2.6(a) の平面グラフを 3 連結成分に分解したものを図 2.7(a) に示し，3 連結成分分解木を図 2.7(b) に示す．(分解木にはちょうど 4 個の葉 l_1, l_2, l_3, l_4 がある.)

既知の格子描画アルゴリズムで得られる描画においては外周は三角形として描画されるのに対し，本研究の格子凸描画においては外周は長方形として描画される．

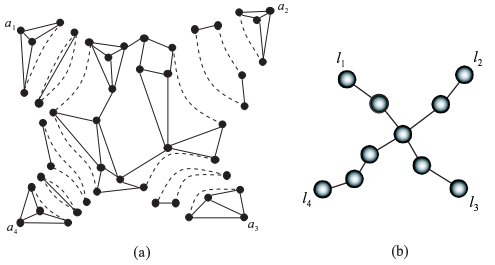


図 2.7: (a) G の 3 連結成分, (b) G の 3 連結成分分解木 $T(G)$.

6　平面グラフの開矩形勢力描画

平面グラフ G の格子描画において，G の辺 e を対角線とする軸平行な長方形を e の**矩形勢力**と呼ぶ．G の各辺 (u, v) の勢力矩形領域内に u，v 以外の点が含まれないような G の格子描画を**矩形勢力描画 (Rectangle-of-Influence Drawing)** と呼ぶ．以下本文では矩形勢力描画のことを簡単のため **RI 描画**と表記する．RI 描画では，単なる格子描画よりも点と辺の距離が離れて描画されるので，同じグラフの描画でもより見やすくなる場合が多い (図 2.8(a) および図 2.8(b) 参照)．

勢力矩形を矩形の境界線を含む閉領域とみなしたものを**勢力閉矩形**と呼び，そのときの RI 描画を**閉 RI 描画**という．同様に，勢力矩形を矩形の境界線を含まない開領域とみなしたものを**勢力開矩形**と呼び，そのときの RI 描画を**開 RI 描画**と

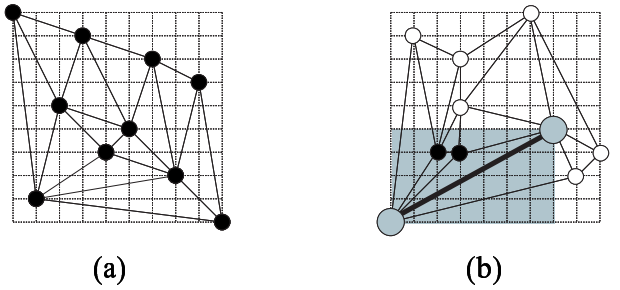


図 2.8: (a) G の RI 描画, (b) RI 描画ではない G の格子描画.

いう．したがって，図 2.9(b) のように，閉 RI 描画では各辺の勢力矩形の内部はもちろん，境界上にもその辺の端点以外の点があってはいけない．一方，図 2.9(c) のように，開 RI 描画では辺の勢力矩形の境界上にその辺の端点以外の点があってもよい．したがって，閉 RI 描画は開 RI 描画であるが，開 RI 描画は必ずしも閉 RI 描画ではない．平面グラフ G が閉 RI 描画を持つための必要十分条件は Biedl らによって与えられており，G がその条件を満足するならば G を $(n-1)\times(n-1)$ の整数格子上に線形時間で閉 RI 描画するアルゴリズムも与えられている．しかし，平面グラフが開 RI 描画を持つための必要十分条件は知られていない．

(外面も含めた) 全ての面が三角形である平面グラフを**三角化**平面グラフという．全ての内面が三角形である平面グラフを**内部三角化**平面グラフという．本研究では，三角化平面グラフ G が開 RI 描画を持つかどうかを判定し，もし持つならば $W+H=n$ なる整数格子に開 RI 描画する線形時間アルゴリズムを与えた．(図 2.10参照.) 更に内部三角化平面グラフ G が開 RI 描画を持つための十分条件を与えるとともに，もし G がその条件を満足するならば G を $(n-1)\times(n-1)$ の整数格子上に開 RI 描画する $O(n^{1.5}/\log n)$ 時間アルゴリズムを与えた．(図 2.11参照.)

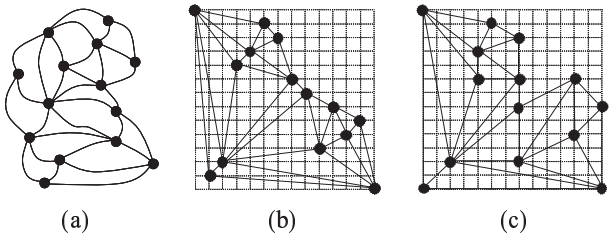


図 2.9: (a) 平面グラフ G, (b) G の閉 RI 描画, (c) G の開 RI 描画.

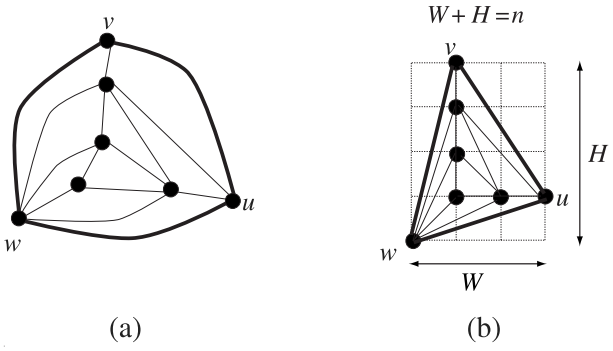


図 2.10: (a) 三角化平面グラフ G, (b) G の開 RI 描画.

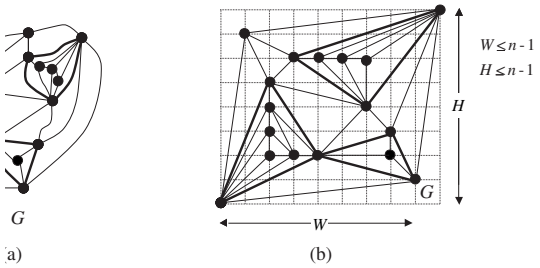


図 2.11: (a) 内部三角化平面グラフ G, (b) G の開 RI 描画.

7 Web 情報検索

近年急速な成長を続ける Web 上には様々な情報が溢れているが，Web 上のページ数は 100 億以上（2006 年 1 月現在）と膨大であるため，目的の情報を含んだページを検索エンジンを使わずに見つけ出すことは非常に困難である．検索エンジンは各ページに対して，入力されたキーワードに関連している度合いや，掲載されている情報の良質さの度合いを示すスコアをスコアリングアルゴリズムによって与え，スコアの高いページから順に，その URL のリストを出力する形式のものが多い．

当初の検索エンジンのスコアリングアルゴリズムは，各ページのテキスト情報をあらかじめ保持

しておき，キーワードがページ内に出現する回数や出現する場所などから，そのページのスコアを決定するような，テキスト情報を用いた手法が取られていた．しかし，このようなテキスト情報のみを用いた手法には以下のような問題点がある．

- 検索キーワードを含んでいないが，キーワードに本来関連したページを見つけることができない．例えば,「web browser」という一般名詞を検索キーワードとしたときに,「internet explorer」などの固有名詞を含んでいるが,「web browser」を含んでいないページは関連ページと見なすことができない．
- 検索キーワードが同音同綴異義語の場合，検索する側が意図していない別の意味のキーワードに関連したページまで見つけてきてしまうことがある．例えば,「ジャガー」という単語は，イギリス車の「ジャガー」，動物の「ジャガー」，Macintosh OS の「ジャガー」のように複数の種類の事物を表すのに用いられる．
- 検索エンジンにおける様々なキーワードに関する関連度スコアを不当に高く出力させることを目的として，そのページのトピックに本来関係のない様々な言葉，すなわちダミーキーワードを故意に含めているページを関連ページと見なして出力してしまうことがある．

テキスト情報のみを用いた手法には，このような言語的な問題点があるため，Web のページが持つリンクの情報を利用した手法が近年提案されている．最近の検索エンジンは，テキスト情報を用いた手法とリンク情報を用いた手法を組み合わせてページのスコア付けを行っているものがほとんどである．リンク情報を用いた手法では，リンクに対して以下の仮定をしている．

仮定 1 リンクはページ u の作者がページ v に価値のある情報が掲載されていると判断したときに，ページ u からページ v に対して張られる．すなわちリンクはページからページへの推薦票である．

Kleinberg は仮定 1 のもと，あるトピックに関連した良質なページを発見するためのページのスコアリングアルゴリズムである HITS（Hyperlink-Induced Topic Search）を提案している．また，HITS の改良版も数多く提案されてきた

しかし，HITS の提案から 10 年近く経過した現在，Web の規模は当時とは比べものにならないほど大きくなり，互いにリンクを張り合うよう悪意を持って作成されたページの集合であるリンクファームが増えたため，HITS や既存の HITS 改良法では，与えられたキーワードに関連していないページに高いスコアを与えてしまうことが多々ある．

本研究では，現在あるいは将来の Web においても，与えられたキーワードに関連している度合いが高いページを発見するアルゴリズムを，HITS を基にして構築する．実際，リンクファーム内のリンクの除去と Gyongyi らによって提案された TrustRank を基に新たに考案した trust スコアを組み合わせることによって，Kleinberg の HITS や各種の HITS 改良法よりも，与えられたキーワードに関連したページを数多く見つけることができる新たな HITS 改良法を与えることができた．

8 グラフの均一分割問題

グラフ $G = (V, E)$ の各点 $v \in V$ には，整定数 q 個の非負整数の重み $\omega_1(v), \omega_2(v), \cdots, \omega_q(v)$ が割当てられているとする．また，q 個の非負整数対 (l_i, u_i) が与えられているとする．ここで $1 \leq i \leq q$ である．本研究では，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 i 番目の合計それぞれがほぼ均一になるようにグラフを分割したい．すなわち，各連結成分に含まれる点重みの i 番目の合計が l_i 以上 u_i 以下になるようにグラフを分割した

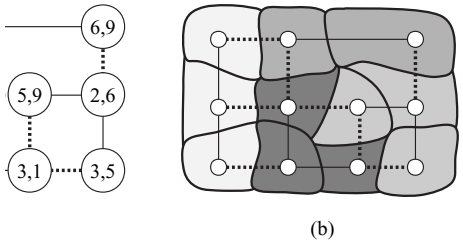


図 2.12: (a) グラフの均一分割の例, (b) 分割に対応する選挙区割.

い．このような分割を G の**均一分割**と呼ぶ．例えば，図 2.12(a) は，グラフ G の均一分割の例である．ここで，$q = 2$ であり，$(l_1, u_1) = (10, 15)$ であり，$(l_2, u_2) = (10, 20)$ である．また，各点 v は丸で描かれ，2 つの点重み $\omega_1(v)$ と $\omega_2(v)$ 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．

グラフの均一分割を見つける問題は，選挙区割り問題に応用される．即ち，グラフの各点 v を都市に，点 v の 1 番目の点重み $\omega_1(v)$ を人口に対応させ，2 番目の点重み $\omega_2(v)$ を都市の面積に対応させる．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や面積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_1, u_1) と (l_2, u_2) に対し，均一分割を見つけてやればよい．例えば，図 2.12(b) は，図 2.12(a) の分割によって制定された選挙区割りである．

本研究では，与えられたグラフ G の均一分割を見つける以下の 3 つの問題を扱う．**最少分割問題**とは，最少の連結成分数を持つ G の均一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．**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 の均一分割を見つける問題である．

3 つの分割問題は，$q = 1$ のときですら直並列グラフに対して NP 困難であり，直並列グラフに対して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，c 倍近似多項式時間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 $q = 1$ のときでさえ強 NP 困難であり，擬多項式時間ですら解けそうにない．

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 $O(u^{4q}n)$ 時間で解けることを示した．ここで，$u = \max\{u_i \mid 1 \leq i \leq q\}$ である．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 $O(p^2u^{4q}n)$ 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．

9 グラフの最大分割の近似

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．

しかし，全てのグラフがこのような分割を持つわけではない．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，最大分割問題で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たい．図 2.13は，与えられたグラフ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 $(2+7)+(8+7)+(6+3)+4 = 37$ であり，これがこのグラフに対しては最大である．ここで，各

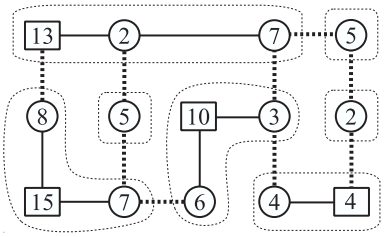


図 2.13: 直並列グラフの最大分割問題の解の一例.

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．

最大分割問題は，木に対してさえNP困難であり，したがって木に対してすら多項式時間で解けそうにない．また，最大分割問題は一般のグラフに対しては強NP困難であり，擬多項式時間でさえ解けそうにない．しかし，現在までに，木に対しては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）が知られている．

本研究では，最大分割問題の近似可能性について明らかにした．まず，一般のグラフに対する最大分割問題はMAXSNP困難であることを示した．したがって，一般のグラフに対しては近似スキーム（PTAS) が存在しそうにない．次に，供給点が1個しかない直並列グラフに対し，完全近似スキームを与えた．この完全近似スキームは，部分k-木に拡張することができる．

10　端子シュタイナー木問題

本研究では，各辺eに非負実数のコスト$c(e)$が与えられたグラフ$G=(V,E)$を扱う．**端子**と呼ばれる点の集合$K\subseteq V$が与えられたとき，Kに対するGの**端子シュタイナー木**Tは，Gの（全域木とは限らない）木であり，Kに含まれる全ての点はTの葉である．与えられたグラフGと端子の集合Kに対し，**端子シュタイナー木問題**では，辺コストの合計が最小である端子シュタイナー木を見つけたい．例えば，図2.14(b)は，図2.14(a)のグラフと端子の集合$K=\{t_1,t_2,t_3\}$に対する端子シュタイナー木の例である．ここで，各端子は黒丸で描かれ，端子でない点は白丸で描かれ，各辺のコストはその辺の側に書かれている．図2.14(b)の端子シュタイナー木の辺コストの合計は$1+2+2+3=8$である．

端子シュタイナー木問題はNP困難であり，したがって多項式時間アルゴリズムは存在しそうになく，近似の観点から多くの研究がなされてきた．端子が必ずしも葉でなくてよい**シュタイナー木問題**に対しては，古くから固定パラメータ容易性（Fixed Parametor Tractability）が知られている．しかし，端子シュタイナー木問題の固定パラメータ容易性は，今まで知られていなかった．

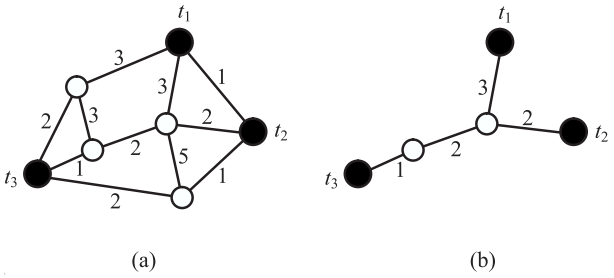


図 2.14:　(a) グラフGと端子の集合$K=\{t_1,t_2,t_3\}$ (b) Kに対するGの端子シュタイナー木.

本研究では，端子シュタイナー木問題の固定パラメータ容易性を示した．より正確には，端子シュタイナー木問題の厳密解を$O^*(3^k)$時間で見つけるアルゴリズムを与えた．ここで，kは端子の個数$k=|K|$であり，O^*記法では多項式の項は無視される．したがって，パラメータkに対して，端子シュタイナー木問題は固定パラメータ容易であることがわかる．

11　リスト全彩色

点集合V, 辺集合Eからなる単純グラフを$G=(V,E)$と書く．グラフ$G=(V,E)$の**全彩色**とは，隣接する任意の2点や，端点を共有する任意の2辺や，任意の点とそれに接続する全ての辺が異なる色になるように, Gの全ての点と辺に色を割り当てることである．したがってGの全彩色fは$V\cup E$から色集合Cへの写像$f:V\cup E\to C$である．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2.15にグラフGとリストLが与えられたときのリスト全彩色の例を示す.

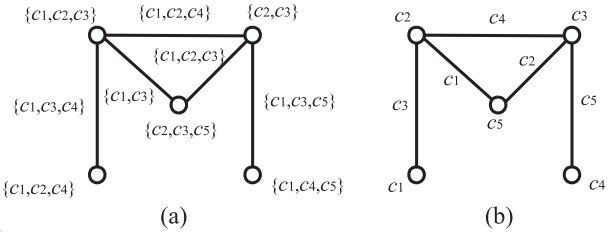


図 2.15: (a) グラフ G とリスト L　(b) リスト全彩色の例

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も, リスト全彩色問題が NP 完全であることを証明した. 更に, 直並列グラフがリスト全彩色をもつための十分条件を与えた. すなわち, 直並列グラフ G の各点 u に $|L(u)| \geq \Delta(u)+2$ なるリスト $L(u)$ が与えられ, 各辺 $e = vw$ に $|L(e)| \geq \max\{d(v)+1, d(w)+1\}$ なるリスト $L(e)$ が与えられたとき, グラフ G はリスト全彩色を持つという定理を証明した. ここで $\Delta(u)$ は点 u とその隣接点の中での最大次数であり, $d(v)$, $d(w)$ は点 v, w の次数である. また, 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次の線形時間アルゴリズム **Color** を構築した.

Algorithm Color(G, L)

(1) グラフ G において部分構造 (a)–(e) を探す.
(2) (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.

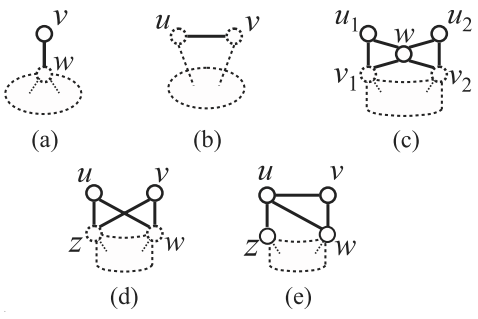


図 2.16: 直並列グラフの部分構造.

研究業績一覧

学術論文

1. K. Miura, M. Azuma and T. Nishizeki: "Convex drawings of plane graphs of minimum outer apices", International Journal of Foundations of Computer Science, 17 巻 5 号, pp. 1115–1127, 2006.
概要: In a convex drawing of a plane graph G, every facial cycle of G is drawn as a convex polygon. A polygon for the outer facial cycle is called an outer convex polygon. A necessary and sufficient condition for a plane graph G to have a convex drawing is known. However, it has not been known how many apices of an outer convex polygon are necessary for G to have a convex drawing. In this paper, we show that the minimum number of apices of an outer convex polygon necessary for G to have a convex drawing is, in effect, equal to the number of leaves in a triconnected component decomposition tree of a new graph constructed from G, and that a convex drawing of G having the minimum number of apices can be found in linear time.

2. K. Miura, H. Haga and T. Nishizeki: "Inner rectangular drawings of plane graphs", International Journal of Computational Geometry and Applications, 16 巻 2-3 号, pp. 249–270, 2006.
概要: A drawing of a plane graph is called an inner rectangular drawing if every edge is drawn as a horizontal or vertical line segment so that every inner face is a rectangle. In this paper we show that a plane graph G has an inner rectangular drawing D if and only if a new bipartite graph constructed from G has a perfect matching. We also show that D can be found in time $O(n^{1.5}/\log n)$ if G has n vertices and

a sketch of the outer face is prescribed, that is, all the convex outer vertices and concave ones are prescribed.

3. K. Miura, S. Nakano and T. Nishizeki: "Convex grid drawings of four-connected plane graphs", International Journal of Foundations of Computer Science, 17 巻 5 号, pp. 1031–1060, 2006.
概要: A convex grid drawing of a plane graph G is a drawing of G on the plane such that all vertices of G are put on grid points, all edges are drawn as straight-line segments without any edge-intersection, and every face boundary is a convex polygon. In this paper we give a linear-time algorithm for finding a convex grid drawing of every 4-connected plane graph G with four or more vertices on the outer face. The size of the drawing satisfies $W + H \leq n - 1$, where n is the number of vertices of G, W is the width and H is the height of the grid drawing. Thus the area $W \cdot H$ is at most $\lceil (n-1)/2 \rceil \cdot \lfloor (n-1)/2 \rfloor$. Our bounds on the sizes are optimal in a sense that there exist an infinite number of 4-connected plane graphs whose convex drawings need grids such that $W + H = n - 1$ and $W \cdot H = \lceil (n-1)/2 \rceil \cdot \lfloor (n-1)/2 \rfloor$.

4. Y. Asano, T. Nishizeki, M. Toyoda and M. Kitsuregawa: "Mining communities on the Web using a max-flow and a site-oriented framework", IEICE Trans. on Information and Systems, E89-D 巻 10 号, pp. 2606–2615, 2006.
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 very 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.

5. T. Ito, K. Goto, X. Zhou and T. Nishizeki: "Partitioning a multi-weighted graph to connected subgraphs of almost uniform size", IEICE Trans. on Information and Systems, E90-D 巻 2 号, pp. 449–456, 2007.
概要: Assume that each vertex of a graph G is assigned a constant number q of nonnegative integer weights, and that q pairs of nonnegative integers l_i and u_i, $1 \leq i \leq q$, are given. One wishes to partition G into connected components by deleting edges from G so that the total i-th weights of all vertices in each component is at least l_i and at most u_i for each index i, $1 \leq i \leq q$. The problem of finding such a "uniform" partition is NP-hard for series-parallel graphs, and is strongly NP-hard for general graphs even for $q = 1$. In this paper we show that the problem and many variants can be solved in pseudo-polynomial time for series-parallel graphs and partial k-trees, that is, graphs with bounded tree-width.

研究会等

1. A. Kamada, K. Miura and T. Nishizeki: "Convex grid drawings of plane graphs with rectangular contours (Extended Abstract)", Proc. of ISAAC 2006, LNCS 4288, pp. 131–140, 2006.
   概要: In a convex drawing of a plane graph, all edges are drawn as straight-line segments without any edge-intersection and all facial cycles are drawn as convex polygons. In a convex grid drawing, all vertices are put on grid points. A plane graph G has a convex drawing if and only if G is internally triconnected, and an internally triconnected plane graph G has a convex grid drawing on an $n \times n$ grid if either G is triconnected or the triconnected component decomposition tree $T(G)$ of G has two or three leaves, where n is the number of vertices in G. In this paper, we show that an internally triconnected plane graph G has a convex grid drawing on a $2n \times n^2$ grid if $T(G)$ has exactly four leaves. We also present an algorithm to find such a drawing in linear time. Our convex grid drawing has a rectangular contour, while most of the known algorithms produce grid drawings having triangular contours.

2. K. Miura, T. Matsuno and T. Nishizeki: "Open rectangle-of-influence drawings of inner triangulated plane graphs", Proc. of GD 2006, LNCS 4372, pp. 138–149, 2007.
   概要: A straight-line drawing of a plane graph is called an open rectangle-of-influence drawing if there is no vertex in the proper inside of the axis-parallel rectangle defined by the two ends of every edge. In an inner triangulated plane graph, every inner face is a triangle although the outer face is not always a triangle. In this paper, we first obtain a sufficient condition for an inner triangulated plane graph G to have an open rectangle-of-influence drawing; the condition is expressed in terms of a labeling of angles of a subgraph of G. We then present an $O(n^{1.5}/\log n)$-time algorithm to examine whether G satisfies the condition and, if so, construct an open rectangle-of-influence drawing of G on an $(n-1)\times(n-1)$ integer grid, where n is the number of vertices in G.

3. T. Ito, K. Goto, X. Zhou and T. Nishizeki: "Partitioning a multi-weighted graph to connected subgraphs of almost uniform size", Proc. of COCOON 2006, LNCS 4112, pp. 63–72, 2006.
   概要: Assume that each vertex of a graph G is assigned a constant number q of nonnegative integer weights, and that q pairs of nonnegative integers l_i and u_i, $1 \leq i \leq q$, are given. One wishes to partition G into connected components by deleting edges from G so that the total i-th weights of all vertices in each component is at least l_i and at most u_i for each index i, $1 \leq i \leq q$. The problem of finding such a "uniform" partition is NP-hard for series-parallel graphs, and is strongly NP-hard for general graphs even for $q = 1$. In this paper we show that the problem and many variants can be solved in pseudo-polynomial time for series-parallel graphs. Our algorithms for series-parallel graphs can be extended for partial k-trees, that is, graphs with bounded tree-width.

4. T. Ito, E. D. Demaine, X. Zhou and T. Nishizeki: "Approximability of partitioning graphs with supply and demand", Proc. of ISAAC 2006, LNCS 4288, pp. 121–130, 2006.
   概要: Suppose that each vertex of a graph G is either a supply vertex or a demand vertex and is assigned a positive real number, called the supply or the demand. Each demand vertex can receive "power" from at most one supply vertex through edges in G. One thus wishes to partition G into

connected components so that each component C either has no supply vertex or has exactly one supply vertex whose supply is at least the sum of demands in C, and wishes to maximize the fulfillment, that is, the sum of demands in all components with supply vertices. This maximization problem is known to be NP-hard even for trees having exactly one supply vertex and strongly NP-hard for general graphs. In this paper, we focus on the approximability of the problem. We first show that the problem is MAXSNP-hard and hence there is no polynomial-time approximation scheme (PTAS) for general graphs unless P = NP. We then present a fully polynomial-time approximation scheme (FPTAS) for series-parallel graphs having exactly one supply vertex. The FPTAS can be easily extended for partial k-trees, that is, graphs with bounded treewidth.

5. T. Ito, Y. Okamoto and T. Tokuyama:
"Algorithms for the full Steiner tree problem", Proc. of ICALP2006 Affiliated Workshop iETA, pp. 39–45, 2006.
概要: Assume that each edge of a graph $G = (V, E)$ is assigned a nonnegative real number cost, and that a set $K \subseteq V$ of vertices, called terminals, is given. A full Steiner tree (or a terminal Steiner tree) of G with respect to K is a subtree T of G such that every vertex in K is a leaf of T. For a given graph G and a given set $K \subseteq V$ of terminals, the (minimum-cost) full Steiner tree problem is to find a full Steiner tree for K which has the minimum total cost of edges. In this paper we first give an exact algorithm to solve the problem for general graphs in time $O^*(3^k)$ where $k = |K|$ and O^*-notation denotes that polynomial factors are suppressed. Thus the problem is fixed-parameter tractable. We then show that the problem can be solved in polynomial time for plane graphs if all the terminals lie only on a fixed constant number of face boundaries.

6. Y. Matsuo, X. Zhou and T. Nishizeki:
"Sufficient condition and algorithm for list total colorings of series-parallel graphs", Proc. of WAAC 2006, pp. 49–56, 2006.
概要: A total coloring of a graph G is a coloring of all elements of G, i.e. vertices and edges, such 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 for given L. In this paper, we give a sufficient condition for a series-parallel graph to have a list total coloring, that is, we prove a theorem that a series-parallel graph G has a list total coloring if $|L(u)| \geq \Delta(u) + 2$ for each vertex u and $|L(e)| \geq \max\{d(v) + 1, d(w) + 1\}$ for each edge $e = vw$, where $\Delta(u) = \max\{d(x)|\text{vertex } x \text{ is either } u \text{ or adjacent to } u\}$ and, $d(v)$ and $d(w)$ are the degrees of the ends v and w of e, respectively. We finally present a linear-time algorithm to find a list total coloring of a given series-parallel graph G if G and L satisfy the sufficient condition.

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　寒野 善博　西田 徹志　今堀 慎治

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　3 次元単体メッシュのロバスト計算法

3 次元領域での物理現象シミュレーションのための有限要素法では，メッシュが必要である．最も基本的なのは四面体メッシュである．しかし，その計算法はいくつかの困難を伴う．困難の一つは，通常の摂動が使えないという事情である．

メッシュ生成に限らず幾何計算において，退化対策は重要課題の一つである．最近の研究により，厳密計算と記号摂動の組合せによって退化を自動回避することができるようになり，これが退化対策の定番となっている．

しかし，記号摂動は万能ではない．なぜなら，この手法はすべての退化を解消するため，意図に反した副作用をもたらすことがあるからである．

そこで，残したい退化はそのまま残し，回避したい退化のみを解消できる選択的退化回避の技術が望まれる場面も少なくない．

そのような場面の具体例の一つに，3 次元単体メッシュ生成問題がある．点の配置が与えられたとき，それらを頂点とする四面体メッシュで比較的よいものが得られる手法の一つがドロネー分割であるが，同一平面上に 4 点が乗るという退化を解消すると，体積が零の四面体（これはスリーバーとよばれる）が現れることがある．しかし，これが含まれるメッシュは有限要素法には使えない．

これを回避するために，スリーバーが発生する心配のない新しい摂動法を開発した [14]．この方法は，与えられた点を半径 0 の球とみなし，この半径に無限小の摂動を与えることによって，点のドロネー分割問題を，球に対するラゲールドロネー分割問題へ変更するものである．これによって，球の中心が同一平面に乗っているという退化はそのまま残るため，副作用のない摂動ができる．

一方，球が与えられたとき，ラゲール距離は使わないで，ユークリッド距離のままボロノイ図を作る問題もバブルメッシュの生成法に必要な重要技術課題である．私たちは，円ボロノイ図および球ボロノイ図に関連するいくつかの算法を開発した．第 1 に円ボロノイ図のボロノイ点の計算（これはアポロニウスの第 10 問題として古くから知られている）のためのアルゴリズムを開発した．この問題は以前から解かれているが，従来の方法は場合分けが複雑であった．それに対して，本方法では，メビウス変換を利用することによって，場合分けを単純ですっきりしたものに改良した [7]．

第 2 に，円の包含関係を検出するアルゴリズムを構成した．これは平面走査法を利用したもので，n 個の円の包含関係を $O(n \log n)$ で列挙することができる [5]．

第 3 に，球ボロノイ図の位相構造を記述するための新しいデータ構造を提案した．球ボロノイ図は，ボロノイ点とボロノイ辺が作るグラフが非連

結となる場合があり，双対構造が単体的複体とはならないため，その構造は複雑なものとなる．本記述法では，非連結なグラフの間に親子関係が見出せることに注目し，複数の単体的複体が階層をなす構造として捉えている [6].

3 M凸関数の変換

M凸関数は効率良く解ける非線形離散最適化問題の枠組を与えるものであるが，最近になって，M凸関数の概念は定パリティジャンプシステム上の関数へと一般化されている．本研究では，このように一般化されたM凸関数に対しても，合成積（畳み込み）やグラフによる変換が定義できることを示した．さらに，グラフによる変換の最も一般化された形として，M凸関数がリンキングシステムによって変換できることを示した．

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．

関数 $f : \mathbf{Z}^V \to \mathbf{R}$ がM凸関数であるとは，f が交換公理:

$\forall x, y \in \mathrm{dom} f$, $\forall s \in \mathrm{Inc}(x,y)$, $\exists t \in \mathrm{Inc}(x+s,y)$:

$f(x) + f(y) \geq f(x+s+t) + f(y-s-t)$

を満たすことを言う．

有限集合 S,T と $\mathbf{Z}^S \times \mathbf{Z}^T$ の部分集合 L の組 (S,T,L) が整数ポリリンキングシステムであるとは，

$$B = \{(x,y) \in \mathbf{Z}^S \times \mathbf{Z}^T \mid (-x,y) \in L\}$$

が整数ポリマトロイドの基多面体をなし，かつ $(\mathbf{0},\mathbf{0}) \in B$ となることをいう．

関数 $f : \mathbf{Z}^S \to \mathbf{R} \cup \{+\infty\}$ の整数ポリリンキングシステム (S,T,L) による変換とは，

$$\tilde{f}(y) = \inf\{f(x) \mid x \in \mathbf{Z}^S,\ (x,y) \in L\} \quad (y \in \mathbf{Z}^T)$$

で定義される関数 $\tilde{f} : \mathbf{Z}^T \to \mathbf{R} \cup \{+\infty, -\infty\}$ ををいう．

以上の定義の下で，次の定理を示した．

定理： $\mathbf{Z}^S$ 上で定義されたM凸関数 f の整数ポリリンキングシステム (S,T,L) による変換 $\tilde{f}$ は（$-\infty$ という値をとらない限り）M凸関数である．

4 ハブ・アンド・スポークネットワーク設計問題

1987年にO'Kelly [10] は，ハブ空港の配置と，非ハブ空港のハブ空港への接続を決定する問題を2次整数計画問題として定式化し，発見的解法を提案している．Sohnら [13] は，ハブ空港の配置を既知として，接続のみを決定する問題は，ハブ空港の数が3のときでさえNP困難であることを示した．現在まで，接続のみを決定する問題に対し，定数の近似比率を持つ多項式時間近似解法は知られていなかった．本研究では，ハブ空港の配置が既知であるとき，接続のみを決定する問題 (ハブ・アンド・スポークネットワーク設計問題) に対し，初めての多項式時間近似解法を提案する．

h 個のハブ空港と n 個の非ハブ空港，および各空港間の輸送量と単位輸送コストが与えられているものとする．非ハブ空港は唯一のハブ空港に接続し，非ハブ空港間の輸送はハブ空港を経由して行われる．また，各ハブ空港間は直行便を持ち，乗り換えは2回までとする．本稿では，以上の条件の下で，総輸送コストを最小化するように非ハブ空港のハブ空港への接続を決定する問題を扱う．

ハブ空港の集合を $H := \{1,2,\ldots,h\}$，非ハブ空港の集合を $N := \{1,2,\ldots,n\}$，空港 i から j への輸送量と単位輸送コストをそれぞれ $w_{ij}(\geq 0)$, $c_{ij}(\geq 0)$ とする．ハブ・アンド・スポークネットワーク設計問題は，

$$\begin{array}{ll}
\min. & \sum_{p\in N}\sum_{q\in N} w_{pq}(\sum_{i\in H} c_{pi}x_{pi} \\
 & \quad + \sum_{i\in H}\sum_{j\in H} c_{ij}x_{pi}x_{qj} + \sum_{j\in H} c_{jq}x_{qj}) \\
\text{s. t.} & \sum_{i\in H} x_{pi} = 1 \qquad (\forall p \in N), \\
 & x_{pi} \in \{0,1\} \qquad (\forall p \in N,\ \forall i \in H),
\end{array}$$

と定式化することができる．ただし，変数 x_{pi} は，非ハブ空港 p をハブ空港 i に接続するときに1，接続しないときに0の値をとる．

現実的な仮定として，単位輸送コストは以下の条件を満たすとする．(1)$c_{ii} = 0$ $(\forall i \in H \cup N)$. (2) 対称性．すなわち，$c_{ij} = c_{ji}$ $(\forall (i,j) \in (H \times H) \cup (H \times N) \cup (N \times H))$. (3) ハブ空港間の三角不等式．すなわち，$c_{ij} \leq c_{ik} + c_{kj}$ $(\forall (i,j,k) \in H^3)$. (4) 非ハブとハブ2つ間の三角不等式．すなわち，$c_{ij} \leq c_{pi} + c_{pj}$ $(\forall (p,i,j) \in N \times H^2)$.

最初に，簡単な近似解法として以下のロバストな解法を提案した．

Theorem 1 各非ハブを最も近いハブに接続する解法は，3-近似解法である．

ここで，新たな変数 y_{piqj} を導入することにより目的関数を線形化し，次に簡単な式変形と制約条件の緩和を行うことにより，以下の線形緩和問題 (LPR)

$$\begin{aligned}
\text{min.}\quad & \textstyle\sum_{p\in N}\sum_{q\in N} w_{pq}(\sum_{i\in H} c_{pi}x_{pi} \\
& \textstyle+\sum_{i\in H}\sum_{j\in H} c_{ij}x_{pi}x_{qj}+\sum_{j\in H} c_{jq}x_{qj}) \\
\text{s. t.}\quad & \textstyle\sum_{i\in H} x_{pi}=1 && (\forall p\in N), \\
& \textstyle\sum_{j\in H} y_{piqj}=x_{pi} && (\forall p,q\in N,\ \forall i\in H), \\
& \textstyle\sum_{i\in H} y_{piqj}=x_{qj} && (\forall p,q\in N,\ \forall j\in H), \\
& 0\le x_{pi}\le 1 && (\forall p\in N,\ \forall i\in H), \\
& y_{piqj}\ge 0 && (\forall p,q\in N,\ \forall i,j\in H).
\end{aligned}$$

を導出することができる．

Saito ら [12] は，CAB データと呼ばれるベンチマーク問題において上記の線形緩和問題を扱い，ハブ空港が 3 つの場合，ほとんどの問題例で整数最適解が得られることを報告している．整数最適解が得られなかった場合でも, 非整数最適解を用いた次の解法を適用することができる．

Theorem 2 LPR の最適解 x^* に対し, 各変数 x_{pi} を確率 x^*_{pi} で 1 に切り上げ, 確率 $1-x^*_{pi}$ で 0 に切り下げる解法は, 2-近似解法である．

本研究では更に, ハブ空港の数が 3 つの場合に対し, 以下の結果を得た．先ず最初に, 従属丸め法と呼ばれる手法を用いて多項式時間 (4/3)-近似解法を提案した．また, 提案した 2-近似解法と (4/3)-近似解法の両方を実行し, 良い方の解を出力する事によって, (5/4)-近似解法となることを示した．

ハブ空港数が 3 つの場合に対する (4/3)-近似解法は，Kleinberg and Tardos [8] により定義されたメトリックラベリング問題に対して，ラベル数が 3 つの場合に同じ近似率で適用可能なものとなっている．本研究では，また，メトリックラベリング問題の基本となるケースであるユニフォームラベリング問題に対して，ラベル数が 4 つの場合に適用できる (5/3)-近似解法を提案し，現在までに知られている近似率 11/6 を改善した．

5 独立偶因子問題の組合せ的解法

効率的に解くことのできる組合せ最適化問題として，無向グラフのマッチング問題とマトロイドの共通独立集合問題がよく知られている．両者の共通の一般化として，Cunnigham–Geelen [1] が，**独立パスマッチング**という概念を導入し, 最大最小定理を示した．彼らは，その後，より一般的な枠組みとして, 有向グラフにおける**独立偶因子**を導入している [2].

有向グラフ中の偶因子とは，有向路と偶閉路の点素な集まりを意味する．枝数最大の偶因子を見出す偶因子問題は一般に NP 困難であるが，奇閉路対称と呼ばれる有向グラフのクラスにおいては, 最大最小定理が成立し，楕円体法や代数的手法を用いた多項式時間解法が存在することも示されている．しかし，これらの解法は，あまり効率的でなく，組合せ的な多項式時間解法の開発が望まれていた．最近，Pap [11] は，交互道を用いた新たなアルゴリズムを設計し，この問題を解決している．

有向グラフの点集合上に二つのマトロイド構造を付加し，偶因子の端点集合（偶因子の枝の始点の集合と終点の集合）が，それぞれのマトロイドにおいて独立集合であるときに，この偶因子を独立偶因子という．Cunningham–Geelen は，奇閉路対称よりも若干特殊な弱対称と呼ばれるクラスの有向グラフにおいて，最大枝数の独立偶因子を見出す独立偶因子問題を，マトロイド共通独立集合問題に帰着することで，多項式時間解法の存在を示している．この解法では，マトロイドの独立性判定オラクルとして，偶因子問題のアルゴリズムを呼び出す形になっている．この部分に Pap のアルゴリズムを採用すれば，純粋に組合せ的なアルゴリズムが構成できたことになるが，決して効率的ではない．ただし，n 有向グラフの点数, Q は付加された

マトロイドの独立判定に要する時間である．

本研究 [4] では，Pap の手法を拡張することにより，独立偶因子問題に対する効率的なアルゴリズムを開発した．新しいアルゴリズムの計算量は, 有向グラフの点数 n，付加されたマトロイドの独立性判定に要する時間 Q に対して，$O(n^4Q)$ であり，既存の解法よりも遥かに効率的である．同時に，このアルゴリズムは，マッチングに関する

Tutte–Berge 公式とマトロイド共通独立集合に関する Edmonds の定理とを拡張して，独立偶因子の枝数の最大値を特徴付ける新たな最大最小定理の構成的証明を与えてもいる．

6 ロバスト半正定値計画のための行列拡大法の効率化

6.1 概要

ロバスト半正定値計画問題は，制御や最適化に多くの応用を持つ重要な最適化問題である．筆者らが提案した行列拡大法はロバスト半正定値計画問題の解法の１つであり，与えられたロバスト半正定値計画問題を近似する半正定値計画問題を構成してこれを解くことを考える．しかし実用的な局面では，近似問題のサイズが大きくなってしまうという問題があった．本研究では，制約式のサイズを小さくすることによって近似問題のサイズを小さくすることを考えた [3]．なお，これ以外にも制約式の数を減らすことによる効率化も考えている [9]．

6.2 行列拡大法

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．

問題 P は無限本の半正定値制約を持ち，一般に直接解くことは困難である．そこで筆者らは，問題 P を近似する問題を作ってそれを解くことを考えた．これが行列拡大法である．

ここで考える近似問題は，多面体 Θ の凸多面体の集合 $\Delta = \{\Theta^{[j]}\}_{j=1}^{J}$ への分割に基づいており，$P(\Delta)$ と記述される．近似問題 $P(\Delta)$ の最小値は一般にもとの問題 P の最小値よりも大きいが，近似誤差 $\min P(\Delta) - \min P$ は分割 Δ の細かさの関数で評価することができる．それによれば，分割 Δ を細かくすれば，近似誤差はいくらでも小さくすることができる．

6.3 制約式のサイズの圧縮

近似問題 $P(\Delta)$ の構成においては，問題 P 中の関数 $F(x,\theta)$ を θ の多項式として表現したときすべての項の係数が非零であることが暗黙のうちに仮定されていた．しかし実際の問題ではこのようなことはまれである．本研究では，$F(x,\theta)$ を θ の多項式とみたとき多くの項の係数は零であるという一種の疎性を仮定することで，近似問題のサイズを小さくすることを考えた [3]．近似問題の構成で鍵になるのは行列 $H(\theta)$ の存在であるが，rectilinear Steiner arborescence という特殊なグラフを使うことにより，疎性を生かしつつ行列 $H(\theta)$ の存在を保証することができる．なお，この新しい近似問題に対しても近似誤差の定量的評価が可能であり，分割を細かくすることでいくらでも近似誤差を小さくすることができる．

7 ボート航行距離方程式の一般化

流れの中の最短時間問題とは，流れを伴う領域で，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である．この問題を最適制御に帰着すると，最善の操縦は，ボートを常に等時間曲線の法線方向へ進めればよいということが分かる．すなわち，始点の集合から領域の各点への最短時間が分かれば等時間曲線を描けるが，その等時間曲線が分かれば解けるということである．

これを解く典型的な方法は，マーカー粒子法と呼ばれる類のものである．等時間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，再び等時間曲線を構築する．これを繰り返しながら計算を進める．このとき，各粒子の法線は，近傍の粒子を使って決定される．

しかし，この問題には，初期条件に滑らかな曲線を与ても，計算途中，等時間曲線が滑らかさを

失う可能性があるという困難がある．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．等時間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，破綻を起こすのである．

昨年度，2 次元の問題に対して，近傍に依存せず法線方向を決定し，破綻を回避する数値計算法を考案した．それは，法線に関して，近傍に依存しない新たな微分方程式を構築する方法である．今回は，n 次元および曲面に対する計算法を考案した．n 次元は，2 次元の式を n 次元にするだけである．ゆえに，—ここでは曲面に関してのみ結果を記す．

直交座標系 (x, y, z) をひとつ固定する．$\Omega \subset \mathbf{R}^2$ を xy 平面上の領域とし，点 $p = (x, y)^{\mathrm{T}} \in \Omega$ での曲面の高さを $z = h(p)$ で表す．$f(p, h(p)) = (u, v, w)^{\mathrm{T}}$ を曲面に接する流れとし，C^1 とする．この流れの中をボートが曲面に沿って常に最大の推進力で動くものとする．そして，時刻 t で得られる等時間曲線をマーカー粒子で近似するとする．$(p(t), z(t))$ をある粒子の時刻 t での位置，$F(p, z)$ をボートの速さ，$n(p(t), z(t)) = (a, b, c)^{\mathrm{T}}$ を点 (p, z) での曲面に接する単位法線ベクトルとする．このとき，近傍に依存しない新しい方程式系は

$$(p(t), z(t))_t^{\mathrm{T}} = F(p(t), z(t))n(p(t), z(t)) + f(p(t), z(t))$$

$$\begin{pmatrix} a \\ b \end{pmatrix}_t = -\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} a^2 & ab \\ ab & b^2 \end{pmatrix} - \frac{1}{1 + h_x^2 + h_y^2} \begin{pmatrix} h_x^2 & h_x h_y \\ h_x h_y & h_y^2 \end{pmatrix} \right\} \times \left\{ \nabla F - F \begin{pmatrix} h_{xx} & h_{xy} \\ h_{xy} & h_{yy} \end{pmatrix} \begin{pmatrix} a^2 & ab \\ ab & b^2 \end{pmatrix} \begin{pmatrix} h_x \\ h_y \end{pmatrix} + \begin{pmatrix} u_x & v_x \\ u_y & v_y \end{pmatrix} \begin{pmatrix} 1 + h_x^2 & h_x h_y \\ h_x h_y & 1 + h_y^2 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \right\}$$

$$c_t = h_x a_t + h_y b_t$$

と表される．ただし，$\times$ は行列ベクトル積を表し，添字 t, x, y は微分を意味する．

今後は，船舶や飛行機の最適航路の設計などに応用して行きたい．

8 カッターパス生成アルゴリズム

平面状の母材と様々な形の製品集合が与えられたとき, なるべく効率よく製品を切り出す問題を考える．この問題は, 次の 2 つのフェーズからなる問題と考えることができる．(1) 様々な形の製品を母材上に重なりなく, できる限り隙間なく配置する問題. (2) 母材上に配置された製品集合を, カッターを用いて順に切り落とす問題. 前者は多角形詰込み問題, 後者はカッターパス生成問題と呼ばれる．本研究では, カッターパス生成問題に対する, 実用的な近似解法の設計を行った.

カッターパス生成問題における目的は, なるべく短い時間で全ての製品を切り出すこと, すなわちカッターの移動距離の最小化である．本問題は, 枝順回路問題の一種であり, 単純な制約条件下では効率的に最適解を求めることができる．しかし, 本研究で扱った問題は, 工学的な応用から生じたものであり, 複雑な制約条件を考慮する必要がある．まずはじめに, 考慮すべき制約条件を, 以下の通りまとめた.

第一の制約として, 指定された辺におけるへそ残りの禁止という条件を与える．カッターを用いて製品を切り出す際には, カッターの歯の太さによる影響で, 各製品の最後に切断された辺の上に, へそと呼ばれる突起が生じてしまう．カッターによって母材から切り出された製品は, この後の工程で他の部品と接合されるのだが, 接合される辺上にへそがあると, 十分な精度で接合を行うことができなくなってしまう.

第二の制約として, 最終形状での切り出しという条件を与える．複数の製品を一つの塊として母材から切り離し, この塊に対して再加工を行うことは, 作業効率や製品の加工精度の観点から禁止される．よって, 全ての製品は, その最終形状で母材から切り出されることが必要となる.

第三の制約として, 切り出す製品の周りに十分な空間をあけるという条件を与える．母材および製品は, 一定の厚みを持つため, 切り出す製品の周りに十分な空間（隙間）がない場合には, 切り落としたつもりの製品が母材にひっかかるという現象が生じる．このとき, 他の製品の切り出しのために動かしたカッターがひっかかった製品と接触し, その結果として, 製品が傷つけられるとい

う状況に陥る.

第四の制約として, 力を支えることのできる形状を母材が常に維持するという条件を与える. カッターで母材を切断する際には, 摩擦による強い力が母材にかかる. (いくつかの製品が切り出された上での) 母材の形状によっては, この力の影響で母材が振動し, 切り出し加工精度の低下という結果が生じる.

最後の制約として, 第三の制約から副次的に得られる, 製品以外の部分に関する条件を与える. 第三の制約を満たすためには, 母材上の非製品部分も切り出す必要が生じ, この部分も安定に切り出されなければならない.

以上の制約条件のもとで, カッターパスを求める実用的な近似解法を提案した. 我々の提案した手法は, 以下に述べる 3 つのステップからなる.

はじめに, 母材の非製品部分を切り出しやすい形状に分割する. 「切り出しやすい」とは, 凸かそれに準ずる形状を意味する. 次に, 母材上の製品および分割された非製品を節点として, 次の性質を満たす根付き木を構成する: 根付き木の葉から根に向けて製品を切り出すことにより, 上で述べた第一, 第二, 第四の制約条件を自動的に満たす. 最後に, 根付き木の葉から根に向けて, 第三, 第五の制約条件を考慮しながら, できる限り距離の短いカッターパスを求める. 各ステップとも, 選択の自由度が残されているが, 本研究では欲張法などの発見的解法を用いることで, 短時間で実用的に良いと思われるものを選択した. 提案手法を実装し, いくつかのデータ, すなわち母材上の製品配置に対して, 実際にカッターパスを求めることに成功した.

参考文献

[1] W. H. Cunningham and J. F. Geelen: The optimal path-matching problem. *Combinatorica*, Vol. 17 (1997), pp. 315–337.

[2] W. H. Cunningham and J. F. Geelen: Vertex-disjoint dipaths and even dicircuits. 2001.

[3] 猪阪, 大石: 疎性の利用によるロバスト半正定値計画法の効率化. 計測自動制御学会論文集, Vol. 43 (2007), No. 2, pp. 93–101.

[4] S. Iwata and K. Takazawa: The independent even factor problem, *Proc. 18th SODA* (2007), pp. 1171-1180.

[5] D.-S. Kim, B. Lee and K. Sugihara: A Sweep-line Algorithm for the Inclusion Hierarchy Among Circles. *Japan Journal of Industrial and Applied Mathematics*, Vol. 23, No. 1 (2006), pp. 127–138.

[6] D.-S. Kim, D. Kim, Y. Cho and K. Sugihara: Quasi-triangulation and Interworld Data Structure in Three Dimensions. *Computer-Aided Design*, Vol. 38 (2006), pp. 808–819.

[7] D. Kim, D.-S. Kim and K. Sugihara: Apollonius Tenth Problem via Radius Adjustment and Mobius Transformation. *Computer-Aided Design*, Vol. 38 (2006), pp. 14–21.

[8] J. Kleinberg and E. Tardos: Approximation algorithms for classification problems with pairwise relationships, *Journal of the ACM*, Vol. 49 (2002), pp. 616–630.

[9] Y. Oishi: Reduction of the number of constraints in the matrix-dilation approach to robust semidefinite programming. *Proceedings of the 45th IEEE Conference on Decision and Control* (San Diego, USA, December 2006), pp. 5790–5795.

[10] M. O'Kelly: A quadratic integer program for the location of interacting hub facilities. *European Journal of Operational Research*, Vol. 32 (1987), pp. 393–404.

[11] G. Pap: A combinatorial algorithm to find a maximum even factor. *Proc. 11th IPCO*, LNCS 3509, Springer-Verlag, 2005, pp. 66–80.

[12] H. Saito, S. Matuura and T. Matsui: A linear relaxation for hub network design problems. *IEICE transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E85-A (2002), pp. 1000–1005.

[13] J. Sohn and S. Park: The single allocation problem in the interacting three-hub network. *Networks*, Vol. 35 (2000), pp. 17–25.

[14] K. Sugihara: Sliver-Free Perturbation for the Delaunay Tetrahedrization. *Computer Aided Design*, Vol. 39 (2007), pp.87-94.

研究業績一覧

著書

1. 来嶋秀治, 松井知己:
“確率的情報処理と統計力学　　章 4 節「CFTP を用いたパーフェクトサンプリング」”, サイエンス社, 2006 年 9 月.
概要: マルコフ連鎖モンテカルロ法（MCMC 法）の基本的なアイデアは非常に簡明で,「マルコフ連鎖の極限分布からサンプリングを行い, モンテカルロ法 (等) を行う.」というものである. MCMC 法を用いる上で, 目標の分布を定常分布に持つマルコフ連鎖の設計は重要である. これに関して, 目標の分布を設計する方法として, M-H（Metropolice-Hastings）法や Gibbs サンプラーがあげられる. 目標の定常分布をもつマルコフ連鎖を手に入れた後の問題点は,「何回推移させれば定常分布 (極限分布) と言えるのか?」と言うことである. しかし, マルコフ連鎖を何回推移させても, 有限回の推移で打ち切ってしまうとひずみは生じる. これに対し, 1996 年に Propp and Wilson は「無限回のシミュレーションを有限時間で実現」する乱択アルゴリズムを提案した. このアルゴリズムは CFTP（coupling from the past：過去からのカップリング) と呼ばれる. 本稿では CFTP について解説を行う.

2. S. Imahori, M. Yagiura, H. Nagamochi:
“Handbook of Approximation Algorithms and Metaheuristics (Chapter 36. Practical Algorithms for Two-dimensional Packing)”, Chapman & Hall/CRC in the Computer & Information Science Series, （刊行予定）.
概要: Cutting and packing problem is the problem to place a given set of small items into one or many large objects without mutual overlap to minimize/maximize a given objective function. This problem is not only a representative combinatorial optimization problems, but also important for industrial applications; e.g., paper, wood, glass, steel and leather industries, LSI and VLSI designing, newspaper paging. Among the numerous studies on cutting and packing problem, we denote practical algorithms for two-dimensional packing problem.

学術論文

1. Tetsushi Nishida, Kokichi Sugihara and Masato Kimura:
“Stable marker-particle method for the Voronoi diagram in a flow field”, Journal of Computational and Applied Mathematics, Vol. 202, pp. 377–391, 2007.
概要: The Voronoi diagram in a flow field is a tessellation of water surface into regions according to the nearest island in the sense of a “ boat-sail distance ”, which is a mathematical model of the shortest time for a boat to move from one point to another against the flow of water. The computation of the diagram is not easy, because the equi-distance curves have singularities. To overcome the difficulty, this paper derives a new system of equations that describes the motion of a particle along the shortest path starting at a given point on the boundary of an island, and thus gives a new variant of the marker-particle method. In the proposed method, each particle can be traced

independently, and hence the computation can be done stably even though the equidistance curves have singular points.

2. Kokichi Sugihara:
"Sliver-free perturbation for the Delaunay tetrahedrization", Computer-Aided Design, Vol. 39, pp. 87–94, 2007.
概要: This paper studies the symbolic perturbation scheme in the context of Delaunay meshing in the three-dimensional space. The symbolic perturbation is a general and powerful technique for removing geometric degeneracy. However, a straightforward application of this technique to Delaunay meshing does not work well, because the perturbation generates volume-zero tetrahedra, called slivers, which should not appear in the meshes for the finite element method. First we characterize the set of directions in which a point can be perturbed without generating slivers. Next, as an application of this characterization, we construct a graph-theoretic method for finding a sliver-free perturbation. We also show that an ordinary symbolic perturbation cannot avoid slivers for the integer-grid points, and point out that a kind of generalized perturbation can avoid slivers completely.

3. Donguk Kim, Deok-Soo Kim and Kokichi Sugihara:
"Apollonius tenth problem via radius adjustment and Mobius transformation", Computer-Aided Design, Vol. 38, pp. 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 the 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.

4. Deok-Soo Kim, Byunghoom Lee and Kokichi Sugihara:
"A sweep-line algorithm for the inclusion hierarchy among circles", Japan Journal of Industrial and Applied Mathematics, Vol. 23, No. 1, pp. 127–138, 2006.
概要: Suppose that there are a number of circles in a plane and some of them may contain several smaller circles. In this case, it is necessary to find the inclusion hierarchy among circles for the various applications such as the simulation of emulsion and diameter estimation for wire bundles. In this paper, we present a plane-sweep algorithm that can identify the inclusion hierarchy among the circles in O(n log n) time in the worst-case. Also, the proposed algorithm uses the sweep-line method and a red-black tree for the efficient computation.

5. Deok-Soo Kim, Donguk Kim, Youngsong Cho and Kokichi Sugihara:
"Quasi-triangulation and interworld data structure in three dimensions", Computer-Aided Design, Vol. 38, pp. 808–819, 2006.
概要: It is well-known that the Voronoi diagram of points and the power diagram for weighted points, such as spheres, are cell complexes, and their respective dual structures, i.e. the Delaunay triangulation and the regular triangulation, are simplicial complexes. Hence, the topologies of these diagrams are usually stored in

their dual complexes using a very compact data structure of arrays. The topology of the Voronoi diagram of three-dimensional spheres in the Euclidean distance metric, on the other hand, is stored in a radial edge data structure which is not as compact as the data structure used for the Voronoi diagram of points and the power diagram for weighted points. In this paper, we define a dual structure of the Voronoi diagram of three-dimensional spheres called a quasi-triangulation and present its important properties. Based on the properties of a quasi-triangulation, we propose a data structure, called an interworld data structure, based on arrays to compactly store the topology of the quasi-triangulation with a guaranteed query performance.

6. Takaharu Yaguchi and Kokichi Sugihara:
"On the Hedstrom nonreflecting boundary condition for C^2 solutions", Journal of Computational and Applied Mathematics, Vol. 197, pp. 150–155, 2006.
概要: This paper shows that Hedstrom's nonreflecting boundary condition works for some nonsimple-wave solutions in the case where the solution is C^2. Hedstrom's boundary condition is a pioneering work in the discipline of characteristic nonreflecting boundary conditions and Hedstrom gave a theoretical assurance of the nonreflectivity for simple-wave solutions. In this paper, we extend Hedstrom's theorem for C^2 solutions, that is, we prove that the Hedstrom boundary condition eliminates the reflection if the solution is C^2 and there do not exist ingoing waves generated by the nonlinear interactions near the boundary.

7. Masaki Moriguchi and Kokichi Sugihara:
"Out-of-core isotropic mesh simplification", Journal of Three Dimensional Images, Vol. 20, No. 3, pp. 47–50, 2006.
概要: In this paper, we present an out-of-core algorithm for simplifying huge meshes into isotropic meshes. Our method is based on k-means clustering, which can be computed by first generating an initial clustering and then by iteratively applying improvement methods. To operate in an I/O-efficient manner, the original mesh is converted to the streaming mesh format. Then we create an initial clustering by Ward ' s method through streaming edge collapse simplification. We use data swapping local search for iterative improvement since it can be implemented I/O-efficiently. After performing several passes of stream processing, we get a high quality mesh in a reasonable time.

8. K. Murota, K. Tanaka:
"A Steepest Descent Algorithm for M-convex Functions on Jump Systems", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E89-A 巻 5 号, 1160–1165, 2006 年 5 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.

9. Y. Kobayashi, K. Murota, K. Tanaka:
"Operations on M-convex Functions on Jump Systems", SIAM Journal on Discrete Mathematics, 21 巻 1 号, 107–129, 2007 年 1 月.
概要: A jump system is a set of integer points with an exchange property, which is a generalization of a matroid, a delta-matroid, and a base polyhedron of an integral polymatroid (or a submodular system). Recently, the concept of M-convex

functions on constant-parity jump systems is introduced as a class of discrete convex functions that admit a local criterion for global minimality. M-convex functions on constant-parity jump systems generalize valuated matroids, valuated delta-matroids, and M-convex functions on base polyhedra. This paper reveals that the class of M-convex functions on constant-parity jump systems is closed under a number of natural operations such as splitting, aggregation, convolution, composition, and transformation by networks. The present results generalize hitherto-known similar constructions for matroids, delta-matroids, valuated matroids, valuated delta-matroids, and M-convex functions on base polyhedra.

10. 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, 73, 042109–042118, 2006.
概要: We show that some two-party Bell inequalities with two-valued observables are stronger than the CHSH inequality for $3 \otimes 3$ isotropic states in the sense that they are violated by some isotropic states in the $3 \otimes 3$ system that do not violate the CHSH inequality. These Bell inequalities are obtained by applying triangular elimination to the list of known facet inequalities of the cut polytope on nine points. This gives a partial solution to an open problem posed by Collins and Gisin. The results of numerical optimization suggest that they are candidates for being stronger than the I_{3322} Bell inequality for $3 \otimes 3$ isotropic states. On the other hand, we found no Bell inequalities stronger than the CHSH inequality for $2 \otimes 2$ isotropic states. In addition, we illustrate an inclusion relation among some Bell inequalities derived by triangular elimination.

11. D. Avis, H. Imai and T. Ito:
"On the Relationship between Convex Bodies Related to Correlation Experiments with Dichotomic Observables", Journal of Physics A: Mathematical and General, Vol. 39, No. 36, 11283–11299, 8 September 2006.
概要: In this paper we explore further the connections between convex bodies related to quantum correlation experiments with dichotomic variables and related bodies studied in combinatorial optimization, especially cut polyhedra. Such a relationship was established in Avis, Imai, Ito and Sasaki (2005 J. Phys. A: Math. Gen. 38 10971-87) with respect to Bell inequalities. We show that several well known bodies related to cut polyhedra are equivalent to bodies such as those defined by Tsirelson (1993 Hadronic J. S. 8 329-45) to represent hidden deterministic behaviors, quantum behaviors, and no-signalling behaviors. Among other things, our results allow a unique representation of these bodies, give a necessary condition for vertices of the no-signalling polytope, and give a method for bounding the quantum violation of Bell inequalities by means of a body that contains the set of quantum behaviors. Optimization over this latter body may be performed efficiently by semidefinite programming. In the second part of the paper we apply these results to the study of classical correlation functions. We provide a complete list of tight inequalities for the two party case with (m, n) dichotomic observables when $m = 4$, $n = 4$ and when $\min\{m, n\} \leq 3$, and give a new general family of correlation inequalities.

12. D. Avis, H. Imai and T. Ito:
"Generating Facets for the Cut Polytope of a Graph by Triangular Elimination", Mathematical Programming, Online First: DOI 10.1007/s10107-006-0018-z, 2007.

概要: The cut polytope of a graph arises in many fields. Although much is known about facets of the cut polytope of the complete graph, very little is known for general graphs. The study of Bell inequalities in quantum information science requires knowledge of the facets of the cut polytope of the complete bipartite graph or, more generally, the complete k-partite graph. Lifting is a central tool to prove certain inequalities are facet inducing for the cut polytope. In this paper we introduce a lifting operation, named triangular elimination, applicable to the cut polytope of a wide range of graphs. Triangular elimination is a specific combination of zero-lifting and Fourier-Motzkin elimination using the triangle inequality. We prove sufficient conditions for the triangular elimination of facet inducing inequalities to be facet inducing. The proof is based on a variation of the lifting lemma adapted to general graphs. The result can be used to derive facet inducing inequalities of the cut polytope of various graphs from those of the complete graph. We also investigate the symmetry of facet inducing inequalities of the cut polytope of the complete bipartite graph derived by triangular elimination.

13. Ayami Suzuka, Ryuhei Miyashiro, Akiko Yoshise and Tomomi Matsui:
"The Home-away Assignment Problems and Break Minimization/Maximization Problems in Sports Scheduling", Pacific Journal of Optimization, 3(1), pp. 113–133, January, 2007.
概要: The home-away assignment problem is to find a home-away assignment that minimizes the total traveling distance of the teams; the break minimization/maximization problem is to find a home-away assignment that minimizes/maximizes the number of breaks, i.e.,. the number of occurrences of consecutive matches held either both at away or both at home for a team. The aim of this paper is to give a unified view to the three problems. We see that optimal solutions of the break minimization/maximization problems are obtained by solving the home-away assignment problem. For these problems, we propose formulations and approximation preserving reductions, and report known approximation algorithms.

14. Shuji Kijima and Tomomi Matsui:
"Polynomial Time Perfect Sampling Algorithm for Two-Rowed Contingency Tables", Random Structures and Algorithms, 29(3), pp. 243–256, Sep., 2006.
概要: This paper proposes a polynomial time perfect (exact) sampling algorithm for $2 \times n$ contingency tables. The algorithm is based on monotone coupling from the past (monotone CFTP) algorithm. The expected running time is bounded by $\mathrm{O}(n^3 \ln N)$ where n is the number of columns and N is the total sum of all entries.

15. Greg Aloupis, Thomas Fevens, Stefan Langerman, Tomomi Matsui, Antonio Mesa, Yurai Nunez, David Rappaport, and Godfried Toussaint:
"Algorithms for Computing Geometric Measures of Melodic Similarity", Computer Music Journal, 30(3), pp. 67-77, Sep., 2006.
概要: Similarity measures for melodies find application in content-based retrieval methods for large music databases such as query by humming but also in other diverse applications such as helping prove music copyright infringement. We describe two algorithms to calculate similarity defined by the minimum area between two given orthogonal melodies. The algorithms may be used for cyclic melodies as well as in the context of retrieving short patterns from a database (open planar orthogonal

chains).

16. Ryuhei Miyashiro and Tomomi Matsui:
"Semidefinite programming based approaches to the break minimization problem", Computers and Operations Research, 33(7), pp. 1975–1982, July, 2006.
概要: This paper considers the break minimization problem in sports timetabling. The problem is to find, under a given timetable of a round-robin tournament, a home-away assignment that minimizes the number of breaks, i.e., the number of occurrences of consecutive matches held either both at away or both at home for a team. We formulate the break minimization problem as MAX RES CUT and MAX 2SAT, and apply Goemans and Williamson's approximation algorithm using semidefinite programming. Computational experiments show that our approach quickly generates solutions of good approximation ratios.

17. Yuichiro Miyamoto and Tomomi Matsui:
"Approximation Algorithms for Minimum Span Channel Assignment Problems", Lecture Notes in Computer Science, 4041, pp. 334–342, June, 2006.
概要: We propose polynomial time approximation algorithms for the minimum span channel (frequency) assignment problems, which is known to be NP-hard. Let α be the approximation ratio of our algorithm and $W \geq 2$ be the maximum of numbers of channels required in vertices. If an instance is define on a perfect graph G, then $\alpha \leq 1 + (1 + \frac{1}{W-1})\mathrm{H}_{\omega(G)}$, where H_i denotes the i-th harmonic number. For any instance defined on a unit disk graph G, α is less than or equal to $(1+\frac{1}{W-1})(3\mathrm{H}_{\omega(G)}-1)$. We also discuss a well-known practical instances called Philadelphia instances and propose an algorithm with $\alpha \leq 83/30$, which improves a trivial algorithm with $\alpha \leq 14/5$.

18. Ayami Suzuka, Ryuhei Miyashiro, Akiko Yoshise and Tomomi Matsui:
"Dependent Randomized Rounding to the Home-Away Assignment Problem in Sports Scheduling", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E89-A(5), pp. 1407–1416, May, 2006.
概要: Suppose that we have a timetable of a round-robin tournament with a number of teams, and distances among their homes. The home-away assignment problem is to find a home-away assignment that minimizes the total traveling distance. We propose a formulation of the home-away assignment problem as an integer program, and a rounding algorithm based on Bertsimas, Teo and Vohra's dependent randomized rounding method. Computational experiments show that our method quickly generates feasible solutions close to optimal.

19. Shu Yamada, Michiyo Matsui, Tomomi Matsui, Dennis K. J. Lin, and Takenori Takahashi:
"A General Construction Method for Mixed-level Supersaturated Design", Computational Statistics and Data Analysis, 50(1), pp. 254–265, January, 2006.
概要: In this paper, we show a general constructing method of mixed-level supersaturated design with small number of experimental runs while the constructing methods by the previous studies generate designs with large number of experimental runs. The method shown in this paper has advantages that it assures the maximum level of dependency of the resulting designs and generates small number of experimental runs.

20. S. Iwata and R. Shimizu:
"Combinatorial analysis of singular matrix pencils", SIAM J. Matrix Anal. Appl., 29, 245–259, 2007.

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.

21. N. Kakimura and S. Iwata:
"Computing inertia from sign patterns", Math. Programming, (掲載予定).
概要: A symmetric matrix 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 symmetric matrices. The algorithm runs in $O(\sqrt{n}m \log n)$ time for a symmetric matrix of order n with m nonzero entries. In addition, it is shown to be NP-complete to decide whether the inertia of a given symmetric matrix is not determined by its pattern.

22. S. Iwata:
"Submodular function minimization", Math. Programming, (掲載予定).
概要: Submodular functions often arise in various fields of operations research including discrete optimization, game theory, queueing theory and information theory. In this survey paper, we give overview on the fundamental properties of submodular functions and recent algorithmic devolopments of their minimization.

23. S. Iwata and T. Matsuda:
"Finding coherent cyclic orders in strong digraphs", Combinatorica, (掲載予定).
概要: A cyclic order in the vertex set of a digraph is said to be coherent if any arc is contained in a directed cycle whose winding number is one. This notion plays a key role in the proof by Bessy and Thomassé (2004) of a conjecture of Gallai (1964) on covering the vertex set by directed cycles. This paper presents an efficient algorithm for finding a coherent cyclic order in a strongly connected digraph, based on a theorem of Knuth (1974). With the aid of ear decomposition, the algorithm runs in $O(nm)$ time, where n is the number of vertices and m is the number of arcs. This is as fast as testing if a given cyclic order is coherent.

24. S. Iwata and N. Kakimura:
"Solving linear programs from sign patterns", Math. Programming, (掲載予定).
概要: This paper is an attempt to provide a connection between qualitative matrix theory and linear programming. A linear program $\max\{cx \mid Ax = b, x \geq 0\}$ is said to be sign-solvable if the set of sign patterns of the optimal solutions is uniquely determined by the sign patterns of A, b, and c. It turns out to be NP-hard to decide whether a given linear program is sign-solvable or not. We then introduce a class of sign-solvable linear programs in terms of totally sign-nonsingular matrices, which can be recognized in polynomial time. For a linear program in this class, we devise an efficient combinatorial algorithm to obtain the sign pattern of an optimal solution from the sign patterns of A, b, and c. The algorithm runs in $O(m\gamma)$ time, where m is the number of rows of A and γ is the number of all nonzero entries in A, b, and c.

25. Y. Oishi:
"Polynomial-time algorithms for probabilistic solutions of parameter-dependent linear matrix inequalities", Automatica, Vol. 43, No. 3, pp. 538–545, March 2007.
概要: A randomized approach is considered

for a feasibility problem on a parameter-dependent linear matrix inequality. In particular, a gradient-based and an ellipsoid-based randomized algorithms are improved by introduction of a stopping rule. The improved algorithms stop after a bounded number of iterations and this bound is of polynomial order in the problem size. When the algorithms stop, either of the following two events occurs: (i) they find with high confidence a probabilistic solution, which satisfies the given linear matrix inequality for most of the parameter values; (ii) they detect in an approximate sense the nonexistence of a deterministic solution, which satisfies the given linear matrix inequality for all the parameter values. These results are important because the original randomized algorithms have issues to be settled on detection of convergence, on the speed of convergence, and on the assumption of feasibility. The improved algorithms can be adapted for an optimization problem constrained by a parameter-dependent linear matrix inequality. A numerical example shows the efficacy of the proposed algorithms.

26. 猪阪・大石:
"疎性の利用によるロバスト半正定値計画法の効率化", 計測自動制御学会論文集, Vol. 43, No. 2, pp. 93–101, 2007 年 2 月.
概要: A computaionally improved matrix-dilation approach is proposed for a robust semidefinite programming problem, whose constraint is a polynomial of uncertain parameters. This approach utilizes a sparse structure of the constraint polynomial and produces a small-size approximate problem to a given robust semidefinite programming problem. It is proved that the optimal value of the approximate problem converges to that of the given robust semidefinite programming problem as the used division of the parameter region becomes finer. In this sense, this approach is asymptotically exact. The size of the approximate problem is evaluated in the degree of the polynomial and is compared with the existing matrix-dilation approach. A numerical example is presented for illustration.

27. Y. Fujisaki and Y. Oishi:
"Guaranteed cost regulator design: a probabilistic solution and a randomized algorithm", Automatica, Vol. 43, No. 2, pp. 317–324, February 2007.
概要: This paper presents a gradient-based randomized algorithm to design a guaranteed cost regulator for a plant with general parametric uncertainties. The algorithm either provides with high confidence a probabilistic solution that satisfies the design specification with high probability for a randomly sampled uncertainty or claims that the feasible set of the design parameters is too small to contain a ball with a given radius. In both cases, the number of iterations executed in the algorithm is of polynomial order of the problem size and is independent of the dimension of the uncertainty.

28. M. Takamatsu, Y. Oishi, and K. Hirata:
"Analysis of a nonlinear system using interval arithmetic: computation of an output admissible set", 計測自動制御学会論文集, Vol. 42, No. 12, pp. 1320–1327, 2006 年 12 月.
概要: Interval arithmetic is applied to analysis of a nonlinear system, in particular, to computation of an output adimissible set, which plays an important role in constrained control. A discrete-time system whose dynamics is expressed in polynomials is considered first. When the initial state of such a system is known to belong to some multi-dimensional interval, interval arithmetic enables us to compute an interval that includes all possible states after some time steps. This fact together with polynomial

optimization is used to compute an output admissible set. Numerical examples show efficacy of the proposed approach. Extensions are considered to non-polynomial systems and continuous-time systems.

29. 西田徹志:
"ボート航行距離方程式とその解法", 応用数理, Vol. 16, No. 3, pp. 31–43, 2006 年.
概要: A new concept called a boat-sail distance is introduced on the surface of water with flow. That concept is a mathematical model of the shortest time for a boat to move from one point to another against the flow of water. The problem of computing this distance 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 proposal method.

30. H. Hashimoto, T. Ibaraki, S. Imahori, M. Yagiura:
"The Vehicle Routing Problem with Flexible Time Windows and Traveling Times", Discrete Applied Mathematics, 154, 2271–2290, November 2006.
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.

研究会等

1. Hiroshi Kawaharada and Kokichi Sugihara:
"Dual subdivision—A new class of subdivision schemes using projective duality", 14th International Conference in Central Europe on Computer Graphics, Visualization and Computer Vision 2006 (WSCG'2006), pp. 9–16, January 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.

2. Hideyuki Sakai and Kokichi Sugihara:
"Stable and topology-preserving extraction of medial axes", Proceedings of the 3rd International Symposium on Voronoi Diagrams in Science and Engineering, pp. 40–47, July 2006.
概要: The paper presents a simple method for extracting global medial axes in a stable

manner. A new index, called the normalized boundary distance, is introduced in order to measure the degree of importance of a point on the conventional medial axis. This index has a remarkable property that the set of points whose index values are greater than an arbitrarily chosen threshold is topologically equivalent to the original figure. In the proposed method, first the boundary of a given figure is replaced with a dense set of points, next the Voronoi diagram for these points is constructed, then the approximation of the medial axis is extracted from the Voronoi diagram, and finally the global medial axis is constructed by pruning the branches according to the new index. The performance of the proposed method is also shown by examples.

3. Masaki Moriguchi and Kokichi Sugihara: "A new initialization method for constructing centroidal Voronoi tessellations on surface meshes", Proceedings of the 3rd International Symposium on Voronoi Diagrams in Science and Engineering, pp. 159–165, 2006.
概要: Centroidal Voronoi tessellations can be constructed using iterative improvement methods such as Lloyd 's method. Using iterative improvement methods implies that the convergence speed and the quality of the results depend on the initialization methods. In this paper, we propose an efficient initialization method for constructing centroidal Voronoi tessellations on surface meshes. The proposed method tries to make initial tessellations mimic the properties of the centroidal Voronoi tessellations. We compare our method with other initialization methods: random sampling, farthest point sampling and Ward 's method. The results show that our method and Ward 's method have the faster convergence speed than random sampling and farthest point sampling, and create better tessellations than random sampling.

4. Hiroshi Kawaharada and Kokichi Sugihara: "Computation of normals for stationary subdivision surfaces", The Fourth International Conference on Geometric Modeling and Processing, pp. 585–594, 2006.
概要: This paper proposes a method for computing of normals for stationary subdivision surfaces. We derived a new necessary and sufficient condition for C^k-continuity of stationary subdivision schemes. First, we showed that tangent plane continuity is equivalent to the convergence of difference vectors. Thus, using "normal subdivision matrix", we derived a necessary and sufficient condition of tangent plane continuity for stationary subdivision at extraordinary points (including degree 6). Moreover, we derived a necessary and sufficient condition for C^1-continuity. Using the analysis, we show that at general points on stationary subdivision surfaces, the computation of the exact normal is an infinite sum of linear combinations of cross products of difference vectors even if the surfaces are C^1-continuous. So, it is not computable. However, we can compute the exact normal of subdivision surfaces at the limit position of a vertex of original mesh or of j-th subdivided mesh for any finite j even if the surfaces arc not regular.

5. Shuji Kijima and Tomomi Matsui: "Randomized Approximation Scheme and Perfect Sampler for Closed Jackson Networks", Second Madrid Conference on Queueing Theory (MCQT), CD-ROM 版のためページ番号無し, July, 2006.
概要: We propose a polynomial-time randomized approximation scheme for calculating the normalizing constant of the product form solution of closed Jackson networks. Our algorithm is based on Markov chain Monte Carlo (MCMC) method. We also

propose two efficient sampling algorithms for closed Jackson networks.

6. Ryuhei Miyashiro and Tomomi Matsui:
"Minimizing the Carry-over Effects Value in a Round-robin Tournament", The 6th international conference on the Practice And Theory of Automated Timetabling (PATAT 2006), pp. 460–463, August, 2006.
概要: In this paper, we consider the problem of minimizing the carry-over effects value in a round-robin tournament. The carry-over effects value is an index of quality of a round-robin tournament schedule. We propose an effective algorithm for generating schedules of small carry-over effects values. The proposed algorithm produces better schedules than the best ones previously known in short computational time.

7. Nobutomo Fujiwara, Shinji Imahori, Tomomi Matsui, and Ryuhei Miyashiro:
"Constructive Algorithms for the Constant Distance Traveling Tournament Problem", The 6th international conference on the Practice And Theory of Automated Timetabling (PATAT 2006), pp. 402–405, August, 2006.
概要: The traveling tournament problem is a problem that abstracts an important issue in sports scheduling, minimizing traveling distance. In this paper, we deal with the constant distance traveling tournament problem, which is a special class of the traveling tournament problem. We propose a lower bound of the optimal value of the constant distance traveling tournament problem, and two constructive algorithms that produce feasible solutions whose objective values are close to the proposed lower bound. For some size of instances, one of our algorithms yields optimal solutions.

8. Masaru Iwasa, Hiroo Saito and Tomomi Matsui:
"Approximation Algorithms for the Single Allocation Problem in Hub-and-Spoke Networks", Optimal Discrete Structures and Algorithms (ODSA), p. 24, Sep., 2006.
概要: Hub-and-spoke network arises in the airline industry, telecommunications and postal delivery systems. We consider a single allocation problem, which allocates each non-hub node to one of hub nodes, and minimizes the total transportation cost. We propose 2-approximation algorithm based on randomized rounding technique. When the number of hubs is three, we propose a specialized dependent rounding technique which gives a (5/4)-approximation algorithm.

9. Yusuke Kuroki and Tomomi Matsui:
"Randomized Approximation Algorithm for a Geometrical Multidimensional Assignment Problem", Optimal Discrete Structures and Algorithms (ODSA), p. 30, Sep., 2006.
概要: A multidimensional assignment problem have found applications as a technique to solve data association problems. This paper deals with a case that the weight of a clique is defined by the sum of given weights of its edges. Additionally, we assume that vertices are embedded in the d-dimensional space and a weight of an edge is defined by the square of the Euclidean distance. We propose a second-order cone programming relaxation of the problem and a polynomial time randomized rounding procedure.

10. S. Iwata and K. Takazawa:
"The independent even factor problem", Proceedings of the 18th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), 1171–1180, 2007.
概要: This paper deals with the independent even factor problem. For odd-cycle-symmetric digraphs, where any odd dicycle has the reverse cycle, a min-max formula is established as a common gener-

alization of the Tutte-Berge formula for matchings and the matroid intersection theorem of Edmonds (1970). We devise an efficient combinatorial algorithm to find a maximum independent even factor in an odd-cycle-symmetric digraph accompanied with general matroids, which commonly extends Pap's even factor algorithm (2005) and the matroid intersection algorithms. The algorithm gives a proof of the min-max formula, and contains a new operation on matroids, which corresponds to shrinking factor-critical components in Edmonds' mathcing algorithm (1965). The algorithm runs in $O(n^4Q)$ time, where n is the number of vertices and Q is the time for an independence test. The algorithm also gives a common generalization of the Edmonds-Gallai decomposition for matchings and the principal partition for matroid intersection.

11. N. Fujiwara, S. Imahori, T. Matsui, R. Miyashiro:
"Constructive Algorithms for the Constant Distance Traveling Tournament Problem", Proceedings of the 6th International Conference on the Practice and Theory of Automated Timetabling, 402–405, August 2006.
概要: The traveling tournament problem is a problem that abstracts an important issue in sports scheduling: minimizing traveling distance. Various studies on the traveling tournament problem have been appeared in recent years, and there are some variants on this problem. In this paper, we deal with the constant distance traveling tournament problem, which is a special class of the traveling tournament problem. This variant is essentially equivalent to the problem of "maximizing breaks" and that of "minimizing breaks," which is another significant objective in sports scheduling. We propose a lower bound of the optimal value of the constant distance traveling tournament problem, and two constructive algorithms that produce feasible solutions whose objective values are close to the proposed lower bound. For some size of instances, one of our algorithms yields optimal solutions.

12. N. Fujiwara, S. Imahori, T. Matsui, R. Miyashiro:
"Constructive Algorithms for the Constant Distance Traveling Tournament Problem", Proceedings of the 6th International Conference on the Practice and Theory of Automated Timetabling, 402–405, August 2006.
概要: The traveling tournament problem is a problem that abstracts an important issue in sports scheduling: minimizing traveling distance. Various studies on the traveling tournament problem have been appeared in recent years, and there are some variants on this problem. In this paper, we deal with the constant distance traveling tournament problem, which is a special class of the traveling tournament problem. This variant is essentially equivalent to the problem of "maximizing breaks" and that of "minimizing breaks," which is another significant objective in sports scheduling. We propose a lower bound of the optimal value of the constant distance traveling tournament problem, and two constructive algorithms that produce feasible solutions whose objective values are close to the proposed lower bound. For some size of instances, one of our algorithms yields optimal solutions.

学会大会等

1. 来嶋秀治, 松井知己:
"閉ジャクソンネットワークに対する MCMC 法", 電子情報通信学会 2006 年総合大会, pp. S13–S14, 2006 年 3 月.

2. 鈴鹿順美, 宮代隆平, 吉瀬章子, 松井知己:
"スポーツのスケジューリングにおける会場割当問題", 電子情報通信学会 2006 年総合大会, pp. S15–S16, 2006 年 3 月.

3. 宮代隆平, 松井知己:
“対戦日程計画における Carry-Over Effect 最小化問題”, 日本オペレーションズリサーチ学会 2006 年春季研究発表会, pp. 14–15, 2006 年 3 月.

4. Ayami Suzuka, Ryuhei Miyashiro, Akiko Yoshise and Tomomi Matsui:
“Home-away Assignment Problems in Sports Scheduling”, INFORMS International Hong Kong 2006 meeting, 2006 年 6 月.

5. Nobutomo Fujiwara, Shinji Imahori, Tomomi Matsui, and Ryuhei Miyashiro:
“The Traveling Tournament Problem with a Constant Distance Matrix”, INFORMS International Hong Kong 2006 meeting, 2006 年 6 月.

6. Ryuhei Miyashiro and Tomomi Matsui:
“Minimizing Carry-Over Effects in a Round-Robin Tournament”, INFORMS International Hong Kong 2006 meeting, 2006 年 6 月.

7. 宮代隆平、松井知己:
“スポーツスケジューリングの近年の展開”, 日本スポーツ産業学会, pp. 39–40, 2006 年 7 月.

8. Tomomi Matsui and Ryuhei Miyashiro:
“Combinatorial Optimization in Sports Scheduling”, Asian Association for Sports Management, 巻号, p. 188, Sep., 2006.

9. 岩佐大, 齊藤廣大, 松井知己:
“ハブ空港配置問題の近似解法”, 日本オペレーションズリサーチ学会 2006 年秋季研究発表会, pp. 66–67, 2006 年 9 月.

10. 澤井賢一, 黒木裕介, 松井知己:
“フルートの運指のモデル化とその最適化に関する研究”, 日本オペレーションズリサーチ学会 2006 年秋季研究発表会, pp. 68–69, 2006 年 9 月.

11. Yusuke Kuroki and Tomomi Matsui:
“Approximation Algorithm for Multidimensional Assignment Problem Arising from Data Association Problem”, 日本オペレーションズリサーチ学会 2006 年秋季研究発表会, pp. 74–75, 2006 年 9 月.

12. Yusuke Kuroki and Tomomi Matsui:
“Approximation Algorithm for Multidimensional Assignment Problem Arising from Data Association Problem”, 情報処理学会アルゴリズム研究会, 108, pp. 49–56, 2006 年 9 月.

13. Shuji Kijima and Tomomi Matsui:
“Random Sampling via Markov Chain”, The International Workshop on Data-Mining and Statistical Science (DMSS2006), 2006 年 9 月.

14. 来嶋秀治, 松井知己:
“多変量離散分布とマルコフ連鎖モンテカルロ法”, 日本計算機統計学会第 20 回シンポジウム, pp. 81–84, 2006 年 10 月.

15. 澤井賢一, 黒木裕介, 松井知己, 合原一幸:
“フルートの運指のモデル化とその最適化に関する研究”, 音楽情報科学研究会, 68, pp. 13–18, 2006 年 12 月.

16. 来嶋秀治, 松井知己:
“閉 BCMP ネットワークに対する MCMC 法”, 待ち行列シンポジウム, pp. 30–39, 2007 年 1 月.

17. 黒木裕介, 松井知己:
“Approximation Algorithm for Multidimensional Assignment Problem Minimizing the Sum of Squared Errors”, 研究集会『統計的離散モデリング』, 2007 年 1 月.

18. 松井知己:
“CFTP を用いた厳密サンプリング”, 研究集会『スケールフリーネットワークとランダムグラフ』, 2007 年 1 月.

19. Y. Oishi:
“Reduction of the number of constraints

in the matrix-dilation approach to robust semidefinite programming", Proceedings of the 45th IEEE Conference on Decision and Control, pp. 5790–5795, December 2006.

20. Y. Fujisaki, Y. Oishi, and R. Tempo:
"A mixed probabilistic/deterministic approach to fixed order H-infinity controller design", Proceedings of the 45th IEEE Conference on Decision and Control, pp. 3554–3559, December 2006.

21. Y. Oishi and Y. Fujisaki:
"Randomized techniques for robust control", Proceedings of the 17th International Symposium on Mathematical Theory of Networks and Systems (MTNS2006), pp. 349–354, July 2006.

22. Y. Oishi:
"A region-dividing approach to robust semidefinite programming and its error bound", Proceedings of the 2006 American Control Conference, pp. 123–129, June 2006.

23. S. Imahori, M. Kushiya, T. Nakashima, K. Sugihara:
"The Traveling Tournament Problem with a Constant Distance Matrix", INFORMS International Conference, June 2006.

24. S. Imahori, N. Fujiwara, T. Matsui, R. Miyashiro:
"The Traveling Tournament Problem with a Constant Distance Matrix", INFORMS International Conference, June 2006.

25. S. Umetani, M. Yagiura, T. Imamichi, S. Imahori, K. Nonobe, T. Ibaraki:
"A Guided Local Search Algorithm based on a Fast Neighborhood Search for the Irregular Strip Packing Problem", Proceedings of International Symposium on Scheduling 2006, 126-131, July 2006.

26. S. Imahori, M. Yagiura:
"Theoretical and Experimental Comparisons of Heuristic Algortithms for Rectangle Packing Problems", 4th ESICUP Meeting, March 2007.

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

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の観点から研究した．

具体的には，システムの設計や通信のプロトコル記述と密接に関係してかつ情報科学の原点ともいえる問題の最大充足化問題を中心に数理計画法の有用性とその限界の解明に取り組んできた．そして，最大充足化問題に対して世界最高の高性能近似アルゴリズムを提案した．その成果は Theoretical Computer Science 誌に掲載された．さらに，アルゴリズムの最近の研究動向を詳細に調査分類した原書（J. Kleinberg and E. Tardos: Algorithm Design, Addison-Wesley, 2005）の翻訳を通して，最先端の研究調査を行った．また，施設配置問題，インターネットフローの混雑最小化問題，ブロードキャストアルゴリズム，パケットルーティングに対する研究を行い，その成果を情報処理学会などで発表した．

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 2 つを以降の節で詳しく述べる．一つはオンデマンドブロードキャスティングに対するアルゴリズムの実験的性能評価であり，もう一つは原書（J. Kleinberg and E. Tardos: Algorithm Design, Addison-Wesley, 2005）の翻訳を通して研究調査したものの一部をまとめたものである．

2 オンデマンド・データ・ブロードキャスティング

2.1 はじめに

オンデマンド・データ・ブロードキャスティングに関する問題の1つに，平均レスポンスタイム最小化問題がある．この問題に対し，Bansal et al. によって2005年に $O(\sqrt{n})$ 近似アルゴリズムが提案され，2006年には2005年の手法を発展させた $O((\log n)^2/\log\log n)$ 近似アルゴリズムが提案されている．

本稿では，この2つのアルゴリズムを実装し，計算機実験を行うことでその性能を評価した．また，2006年の手法を改善することで，その計算時間を短縮できることを示す．

2.2 問題定義

オンデマンド・データ・ブロードキャスティング (on-demand data broadcasting) とは，サーバに n 種類のページが存在し，クライアントから受信したリクエストに対してサーバがページを送信するというものである．ここで，サーバは送信するページをブロードキャストすることにより，すべてのクライアントにページを送信することができる．

このオンデマンド・データ・ブロードキャスティングの中に，**平均レスポンスタイム最小化問題** (average response time minimization problem) がある．これは，サーバに存在するページ数 n と，時刻 t でのページ p に対するクライアントからのリクエストの量 r_t^p が入力として与えられる．リクエスト r_t^p は，サーバが時刻 $t'(t'>t)$ にページ p を送信することにより満たされ，この待ち時間 $t'-t$ を**レスポンスタイム** (response time) と呼ぶ．本問題の目的は，すべてのリクエストを満たし，平均のレスポンスタイムを最小化することである．

また，単位時間にサーバが送信できるページの数が k であるとき，k-スピードと呼ばれる．$k=1$ のとき，NP-困難であることが証明されており，本稿においてもこれを扱っていく．

この問題は，以下のように整数計画問題として定式化できる．なお T は，リクエストの最大到着時刻である．$x_{tt'}^p$ は時刻 t でのページ p に対するリクエストが時刻 t' に満たされたとき1となり，そうでないときは0である．また，$y_{t'}^p$ は時刻 t' でページ p を送信したとき1となり，そうでないときは0である．

$$
\begin{aligned}
\min \quad & \sum_p \sum_t \sum_{t'=t+1}^{T+n} (t'-t)\cdot r_t^p \cdot x_{tt'}^p \\
\text{s.t.} \quad & y_{t'}^p - x_{tt'}^p \geq 0, && \forall p,t,t'>t \\
& \sum_{t'=t+1}^{T+n} x_{tt'}^p \geq 1, && \forall p,t \\
& \sum_p y_{t'}^p \leq 1, && \forall t' \\
& x_{tt'}^p \in \{0,1\}, && \forall p,t,t' \\
& y_{t'}^p \in \{0,1\}, && \forall p,t'
\end{aligned}
$$

2.3 Bansal et al. (2005) の手法 [1]

2005年の手法は，緩和した整数計画問題を解き，その解を利用して**暫定的スケジュール** (tentative schedule) を求め，キューを用いてこの暫定的スケジュールを実行可能なスケジュールにするというものである．

以下にアルゴリズムの詳細を示す．

1. 緩和した整数計画問題を解きLP解を求める．
2. 各ページ p ごとに $\alpha_p \in [0,1]$ をランダムに定める．
3. $i=0,1,2,\cdots$ に対し，LP解においてページ p が合計で $i+\alpha$ 送信された時刻を t_i^p とする．
4. $t_0^p, t_1^p, \cdots$ をページ p の暫定的スケジュールとする．
5. キューを使用して，暫定的なスケジュールを実行可能なスケジュールにする．

2.4 Bansal et al. (2006) の手法 [2]

本質的には，2005年の手法の発展である．2006年の手法における2つの改良点を以下に示す．

(改良点1) 各ページ p ごとに**ブロック** (block) と呼ばれる時間枠 $B(p,i)$ を定め，そのブロック内で暫定的スケジュールを求める．

(改良点 2) 各ブロックごとに $\alpha \in [0,1]$ を定める．このとき，新たに線形計画問題を定義し α の値を決定する．

α の値は，$\delta = 1/(T+n)^2$ の j (j は正整数) 倍としてよいことが証明されている [2]．ここで，$B(p,i,j)$ を $B(p,i)$ 内で $\alpha = \delta \cdot j$ と決定したときの暫定的スケジュールであるとする．

以下の線形計画問題を解くことで，α の値を決定することができる．

$$\min \quad \sum_p \sum_i \sum_j R(B(p,i,j)) \cdot z_{pij}$$

$$\text{s.t.} \quad \sum_j z_{pij} = 1, \qquad \forall p,i \tag{2.16}$$

$$\sum_p \sum_i \sum_j w(B(p,i,j),t) \cdot z_{pij} = 1, \ \forall t \tag{2.17}$$

$$z_{pij} \geq 0, \qquad \forall p,i,j \tag{2.18}$$

なお，$R(B(p,i,j))$ は $\alpha = \delta \cdot j$ を選んだときの $B(p,i)$ 内のレスポンスタイムであり，$w(B(p,i,j),t)$ は，$t \in B(p,i,j)$ であるとき 1 となり，それ以外は 0 となる．また，制約式 (2) は各時刻 t において，1 ページのみ送信するということを表している．

この式の整数解を求めるために，制約式 (2) を緩和する．具体的には $I = (t_1, t_2]$ とし，この時間枠内で送信するページをまとめて選択する．そして，線形計画問題を解き，$z_{pij} = 1$ となった変数を除き線形計画問題を再構築する．これを $O(\log(T+n))$ 回繰り返し，整数解を求める．

2.5 提案手法

(2005 年の手法に対する改善)

2005 年の手法では，まだ満たされていないリクエストがあるにも関わらず，サーバがどのページも送信しない時刻が存在する．そこで，その時刻に満たされていないリクエストが最も多いページを送信することで，解を改善する．

(2006 年の手法に対する改善)

2006 年の手法では，α の値を定めるために，線形計画問題を $O(\log(T+n))$ 回解く必要がある．また，j は 1 から $(T+n)^2$ の値をとるために，変数の数が膨大になってしまう．この 2 つの点から，2006 年の手法では，計算時間がかかってしまう．そこで，本稿では計算時間を減らすために，j の値を制限する．

具体的には，各 $B(p,i)$ に対しすべての j で暫定的スケジュールを求め，連続した同じ暫定的スケジュールを 1 つの j として考える．暫定的スケジュールが変わったときの j を新たな j と考え，同様に繰り返していく．これをすべての $B(p,i)$ について行い，j の値を制限していく．

2.6 実験的性能評価

2005 年，2006 年の手法とそれぞれに改善を加えたものを，近似率と計算時間の観点から比較した．実験のデータは，両実験共に 100 種類の入力に対し平均を取ったものであり，入力である各時刻のリクエスト数には 0 から 5 の一様乱数を与えている．また，両実験共にリクエストの最大到着時刻を 30 と固定し，ページ数を変化させている．なお，最適解としては整数計画問題を線形計画ソフト NUOPT で解くことにより得られる整数解を用いた．

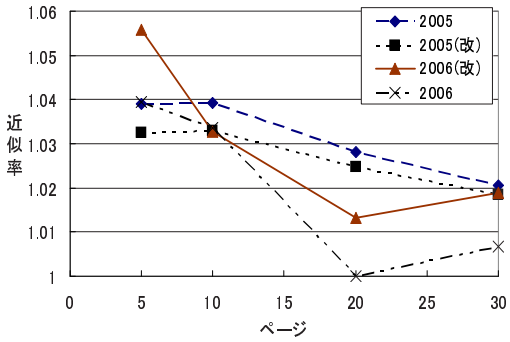


図 2.1: 近似率に対する比較

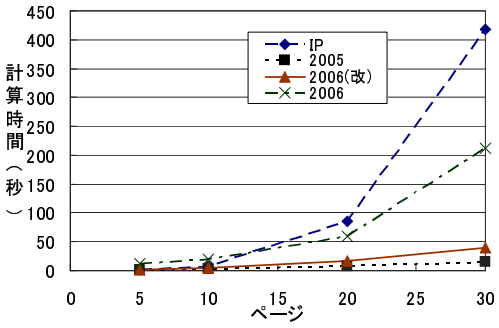


図 2.2: 計算時間に対する比較

図 2.1が近似率について比較したグラフである．ページ数が少ないときには 2006 年の手法は，改善前，改善後共にあまり有効ではないのがわかる．これは，ページ数やリクエストの最大到着時刻が小さいときにはブロックの概念が効果的ではなくなってしまうためだと考えられる．ページ数が多くなるにつれて，2006 年の手法がよい近似率を求めていることがわかる．

図 2.2が計算時間について比較したグラフである．こちらに関しては，整数計画問題の計算時間についても比較した．また，2005 年の計算時間は，提案手法も合わせた計算時間である．このグラフを見ると，改善した 2006 年の手法が，改善していない 2006 年の手法よりかなり計算時間が短いことがわかる．

2.7 結論

2006 年の手法に対する改善は，もともとの手法の計算時間を大幅に短縮することができた．特に，ページ数やリクエストの最大到着時刻が大きいほど効果的である．2006 年の手法は，近似率に関する結果を見てもわかるように，大きな入力に対して有効である．大きな入力では計算時間が大きくなってしまうのを，改善を加えることで，短縮することができた．

以上のことから，2006 年の手法に対する改善は有用であるといえる．

参考文献

[1] N. Bansal, M. Charikar, S. Khanna, J. S. Naor: Approximating the Average Response Time in Broadcast Scheduling. *Proceedings of the 16th Annual ACM-SIAM Symposium on Discrete Algorithms*, Vancouver, January 2005, pp. 215–221.

[2] N. Bansal, D. Coppersmith, M. Sviridenko: Improved Approximation Algorithms for Broadcast Scheduling. *Proceedings of the 17th Annual ACM-SIAM Symposium on Discrete Algorithms*, Miami, January 2006, pp. 344–353.

3 マルティキャストルーティング

インターネットのようなネットワークでは，多数の点から 1 個の**発信点**（source node）s への接続を確立したいというような状況がしばしば生じる．そこで，対象とするネットワークを，各辺 e にコスト $c_e \geq 0$ が付随する有向グラフ $G = (V, E)$ で表現してモデル化する．特別視された発信点 $s \in V$ と**受信点**（terminal nodes）$t_1, t_2, \ldots, t_k \in V$ に位置する異なる k 個のエージェントの集合がある．簡単のため，$t_1, t_2, \ldots, t_k$ をエージェントと考えることにする．各エージェント t_j は，s から t_j へのパスをできるだけ少ないコストで構成したいと考えている．

もちろん，エージェント間に相互影響がなければ，これは単純である．各エージェント t_j は，総コストが最小となる s-t_j パスを求め，これをパス P_j とするという k 個それぞれの最短パス問題となるからである．一方，エージェントが辺のコストを**共有**できると考えると，この問題は極めておもしろくなる．すべてのエージェントが各自のパスを求めた後，エージェント t_j は，そのパス P_j 上の各辺 e のコストの “公正な分担金” を支払えばよいとしよう．すなわち，P_j 上の各 e に対して c_e を支払うのではなく，e を含むパスの個数で c_e を割って得られる分だけ支払えばよいものとするわけである．こうすると，エージェントは，多くのパスと辺を共有するようなパスを選びたいという気持ちが生じる．支払うコストが分担できて得することができるようになるからである．（この共有分担モデルは，辺を共有する多数のエージェントの存在により，混雑や遅延が生じて伝送の質が格段に落ちる，ということのないような状況でのみ適切である．遅延も考慮しなければならないとなると，共有には，その利得を相殺するようなペナルティが生じる．このモデルも，アルゴリズム的に興味深い問題を多数含むが，ここでは，共有による混雑や遅延が生じないモデルに限定して議論することにする．）

3.1 最善反応行動と Nash 均衡：定義と例題

共有の選択肢がエージェントの行動にどのように影響するか見るために，手始めとして，図 2.3の非常に簡単な 2 つの例で考えてみよう．図の例の (a) では，2 つのエージェントのそれぞれが，パスを構成する選択肢は，v を通るルートと外側の 1 本の辺を通るルートの 2 通りである．各エージェ

ントが，最初，外側のパスから出発して，常に現在の状況を評価して，より良いパスができればそちらに移るものとする．

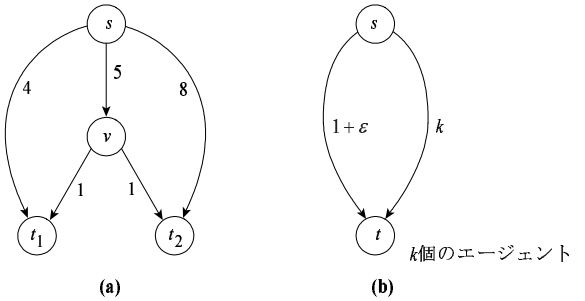


図 2.3: (a) 中央のパスを用いて辺を共有することに 2 つのエージェントは興味をもっている．(b) すべてのエージェントが左側の辺を共有する方がより良い．しかし，k 個のエージェントすべてが最初右側の辺を共有していると，どのエージェントも単独で右から左へ移りたいという気にはならない．すなわち，すべてのエージェントが右側の辺を共有する解は，悪い Nash 均衡解である．

図に例題の (a) において，2 つのエージェントはそれぞれ，外側のパスから出発するとする．すると，t_1 はパスを変えても（$4 < 5+1$ であるので）得はしないとわかるが，t_2 はパスを変えると（$8 > 5+1$ であり）得をするので，中央のパスに移る．すると今度は，状況は t_1 にとっても一変する．すなわち，突然，t_1 は，パスを変えて中央の辺を共有して中央のパスを用いると，$2.5+1 < 4$ から得することができるようになる．したがって，t_1 は中央のパスに移る．両方とも中央のパスを用いる状況になると，交換しても得できないので，交換しようという気はなくなり，これは安定な解になる．

この単純な例で，どんなことが起こっているのかを把握するため，ゲーム理論の分野からの 2 つの定義を議論する．マルティキャストのルーティング問題に限定して今後も話を進めるが，これから述べる定義は，複数のエージェントが，それぞれ，独自の目的をもって，相互に影響を及ぼしながら解を生み出す任意の状況で，通用するものである．そのようなことで，定義は一般的な用語を用いて述べることにする．

- まず最初に，例題では，どのエージェントも，他のエージェントの行動により変更が生じたときは，つねにすぐに対応して自分の解を改善する用意をしていた．このプロセスを**最善反応行動**（best-response dynamics）と呼ぶことにする．言い換えると，各エージェントが現在の状況に対して最善の反応をするということに基づくプロセスの動的な行動に興味をもっている．

- 第二に，安定な解，すなわち，どのエージェントも，最善の反応は何もしないこととなるような解，に特に興味をもっている．どのエージェントも変化しようという気にならないこのような解を，**Nash 均衡解**（Nash equilibrium）ということにする．したがって，例題の (a) では，両方のエージェントが中央のパスを用いる解が Nash 均衡解である．最善反応行動が終了して得られる解は，常に Nash 均衡解であることを注意しておく．

図 2.3(b) の例は，複数の Nash 均衡解をもちうる例である．この例では，k 個のエージェントが同一の点 t にいる（$t_1 = t_2 = \cdots = t_k = t$）とし，$s$ から t へ 2 本の辺があり，それらが異なるコストをもっているとする．すべてのエージェントが左側の辺を用いる解は Nash 均衡解であり，どのエージェントも $(1+\varepsilon)/k$ 支払う．すべてのエージェントが右側の辺を用いる解も Nash 均衡解であるが，この解ではどのエージェントも $k/k = 1$ 支払うことになる．後者の解も Nash 均衡解であることは，最善反応行動に関する重要な問題点を示している．もしエージェントすべてが協力して右側の辺から左側の辺に移ることに賛成すると，より良い状態になれる．しかし，最善反応行動のもとでは，各自の単独の行動で得られる結果の評価のみに基づいている．その結果，どのエージェントも他のエージェントの将来の行動を仮定することはできない．インターネットでもこの状況は同様である．他のエージェントや現在の解については何も仮定できない．したがって，どのエージェントも各自の直接的な改善に結びつく更新のみを積極的に実行することになる．

図 2.3(b) の Nash 均衡解の一方が他方よりどの程度良いかを定量化するには，もう一つ定義が必要となる．すべてのエージェントの総コストを最小とする解を**社会的最適解**ということにする．そ

のような解は，すべてのエージェントの状況を正確に把握できるような中央の集中管理者がいて，各エージェントを平等に見なしてコストを均等化して足し合わせて解の質を評価して得られた解と見なせる．(a) と (b) の両方の例において，社会的最適解は Nash 均衡解でもあるが，(b) においては他の Nash 均衡解もあり，それはコストが極めて大きいものになっていることを注意しておく．

3.2 局所探索との関係

局所探索との関係について考える．最善反応行動に従うエージェントの集合は，可能な解集合の “景観図” を探査しながらそれぞれのコストを最小化しようとして，一種の最急降下法のプロセスに従事しているといえる．Nash 均衡解は，このプロセスでこれ以上改善できない局所最適解と考えてもよいような自然なものである．エージェントは個々に独自の改善につながる解のみ更新しているので，この探索の “局所的” な性質も同様に明らかである．

しかし，ここで立ち止まって，標準的な局所探索とどこが本質的に異なるのか，気づくことが大切である．組合せ最適化問題に対する最急降下法アルゴリズムは終了して，局所最適解が得られることを導き出すのは簡単であった．各更新で解のコストは減少し，可能な解は有限個であるので，この更新の系列は永遠に続くことはなかった．言い換えると，コスト関数そのものが終了への進展の尺度になっていた．

これに対して，最善反応行動では，各エージェントは，独自の最小化する目的関数をもち，したがって，全体の “進展” に何が寄与するのか明らかでない．たとえば，エージェント t_i が s からの自身のパスを更新すると決定したとする．すると，コストが減少するので t_i に対する進展はもちろんであるが，これにより，他のエージェントのコストの増加がこの減少分よりも大きくなって，相殺されてしまうかもしれない．たとえば，図 2.4のネットワークを考えてみよう．両方のエージェントが，最初中央のパスから出発するとする．すると，実際には t_1 は，外側のパスに移りたいという気持ちになる．それにより，コストが 3.5 から 3 に減るからである．しかし実際にそうなると，t_2 のコストは 3.5 から 6 へ増加する．(いったんこうなってしまうと，t_2 も外側のパスに移動し，両方とも外側のパスを用いる解になるが，これが唯一の Nash 均衡解である．)

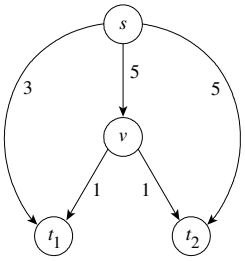


図 2.4: 社会的最適解と異なる唯一の Nash 均衡解をもつネットワーク．

実際には，最善反応行動のコスト増大の影響がこれ以上に悪くなる例もある．k 個のエージェントが（$\varepsilon > 0$ をある小さい数として）コスト $1+\varepsilon$ の共通の外側のパスとそれぞれエージェント独自のパスのある図 2.5の状況を考えてみよう．

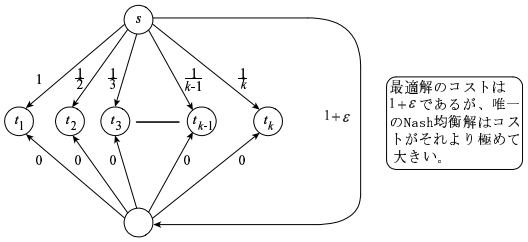


図 2.5: 社会的最適解の $H(k) = \Theta(\log k)$ 倍のコストの唯一の Nash 均衡解をもつネットワーク．

t_j に対する独自のパスのコストは $1/j$ である．そこで，最初すべてのエージェントが外側のパスを共有する解から始めたとする．各エージェントは $(1+\varepsilon)/k$ 支払うことになり，この解は，すべてのエージェントのコストの総和を最小とする解になっている．しかし，この解から出発して最善反応行動をすると，急速に以下のように変化する．まず最初に，t_k が，$1/k < (1+\varepsilon)/k$ であるので，独自のパスへ変える．すると $k-1$ 個のエージェントのみが外側のパスを共有することになり，$1/(k-1) < (1+\varepsilon)/(k-1)$ であるので，その結果を受けて，t_{k-1} が独自のパスへ変える．この後 t_{k-2} がパスを変更し，すると t_{k-3} も続き，そして，最終的には，k 個のすべてのエージェントが，

s から自身に直接くる独自のパスを用いることになってしまう．そこで，以下の結果が成立するようになり，これ以上進まなくなる．

定理 1 図 2.5のインスタンスにおいて，各エージェントが s からの直接のパスを用いる解は，Nash 均衡解であり，さらに，このインスタンスでの唯一の Nash 均衡解である．

証明. 上記の解が Nash 均衡解であることを示すためには，どのエージェントも，現在のパスを変えようとする気持ちのないことを確かめるだけでよい．しかし，これは明らかである．実際，すべてのエージェントが高々1 しか払っていないし，残りの唯一の選択肢である現在どのエージェントも使用していない外側のパスはコスト $1+\varepsilon$ であるからである．

他の Nash 均衡解があったとしよう．上記の解と異なるためには，少なくとも 1 個のエージェントが外側のパスを用いていることになる．そこで，外側のパスを共有しているエージェントを $t_{j_1}, t_{j_2}, \ldots, t_{j_\ell}$ とする．なお，$j_1 < j_2 < \cdots < j_\ell$ と仮定する．すると，これらのエージェントはいずれも $(1+\varepsilon)/\ell$ 支払っている．しかし，$j_\ell \geq \ell$ であることと，エージェント t_{j_ℓ} は，$1/j_\ell \leq 1/\ell$ 支払うことになる s から自身へ直接くる別の選択肢のあることに注意しよう．したがって，t_{j_ℓ} は現在の解のパスから離れたくなる．これは，現在の解が Nash 均衡解であることに反してしまう． ■

図 2.3(b) で，社会的最適解よりコストが極めて悪くなる Nash 均衡解が存在することを例示したが，図 2.4と図 2.5は，さらに踏み込んだことに言及している．**最善の** Nash 均衡解でも，エージェントの支払う総コストは社会的最適解の総コストより悪くなりうる．どれほど悪くなりうるだろうか? この例では，社会的最適解の総コストは $1+\varepsilon$ であり，Nash 均衡解の総コストは $1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{k} = \sum_{i=1}^{k} \frac{1}{i}$ である．この和は**調和関数** $H(k)$ としてよく用いられるものである．そして漸近的な値は $H(k) = \Theta(\log k)$ である．

これらの例は，社会的最適解を，伝統的な局所探索手続きの大域最適解と同列で見ることができないことを示している．その伝統的な標準的局所探索では，大域最適解は常に安定な解であり，改善は不可能である．一方，ここでの社会的最適解では，離れたがるエージェントが存在しうるので，不安定な解となりうる．

3.3 2 つの基本的質問

最善反応行動では，エージェントが様々な行動をするため，異なった現象が生じる例を広い範囲にわたって眺めてきた．この時点で立ち止まって現在の理解がどこまで到達しているか整理して，それに基づいた質問をしてみることは有効であろう．以下の 2 つに点からこれらの質問をグループ化しよう．

- **Nash 均衡解の存在.** マルティキャストルーティング問題のすべてのインスタンスで，Nash 均衡解が**存在する**ということさえ，現時点では証明を与えていない．また，進行の尺度の候補として最も自然なものは，すべてのエージェントの総コストであろうが，それは，一つのエージェントのパスの更新で必ずしも減少するとは限らない．

  こうしてみると，最善反応行動が必ず終了することの議論をどうすればよいか必ずしも明快でない．エージェント t_1 の自身の解の改善が t_2 の犠牲に基づき，次に，t_2 の解の改善が t_1 の犠牲に基づき，というようなことが永遠に続いて無限ループに陥ることはないとどうしていえるだろうか？実際，このようなことが起こる別の問題を定義することは困難でなく，そこでは Nash 均衡解が存在しない．したがって，マルティキャストルーティング問題において，最善反応行動で Nash 均衡解に到達できることを議論しようとすると，それが可能になる特別なものは何なのかをはっきりとしなければならない．

- **安定性の代価.** これまでは，主として “オブザーバー” として Nash 均衡解を考えてきた．ある初期状態のものでグラフ上にエージェントを置き，その後エージェントがどう行動するか眺めていた．しかし，プロトコル設計者の立場からこれをとらえ，各エージェントが s からのパスを獲得できるような手続きを定義しようとすると，以下のアプローチを追求

したくなるものと思われる．点 $t_1, t_2, \ldots, t_k$ に置かれたエージェントの集合が与えられたとする．このとき，各エージェントに対して 1 本のパスからなるパスの集合で，以下の性質を満たすものを提案したい．

(i) パスの集合は，Nash 均衡解である．

(ii) (i) の制約のもとで，すべてのエージェントの総コストが最小である．

もちろん，ここでの総コスト最小である解が，社会的最適解と一致するときは理想的である．しかし，社会的最適解が Nash 均衡解でないとすると，それは安定ではなくなり，エージェントは現在のパスから離れて新しいパスを構成することになってしまう．性質 (i) と (ii) が一緒になって，安定性を前面に出して最適化して，どのエージェントも離れないような最善の解を求めるプロトコルを表現することになる．

そこで，与えられたインスタンスに対して，最善の Nash 均衡解のコストと社会的最適解のコストの比を**安定性の代価**（price of stability）と定義する．これは，解に対して，エージェントの自己都合を考慮した安定性が満たされることを要求したために引き起こされるコストの増大を定量的に表すものになっている．

この 2 つの質問は，自己都合を主張する複数のエージェントが相互作用して解を生成するという問題では，本質的にどの問題でも起こる質問である．ここで取り上げているマルティキャストルーティング問題に対して，これからこの 2 つの質問に答えていくことにしよう．本質的には，図 2.5の例題が，一般の問題に対する重要な点を凝縮していることを眺めることになる．任意のインスタンスに対して，社会的最適解から出発する最善反応行動により，社会的最適解のコストの $H(k) = \Theta(\log k)$ 以下のコストの Nash 均衡解が得られることを示すことにする．

3.4 良い Nash 均衡解を求める

まずはじめに，第一の質問に対する回答を取り上げ，マルティキャストルーティング問題では，最善反応行動が必ず終了して，Nash 均衡解が得られることを示す．この質問に対する回答で用いるアプローチが，実は，安定性の代価を抑えるための必要な道具も与えていることになる．

最善反応行動のステップ数を抑えるための進行尺度として，エージェントの総コストを用いなくてもよい，ということがキーアイデアである．エージェントのパスの更新で真に減少する非負の量ならば何でもよいのである．実際，必ず減少するのでパスの更新は有限回になり，したがって，完全にうまく働くのである．これを頭にとどめておいて，この性質をもつ尺度を定式化してみよう．尺度は，総コストのように直感的にわかりやすいものであるとは限らないかもしれないが，それでも解析には何ら問題がない．

はじめに，単なる総コストでは，なぜだめなのか，簡単な例で考えてみよう．エージェント t_j が，現在 1 本の辺 e からなるパスを，他の x 個のエージェントを共有していたとする．ここで，t_j は，現在どのエージェントも使用していない 1 本の辺 f からなるよりやすいパスに変更することを決めたとする．これが起こるためには，$c_f < c_e/(x+1)$ でなければならない．この変更の結果として，エージェントの総コストは c_f だけ増加する．変更前は，$x+1$ 個のエージェントがコスト c_e に寄与していて f のコスト c_f は誰にも課せられていなかったが，変更後は，x 個のエージェントが依然としてコスト c_e に寄与していて t_j が新しく c_f を支払うことになったからである．

このパスの変更を進行と見るためには，“進行” で意味するものが何であるかを再定義することが必要となる．特に，全体的なシステムの “位置エネルギー” が $c_e/(x+1)$ だけ減少するという概念を用いて，追加されたコスト c_f を相殺できるような尺度を導入できれば，有効であろう．これにより，$c_f < c_e/(x+1)$ から，t_j のパスの更新は，正味として減少と見なせるようになるからである．これがうまくいくためには，各辺 e の “位置エネルギー” を，e を利用しているエージェント数が $x+1$ から x に減ったとき e の位置エネルギーが $c_e/(x+1)$ だけ減少するという性質を満たすように，管理できればよい．（もちろん，e を利用するエージェント数が x から $x+1$ に増えるときは $c_e/(x+1)$ だけ増加することになる．）

したがって，直感に基づいて位置エネルギーを以下のように定義しよう．x 個のエージェントが辺 e を共有しているときに，最初一人が辺 e を使用することをやめるときは位置エネルギーが c_e/x だけ減り，2 番目のエージェントが辺 e を使用することをやめるときは位置エネルギーが $c_e/(x-1)$ だけ減り，3 番目のエージェントが辺 e を使用することをやめるときは位置エネルギーが $c_e/(x-2)$ だけ減り，以下同様に進むとする．すなわち，x 個のエージェントが辺 e を共有しているときはその位置エネルギーを $c_e(1/x + 1/(x-1) + \cdots + 1/2 + 1) = c_e \cdot H(x)$ と定義すればよい．より具体的には，パス集合 $P_1, P_2, \ldots, P_k$ の**位置エネルギー**を $\Phi(P_1, P_2, \ldots, P_k)$ と表すことにする．そして，各辺 e に対して辺 e を含むエージェントのパスの個数を x_e として，

$$\Phi(P_1, P_2, \ldots, P_k) = \sum_{e \in E} c_e \cdot H(x_e)$$

と定義する．なお，パスに含まれない辺の寄与は 0 であるので，ここので調和数 $H(0)$ は 0 としている．

以下の命題は，Φ が実際に進行尺度としてうまく働くことを示している．

定理 2 現在のパスの集合を $P_1, P_2, \ldots, P_k$ とし，エージェント t_j がそのパスを P_j から P'_j に更新したとする．すると，新しい位置エネルギー $\Phi(P_1, \ldots, P_{j-1}, P'_j, P_{j+1}, \ldots, P_k)$ は，古い位置エネルギー $\Phi(P_1, \ldots, P_{j-1}, P_j, P_{j+1}, \ldots, P_k)$ より，真に小さい．

証明． t_j が P_j から P'_j にパスを更新する前は，各辺 e のコストを $x_e - 1$ 個の他のエージェントと共有していたので，t_j は $\sum_{e \in P_j} c_e/x_e$ 支払っていた．更新後は，共通部分 $P_j \cap P'_j$ に含まれる辺に対しては更新前と同じコストを支払い，各辺 $f \in P'_j \setminus P_j$ に対しては，$c_f/(x_f + 1)$ 支払う．したがって，t_j がこの更新を改善と見たことから以下が成立する．

$$\sum_{f \in P'_j \setminus P_j} \frac{c_f}{x_f + 1} < \sum_{e \in P_j \setminus P'_j} \frac{c_e}{x_e}.$$

そこで，位置エネルギー関数 Φ では何が起きているか考えてみよう．位置エネルギーが変化するのは，$P'_j \setminus P_j$ に含まれる辺と $P_j \setminus P'_j$ の辺でのみである．前者の総増加分は

$$\sum_{f \in P'_j \setminus P_j} c_f[H(x_f + 1) - H(x_f)] = \sum_{f \in P'_j \setminus P_j} \frac{c_f}{x_f + 1}$$

となり，後者の総減少分は

$$\sum_{e \in P_j \setminus P'_j} c_e[H(x_e) - H(x_e - 1)] = \sum_{e \in P_j \setminus P'_j} \frac{c_e}{x_e}$$

となる．したがって，t_j がパスの更新を改善と見なしたことから，総増加分は総減少分未満であることが得られ，位置エネルギー Φ は t_j のパスの更新により真に減少する． ■

各エージェント t_j に対してパスの選択肢は有限個であり，また，定理 2 より，最善反応行動では，あるエージェントによる改善により一度離れられたパスの集合 $P_1, \ldots, P_k$ は，二度と現れることはない．したがって，以下が示されたことになる．

定理 3 最善反応行動は，常に Nash 均衡解となるパスの集合をもたらす．

安定性の代価を抑える

上記の位置エネルギー関数 Φ は，安定性の代価を抑えるのにも極めて有効になる．Φ は，エージェントの総コストとは異なるが，密接な関係があるという点がポイントである．

以下それを確認することにしよう．選んだパスの集合が $P_1, \ldots, P_k$ であるときのエージェントの総コストを $C(P_1, \ldots, P_k)$ とする．これは，これらのパスに含まれるすべての辺 e のコスト c_e の和である．そのような辺のコストは，その辺を通るエージェントのパスで完全にカバーされるからである．

したがって，コスト関数 C と位置エネルギー関数 Φ の関係は以下のようになる．

定理 4 任意のパス集合 $P_1, \ldots, P_k$ に対して，以下が成立する．

$$\begin{aligned} C(P_1, \ldots, P_k) &\leq \Phi(P_1, \ldots, P_k) \\ &\leq H(k) \cdot C(P_1, \ldots, P_k). \end{aligned}$$

証明. x_e は辺 e を含むパスの個数であったことを思いだそう．C と Φ を比べるために，パス $P_1, \ldots, P_k$ のいずれかに含まれる辺のすべての集合を E^+ とする．すると，C の定義より，$C(P_1, \ldots, P_k) = \sum_{e \in E^+} c_e$ である．

すべての辺 e で $x_e \leq k$ であることに注意しよう．したがって，

$$\begin{aligned} C(P_1, \ldots, P_k) &= \sum_{e \in E^+} c_e \\ &\leq \sum_{e \in E^+} c_e H(x_e) = \Phi(P_1, \ldots, P_k) \end{aligned}$$

となり，

$$\begin{aligned} \Phi(P_1, \ldots, P_k) &= \sum_{e \in E^+} c_e H(x_e) \\ &\leq \sum_{e \in E^+} c_e H(k) \\ &= H(k) \cdot C(P_1, \ldots, P_k) \end{aligned}$$

が得られる． ■

これを用いて，安定性の代価の上界を与えることができる．

定理 5 任意のインスタンスにおいて，エージェントの総コストが高々社会的最適解のコストの $H(k)$ 倍の Nash 均衡解が存在する．

証明. 所望の Nash 均衡解を得るために，パス $P_1^*, \ldots, P_k^*$ からなる社会的最適解から出発して，最善反応行動をすることにする．定理 3により，これは Nash 均衡解 $P_1, \ldots, P_k$ で終了することになる．

この最善反応行動の実行で，エージェントの総コストは増加するが，定理 2より位置エネルギーは減少する．したがって，$\Phi(P_1, \ldots, P_k) \leq \Phi(P_1^*, \ldots, P_k^*)$ が得られる．

これが基本的には必要なすべてである．実際，任意のパスの集合に対して，C と Φ の値は，高々 $H(k)$ 倍の相異があるだけであるからである．したがって，

$$\begin{aligned} C(P_1, \ldots, P_k) &\leq \Phi(P_1, \ldots, P_k) \\ &\leq \Phi(P_1^*, \ldots, P_k^*) \\ &\leq H(k) \cdot C(P_1^*, \ldots, P_k^*) \end{aligned}$$

が得られる． ■

上記の議論と通して，Nash 均衡解が常に存在すること，しかも社会的最適解の高々 $H(k)$ 倍のコストの Nash 均衡解も常に存在することが確立できた．図 2.5の例題は，最悪の場合，この上界 $H(k)$ をこれ以上改善できないことを示している．

上記の結果は，マルティキャストルーティング問題のある側面をきれいにまとめているが，この問題にはまだ未解決な質問も多数存在する．特におもしろい質問の一つとして，Nash 均衡解を多項式時間で求めることができるかどうかということが挙げられるだろう．上記の Nash 均衡解の存在証明は，最善反応行動で得られるパスの集合は二度と同じ集合になることはなく，したがって，反復の更新が無限に続けられることはないというものに基づいている．しかし，パスの集合は指数個になりうるので，これは多項式時間のアルゴリズムを与えるものではない．Nash 均衡解を効率的に求める質問より難しい質問としては，社会的最適解と相対的に比較して，定理 5で保証された $H(k)$ 倍以内の Nash 均衡解を効率的に求める問題も未解決問題である．

前述のいくつかについても再度述べておくことが大切であろう．最善反応行動では無限ループに陥るような問題を見つけることは困難ではない．もちろん，そのような問題に対しては Nash 均衡解は存在しない．マルティキャストルーティング問題では，幸運にも，最善反応行動で，**位置エネルギー関数**を改善することができて，Nash 均衡解に向かって確実に歩を進めることができた．しかし，この例のような位置エネルギー関数が，エージェントが相互影響するすべての問題では，必ずしも存在するとは限らないことである．

3.5 注意

本節は，原書（J. Kleinberg and E. Tardos: Algorithm Design, Addison-Wesley, 2005）の 12.7 節の翻訳（浅野孝夫，平田富夫，小野孝男，浅野泰仁：アルゴリズムデザイン，共立出版，出版予定）に基づいている．

研究業績一覧

学術論文

1. Takao Asano:
   “An Improved Analysis of Goemans and Williamson’s LP-relaxation for MAX SAT”, Theoretical Computer Science, 354, 339–353, 2006.
   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. S. Taoka, D. Takafuji, T. Iguchi, and T. Watanabe:
   “Performance Comparison of Algorithms for the Dynamic Shortest Path Problem”, IEICE Trans. Fundamentals, Vol. E90-A, No. 4, （掲載予定）.
   概要: 動的最短経路問題（辺重みつき有向グラフにおける最短経路問題で，辺重みの増減に伴う最短経路木の再構成アルゴリズム設計）に関する成果である．既存アルゴリズムをほぼ網羅する形で実装し，それらの性能を計算機実験により検証した．

3. S. Shimada, S. Taoka, M. Yamauchi and T. Watanabe:
   “An Improved Heuristic Algorithm FEIDEQ for the Maximum Legal Firing Sequence Problem of Petri Nets”, Proc. 2006 IEEE International Symposium on Circuits and Systems (ISCAS 2006), pp. 4483–4486, May, 2006.
   概要: ペトリネットの最大発火系列問題とは，ペトリネット，初期マーキング，発火回数ベクトル（各トランジションの発火回数を規定）が与えられたとき，各トランジションが規定回数以下発火するようなできるだけ長い発火系列を求める問題であり，スケジューリングやネットワークプロトコル設計などに応用がある．新しく発見的解法を提案し，多くの計算機実験結果によりその性能の良さを示した．

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, 1035–1041, 2006.
   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. 松本雄介，鈴木一平，今井桂子:
   “多角形障害物のある領域における車両型ロボットの安全で滑らかな経路生成”, 日本応用

数理学会論文誌, 16(4), 631–649, 2006.
概要: 多角形障害物のある領域において，車両型ロボットを対象として，安全で制御しやすい経路を生成する手法を提案し，新しいVoronoi 図の概念に拡張を行っている．

研究会等

1. H. SUMIYOSHI, D. TAKAFUJI, S. TAOKA and T. WATANABE:
“Experiment-based Evaluation of Algorithm Performance for the 2- or 3-Vertex Connectivity Augmentation Problem”, Tech. Rep. CAS2007 IEICE of Japan, 巻号, 掲載ページ, January, 2007.
概要: グラフの辺付加問題とは，与えられたグラフに対し，付加して所望の（点あるいは辺）連結度を得るような辺重み総和最小の辺集合を求める問題で，耐故障ネットワークの構成などに応用がある．2 点連結化問題と 3 点連結化問題の発見的解法を提案し，計算機実験結果により，その性能を評価した．

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

近年，データを中心とした研究が盛んに行われている．現実の問題解決においては，計算を行う作業より，むしろデータを収集する作業がボトルネックとなることが多い．一方で，IT 技術の発達により，データを楽に大量に蓄積することが可能となっている．そのため，手に入るデータ利用して，いかに問題を解くか，というように問題が考えられている．いわば，データ中心科学である．データ中心の科学では，基本的にデータは問題解決のために集められたものではなく，そのために不完全性，エラー，粒度の違いなど，多くの潜在的な問題を抱えている．そのため，従来の最適化によるアプローチのような，単一の，極みを表現する解のみを出力する，というアプローチは運用上好ましくなく，列挙のように，多くの解を出力するアプローチが求められている．

これらのデータ中心科学は，人工知能，データベースなどの情報学分野を中心に発達しており，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，応用されている．これらの分野では，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・解法の研究が増加している．

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．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．

研究は大きく分けて，３つのトピックに分かれる．１つは，基礎的な列挙問題に対して，単純かつ効率の良いアルゴリズムを開発すること．単純さは，アルゴリズムを他分野に応用する際，あるいはより複雑な問題を解く基礎とする場合にアドバンテージとなるため，基礎研究としては重要な要因である．2 つ目は，現実問題を意識した，多少複雑な構造に対して，効率の良い列挙アルゴリズムを与えることである．単純な手法では列挙が困難な構造に対して，効率良いアルゴリズムが存在すれば，それを利用して応用的なアルゴリズムが開発できるようになり，応用分野での効率良く解けるモデルの範囲を大きく広げることができる．3 つ目は，列挙のアイディアを用いて，他の理論分野，特に組合せ最適化や組合せ数学の分野で，未解決な問題を解こうというものである．

１つ目の，基礎的な列挙問題に関しては，方形描画，整数分割に対して，効率的な列挙アルゴリズムを開発した．さらに，応用上の観点から，昨年度開発したフロアプランの列挙アルゴリズムの解を効率的に蓄えるための，圧縮技術について，シンプルかつ効率の良い手法を開発した．

全ての面が方形である平面描画を方形描画とよぶ．方形描画の外面と隣接している内面を窓つ

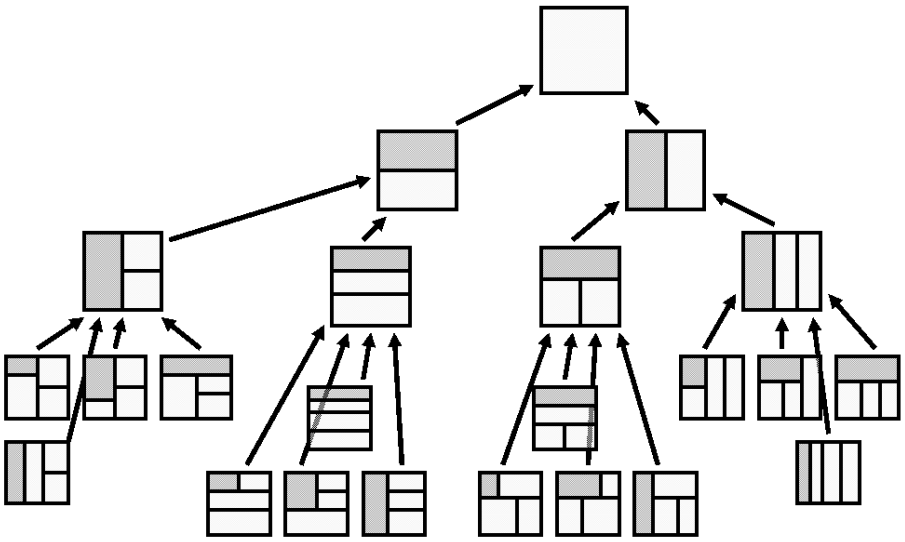


図 2.1: 大きさ 4 以下の方形描画に対して定義された親子関係

き部屋とよび, 外面と隣接していない内面を窓なし部屋とよぶ. 今年度の研究では，内面の個数がちょうど n である方形描画を, 描画ひとつあたり $O(1)$ 時間で, 重複も抜けもなく, 列挙するアルゴリズムを開発した．さらに，内面の個数が n であり, 窓なし部屋の個数が高々k である底辺つき方形描画を, 描画ひとつあたり $O(1)$ 時間で, 重複も抜けもなく, 列挙するアルゴリズムも開発した．方形描画は，単純な場合分けなどで列挙するのは簡単ではないため，技術的な革新が行われた．アルゴリズムのアイディアは，各方形描画に親を定義することで，方形描画間に親子関係と呼ばれる連結な非巡回的関係を定義し，それを探索ルートにして探索を行うことにより，全ての方形描画を重複なく列挙する．親子関係の例を図 2に示す．これまではそのような描画を平均 $O(1)$ 時間で列挙するアルゴリズムしか知られていなかったが，今年度開発したアルゴリズムは，任意の 2 つの出力の間の時間 (遅延時間とよばれる) が $O(1)$ 時間である．

また，方形描画に対しては，m 本の辺からなる方形描画を $2m$ ビットを用いてコード化する簡単な方法が知られている．今年度の研究では, よりコンパクトなコード化を提案した. 我々の方法は, 実装が容易であり, 各フロアプランを $5m/3$ ビットでコード化する.

整数 n の整数分割を列挙するアルゴリズムを開発した．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. 今年度の研究では，与えられた整数の整数分割を, 遅延時間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た.

2 つ目の，応用を意識した複雑な構造を列挙するアルゴリズムとしては，コーダルグラフ，インターバルグラフ，極大モチーフ，擬似クリークの列挙アルゴリズムを開発した．どれも，単調性がなりたたず，単純なアイディアでは効率良く列挙

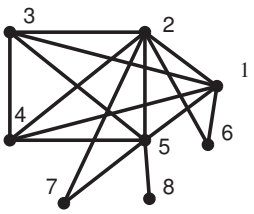


図 2.2: コーダルグラフの例

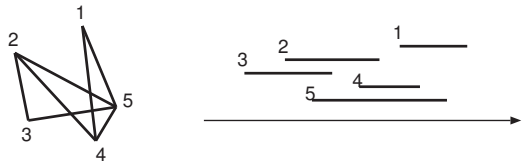


図 2.3: インターバルグラフの例

できないが，応用上は利用価値の高いモデルであり，効率良い列挙アルゴリズムの果たす役割は大きい．

1つ目のアルゴリズムは与えられたグラフを含む，あるいは与えられたグラフに含まれるコーダルグラフ，およびインターバルグラフを列挙するアルゴリズムである．コーダルグラフとは，任意の長さ4以上の閉路が弦 (閉路の頂点同士を結ぶ閉路に属さない辺) を持つようなグラフのことであり，インターバルグラフとは，直線状に置かれた線分のインターセクショングラフ，つまり，各線分が各頂点に対応し，線分と線分が交わりを持つときに対応する頂点間に枝を張って得られるグラフである．図2, 2 に，コーダルグラフとインターバルグラフの例を示した．コーダルグラフは，密な構造が重なり合って木構造を構成しているような状態を表し，グラフィカルモデリングなどで，相関関係を表すために用いられる．また，インターバルグラフは，ゲノムなどの文字列の部分構造の関係を表す．どちらも応用上で価値が高い．この問題に対して，今年度の研究で，与えられた n 頂点のグラフを含む，あるいは与えられたグラフに含まれるコーダルグラフを1つあたり $O(n^3)$ 時間で求めるアルゴリズム，および，そのグラフを含む，あるいはそのグラフに含まれるインターバルグラフを列挙する，1つあたり $O(n^3)$ 時間のアルゴリズムを開発した．

与えられたグラフの密な部分構造を見つけ出す

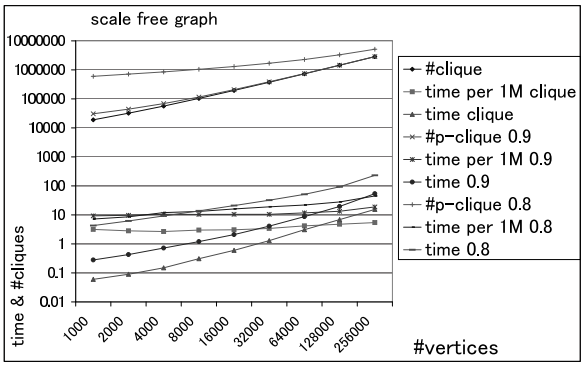


図 2.4: ランダムに生成したスケールフリーグラフに対する，擬似クリーク列挙の計算時間と個数

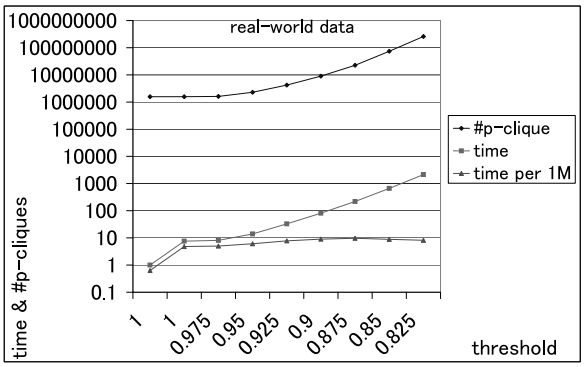


図 2.5: 頂点数約3万のソーシャルネットワークに対する計算時間

問題は，データマイニングやデータ工学を始めとする情報学の分野での基礎的な問題である．密な構造をモデル化したものとしてクリーク（完全グラフとなっている部分グラフ）があり，これはモデルの単純さと解法の構築しやすさから重宝されており，今までに多くの研究でクリーク，あるいは極大クリーク列挙が使われてきた．その一方で，近年，本来の動機であるグラフの密な構造を見つける，という問題を直接解こうという機運が高まりつつある．クリークだけでなく，クリークから枝を少し抜いたような，擬似クリークを見つけようというものである．擬似クリークの定義はいくつか考えられるが，ここでは枝数がクリークと比べて閾値以上の割合になっている部分グラフで定義する．今年度の研究では，このように定義された擬似クリークを全て列挙する問題を考えた．この問題に対する分割統治法的アプローチが計算量的には絶望的であることを示し，逆探索法に基づく多項式時間アルゴリズムを提案した．さらに，計算実験から実用上の効率の良さを示した．計算実験の結果を図 2に示す．これは，ランダムに生成したスケールフリーグラフに対する結果で，横軸が入力したグラフの頂点数，縦軸が計算時間／擬似クリーク数／擬似クリーク 100 万個あたりの計算時間である．グラフの枝数は頂点数の 5 倍となっている．また，実データから得たグラフに対しても計算実験を行った．図 2 は，頂点数が 3 万ほどのソーシャルネットワークに対して擬似クリーク列挙を行った結果である．計算時間，個数，100 万個あたりの計算時間を，閾値を変化させて計測した．

また，同様にデータマイニングの問題に，文字列データの中から頻出する極大モチーフを全て発見するというものがある．モチーフとはワイルドカード (任意の文字と対応できる) を含められる文字列パターンであり，多少の変化が意味的な変化を起さないゲノム列の解析などに有効なモデルである．図 2に例を示した．既存の研究にて開発されたアルゴリズムは，時間的に高速性の保証がなく，また多大なメモリを使うという欠点があり，実用的な実装を行うことは難しかった．今回，近傍の大きさが多項式で抑えられるような，極大モチーフの隣接性を明らかにし，それを用いて，ppc 拡張とよばれる極大モチーフから極大モチーフを生成する手法を開発し，それを用いて多項式時間のアルゴリズムを開発した．また少ないメモリしか使用しないようになった．隣接性の例を図 2 に示した．実用的な実装の開発も可能である．また，長さの制限や，冗長性の排除などの改良を行った．

同じくデータマイニングの分野で，実験結果の中からモデルを説明できるような項目の組合せを見つける問題がある．この問題に対して，今年度の研究で，そのような項目の組合せの中から，極小なものを列挙するアルゴリズムを開発した．双対化というアルゴリズムを用いて無駄な探索を省き，高速に列挙することに成功した．同様のアルゴリズムは，UML とよばれるプログラム設計システム上の矛盾点を発見し，矛盾を無くすための最小の改良手段を見つける目的にも使える．

3 つ目は，列挙のアイディアを用いて，他の理論分野，特に組合せ最適化や組合せ数学の分野で，未解決な問題を解こうというものである．

1 つ目の問題は，いくつかの多面体を，共通部分が最大になるように，向きを変えずに重ね合わせる問題である．d 次元の多面体 $P_1, ..., P_n$ があるときに，これらを平行移動して重ね合わせ，その際の共通部分の体積を考える．この体積が最大になるような，平行移動の仕方を考える問題は，目的関数が凸にも凹にもならず，一見難しい問題のように見える．しかし，この体積の d 乗根は，凸であることが証明できる．そのため，楕円体法による，体積計算をオラクルとした多項式時間アルゴリズムが設計できる．また，次元が低い場合，多面体の和集合であらわされるような，非凸な集合の共通部分を最大化することもできる．実行可能領域を，多面体の重なり方のトポロジーが等価な領域に分割することが可能であること，およびその領域の数がそれほど大きくないことが証明できる．図 2 に例を示す．各領域内では，問題が多項式時間で解けるため，領域を列挙することで効率的な計算ができる．非凸な集合の個数が指数部にかかるオーダーとなるが，多項式時間アルゴリズムとなる．

2 つ目の問題は，最小重み三角形分割に関するアルゴリズムである．最小重み三角形分割問題とは，平面上に与えられた n 個の点から成る集合の凸包を三角形に分割する方法の中で辺長の総和が最も小さくなるものを求める問題であり，多項式

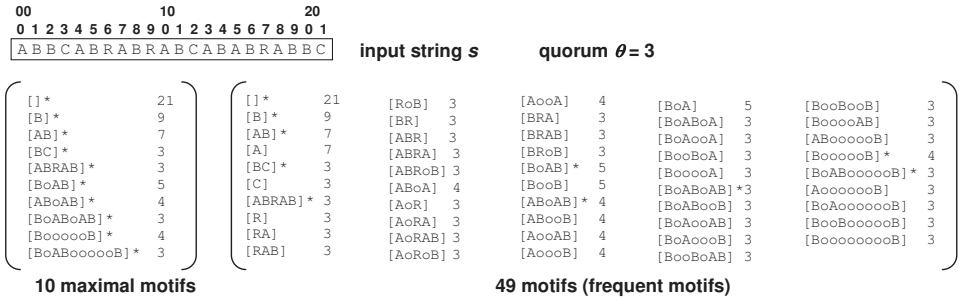


図 2.6: 文字列に対するモチーフと極大モチーフ

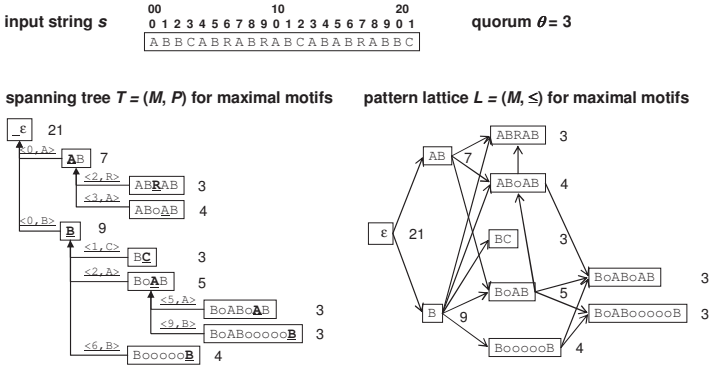


図 2.7: 極大モチーフが作る木構造（列挙木）

時間で解けるかどうか 30 年もの間未解決であった重要な計算幾何の問題である．この問題に対して凸包の境界上にない点に着目し，そのような点の個数が k であるとき，$O(6^k n^5 \log n)$ 時間で最適解を求めるアルゴリズムを考案した．そのアルゴリズムの主要な部分では解くべき部分問題の列挙を行なっているが，その数を巧みに減らすことで上記の計算量を得ている．

協力ゲーム理論におけるコア安定性問題という未解決問題に組合せ最適化ゲームの観点から接近を試みた．特に，理想グラフ上の最小彩色ゲームと呼ばれる協力ゲームに注目し，そのようなゲームに対してはコア安定性の判定が多項式時間で行なえ，また，関連するコア厳密性，コア拡張性，コア広大性の判定問題が coNP 完全であることを示した．また，後者の問題に対しては列挙アプローチに基づく $O(1.443^n n^{2.376})$ 時間厳密アルゴリズムを構築した．

線型相補性問題に対する組合せ的アプローチを模索する中で，Stickney と Watson は「3 次元以上の PLCP 超立方体において，出次数が偶数の頂点が 1 つのファセットに集まることはない」という予想を掲げた．この研究では，Moriyama によって単体的複体のシェラビリティー判定のために考案された h-割当という概念をこの問題に適用し，5 次元非巡回 PLCP 超立方体の中から予想の反例と成り得るものを全て列挙し，それら反例候補を調べることで，5 次元非巡回 PLCP 超立方体に関して Stickney と Watson の予想が成立することを示した．

与えられた無向グラフの中に閉路を含まない部分グラフ (森と呼ばれる) がいくつあるか数える問題はネットワークの信頼性計算などと関連し，多く研究がなされている．しかし，大抵そのような問題は#P 完全，すなわち，多項式時間で解ける望みのない問題であることが証明されている．

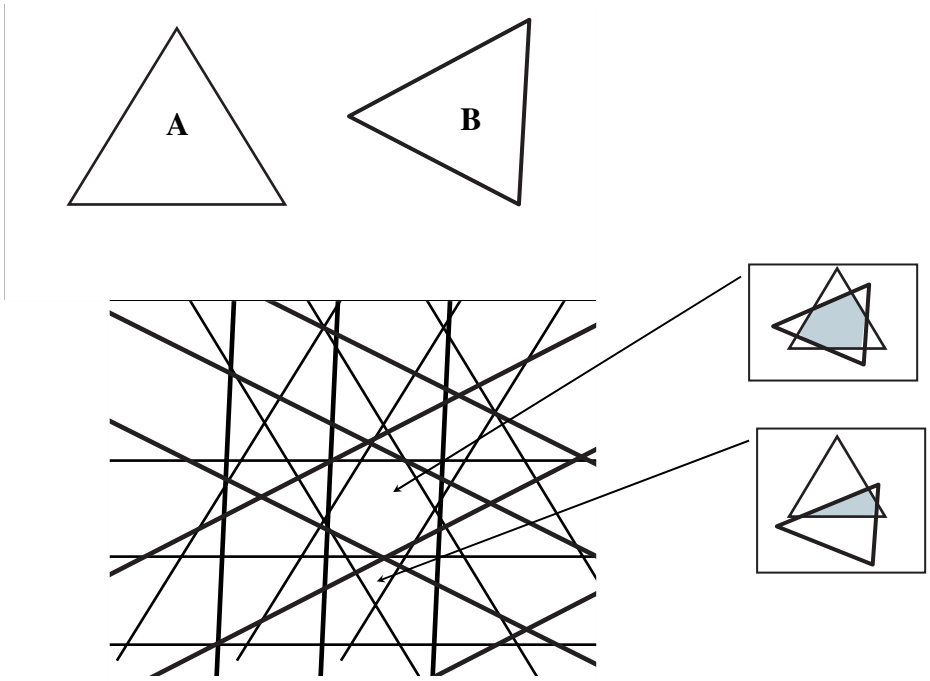


図 2.8: 2 次元の多面体の重なり方が等しい領域への分割

この研究では与えられるグラフをどこまで制限しても $\#P$ 完全のままであるのか議論し，平面的 3 正則グラフやコーダルグラフに対しても $\#P$ 完全であることを証明した．また，3 正則グラフに対して $O^*(1.8494^m)$ 時間，単位区間グラフに対して $O^*(1.9706^m)$ 時間の厳密アルゴリズムを構築した (ただし，m は入力グラフの辺数で，O^* という記法は定数だけではなく多項式因子も無視したものである)．これらのアルゴリズムは解くべき部分問題の列挙に基づいているが，その数を巧みに抑えることで上記の計算量を達成している．

研究業績一覧

学術論文

1. 宇野 毅明:
   “擬似クリークを列挙する多項式時間遅延アルゴリズム”, 情報処理学会アルゴリズム研究会, 第 111 回, 20067 年 3 月.
   概要: 与えられたグラフの密な部分構造を見つけ出す問題は，データマイニングやデータ工学を始めとする情報学の分野での基礎的な問題である．密な構造をモデル化したものとしてクリーク（完全グラフとなっている部分グラフ）があり，これはモデルの単純さと解法の構築しやすさから重宝されており，今までに多くの研究でクリーク，あるいは極大クリーク列挙が使われてきた．その一方で，近年，本来の動機であるグラフの密な構造を見つける，という問題を直接解こうという機運が高まりつつある．クリークだけでなく，クリークから枝を少し抜いたような，擬似クリークを見つけようというものである．擬似クリークの定義はいくつか考えられるが，ここでは枝数がクリークと比べて閾値以上の割合になっている部分グラフで定義する．本稿では，このように定義された擬似クリークを全て列挙する問題を考える．まず，この問題に対する分割統治法的アプローチが計算量的には絶望的であることを示し，続いて逆探索法に基づく多項式時間アルゴリズムを提案する．さらに，計算実験から実用上の効率の良さを示す.

2. Komei Fukuda and Takeaki Uno:

"Polynomial Time Algorithms for Maximizing the Intersection Volume Polytopes", Pacific Journal of Optimization, Vol 3, no. 1, 37-52, 2007.

概要: Suppose that we have several polytopes in R^d and we can translate them without rotation. Here we consider the intersection maximization problem, which asks the positions of the polytopes which maximizes the volume of their intersection. In this paper, we address this problem, and show that the problem can be solved in oracle polynomial time by an ellipsoid method, exploiting two important facts. Namely, the objective function is a continuous piecewise-polynomial function and its dth root is concave. We further study the structure of the problem in depth for the two dimensional case, and propose an algorithm which solves it in $O(n^4)$ time for two non-convex polygons, where n is the total number of vertices.

3. Hiroki Arimura and Takeaki Uno:
"An Efficient Polynomial Space and Polynomial Delay Algorithm for Enumeration of Maximal Motifs in a Sequence", Journal of Combinatorial Optimization, 2006.

概要: In this paper, we consider the problem of enumerating all maximal motifs in an input string for the class of repeated motifs with wild cards. A maximal motif is such a representative motif that is not properly contained in any larger motifs with the same location lists. Although the enumeration problem for maximal motifs with wild cards has been studied in (Parida et al., CPM '01), (Pisanti et al.,MFCS '03) and (Pelfrene et al., CPM '03), its output-polynomial time computability has been still open. The main result of this paper is a polynomial space polynomial delay algorithm for the maximal motif enumeration problem for the repeated motifs with wild cards. This algorithm enumerates all maximal motifs in an input string of length n in $O(n^3)$ time per motif with $O(n)$ space, in particular $O(n^3)$ delay. The key to the algorithm is depth-first search on a tree-shaped search route over all maximal motifs based on a technique called prefix-preserving closure extension. We also show an exponential lower bound and a succinctness result on the number of maximal motifs, which indicate the limit of a straightforward approach. The results of the computational experiments show that our algorithm can be applicable to huge string data such as genome data in practice, and does not take large additional computational cost compared to usual frequent motif mining algorithms.

4. Kevin Buchin, Andreas Razen, Takeaki Uno and Uli Wagner:
"Transforming Spanning Trees: A Lower Bound", 23nd European Workshop on Computational Geometry, 2007.

概要: For a planar point set we consider the graph of crossing-free straight-line spanning trees where two spanning trees are adjacent in the graph if their union is crossing-free. An upper bound on the diameter of this graph implies an upper bound on the diameter of the flip graph of pseudo-triangulations of the under- lying point set. We prove a lower bound of $O(\log n/\log(\log(n))$ for the diameter of the graph of spanning trees on a planar set of n points. This nearly matches the known upper bound of $O(\log n)$. If we measure the diameter in terms of the number of convex layers k of the point set, our lower bound construction is tight, i.e., the diameter is in $\log k$ which matches the known upper bound of $O(\log k)$. So far only constant lower bounds were known

5. Ken Satoh, Ken Kaneiwa and Takeaki Uno:
"Contradiction Finding and Minimal Recover for UML class diagrams", ASE2006, 2006.

概要: UML (Unified Modeling Language) is the de facto standard model representation language in software engineering. We believe that automated contradiction detection and repair of UML becomes very important as UML has been widely used. In this paper, we propose a debugging system using logic programming paradigm for UML class diagram with class attributes, multiplicity, generalization relation and disjoint relation. We propose a translation method of a UML class diagram into a logic program, and using a meta-interpreter we can find minimal sets of rules which leads to contradiction. Then, we use a minimal hitting set algorithm developed by one of the authors to show minimal sets of deletion of rules in order to avoid contradiction.

6. Marc Benkert, Martin Noellenburg, Takeaki Uno and Alexander Wolff:
"Minimizing Intra-Edge Crossings in Wiring Diagrams and Public Transport Maps", GD2006, to appear in Lecture Notes in Computer Science, 2006.
概要: In this paper we consider a new problem that occurs when drawing wiring diagrams or public transportation networks. Given an embedded graph $G = (V, E)$ (e.g., the streets served by a bus network) and a set L of paths in G (e.g., the bus lines), we want to draw the paths along the edges of G such that they cross each other as few times as possible. For esthetic reasons we insist that the relative order of the paths that traverse a node does not change within the area occupied by that node. Our main contribution is an algorithm that minimizes the number of crossings on a single edge $(u, v) \in 2^E$ if we are given the order of the incoming and outgoing paths. The difficulty is deciding the order of the paths that terminate in u or v with respect to the fixed order of the paths that do not end there. Our algorithm uses dynamic programming and takes $O(n^2)$ time, where n is the number of terminating paths.

7. Ken Satoh and Takeaki Uno:
"Enumerating Minimal Explanations by Minimal Hitting Set Computation", KSEM 2006, Lecture Notes in Computer Science, 4092, 354-365, 2006.
概要: We consider the problem of enumerating minimal explanations in propositional theory.We propose a new way of characterizing the enumeration problem in terms of not only the number of explanations, but also the number of unexplanations. Maximal unexplanations are a maximal set of abducible formulas which cannot explain the observation given a background theory. In this paper, we interleavingly enumerate not only minimal explanations but also maximal unexplanations. To best of our knowledge, there has been no algorithm which is characterized in terms of such maximal unexplanations. We propose two algorithms to perform this task and also analyze them in terms of query complexity, space complexity and time complexity.

8. Masashi Kiyomi, Shuji Kijima and Takeaki Uno:
"Listing Chordal Graphs and Interval Graphs", WG 2006, Lecture Notes in Computer Science, 4271, 68-77, 2006.
概要: We propose algorithms for enumeration problems; given a graph G, to find every chordal supergraph (in K^n) of G, to find every interval supergraph (in K^n) of G, and to find every interval subgraph of G in K^n. The algorithms are based on the reverse search method. A chordal graph is a graph which has no induced chordless cycle of length more than three. An interval graph is a graph which has an interval representation. To the best of our knowledge, these are the first results about the enumeration problems of them that can find

each graph in polynomial time. The time complexities of the former two algorithms are $O(n^3)$ for each output graph, and that for the latter is $O((n+m)^2)$ for each output graph, where m is the number of edges of input graph G. We also show that a straightforward depth-first search type algorithm works badly for these problems.

9. Katsuhisa Yamanaka and Shin-ichi Nakano: "Coding Foorplans with Fewer Bits", IEICE TRANS. FUNDAMENTALS, Vol.E89-A, no. 5, 1181-1185, 2006 年 5 月.
概要: m 本の辺からなるフロアプランを, $2m$ ビットを用いてコード化する簡単な方法が知られている. 本文では, よりコンパクトなコード化を提案する. 我々の方法は, 実装が容易であり, 各フロアプランを $5m/3$ ビットでコード化する.

10. Satoshi Yoshii, Daisuke Chigira, Katsuhisa Yamanaka and Shin-ichi Nakano: "Constant Time Generation of Rectangular Drawings with Exactly n Faces", IEICE TRANS. FUNDAMENTALS, Vol.E89-A, no. 9, 2445-2450, 2006 年 9 月.
概要: 全ての面が方形である平面描画を方形描画とよぶ. 本論文は, 内面の個数がちょうど n である方形描画を, 描画ひとつあたり $O(1)$ 時間で, 重複も抜けもなく, 列挙するアルゴリズムを与える.

11. 千明大介, 中野眞一: "窓なし部屋の個数が高々k の方形描画の高速列挙アルゴリズム", 電子情報通信学会論文誌 A, Vol.J90-A, no. 2, 122-130, 2007 年 2 月.
概要: 全ての面が方形である平面描画を方形描画とよぶ. 方形描画の外面と隣接している内面を窓つき部屋とよび, 外面と隣接していない内面を窓なし部屋とよぶ. 本論文は, 内面の個数が n であり, 窓なし部屋の個数が高々 k である底辺つき方形描画を, 描画ひとつあたり $O(1)$ 時間で, 重複も抜けもなく, 列挙するアルゴリズムを与える. これまではそのような描画を平均 $O(1)$ 時間で列挙するアルゴリズムしか知られていなかった.

12. Katsuhisa Yamanaka, Shin-ichiro Kawano, Yosuke Kikuchi and Shin-ichi Nakano: "Constant Time Generation of Integer Partitions", Proc. of WAAC06, The 9th Japan-Korea Joint Workshop on Algorithms and Computation, 57-64, 2006 年 7 月.
概要: 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.

13. Michael Hoffmann and Yoshio Okamoto: "The minimum weight triangulation problem with few inner points", Computational Geometry: Theory and Applications, 34, 149-158, July 2006.
概要: We look at the computational complexity of 2-dimensional geometric optimization problems on a finite point set with respect to the number of inner points (that is, points in the interior of the convex hull). As a case study, we consider the minimum weight triangulation problem. Finding a minimum weight triangulation for a set of n points in the plane is not known to be NP-hard nor solvable in polynomial time, but when the points are in convex position, the problem can be solved in $O(n^3)$ time by dynamic programming. We extend the dynamic programming approach to the general problem and describe an exact algorithm which runs in $O(6^k n^5 \log n)$ time where n is the total number of input points and k is the number of inner points. If k is taken as a parameter, this is a fixed-parameter algorithm. It also shows that the problem can be solved in polynomial time if

$k = O(\log n)$. In fact, the algorithm works not only for convex polygons, but also for simple polygons with k inner points.

14. Thomas Bietenhader and Yoshio Okamoto: "Core stability of minimum coloring games", Mathematics of Operations Research, 31, 418-431, May 2006.
概要: In cooperative game theory, a characterization of games with stable cores is known as one of the most notorious open problems. We study this problem for a special case of the minimum coloring games, introduced by Deng, Ibaraki & Nagamochi, which arise from a cost allocation problem when the players are involved in conflict. In this paper, we show that the minimum coloring game on a perfect graph has a stable core if and only if every vertex of the graph belongs to a maximum clique. We also consider the problem on the core largeness, the extendability, and the exactness of minimum coloring games. As a consequence, we show that it is coNP-complete to decide whether a given game has a large core, is extendable, or is exact.

15. Sonoko Moriyama and Yoshio Okamoto: "The even outdegree conjecture for acyclic PLCP-cubes in dimension five", IEICE Transactions on Information and Systems, E89-D, 2402-2404, August 2006.
概要: The behavior of Bard-type pivoting algorithms for the linear complementarity problem with a P-matrix is represented by an orientation of a hypercube. We call it a PLCP-cube. In 1978, Stickney and Watson conjectured that such an orientation has no facet on which all even outdegree vertices appear. We prove that this conjecture is true for acyclic PLCP-cubes in dimension five.

16. Heidi Gebauer and Yoshio Okamoto: "Fast exponential-time algorithms for the forest counting in graph classes", Proceedings of 13th Computing: The Australasian Theory Symposium (CATS 2007), Conferences in Research and Practice in Information Technology, 65, 63-69, January 2007.
概要: We prove #P-completeness for counting the number of forests in regular graphs and chordal graphs. We also present algorithms for this problem, running in $O^*(1.8494^m)$ time for 3-regular graphs, and $O^*(1.9706^m)$ time for unit interval graphs, where m is the number of edges in the graph and O^*-notation ignores a polynomial factor. The algorithms can be generalized to the Tutte polynomial computation.

17. Takehiro Ito, Yoshio Okamoto, and Takeshi Tokuyama: "Algorithms for the full Steiner tree problem", Proceedings of ICALP'06 Affiliated Workshop "Improving Exponential Time Algorithms", 39-45, July 2006.
概要: Assume that each edge of a graph $G = (V, E)$ is assigned a nonnegative real number cost, and that a set $K \subseteq V$ of vertices, called *terminals*, is given. A *full Steiner tree* (or a *terminal Steiner tree*) of G with respect to K is a subtree T of G such that every vertex in K is a leaf of T. For a given graph G and a given set $K \subseteq V$ of terminals, the (minimum-cost) *full Steiner tree problem* is to find a full Steiner tree for K which has the minimum total cost of edges. In this paper we first give an exact algorithm to solve the problem for general graphs in time $O^*(3^k)$ where $k = |K|$, and hence it shows the fixed-parameter tractability of the problem. We then show that the problem can be solved in polynomial time for plane graphs if all the terminals lie only on a fixed constant number of face boundaries.

18. Heidi Gebauer and Yoshio Okamoto: "Fast exponential-time algorithms for the

forest counting in graph classes", Proceedings of ICALP'06 Affiliated Workshop "Improving Exponential Time Algorithms", 25–30, July 2006.

概要: We prove #P-completeness for counting the number of forests in regular graphs and chordal graphs. We also present algorithms for this problem, running in $O^*(1.8494^m)$ time for 3-regular graphs, and $O^*(1.9706^m)$ time for unit interval graphs, where m is the number of edges in the graph and O^*-notation ignores a polynomial factor. The algorithms can be generalized to the Tutte polynomial computation.

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．

本グループでは「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」という点に焦点を合わせながらも，本特定研の他のグループとの共同研究にも力を注いだ．その結果として，計算幾何とグラフの領域で様々な新発見を得ることができた．それらの成果は異なる国際ジャーナルに発表しているが，SIAM Journal on Computing, Avdances in Mathematics, Algorithmica, Thoery of Computing System など国際的にも評価の高いジャーナルに発表している．国際会議の論文も多数あるが，いずれも査読のある国際会議であり，世界的なレベルで評価を得ている．

以下では，指紋同定に関する研究について詳しく述べた後，その他の業績について概要を述べる．

2 A Combinatorial Approach to Fingerprint Binarization and Minutiae Extraction Using Euclidean Distance Transform

2.1 Introduction

Automatic fingerprint identification systems (AFIS) are used for personal identification. Fingerprints have 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, 12, 13]. Minutiae, or Galton's characteristics [9] are local discontinuities in terms of ridge endings and bifurcations of ridge flow patterns that constitute a fingerprint. These two types of minutiae have been considered by the Federal Bureau of Investigation for identification

purposes [20]. AFIS based on minutiae matching involves different stages (see Fig. 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 [12, 15], and as such to avoid repetition, we refer the reader to them.

It is well known that performance of fingerprint identification and verification depends heavily on the preprocessing phase [5]. For the AFIS to perform better in terms of correct verification and time, the preprocessing phase has a contradictory objective - give better performance in less time. For this reason, a considerable amount of research has been focused in this area. Our work in this paper focuses on binarization preceded by an enhancement step and minutiae extraction (see Fig. 2.1(b)). Below we briefly discuss the enhancement method we used.

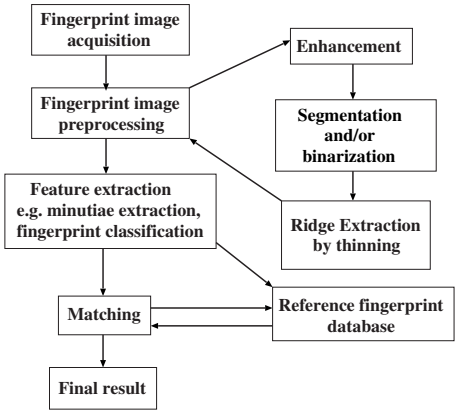
2.2 Enhancement of Fingerprint Images

Fingerprint images require specialized enhancement techniques owing to their inherent characteristics like 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 [13]. We have also used this enhancement algorithm in our work owing to its simplicity and elegance.

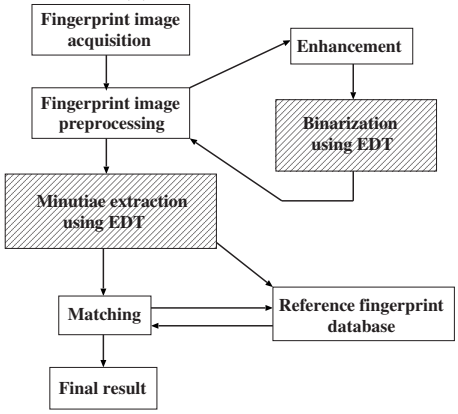
2.3 Our Contributions

Most of the previous algorithms designed for fingerprint binarization [6, 16, 17] are heuristics because they do not start with a definition of a desirable threshold. In contrast, we define a condition for a desirable threshold based on almost equal widths of ridges and valleys and then design a combinatorial algorithm for finding such a threshold. Width is estimated using Euclidean distance transform (EDT). Using EDT values has its added advantages. With EDT value of each pixel, mathematical morphological operators can be efficiently and flexibly applied for ridge smoothing, denoising, elimination of useless components, etc [14]. Moreover, most of the current fingerprint methods that use binarization, perform thinning to get a 1-pixel thick ridge (see Fig. 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. We also show that EDT values help in eliminating false minutiae. 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. In contrast, our work depends minimally on arbitrary choices of parameters because EDT values adapt itself to the data. The highlights of our work are: (i) a deterministic algorithm for binarization; (ii) minutiae detection, including elimination of false minutiae without thinning and (iii) minimal use of arbitrary parameters.

The rest of the paper is organized as follows. Section 2.4 contains discussions on EDT, measuring the width of ridges and valleys of a fingerprint using average EDT values, the threshold criteria and the deterministic algorithm for binarization. Section 2.9 discusses minutiae extraction using EDT values. Section 2.13 shows results on minutiae detection and its robustness. Finally, we finish with some discussions in Section 2.16.



(a) Usual approaches.



(b) Our approach.

図 2.1: Two flowcharts show 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.

2.4 The Binarization Algorithm

2.5 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 foreground pixel (1). Breu et al. [3] proposed an optimal $O(N \times N)$ algorithm using Voronoi diagrams. In [10], Hirata and Katoh gave 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, $DT_{1,0}$ is the value assigned to a 1 pixel equal to the Euclidean distance to the closest 0 pixel. Using the results given in [10], we have the following fact:

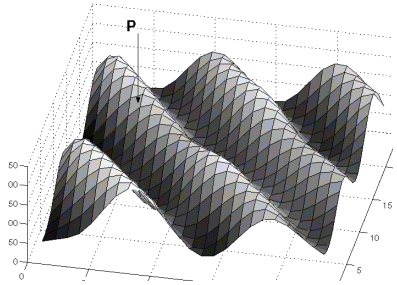
Fact 1 *Both $DT_{1,0}$ and $DT_{0,1}$ can be computed in optimal time $\theta(N^2)$ for an $N \times N$ binary image. Also, the values of both $DT_{1,0}$ and $DT_{0,1}$ are greater than or equal to* 1.

2.6 Euclidean Distance Transform and Width

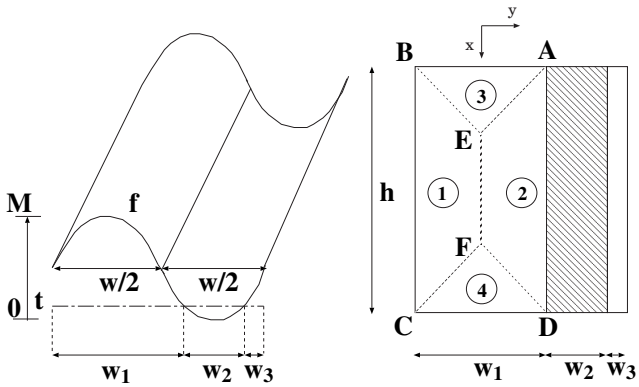
Fingerprint images are characterized by almost equal width ridges and valleys as shown in Fig. 2.2(a). We will use this particular characteristic of the fingerprint image for binarization. Measuring the width for arbitrary shapes is a difficult, non-trivial problem. In this section, we model the problem 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 as shown in Fig. 2.2(b). In the continuous domain,



(a) Magnified view of the gray scale topology of a fingerprint image.



(b) Diagram for the model.

図 2.2: Diagram for computing total distance transform.

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. See Fig. 2.2(b). The highlighted part shown in the middle is the part mapped to 0. After thresholding, the parts would be rectangles as shown in Fig. 2.2(b). 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

$$\begin{aligned} \phi^1_{dt}(w_i) &= \int_0^{w_i/2} \int_{-y+w_i/2}^{y+(h-w_i/2)} (w_i/2 - y)dxdy \\ &= (w_i^2 h)/8 - w_i^3/12 \,. \end{aligned} \tag{2.19}$$

Similarly, the total EDT value for region 3 is

$$\begin{aligned} \phi^3_{dt}(w_i) &= \int_{x-w_i/2}^{-x+w_i/2} \int_0^{w_i/2} xdxdy \\ &= w_i^3/24 \,. \end{aligned} \tag{2.20}$$

So, the total EDT value $\phi_{dt}(w_i)$ of the rectangle $ABCD$ is

$$\begin{aligned} \phi_{dt}(w_i) &= \phi^1_{dt}(w_i) \times 2 + \phi^3_{dt}(w_i) \times 2 \\ &= w_i^2 h/4 - w_i^3/12 \\ &= w_i^2/4(h - w_i/3) \,. \end{aligned} \tag{2.21}$$

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 values of ridges $\mathbb{DT}_{1,0}$ is

$$\begin{aligned} \mathbb{DT}_{1,0} &= \phi_{dt}(w_1) + \phi_{dt}(w_3) \\ &= w_1^2 h/4 - w_1^3/12 + w_3^2 h/4 - w_3^3/12 \,, \end{aligned} \tag{2.22}$$

and the total distance transform values of valleys $\mathbb{DT}_{0,1}$ is

$$\mathbb{DT}_{0,1} = \phi_{dt}(w_2) = w_2^2 h/4 - w_2^3/12 \,. \tag{2.23}$$

Now, as t increases, both w_1 and w_3 decrease and w_2 increases. This implies that with increase of t, $\mathbb{DT}_{1,0}$ decreases and $\mathbb{DT}_{0,1}$ increases. So, $\mathbb{DT}_{1,0}$ and $\mathbb{DT}_{0,1}$ can intersect only once (see Fig. 2.3), and evidently, $\mathbb{DT}_{1,0}$ is equal to $\mathbb{DT}_{0,1}$ when $w_1 = w_2$. That is, the desirable value of threshold is reached when $\mathbb{DT}_{0,1} = \mathbb{DT}_{1,0}$, 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 desirable threshold.

Definition 1 *The desirable threshold is a value* $t \in [0, M]$ *that binarizes the image such that the ridge width is equal to the valley width or* $\mathbb{DT}_{1,0} = \mathbb{DT}_{0,1}$.

Model in the discrete domain

In the continuous domain, the desirable threshold can be a fraction. A threshold with fraction guarantees equal width ridges and valleys. On the contrary, in the discrete model, the gray-level intensity of a pixel is discrete. Therefore, the threshold must be an integer. So, the observations from the previous subsection do not directly apply. But, the crucial observation does not change in the discrete domain, which is $\mathbb{DT}_{1,0}$ value decreases and the $\mathbb{DT}_{0,1}$ value increases with t increasing. Then, we have the following lemma:

Lemma 1 *The* $\mathbb{DT}_{1,0}$ *value decreases with the threshold* t *(or strictly, they are non-increasing). Similarly, the* $\mathbb{DT}_{0,1}$ *value increases with the threshold* t.

Then, the desirable threshold t can be computed from the intersection of these two curves (See Fig. 2.3). But, in the discrete domain, we may not be able to locate a single value, where the functions of sum $\mathbb{DT}_{1,0}$ and $\mathbb{DT}_{0,1}$ meet. Moreover, the widths of ridges and valleys are not always equal in real fingerprint images because of various pressure. So, we modify the definition of the desirable threshold in the discrete domain as follows.

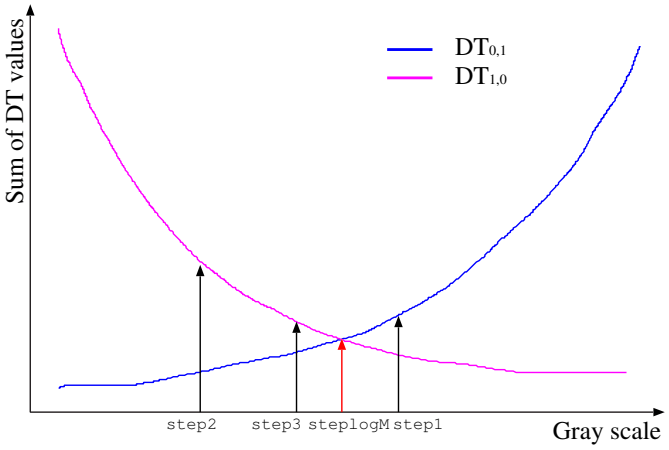


図 2.3: Diagram of binary search for binarization algorithm.

Definition 2 *The desirable threshold can be two values* t_1 *and* t_2 *such that* $t_2 - t_1 = 1$ *and* $\mathbb{DT}_{1,0}$ *is greater than* $\mathbb{DT}_{0,1}$ *at* t_1 *and their relation reverses at* t_2.

2.7 Algorithm for Binarization

To take care of different contrast and intensity across different image regions, local thresholding is applied. We cut out 32×32 sub-blocks of the image region and apply the enhancement algorithm proposed in [2] followed by our binarization algorithm. Due to the monotonically increasing (decreasing) property of the sum $\mathbb{DT}_{0,1}$ ($\mathbb{DT}_{1,0}$) with the threshold t ($t \in [0, M-1]$), we can employ binary search to find the desirable threshold according to Def. 2.

Algorithm for binarization

Input: An $N \times N$ gray-level fingerprint image I with intensity varying from 0 to $M-1$;
Output: A thresholded binary image

1. **do for all** sub-block B_i of the image I;
2. Apply the enhancement algorithm given in [2];
3. $t_1 = 0$, $t_2 = M - 1$;
4. **do**
5. $mid \leftarrow \lceil (t_1 + t_2)/2 \rceil$;
6. Compute $\mathbb{DT}_{1,0}^{mid}$ and $\mathbb{DT}_{0,1}^{mid}$;
7. **if** $(\mathbb{DT}_{1,0}^{mid} > \mathbb{DT}_{0,1}^{mid})$ $t_1 \leftarrow mid$;
8. **else** $t_2 \leftarrow mid$;
while $(t_2 - t_1 > 1)$
9. Threshold obtained for binarization is t_1 or t_2;

Theorem 1 *The binarization algorithm runs in time $O(N^2 \log M)$ for an $N \times N$ image.*

Remark 1 *Note that the monotonic curves corresponding to sum $\mathbb{DT}_{1,0}$ and sum $\mathbb{DT}_{0,1}$ may not intersect when sum $\mathbb{DT}_{1,0}$ is always greater than sum $\mathbb{DT}_{0,1}$. This happens for image blocks which are noisy or do not have a proper gray level distribution, like a non-fingerprint region. We characterize such blocks as non-binarizable blocks. Thus, our binarization algorithm has an added property of segmenting the fingerprint image region.*

For the visible results of our binarization algorithm, please refer the technical report on web page: http://www.jaist.ac.jp/∼xliang/ .

2.8 De-noising of binary images

The performance of our minutiae detection algorithm also relies on the quality of the input binary fingerprint images. Although, the enhancement phase improves the clarity of the ridge structure, a few percentage of binarized images still contains impulsive noise, bridges and useless components. With the aim of improving the quality, some researchers have introduced morphological operators for this purpose [11, 17, 19]. However, conventional morphological operation faces two serious problems in real time applications: (i) time consuming; (ii) appropriate choice of structuring elements. In our work, EDT values are employed for efficiently implementing both ordinary and generalized morphological operators in linear time, and automatically choosing appropriate-sized structuring element. Finally, we obtain fairly clear binary images. For more detail, please refer [14].

2.9 Minutiae Detection using Euclidean distance transform

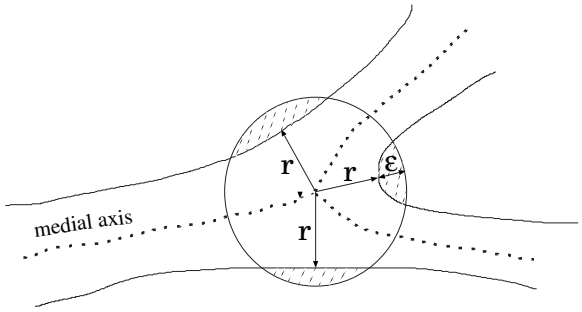
Most of the minutiae detection algorithms find out the minutiae from the one-pixel thick ridge image obtained by thinning after binarization (see, for example, [7]). Once our binarization process finishes, we have a matrix with each ridge pixel having a corresponding EDT value. Our goal is now to exploit 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 applications. In most cases, the location of the minutiae will not be exactly 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 bifurcations and ridge endings.

2.10 Bifurcation minutiae detection

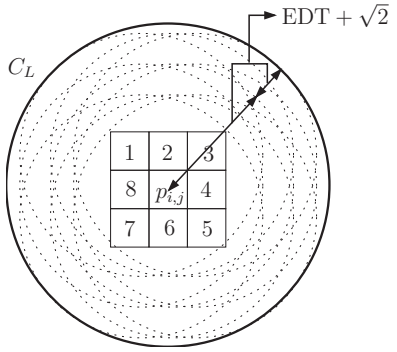
Bifurcation minutiae in the continuous domain

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*



(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 2.4: Finding bifurcation minutiae.

small positive real number), then C must contain three background components. See Figure 2.4(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.

Bifurcation minutiae in the discrete domain

Note that, in a digital grid there does not exist a perfect circle and also ϵ can not be arbitrarily small. The issue here is to define an appropriate radius for a circle so that Observation 1 holds in the discrete domain. First, we define an *EDT* cirlce.

Definition 3 *An EDT circle is a circle centered at a grid point $p_{(i,j)}$ with a radius r, where r is the EDT value of the grid point $p_{(i,j)}$.*

EDT in the discrete domain has a geometric significance as mentioned in the following fact.

Fact 2 *For a ridge pixel $p_{(i,j)}$ having an EDT value r, if we draw a circle C centered at $p_{(i,j)}$ with a radius r, then there will be at least one valley pixel on the circumference of C.*

Unlike in a continuous domain, it is very difficult to choose a unique pixel as a bifurcation point (mentioned in Observation 1) in a digital image. This happens because the medial axis is not uniquely defined for a digital image. The medial axis of simple polygon in $\mathbb{R}^2$ can be defined as the locus of all centers of circles contained in the simple polygon that touch its boundary in at least two points. Alternatively, it can be defined as the Voronoi diagram of the edges minus the Voronoi edges incident to reflex vertices. But, no such concrete definition exists for a digital grid. For instance, if the number of ridge pixels lying on the line segment perpendicular to the ridge is even, then the medial axis can pass through a region in between two pixels.

In this case, none of the EDT circles contain three background components. So, we mark a set of 3×3 connected pixels as a region where a bifurcation lies.

Observation 2 *If there is a bifurcation region in a* 3×3 *window of pixels, there are three different background components of connected pixels inside the union of those* 9 *EDT circles. See Fig. 2.4(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 are at least one pixel; and these 9 EDT circles will cover three different background components. But, finding out the correct union of these 9 circles is somewhat time consuming. So, we will define a circle C_L with the least radius centered at $p_{(i,j)}$ that covers the union of the 9 EDT circles centered at $p_{(i,j)}$ and its 8 neighbors.

The radius 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 3 *Let the EDT value at a grid point* $p_{(i,j)}$ *and any of its* 8*-neighbors be* r *and* $r_k, (k = 1, \ldots, 8)$ *respectively. Then, surely* $r - \sqrt{2} \leq r_k \leq r + \sqrt{2}$.

The equality is attained when $p_{(i,j)}$, p_k and the background pixel that contributes to the EDT value lie on a straight line.

With the above facts and observations, the radius of C_L is found as follows:

Fact 3 *The radius of the circle* C_L *centered at a ridge pixel* $p_{(i,j)}$ *is given by EDT value at* $p_{(i,j)}$ *plus* $\sqrt{2}$.

So, to detect a bifurcation region, we form the circle C_L; and if this circle contains three separate background components, we mark the pixels in this region as bifurcation.

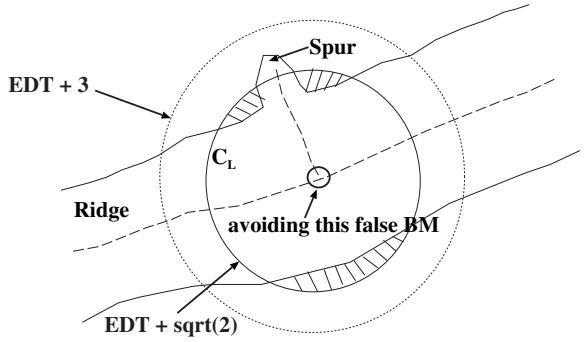
Avoiding spurs and bridges to find bifurcation minutiae

The theory developed earlier for detecting bifurcation fails when there are spurs or bridges, which are deformities in the ridge structure. A *spur* [15] is a small protrusion from the original ridge and gives rise to a false minutia. A *bridge* [15] is a structure that joins two ridges across a valley and gives rise to two false minutiae. See Fig. 2.5(a) and (b) for examples. To avoid the false minutiae thus generated, we develop 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. See the three dashed regions in Fig. 2.5(a). To avoid that, we increase the radius of C_L, to find only two connected background 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. Statistics found from massive experiments with different data sets show that the average width of ridges (valleys) is around $5 \sim 6$ pixels 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 value $+ 3$ $(3 = \lceil (5/2) \rceil = \lceil (6/2) \rceil)$. We now apply the same method of the previous subsection with a new circle C'_L whose radius is EDT value $+ 3$. The only modification is that we detect the intersection of C'_Ls to avoid false minutiae. See Fig. 2.5(a) and (b) for an illustration of spur and bridge removal respectively. It is to be noted that this is the only place where we used an arbitrary parameter.

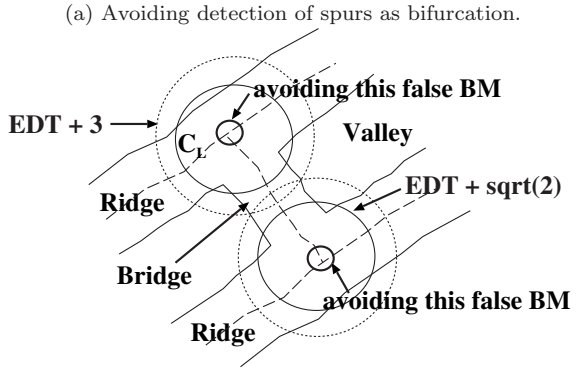
2.11 Ridge ending minutiae detection

A real property of ridge ending minutiae

There is a widely held belief that a ridge ending is the dual of a valley bifurcation as pointed



(a) Avoiding detection of spurs as bifurcation.



(b) Avoiding detection of bridges as bifurcation.

図 2.5: Finding correct bifurcation minutiae(BM) by avoiding spurs and bridges.

out in [15] (see Pg. 85-86 of [15] and Fig. 2.6(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 ending. But, during our experiments on different data sets, we came across a counter example to this duality principle as shown in Fig. 2.6(b), where a ridge ending does not correspond to a valley bifurcation. This phenomenon often happens in singular regions.

Refer to Fig. 2.6(c) for the following part of the discussion. When we use the circle C'_L (defined for determining bifurcation minutiae) to detect the ridge ending minutiae, the following observation holds.

Observation 4 *A ridge ending minutiae has the following two properties: (i) it is surrounded by a single component of valley pixels inside the circle C'_L and (ii) the length of the elongated part of the ridge ending (estimated by $\overline{bd}$) is greater than the width of the part of the ridge (estimated by $\overline{ac}$) inside the union circle.*

Based on the above observation, we developed a heuristic method to detect such minutiae. The heuristic method can differentiate between spurs [15] and real ridge ending minutiae, and to some extent can avoid breaks. Our heuristic method for finding a ridge ending is as follows:

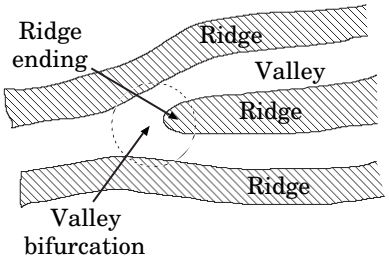
1. Find a and c, the two intersection points of the ridge with the union circle C'_L and compute the length W of the line segment $\overline{ac}$.

2. Find the middle point b of the arc $\widehat{ac}$ of C'_L; and the farthest point d on the ridge boundary from b. Compute the length H of $\overline{bd}$.

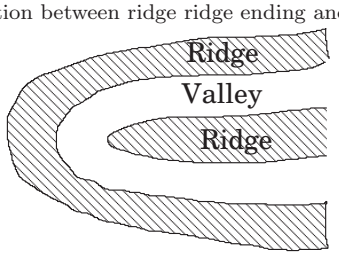
3. If $H > W$, then the origin of C'_L is a ridge ending minutiae.

Avoiding spurs and breaks to find ridge ending minutiae

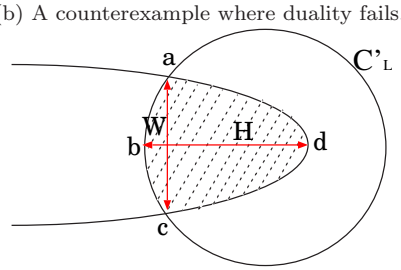
The end of a spur may be falsely detected as a ridge ending minutiae. We can remove such



(a) The duality relation between ridge ridge ending and valley bifurcation.



(b) A counterexample where duality fails.



(c) Finding ridge ending minutiae.

図 2.6: Finding ridge ending minutiae.

spurs in our heuristic for finding ridge endings because spurs do not follow property (ii) of the structural information stated in Observation 4. A *break* [15] is a small cut on the original ridge and gives rise to two false ridge endings. In enhanced images, the widths of the breaks are less than the average width of valleys. So, both the false ridge endings occuring due to the break can be removed by detecting the intersection of two union circles C'_L of corresponding false ridge endings.

2.12 Algorithm for minutiae detection

To avoid boundary pixels, we work with pixels whose EDT values are not less than 2.

Input: A matrix $\mathcal{M}$ of EDT values corresponding to a binary fingerprint image;

Output: Minutiae - bifurcations and ridge endings.

Mark minutiae

1. **do for all** ridge points $\{ p^r \mid DT_{0,1} \geq 2 \}$ of the matrix $\mathcal{M}$ that are not marked 'visisted';
2. Count n_c, the number of background components in union circle C'_L centered on $p^r_{(a,b)}$ with radius of $DT_{0,1} + 3$;
3. **if** $n_c = 3$
4. Mark $p^r_{(a,b)}$ as bifurcation minutia and $\{ \forall p^r_{(i,j)} \mid p^r_{(i,j)} \in C'_L, i \neq a, j \neq b\}$ mark 'visited';
5. **elseif** $n_c = 1$
6. Mark $p^r_{a,b}$ as ridge ending minutia and $\{ \forall p^v_{i,j} \mid p^v_{i,j} \in C'_L\}$ mark 'visited';

Detect false minutia

7. **if** $\{ \exists p^r_{(i,j)} \mid p^r_{(i,j)} \in C'_{L1} \bigcap C'_{L2}, C'_{L1}$ and C'_{L2} belong to distinct bifurcation regions.$\}$

8. Mark as bridge and remove corresponding two false bifurcation regions;
9. **if** { $\exists p^v_{(i,j)} \mid p^v_{(i,j)} \in C'_{L1} \bigcap C'_{L2}, C'_{L1}$ and C'_{L2} belong to distinct ridge ending regions.}
10. Mark as break and remove corresponding two false ridge ending regions;
11. Output genuine minutiae regions;

Fig. 2.7 shows two real minutiae regions obtained by our algorithms.

2.13 Experimental results

We used fingerprint images from several standard databases to show that our method is general and it does not depend on arbitrary selection of parameters. The databases used are: (i) NIST Special Database 4[18], (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, one set of good quality images and one set of bad quality iamges were manually selected.

To illustrate the robustness of our algorithm, in Section 2.14 we explore the minutiae density to show that the union circle C'_L does not drop genuine minutiae while avoiding false minutiae. Section 2.15 shows the accuracy achieved in minutiae extraction by our algorithm.

2.14 Robustness of union circle for avoiding false minutiae

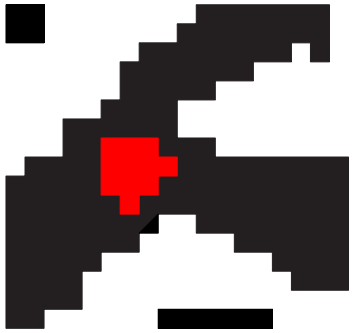
Union circle C'_L is designed not only for minutiae extraction, but also for false minutiae avoidance. So, the natural question is: whether genuine minutiae would also be removed while detecting false minutiae? It depends on the actual relation between the size of C'_L and distances among genuine minutiae. Next, we give an experimental validation of the question posed here.

As shown in subsection 2.10, each union circle C'_L for minutiae points has radius of EDT value + 3. In practice, EDT values of minutiae points lie in the range $[2, 5)$. Our algorithm will report false minutiae when two union circles C'_Ls, belonging to distinct minutiae regions, intersect. It indicates that our algorithm does not find more than one of the same type of minutiae located in a small region, like C'_L. To show that the union circle C'_L is robust in real data, we explore the closeness of minutiae. The distances between a minutia and its closest neighbor minutiae are found using Delaunay triangulation. We equably selected 100 prints from these 5 databases used for testing. Table 2.1 summarizes the average distance between minutiae, ridge endings and bifurcations respectively. Additionally, Fig. 2.8 plots the distribution of distances on these data. These three graphs well explain the large standard deviation values, that is the shortest distances greatly vary for ridge endings and bifurcations, and they do not evenly distribute in fingerprint images.

Table 2.1 and Fig. 2.8 explicitly show that rarely minutiae have neighbors within distance of 16 pixels (the upper bound of diameter of C'_L, i.e. $(5 + 3) \times 2$). This fact guarantees that the union circle has the ability of avoiding spurs, bridges and breaks without removing the genuine minutiae.

2.15 Genuine minutiae extraction results

The bifurcation and ridge ending minutiae detected by our algorithm were compared manually with the minutiae present in the enhanced images. All the images were classified into either of the two sets - good quality and bad quality. Good quality image has few bridges and breaks; ridges and valleys alternate and flow in a locally



(a) A magnified view of a bifurcation minutiae region.

(b) A magnified view of a ridge ending minutiae region.

図 2.7: A figure showing minutiae regions.

表 2.1: The average distances between closest minutiae

Minutia type	Average distance (pixels)	Standard deviation
Minutiae	25.32	12.68
Ridge ending	35.65	19.89
Bifurcation	32.08	18.26

constant direction. On the contrary, in bad quality images, even after enhancement, ridges are not strictly continuous; parallel ridges are not well separated; a lot of creases and bruises exist. Even enhancement algorithms can not repair them all.

We also further classify the error type into dropped, false and exchanged error. Dropped error means losing genuine minutiae; false error recognizes non-minutiae points as minutiae; exchanged error mistakes the bifurcation as ridge ending or vice-versa.

The experimental results are given in Table 2.2. 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 owing to exchange of ridge ending and bifurcation minutiae. Fig. 2.9 shows 5 instances. They are enhanced, binarized and minutiae detected images of a representative image from each of the five data sets considered, respectively. The time taken for minutiae detection averages 0.177 sec. on an IBM x40, intel Pentium M, WinXP, 1.4GHz.

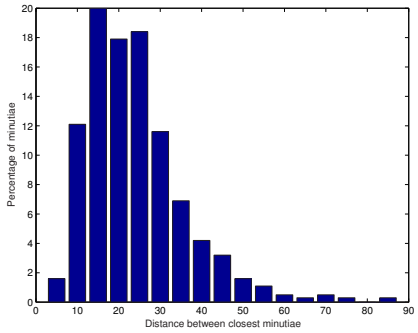
2.16 Conclusion

In this paper, we focused on binarization and minutiae extraction of fingerprints using Euclidean distance transform. The particular choice of EDT helped us in developing a deterministic algorithm for binarization. We used the same EDT value to straightaway detect bifurcation and ridge ending minutiae directly from bi-

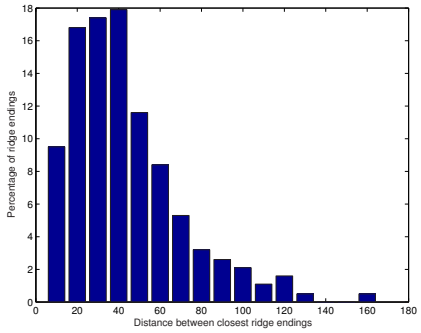
表 2.2: Minutiae detection results; R: ridge ending, B: bifurcation

Good Quality Fingerprint Image						
	Dropped		False		Exchanged	Total error
	R	B	R	B		
Percentage	2.53%	0.0%	0.0%	3.80%	0.0%	6.33%

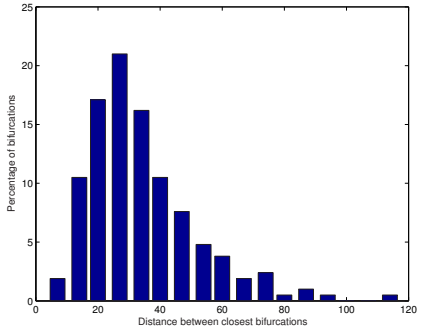
Bad Quality Fingerprint Image						
	Dropped		False		Exchanged	Total error
	R	B	R	B		
Percentage	3.03%	0.0%	5.05%	7.07%	0.0%	15.15%



(a) All minutiae.



(b) Ridge ending.



(c) Bifurcation.

図 2.8: Distance distribution of closest minutiae. *x-axis*: Distance between minutiae; *y-axis*: Percentage of minutiae.

nary images without thinning. Working with the original binary image (not the thinned one) has its added advantage: spurs, bridges and breaks 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.

For the first author, this research was conducted as a program for the "Fostering Talent in Emergent Research Fields" in Special Coordination Funds for Promoting Science and Technology by Ministry of Education, Culture, Sports, Science and Technology. The third author was partially supported by the same Ministry, Grant-in-Aid for Scientific Research (B) and Exploratory Research.

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", 10^{th} *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.,

(a) Scanned by the FUJITSU Fingerprint Sensor (model: FS-210u).

(b) From FCV2000 database.

(c) From FCV2002 database.

(d) From NIST14 database.

(e) From NIST4 database.

図 2.9: Enhanced, binarized and minutiae detected images of a representative image from each of the 5 databases. The cross marks indicate ridge endings and the boxes indicate bifurcation.

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] Ikeda, N., et al., "Fingerprint Image Enhancement by Pixel-Parallel Processing", *Proc. of Int. Conf. on pattern recognition (16th)*, vol. 3, pp. 752-755, 2002.

[12] 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.

[13] 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.

[14] Liang, X.F., and Asano, T., “A Linear Time Algorithm for Binary Fingerprint Image Denoising using Distance Transform”, *IEICE Trans. on INF. & SYST.*, Vol.E89-D, No. 4, pp. 1534-1542, 2006.

[15] Maltoni, D., Maio, D., Jain, A. K., and Prabhakar, S., *Handbook of Fingerprint Recognition*, Springer-Verlag, New York, 2003.

[16] Moayer, B. and Fu, K., “A Tree System Approach for Fingerprint Pattern Recognition”, *IEEE Trans. PAMI*, vol. 8, no. 3, pp. 376-388, 1986.

[17] 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.

[18] Watson, C. I., Wilson, C. L., *Fingerprint Database*, National Institute of Standards and Technology, Special Database 4, FPDB, April, 1992.

[19] Wahab, A., Chin, S.H., and Tan, E.C., “Novel Approach to Automated Fingerprint Recognition”, *IEEE Trans. on PAMI*, vol. 145, no. 3, pp. 160-166, 1998.

[20] 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「計算幾何：理論の基礎から実装まで」”, 共立出版, 2007 年.
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 binariza-

tion 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 $0, ..., n^2$ 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. T. Asano, J. Matousek, and T. Tokuyama:
"Zone diagrams: Existence, Uniqueness and Algorithmic Challenge", SIAMJ. on Computing, to appear.
概要: A *zone diagram* is a new variation of the classical notion of Voronoi diagram. Given points (sites) $p_1, \ldots, p_n$ in the plane, each p_i is assigned a region R_i, but in contrast to the ordinary Voronoi diagrams, the union of the R_i has a nonempty complement, the *neutral zone*. The defining property is that each R_i consists of all $x \in R^2$ that lie closer (non-strictly) to p_i than to the union of all the other R_j, $j \neq i$. Thus, the zone diagram is defined implicitly, by a "fixed-point property," and neither its existence nor its uniqueness seem obvious. We establish existence using a general fixed-point result (a consequence of Schauder's theorem or Kakutani's theorem); this proof should generalize easily to related settings, say higher dimensions. Then we prove uniqueness of the zone diagram, as well as convergence of a natural iterative algorithm for computing it, by a geometric argument, which also relies on a result for the case of two sites in an earlier paper. Many challenging questions remain open.

4. X. Liang and T. Asano:
"Combinatorial Approach to Fingerprint Binarization and Minutiae Extraction Using Euclidean Distance Transform", International Journal of Pattern Recognition and Artificial Intelligence, to appear.
概要: Most of the fingerprint matching techniques require extraction of minutiae that are ridge endings or bifurcations of ridge lines in a fingerprint image. Crucial to this step is either detecting ridges from the gray-level image or binarizing the image and then extracting the minutiae. In this work, we firstly exploit the property of almost equal width of ridges and valleys for binarization. Computing the width of arbitrary shapes is a non-trivial task. So, we estimate the width using Euclidean distance transform (EDT) and provide a near-linear time algorithm for binarization. Secondly, instead of using thinned binary images for minutiae extraction, we detect minutiae straightaway from the binarized fingerprint images using EDT. We also use EDT values to get rid of spurs and bridges in the fingerprint image. Unlike many other previous methods, our work depends minimally on arbitrary selection of parameters.

5. T. Asano, J. Matousek, and T. Tokuyama:
"The distance trisector curve", Advances in Mathematics, to appear.

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. We provide an algorithm that, given $x \in$ and $\epsilon > 0$, computes an approximation to $f(x)$ with error at most ϵ in time polynomial in $\log \frac{1+|x|}{\epsilon}$. The separation of two points by two "trisector" curves considered here is a special (two-point) case of a new kind of Voronoi diagram, which we call the zone diagram and which we investigate in a companion paper.

6. S. Teramoto T. Asano, N. Katoh, and B. Doerr:
"Inserting Points Uniformly at Every Instance", IEICE Trans. on Info. and Systems, E89-D, 8, pp.2348-2356, 2006.
概要: Arranging a predetermined number n of points over a unit cube in the d-dimensional space or over a polyhedral region is frequently asked in many applications. What is required is a set of points that are uniformly distributed over the region. In this paper we would like to insert n points in a given region in such a way that points are distributed as uniformly as possible at every instance of inserting a point. 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 preliminary result for this problem, that is, we give 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 simple local search heuristics for finding a good solution.

7. 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, 16(2-3), pp.97-116, 2006.
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.

8. T. Asano, P. Evans, R. Uehara, G. Valiente:
"Site consistency in phylogenetic networks with recombination", Iliopoulos, C.S., Park, K., Steinhöfel, K., eds.: Algorithmics in Bioinformatics, Volume 6 of Texts in Algorithmics. College Publications, 2006.
概要: Perfect phylogeny is a fundamental model for the study of evolution. Given a set of binary sequences of the same length, perfect phylogeny is the problem of fitting the sequences as leaves of a rooted tree such that no site mutates more than once, and site consistency is the problem of finding a largest subset of sites that can fit a perfect phylogeny. The site consistency problem is known to be NP-hard, but polynomial-time solvable if the set of sequences can be derived on a particular form of phylo-

genetic network with recombination, called a galled-tree. In this paper, we introduce the problem dual to site consistency, called sequence consistency, provide a linear-time algorithm for site consistency when the set of sequences can be derived on a galled-tree, and study the parameterized complexity of both site and sequence consistency.

9. 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, to appear.
概要: A semimagic square of order n is an $n \times n$ matrix containing the integers $0, \ldots, n^2 - 1$ 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. Further, the existence is also guaranteed whenever $n = k^m$, for some integers $k, m \geq 2$. We present a space-efficient algorithm for constructing such a matrix. Another class that we call constant-gap matrices arises in this construction. We give a characterization of such matrices. An application to digital halftoning is also mentioned.

10. T. Asano, J. Matousek, and T. Tokuyama:
"Zone diagrams: Existence, Uniqueness and Algorithmic Challenge", Proc. SIAM-ACM Symposium on Discrete Algorithms, 2007.
概要: A *zone diagram* is a new variation of the classical notion of Voronoi diagram. Given points (sites) $p_1, \ldots, p_n$ in the plane, each p_i is assigned a region R_i, but in contrast to the ordinary Voronoi diagrams, the union of the R_i has a nonempty complement, the *neutral zone*. The defining property is that each R_i consists of all $x \in R^2$ that lie closer (non-strictly) to p_i than to the union of all the other R_j, $j \neq i$. Thus, the zone diagram is defined implicitly, by a "fixed-point property," and neither its existence nor its uniqueness seem obvious. We establish existence using a general fixed-point result (a consequence of Schauder's theorem or Kakutani's theorem); this proof should generalize easily to related settings, say higher dimensions. Then we prove uniqueness of the zone diagram, as well as convergence of a natural iterative algorithm for computing it, by a geometric argument, which also relies on a result for the case of two sites in an earlier paper. Many challenging questions remain open.

11. X. Liang and, A. Bishnu, and T. Asano:
"Fingerprint Matching Using Minutia Polygons", Proc. ICPR: 18th Intl. Conf. on Pattern Recognition, Hong Kong, pp.1046-1049, 2006.
概要: Fingerprint distortion changes both the geometric position and orientation of minutiae, and leads to difficulties in establishing a match among multiple impressions acquired from the same finger. In this paper, minutia polygons are used to match distorted fingerprints. A minutia polygon describes not only the minutia type and orientation but also the minutia shape. This allows the minutia polygon to be bigger than the conventional tolerance box without losing matching accuracy. In other words, a minutia polygon has a higher ability to tolerate distortion. Furthermore, the proposed matching method employs an improved distortion model using a Multi-quadric basis function with parameters. Adjustable parameters make this model more suitable for fingerprint distortion. Experimental results

show the proposed method is two times faster and more accurate (especially, on fingerprints with heavy distortion) than the exisiting method.

12. X. Liang, T. Asano, and H. Zhang:
"A Combined Radial Basis Function Model for Fingerprint Distortion", Proc. ICIAR: Intel. Conf. on Image Analysis and Recognition, Portugal, September, 2006.
概要: Most fingerprint recognition techniques are based on minutiae matching and have been well studied. However, this technology still suffers from problems associated with the handling of poor quality impressions. One problem besetting fingerprint matching is *distortion*. Distortion changes both geometric position and orientation, and leads to difficulties in establishing a match among multiple impressions acquired from the same finger tip. In this paper, according to the particularity of fingerprint distortion, we propose a combined radial basis function (RBF) model, which separately builds rigid and nonrigid transformations, for attacking the distortion problem. Combined RBF model provides more accurate mapping function between a possible matched-pair. Experiments on real data demonstrate the efficacy of the proposed method in improving the compensation of fingerprint distortion.

13. T. Asano, N. Katoh, H. Tamaki, T. Tokuyama:
"Angular Voronoi Diagram with Applications", Proc. International Symposium on Voronoi Diagram in Science and Engineering, Banff, Canada, July, 2006.
概要: Given a set of line segments in the plane, we define an angular Voronoi diagram as follows: a point belongs to a Voronoi region of a line segment if the visual angle of the line segment from the point is smallest among all line segments. The Voronoi diagram is interesting in itself and different from an ordinary Voronoi diagram for a point set. After introducing interesting properties, we present an efficient algorithms for finding a point to maximize the smallest visual angle. Some applications to mesh improvement are also mentioned.

14. T. Asano:
"Aspect-ratio Voronoi Diagram with Applications", Proc. International Symposium on Voronoi Diagram in Science and Engineering, Banff, Canada, July, 2006.
概要: This paper considers a problem of finding an optimal point within a polygon P in the sense that when we connect the point to every vertex of P by straight line then the worst aspect ratio among all resulting triangles is optimized. This problem has an important application to triangular mesh improvement. We propose three different approaches toward this problem. The first one is based on some new Voronoi diagram defined by an aspect ratio, which is interesting in itself. The second approach is essentially a binary search defined by geometric intersection. The third one is grid-based heuristic, which might be practically best but has no theoretical guarantee on its performance.

15. X. Liang, A. Bishnu, and T. Asano:
"Distorted Fingerprint Indexing Using Minutia Detail and Delaunay Triangle", Proc. International Symposium on Voronoi Diagram in Science and Engineering, Banff, Canada, July, 2006.
概要: This paper is concentrated on an accurate and efficient fingerprint indexing algorithm, which efficiently retrieves the top $\mathcal{N}$ possibly matched candidates from a huge database. In order to have ability of coping with distorted fingerprints, the proposed algorithm uses novel features, which are insensitive to distortion, formed by the De-

launay triangulation of minutiae set as the representation unit. These features include minutia detail and Delaunay triangle (its handedness, angles, maximum edge, and related angle between orientation field and edges). Experiments on database FVC 2000 and scanned fingerprints with heavy distortion show our algorithm considerably narrows down the search space in fingerprint databases and is also available for distorted fingerprints. We also compared with other indexing approaches, and results show our algorithm has a better performance, especially on fingerprints with heavy distortion. This algorithm has another significant advantage that is it provides the control points for fingerprint distortion compensation.

16. T. Asano and D. Kirkpatrick:
"Distance Trisector Curves in Regular Convex Distance Metrics", Proc. International Symposium on Voronoi Diagram in Science and Engineering, Banff, Canada, July, 2006.
概要: Given two points A and B in the plane, we are interested in separating them by two curves C_A and C_B such that C_A is equidistant from A and C_B, and C_B is equidistant from B and C_A. Such curves generalize the familiar notion of a bisector curve, and form the basis of a new kind of Voronoi diagram called a Zone diagram. These curves, which are referred to as distance trisector curves, have been studied in the Euclidean metric where they exist, are unique, and admit efficient approximations. Nevertheless, they have no known expression in terms of elementary functions and are conjectured to be non-algebraic. In this paper, we study distance trisector curves with respect to a parameterized family of distance metrics that provide arbitrarily close approximations to the Euclidean distance. The advantage of studying distance trisectors in this setting is that they have a simple piecewise-linear description and an efficient (exact) construction.

17. T. Asano, J. Matousek, and T. Tokuyama:
"The Distance Trisector Curve", Proc. ACM Symposium on Computing Theory, 2006.
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. We provide an algorithm that, given $x \in R$ and $\epsilon > 0$, computes an approximation to $f(x)$ with error at most ϵ in time polynomial in $\log \frac{1+|x|}{\epsilon}$. The separation of two points by two "trisector" curves considered here is a special (two-point) case of a new kind of Voronoi diagram, which we call the Voronoi diagram with neutral zone and which we investigate in a companion paper.

18. T. Asano, F. Rosselló, G. Valiente:
"Template Matrices for Perfect Phylogeny Haplotyping and Site Consistency", RECOMB, 2006.
概要: The problem of inferring haplotype phase from a population of genotypes has received much attention recently, especially on the light of current large-scale efforts to characterize populations in terms of hyplotypes. The site consistency problem in perfect phylogeny has also received much attention lately, motivated in part by the characterization of a particular form of phylogenetic networks under mutation

and constrained recombination that admit a polynomial-time solution to the site consistency problem. Perfect phylogeny haplotyping is the problem of resolving a given set of n diploid sequences into a set of $2n$ haploid sequences that form a perfect phylogeny. The bottleneck of current algorithms for the perfect phylogeny haplotyping problem lies in the efficient computation of the genotype graph, and the usual algorithm for computing the genotype graph for a given $n \times m$ genotype matrix takes $O(nm^2)$ time. However, the genotype graph for a given genotype matrix can be obtained by a simple combination of eight template matrices over the alphabet $\Sigma = \{0, 1, 2\}$.

19. Ryuhei Uehara and Gabriel Valiente:
"Linear Structure of Bipartite Permutation Graphs with an Application", Information Processing Letters, to appear.
概要: 2 部 permutation グラフと呼ばれるグラフのクラスに対して，それが線形な構造を持つことを示した．これによって線形計画法を効率良く行なうことができるようになり，その例として最長路問題を取り上げ，これを線形時間で解くアルゴリズムを示した．

20. Ryuhei Uehara and Yushi Uno:
"On Computing Longest Paths in Small Graph Classes", International Journal of Foundations of Computer Science, to appear.
概要: 最長路問題を多項式時間で解くことができるグラフクラスが持つ性質をいくつか示した．実際には木に近い構造を持つグラフクラスと，区間表現と呼ばれる表現を持つクラスをとりあげ，これらのクラスの上で最長路問題を多項式時間で解くアルゴリズムを示した．

21. Andreas Brandstaedt, Feodor F. Dragan, Hoang-Oanh Le, Van Bang Le, and Ryuhei Uehara:
"Tree Spanners for Bipartite Graphs and Probe Interval Graphs", Algorithmica, 47(1), pp.27–51, 2007.
概要: 木スパナーとは，与えられたグラフの距離空間を近似するような木のことである．この論文では，2 部グラフやプローブ区間グラフと呼ばれるグラフのクラスをいくつかとりあげ，木スパナー問題の困難性や多項式時間アルゴリズムを示した．

22. Shin-ichi Nakano, Ryuhei Uehara and Takeaki Uno:
"Efficient Algorithms for Airline Problem", 4th Annual Conference on Theory and Applications of Models of Computation, (TAMC 07), to appear.
概要: 空港およびその利用者数が与えられた時，利用者にとって利便性の高い路線と，経営者にとって無駄の少ない路線とは互いに矛盾する．この論文では，経営者にとって無駄の少ない路線を構築する問題をとりあげ，その困難性や多項式時間アルゴリズムを示した．

23. Shin-ichi Nakano, Ryuhei Uehara and Takeaki Uno:
"A New Approach to Graph Recognition and Applications to Distance Hereditary Graphs", 4th Annual Conference on Theory and Applications of Models of Computation, (TAMC 07), to appear.
概要: 距離に関して遺伝性を持つグラフに対する，新たな特徴づけを示した．このクラスを効率良く認識するアルゴリズム，および効率良く符号化を行なう方法を示した．これらにより，同型性や数えあげなどが容易に行なえるようになった．また個数に関する理論的な上界を改善することができた．

24. Ryuhei Uehara and Sachio Teramoto:
"The complexity of a Pop-up book", 18th Canadian Conference on Computational Geometry , (CCCG 2006), pp.3-6, 2006.
概要: 飛び出す絵本を，計算幾何の問題として定式化し，その困難性を議論した．その結果，飛び出す絵本と同等の構造をもつ問題は，開く問題も閉じる問題も計算量的には困難な問題であることを示した．

25. Sachio Teramoto, Erik D. Demaine, and Ryuhei Uehara:
"Voronoi game on graphs and its complexity", 2nd IEEE Symposium on Computational Intelligence and Games, (CIG 2006), pp.265-271, 2006.
概要: 幾何的な構造を持つグラフ上で，競争的に資源を獲得する問題を，ゲームとして定式化し，その困難性を議論した．特殊な木に関しては多項式時間で必勝手順を得ることができることと，一般の場合には計算量的に困難な問題であることを示した．

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．

3. 高原祥浩，寺本幸生，上原隆平:
"Ptolemaic Graph 上の最長路問題に関する研究", 計算機科学の理論とその応用 (冬の LA シンポジウム), pp.18:1-18:10, 2007.
概要: Ptolemaic グラフと呼ばれる，幾何的な特徴を持つグラフのクラスに対する最長路問題を考察した．最長路問題，最長閉路問題に対する多項式時間アルゴリズムを得た．

4. 斎藤寿樹，清見礼，上原隆平:
"区間表現から MPQ-tree を構築するアルゴリズム", 計算機科学の理論とその応用 (冬の LA シンポジウム), pp.16:1-16:10, 2007.
概要: 区間グラフと呼ばれる，幾何的な特徴づけを持つグラフのクラスがある．このクラスの有用な表現として，MPQ-tree と呼ばれるデータ構造がある．与えられた区間表現から，この有用なデータ構造である MPQ-tree を構築する効率の良いアルゴリズムを与えた．

5. 上原隆平:
"グラフクラスとアルゴリズム", IEICE Technical Report, Lecture talk, 2006.
概要: 近年，多くのグラフのクラスが提案され，その理論的な特徴づけや，そのクラス上で高速に動作するアルゴリズムの研究が活発に行なわれている．こうした一連の研究に関するサーベイ講演を行なった．

6. 平山亮，上原隆平:
"スケールフリーグラフ上における局所情報を用いたランダムウォークについて", IPSJ SIG Technical Report, 2006-AL-107-6, pp.31-37, 2006.
概要: 近年スケールフリーグラフと呼ばれる概念が注目を集めている．これは Web などの社会ネットワークをモデル化できるものと考えられている．一方で，周囲の情報を少しだけ活用すると，ランダムウォークの効率が良くなることが理論的に示されている．この論文では，スケールフリーグラフ上で，こうしたランダムウォークがどれくらい効率が改善されるのか，を，実験的に調査した．

7. Sachio Teramoto, Mitsuo Motoki, Ryuhei Uehara, and Tetsuo Asano:
"Heuristics for Generating a Simple Polygonalization", IPSJ SIG Technical Report, 2006-AL-106-6, pp.41-48, 2006.
概要: 与えられた点を使った単純多角形の生成は，多くの応用をもつ重要なテーマであ

るが，いまだに完全な解決にはいたっていない．この論文では，この問題に対する新しい発見的手法を提案し，その有用性を実験的に示した．

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 † 趙 亮 † 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 工芸科学研究科
〒 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 堺市中区学園町 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），数理計画法に基づいたアルゴリズム，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そのまま離散最適化問題として定式化し，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するだけでは，計算効率のよいアルゴリズムを得ることはできない．そこで，問題の本質的な構造を抽出し，この構造を利用した効率の良いアルゴリズムの設計が重要となる．本研究では，特にグラフ構造に焦点を置き，離散数学，数理計画法の成果を応用した厳密解法，理論保障付き近似アルゴリズム，発見的手法の設計，理論的基盤の確立を目指す．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する研究を中心に行い，2 年目においては，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の研究成果を加えた．今年度は，これまでの研究課題に対して結果をさらに改良させるとともに，グラフ連結度に関する近似アルゴリズムに対する統一的なアプローチの確立やデタッチメント操作の化学グラフ推定問題への新しい応用などの発見をすることができた．このほか，食品の袋詰め問題やファイアウォール高速化のためのデータ構造など応用に直結する課題についても成果を収めることができた．今年度得られた研究成果を以下の七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
- 食品の袋詰め問題
- 最長路問題
- グラフのランキング問題
- ファイアウォール高速化のためのデータ構造

2 グラフ連結度問題

2.1 ネットワーク設計

与えられた連結度要求を満たすネットワークを構築する問題は，代表的なネットワーク設計問題の一つであり，これまでも活発に研究されている．我々は，2 節点間の枝連結度要求 $r : \binom{V}{2} \to \mathbb{Z}_+$ と節点の次数の上下限 $a, b : V \to \mathbb{Z}_+$ を満たす

コスト最小多重グラフを構築するネットワーク設計問題を考え，r, a, b がある条件を満たすいくつかの場合に対して近似アルゴリズムを与えた．ただし，ここでコストは各枝に対して定義されており，三角不等式を満たすとしている．

具体的には，任意の $u, v \in V$ に対し $r(u, v) \geq 2$ が成立し，さらに，次数上限 a が常に一定値であるか，もしくは次数下限が $b(v) = 0$, $v \in V$ を満たすときに対し，我々は $(2+2/\min_{u,v} r(u, v))$-近似アルゴリズムを与えた．また，任意の $u, v \in V$ に対し $r(u, v) = k$ であり，$a(v) = b(v)$, $v \in V$ の場合に対しては，k が偶数の場合近似度 2.5，k が奇数の場合近似度 $2.5 + 1.5/k$ を達成するアルゴリズムを提案した (T. Fukunaga, H. Nagamochi, Network design with edge-connectivity and degree constraints, Proceedings of Fourth Workshop on Approximation and Online Algorithms, Lecture Notes in Computer Science, vol. 4368, pp. 188-201, 2006)．

これらのアルゴリズムでは，枝遊離操作と呼ばれるグラフ変形法が使用されている．これは，巡回セールスマン問題や枝連結度増大問題などのネットワーク設計問題において従来より広く応用されている操作であり，遊離される枝が接続する節点を除く 2 節点間の枝連結度を保存するための条件が，Lovasz や Mader らによって得られている．我々は，この結果をさらに強め，任意の 2 節点間の局所枝連結度を保存するための条件について考察し，それに基づいて，上記のアルゴリズムを設計している．また，この枝遊離操作に関する結果を元に，ディタッチメントと呼ばれる枝遊離操作を一般化した操作が，局所枝連結度を保存するための新たな条件を求めることにも成功した．

より柔軟なネットワーク設計を行う上で，従来の連結度を拡張することは重要である．我々は，従来は 2 節点間に対して定義されるこのが多い枝連結度を，節点集合族 $\mathcal{V} \subseteq 2^V$ に対して拡張した定義を与えた．その上で，無向グラフ $G = (V, E)$ 上の節点集合族 $\mathcal{V}_1, \ldots, \mathcal{V}_m \subseteq 2^V$ を連結にする G の部分グラフ（集合連結グラフ）のうちコスト最小のものを求める問題を提案した．この問題はシュタイナー森問題，集合シュタイナー木問題，1-NA-連結度増大問題などを含んでいる．我々は，Chekuri, Shepherd によって得られたシュタイナー森の詰め込み定理を集合連結グラフの詰め込みへと一般化することで，上記の問題に対して，2α-近似アルゴリズムを導いた (T. Fukunaga, H. Nagamochi, The set connector problem in graphs, Proceedings of the 12th Conference on Integer Programming and Combinatorial Optimization, (発表決定))．ここで，$\alpha = \max_{1 \leq i \leq m}(\sum_{X \in \mathcal{V}_i} |X|) - 1$ である．

2.2 デタッチメントを利用した化学グラフの推定アルゴリズム

多重グラフ G のある節点 s におけるデタッチメント (detachment) とは，節点 s をいくつかの複製に分離し，s の接続枝は複製のどれかに付け直す操作，あるいはそうして得られたグラフを指す．複製節点をすべて 1 点に縮約すれば元のグラフ G に戻る．例えば，図 2.1(a) のグラフ G の節点 s を 3 個の節点 s^1, s^2, s^3 に分離して得られたデタッチメント H を図 2.1(b) に示す．デタッチメントは通常，節点数を増やしてしまう．連結度に関する定理を帰納法で証明する場合に，連結度を保存したままグラフを小さくする変形操作が望まれる．図 2.1(c) のように，s を次数 2 の節点と次数 $d_G(s)-2$ の節点の二つに分離するデタッチメントにおいて，この次数 2 の節点を無視して接続する 2 本の枝を 1 本の枝に置き換える (図 2.1(c) では e_1, e_3 を uv を直結する 1 本の枝と見る)．枝遊離 (edge-splitting) と呼ばれるこの変形操作では，節点数は変わらず枝のみが 1 本減る．s の接続枝の対をうまく選ぶと枝対の枝遊離後も $V - \{s\}$ 上の枝連結度が保持されることが知られており，s の次数が偶数ならそのような枝遊離を $d_G(s)/2$ 回行い，次数 0 となった s を削除することで，枝連結度を保

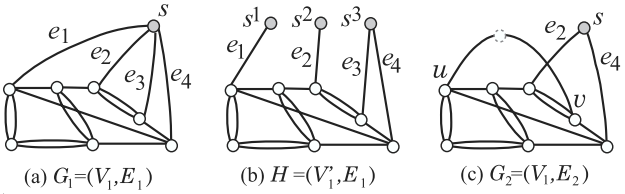
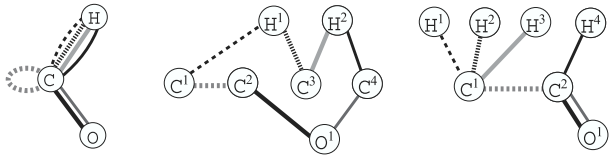


図 2.1: (a) 多重グラフ $G = (V, E)$; (b) s におけるデタッチメント H; (c) s における枝遊離操作.



(a) G=(V,E) (b) H'=(W',E) (c) H=(W,E)

図 2.2: (a) 多重グラフ $G = (V, E)$; (b) 単純閉路のデタッチメント $H' = (W', E)$; (c) 次数制約を満たし自己ループを持たない連結なデタッチメント $H = (W, E)$.

持したまま 1 節点減らす帰着が得られる．s の接続枝を完全に枝遊離する問題も MAO のみを使い $O(mn+n^2 \log n)$ 時間で解くことを示した (Hiroshi Nagamochi, A fast edge-splitting algorithm in edge-weighted graphs, Inst. Electron. Inform. Comm. Eng. Trans. Fundamentals, E89-A, pp. 1263-1268, 2006)．枝遊離問題が解けると $2k$ 枝連結グラフの k 弧連結有向グラフへの向き付け問題も効率よく解くことができる．

以下では，連結性を保存するデタッチメントを考える．よく知られているように多重グラフ G が一筆書きを持つ必要十分条件は「各節点の次数が偶数であり，かつ連結であること」である (起点に戻る一筆書きとする)．一筆書きは枝を 1 度のみ通過するが各節点 v は $d_G(v)/2$ 回通過する．よって一筆書きの定理は次のようにも述べることができる.「各次数が偶数である連結グラフ G には，各節点 v を $d_G(v)/2$ 個の次数 2 の複製に分離するデタッチメント H の中で，連結性を保存するものが存在する (故に単純閉路になるものが存在する).」例えば，図 2.2(a) のグラフ G の一筆書きに対応する単純閉路のデタッチメントが図 2.2(b) の H' ように得られる．一般に，k 枝連結性を保存するデタッチメントが存在する必要十分条件は Nash-Williams (1985) により与えられている (ただし，次数の指定も可能であるが自己ループを含み得る).

本研究では，連結性を保存するデタッチメントが化合物の構造推定へ応用できることを示した (Hiroshi Nagamochi, A detachment algorithm for inferring a graph from path frequency, The Twelfth Annual International Computing and Combinatorics Conference (COCOON'06) Taipei, Taiwan, August 15-18, 2006, Lecture Notes in Computer Science, Editors: Danny Z. Chen, D. T. Lee, vol. 4112, pp. 274–283, 2006). 元素の組成のみを表す化学式から異性体を列挙する問題は Pólya らにより既に研究されているが，ここでは，結合の組合せまで指定された次のような問いを考える.「C2 個，O1 個，H4 個の 7 個の原子からなり，原子間の結合が CH 結合 4 通り，CO 結合 2 通り，CC 結合 1 通りと指定された化合物が (組合せの意味で) 存在するか？」

この種のグラフ推定問題は最近，創薬への応用等から研究が盛んとなっている．一般的に 3 原子以上の結合列の指定も扱うと問題は NP 困難になるが，幸いにも 2 原子の結合列の問題はデタッチメントの概念を使って解けることを示した．上の例を解く場合には，元素の種類 C,O,H ごとにひとつの節点を用意し，結合を指定する 7 本の枝でこれらを結んだ「種グラフ」を図 2.2(a) の G のように構成する．すると，問題は，C を 2 個に，H を 4 個に分離する G のデタッチメント H の中で，連結で自己ループがなく，かつ，節点の次数が対応する元素の原子価となっているものを求めることと等価になる．図 2.2(c) に条件を満たすデタッチメント H の例を示す．Nash-Williams の結果は自己ループを許すものなので直接は利用できないため，自己ループを禁止する設定で連結なデタッチメントが存在するための必要十分条件を導いた．これに基づきグラフ推定問題を解く $O(n^{3.5} + m)$ 時間アルゴリズムを得ることができる．

2.3 最小深さ根付き生成木についての研究

根付き生成木のうち深さを最小にするものを求める問題は，P2P ネットワークで（テレビ）放送を行うことに関連している．P2P ネットワークは，視聴者同士で放送コンテンツを中継することにより，放送を行うサーバの負荷を軽減でき，ネットワーク障害につよい方法とされている．しかし，あらゆる可能性の中，どのように中継すればよいかが問題になる．特に中継を行うノードには，一般に中継できる数（子ノードの数）に上限がある．

この問題をグラフの用語を用いてモデル化すると，次のようになる．すなわち,「枝に重み付きの完全有向グラフ，その中にあるソースノード，及び各

ノードの次数制約が与えられた時に，このソースノードを根とする有向生成木の中で，各ノードにおいて出次数制約を満たして，深さ深さ（根から葉への最長路長）が最小となるものを見つけよ」．この問題について，重み無しの場合や次数制約が無限大の場合は簡単に解けるが，一般に実行可能解を探すのも NP 完全である．そこで近似アルゴリズムの適用が考えられるが，本研究では，いくつかの戦略を提案し，性能を考察してみた．

戦略１は，ダイクストラ法の改造版と言え，根からスタートし，ラベルを更新する際に次数制約もチェックする．満たしていたら問題ないが，満たさなかったら次善のノートを採用する．戦略２は，次数制約が１以上のノードだけで部分木を欲張り法で作り，最後に次数０のノードを欲張り法で加える．戦略３は，次数制約の大きい順にノードをグループに分けて,（同じ次数制約のノードが同じグループになる,）順に欲張り法で適用する．

ランダムなグラフでテストしてみた結果，多くの場合は戦略２のほうがよい結果を出していることが確認できた．しかし，時間の関係でその理由の究明までは至らず，今後厳密解を求め，さらにグラフの密度，欲張り法の精度などとの関係を考察して予定である．

3　図形処理に関する問題

3.1　グラフ描画問題

２項関係の数学的な表現であるグラフを平面に埋め込む研究は，古くは Fáry (1948) の直線描画や Tutte (1960) の凸描画に起源を持ち，1970 年代には VLSI の設計への応用に関して，グラフの矩形描画に関する研究が盛んに進められてきた．その後，計算機の普及に伴い，有限要素法における曲面の三角形分割，建築物における部屋の間取設計，フローチャートの図示，地理情報の表現などあらゆる分野において情報を効率よく分かりやすく可視化することが要求されてきており，その中でグラフの自動描画はコア技術として大変重要な役割を果たしている．可視化の目的も含めたグラフの自動描画に関する研究は 1980 年頃から始まり，様々描画表現法とその数学的構造，計算の複雑さの研究が押し進められている．特に，平面上に枝を交差なく埋め込めることのできるグラフは平面グラフと呼ばれ，その描画問題は最も基本的な研究課題であり，本研究でもこの問題を取り扱う．平面グラフ $G = (V, E, F, c_0)$ は，節点集合 V，枝集合 E，内面集合 F および外面 c_0 により定められる．ここで，本研究で扱う平面グラフのクラスを３通り与えておく．分割グラフとは，長方形を垂直または水平な直線で再帰的に分割することで得られる分割図において，各交点と四隅に節点を置いて作られる平面グラフ（この再帰的な分割過程を表す 2 分木 T を分割木という）．長方形グラフとは，外周と内面をすべて長方形で描くことのできる平面グラフ，平面３連結グラフとは，任意の２節点とそれらに接続する枝を取り除いても連結である平面グラフと定義される．

平面グラフ $G = (V, E, F, c_0)$ の直交描画 (orthogonal drawing) とは，外面 c_0 は長方形で，各枝が垂直直線分，水平直線分の系列で描かれたものである．特に，自然数 k に対し，各内面 $c \in F$ の持つ多角形の角の個数が高々k 個であるとき k 角形直交描画という．例えば，長方形描画（各内面が長方形であるもの）は，どの面の角数も４個以下であるので, 4 角形直交描画とみなせる．さらに，G の各内面 $c_i \in F$ に面積 $a_i > 0$ が与えられた平面グラフを面積付き平面グラフと呼ぶ．面積付き平面グラフ G に対する直交描画とは，さらに，各内面 c_i の面積を a_i と等しくさせるものである．

本研究では，各内面に描画において実現すべき面積が指定されている平面グラフに対する直交描画法を取り扱う．これまで面積付き平面グラフの描画法については，Rahman らが分割グラフのある特別な場合に対して示した 8 角形直交描画の結果しか知られていなかったが，本研究では上記で示した三つのクラスすべてに対して面積付きの描画に関する以下の結果を導いた (Akifumi Kawaguchi, Hiroshi Nagamochi, Orthogonal drawings for plane graphs with specified face areas, The 4th Annual Conference on Theory and Applications of Models of Computation (TAMC07) Shanghai, China, 2007（発表決定)).

1. 面積付き分割グラフは必ず 10 角形直交描画を持つ．分割木と外周の長方形およびその 4 頂点に対応する節点が与えられたとき，描画

を線形時間で求めることができる．

2. 面積付き長方形グラフは必ず 18 角形直交描画を持つ．外周の長方形およびその 4 頂点に対応する節点が与えられたとき，描画を $O(|V|\log|V|)$ 時間で求めることができる．

3. 最大次数が 3 である面積付き 3 連結グラフは必ず 46 角形直交描画を持つ．描画を $O(|V|\log|V|)$ 時間で求めることができる．

4. 最大次数が 4 であり，外周上に次数 4 の節点がない面積付き 3 連結グラフは，全体の描画の線分数は高々$6n$ 本であり，かつ，各内面 $c \in F$ を高々$10p_c+46$ 個の角を持つ多角形による直交描画を持つ (p_c は内面 c の周上にある次数が 4 の節点数)．描画を $O(|V|\log|V|)$ 時間で求めることができる．

結果１の証明の概略を示す．入力として面積付き分割グラフ G，四隅の節点が定められた G の外周となる長方形 P_r，および G を与える再帰的分割を記述する分割木 T が与えられている．分割木 T に対する深さ優先探索順に，P_r を再帰的に分割して分割線上の節点を適切な位置に固定していくことで G 全体の描画を構築する．ここで，指定された面積を実現するためには，分割部分で直線分かあるいは縦・横・縦または横・縦・横の直交線分列を用いる必要が生じる．しかし，適当に分割部分を固定したのでは後で処理する内面の角数が定数個に収まらなくなる．これを回避するために，用いる線分の長さを適切な範囲に制御することが必要になるが，これを再帰的に正しく実行させるために２０種類に上る動作ルールを抽出することで解決した．その結果，計算の進行中に決して 10 角形を超える内面が形成されないことを示すことができた．

結果 2-4 については，適当なグラフの変形を導入することで分割グラフに変換して，結果１を利用することで導かれる．

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，本研究で得られた非凸多角形を容器内に最適に配置する解法について報告する (Takashi Imamichi, Hiroshi Nagamochi, Mutsunori Yagiura, An iterated local search algorithm based on nonlinear programming for the irregular strip packing problem, Proc. of International Symposium on Scheduling 2006 (ISS2006) July 18-20, 2006 in Arcadia Ichigaya, Tokyo, Japan, pp. 132–137, 2006)．

多角形の詰め込み問題とは, 平面図形の配置問題の一つであり，与えられた複数の多角形を長方形の形状をした容器の内部に互いに重複しないように配置する問題である．ここで，容器の幅は固定で長さだけが可変であり，問題の目的は多角形を重複なく配置するために必要な容器の長さを最小にすることである．本研究では, 多角形としては非凸であるものを許し，各多角形の配置の仕方においてはいくつかの決められた方向への回転も取り扱う．この非凸多角形の詰め込み問題は, 紙や布などのロール状の材料を用いる産業などにおいて広い応用をもつ問題であるが, 凸形状のみの多角形で回転がない場合でも NP 困難であることが知られている．

非凸多角形を取り扱う問題に対しては比較的最近になり研究成果が報告されている．Gomes と Oliveira は, 線形計画法に基づく多角形の圧縮操作と分離操作を焼き鈍し法と組合せた手法を提案している．Burke 他は, bottom-left-fill というヒューリスティクスとタブー探索法を組合せた手法を提案した．Egeblad 他は, 1 枚の多角形を他の多角形との重複面積が最小となる場所を効率的に見つけるアルゴリズムを考案し, それと誘導反復局所探索法を組合せた手法を提案した．非凸多角形の詰め込み問題に対する代表的なベンチマークの問題例に対しては, 現在 Gomes と Oliveira や Egeblad 他が最良の解を与えている．

本研究では, 従来手法よりも高性能なアルゴリズムの開発を目指し，容器の長さを変化させる部分と, 固定された容器の中で多角形を再配置する部分に分け，再配置の問題の解決に非線形計画法の最適化手法を取り入れることを考えた．再配置に対しては，重複多角形の分離操作と多角形の配置交換操作を用意し，ここで，重複多角形の分離問題を制約なし非線形計画問題として解く点が特

徴である．再配置に対する 2 種類の操作に基づく反復局所探索法を提案し，最終的には, その反復局所探索法のアルゴリズムと容器の長さを変化させるアルゴリズムを組み合せることで, 詰め込み問題に対するアルゴリズムを構築した. 代表的なベンチマーク問題例に対して計算実験を行い，いくつかの問題例に対して最良解を更新するなど提案法の高い性能を確認することができた.

多角形の再配置では, 容器の幅と長さをともに固定した容器の中で, 多角形同士の重複と容器からの突出の度合を最小化することを考える. 本研究では, 与えられた多角形の配置に対して, 各多角形を同時に微小に動かすことで重複を減らす分離操作を提案している．この分離操作は, 与えられた配置を初期解として, 重複度最小化問題を準ニュートン法で解き, 局所解を得ることで実現している．重複度最小化問題は, 各多角形の容器からの突出度と多角形同士の重複度の総和を目的関数して, この目的関数を最小化する制約なし非線形計画問題として定式化した．さらに, 突出度を表す関数を多角形と容器の外部領域の最小分離距離の 2 乗, 重複度を表す関数を 2 枚の多角形の最小分離距離の 2 乗としてやることで, 効率的に目的関数とその勾配を計算できることを示した. 最小分離距離とは, 2 枚の重複する多角形を平行移動させて分離する際に必要となる最小の距離である.

目的関数と勾配の計算には No-fit polygon という多角形の詰め込み問題でしばしば用いられるデータ構造を利用している. 多角形 A に対する多角形 B の No-fit polygon は, 多角形 A の参照点を原点に固定した時に, 多角形 B が A と重なるか接するような多角形 B の参照点の位置の集合で定義される．No-fit polygon を用いることで, 面と面が重複するかどうかの判定を, 点が面の中に入っているかを判定することで行うことができ効率的である. また, 最小分離距離が, 多角形の参照点から No-fit polygon の境界までの最小の距離に等しく, その性質を利用して目的関数とその勾配の計算を行う.

多角形の交換操作は, 他の多角形が固定されているとする条件の下で, 1 枚の多角形を他の多角形との重複度および容器からの突出度が最小となる点を探すヒューリスティクスを用いて実現した. このヒューリスティクスは No-fit polygon を用いて実現していて, 一般には重複度最小の点は見つけられないが, 重複度と突出度の総和が 0 になる点がある場合には, 必ずその点を見つけることができることを示した.

準ニュートン法に基づく分離操作と, 多角形の交換操作を組合せて, 重複度最小化問題に対する反復局所探索法のアルゴリズムを構築した. 反復局所探索法とは, 過去の探索で得られた最も良い解を暫定解として持ち, この暫定解にランダムな摂動を加えたものを初期解として局所探索を行い, 得られた局所解が暫定解よりも良ければ暫定解の更新を行うという一連の操作を繰り返すメタ戦略である. 提案手法の重複度最小化問題に対する反復局所探索法のアルゴリズムは, 多角形の交換操作を暫定解に対する摂動として, 多角形の分離操作を局所探索として用いた.

そして, 重複度最小化問題に対する反復局所探索法のアルゴリズムを用いて, 詰め込み問題に対するアルゴリズムを構築した. 実行可能な配置に対して, まず容器の長さを短縮する. そうすると, いくつかの多角形が容器から突出するので, 重複度最小化問題に対する反復局所探索法のアルゴリズムを呼んで重複を減少させる．もしも, 多角形の重複や突出が全くない配置が得られた場合は, さらに容器の長さを短かくし, さもなければ, 容器の長さを伸ばして実行可能解を探索する. 以上を繰り返すというのが, 提案手法の概要である.

計算実験では, まず, パラメータがアルゴリズムに与えている影響を調べている． 容器の長さを変化させる割合や方向, 初期解の生成法, 反復局所探索法の終了条件などについて計算実験を行い, これらのパラメータがアルゴリズムに与える影響はあまり大きくなく, 提案手法が比較的ロバストであることを確認した. そして, この実験からアルゴリズムのパラメータを決めてやり, 代表的なベンチマークの問題例に対して実験を行った. 現在最良の解を与えている Gomes と Oliveira や Egeblad 他と比べて, 全体の計算時間は同等もしくは短くなるようにして実験を行い, 提案手法がいくつかの問題例で新しい最良解を与え, また残りの問題例に対しても同等の結果を得ていることを観察した.

充填率は大きい程良く, 太文字で書かれている数字は四つの中で最良の値を表している. 提案手

法は 15 題の問題例の中の 5 題のベンチマーク問題例に対して最良解を与えている.

本研究では, 重複度最小化問題に対して, 非線形計画法に基づく多角形の分離操作を構成し, さらに分離操作を多角形の交換操作と組合せることで反復局所探索法のアルゴリズムを構築した. このアルゴリズムを基に, 容器の長さを最小化する詰め込み問題のアルゴリズムを作り, 体表的なベンチマーク問題例に対する計算実験を通して有効性を示した.

4　スケジューリング問題

スケジューリングの問題としては，配送スケジューリング問題と機械スケジューリング問題を取り上げ，それらに対する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おける離接グラフのように，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．スケジューリングでは，ジョブの処理順序が主要な決定事項の一つとなるが，優れたアルゴリズムを実現するためには，その設計においてグラフ構造の特徴を十分に考慮することが必要である．

4.1　配送スケジューリング

配送スケジューリング問題は，与えられたグラフの各節点に置かれたジョブの集合からなる．例えば，収集すべき品物や検査すべき施設のような作業を受ける対象がジョブに相当する．各ジョブは準備時間，処理時間および納期によって特徴づけされる．一台あるいは複数台の搬送車が，与えられたグラフ上を移動しながら，ジョブの処理をおこなう．なお，複数の搬送車を扱う場合，理論モデルではそれらの性能は等しいとされることが多い．問題の目的は，定められた目的関数に対して，その値を最小化（あるいは最大化）するような搬送車のジョブ処理スケジュールを求めることである．配送スケジューリング問題は，製造業やサービス業において解決されなければならない最重要課題の一つである．

エレベータ搭乗機能を備えた自律的搬送ロボットや海岸線に沿って移動する輸送船など，グラフをパス構造グラフや木構造グラフに限っても，配送スケジューリング問題は，さまざまな実際の場面に現れる．そのため，この十数年，パス構造グラフや木構造グラフにおける配送スケジューリングについて，問題の計算の複雑さや近似可能性などの理論研究が精力的に続けられている．

本年度は，パス構造グラフを直進する一台の搬送車の選択的配送スケジューリング問題を考察した．グラフの節点に置かれた各ジョブには，処理時間と納期が定められている．ジョブの準備時間制約はない，すなわち，準備時間はすべて 0 と仮定する．搬送車が与えられたパス構造グラフの一方の端点を出発し，各枝をちょうど一度だけ訪れるならば，すなわち，単純に一方の端点からもう一方の端点まで移動するならば，そのスケジュールは直進スケジュールと呼ばれる．本研究では，搬送車が直進スケジュールに従って移動する場合の配送スケジューリング問題を取り扱った．この問題では，搬送車は，任意の節点でそのジョブの処理を行わずに，次の節点に進むことを許される．ただし，処理しなかったジョブについては違反コスト α (≥ 1) が要求される．よって，各ジョブに対して，搬送車にそれを処理させるかどうか，を決めるという選択が必要である．搬送車によって処理を受けたジョブに対しては，その処理完了時刻が納期より早ければ，違反コストは要求されない．しかし，処理完了時刻が納期を越えたならば，単位違反コスト（すなわち，違反コスト 1）を支払わなければならない．最小化すべき目的関数は，すべてのジョブについての総違反コストである．これを納期違反コストと呼ぶ．本研究では，この配送スケジューリング問題に対して，動的計画法に基づく厳密アルゴリズムを与えた（軽野・永持・内田，パス構造グラフにおける納期違反コスト最小化選択的配達スケジューリング，日本機械学会論文集（C 編），vol. 73，pp. 911-918，2007）．違反コスト α が正整数で与えられるならば，このアルゴリズムは $O(n^2 \min\{\alpha, n\})$ で動作する．

なお，この問題は，納期遵守ジョブ数最大化の一般化になっている．なぜならば，$\alpha = 1$ のとき，納期違反コストの最小化と納期遵守ジョブ数の最大化は等価だからである．納期遵守ジョブ数最大

化問題を解くことにより，直面する納期制約がどれくらい厳しいのかについて，一つの数値指標が得られる．また，鉛直方向に延びるパスやループ状経路（デポを仮想的に二つの端点に分けることで，パス構造グラフに置き換え可能となるケースは珍しくない）を移動する搬送車（あるいは人）にとっては，駆動系の能力特性（あるいは安全性の確保，運転者の負担軽減）のために，与えられた経路を双方向に移動することがしばしば困難である．

この成果の一つの応用例として，複数台の搬送車に対して，走行区間分離型の直進スケジュールを求めるということが挙げられる．これには，先行研究の成果である二段構え動的計画法 (Y. Karuno, H. Nagamochi, 2-approximation Algorithms for the Multi-vehicle Scheduling Problem on a Path with Release and Handling Times, Discrete Applied Mathematics, vol. 129, pp. 433-447, 2003) を適用し，提案アルゴリズムを内側に組み込めばよい．

ところで，これまでの配送スケジューリング問題に対する理論研究で，納期違反規準の目的関数を扱ったものは多くない．燃料費や移動距離の削減よりも，販売の機会損失を削減する方が，企業の競争力の強化にとって重要である場合も少なくない．納期違反規準の配送スケジューリング問題に対して，実用的なアルゴリズムの開発だけでなく，理論研究のさらなる進展が望まれる．

4.2 機械スケジューリング

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があるが，本年度はタイムラグを考慮したメイクスパン最小化 2 機械フローショップのある一般化問題を扱った．

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) スケジューリングでもしばしば扱われる．タイムラグを考慮した古典的 2 機械フローショップ問題に対しては，$O(n \log n)$ 時間で動作する 2 倍近似アルゴリズム（M. Dell'Amico, Operations Research, vol. 44, pp. 777–787, 1996），$O(n \log n)$ 時間で動作する 11/6 倍近似アルゴリズム（Y. Karuno, H. Nagamochi, Lecture Notes in Computer Science 2906, Springer, pp. 309–318, 2003），多項式時間近似スキーム（L. A. Hall, Mathematical Programming, vol. 82, pp. 175–190, 1998）が知られている．

近似比を 2 倍未満にするための一つの重要なポイントは，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．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 11/6 倍近似アルゴリズムでは，ある適切な閾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．理論的な近似精度の観点からは多項式時間近似スキーム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閾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．しかし，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ので，本年度はこの方面からのアプローチを検討した．本研究では，有限容量の中間ステーションを持つ 2 機械フローショップ型 FMC のメイクスパン最小化問題に対して，遺伝アルゴリズムと閾値による非順列スケジュールで構成される解空間と順列スケジュールで構成される解空間の探索切替を適用したヒューリスティックを提案した（Y. Karuno, T. Uehata, Y. Hata, H. Kise, A Non-permutation Heuristic for the Two-machine Flow-shop Scheduling Problem with a Bounded Intermediate Station, ASME/ISCIE 2006 International Symposium on Flexible Automation, pp. 496-502, 2006）．そして，計算実験を行い，閾値による探索切替が有効に機能していることを確かめた．

また，同様の枠組みを重み付き完了時間和問題にも適用した（T. Uehata, J. Li, Y. Karuno, H. Kise, Heuristic for a Non-permutation Two-machine Flow-shop Scheduling of Minimizing Total Weighted Completion Time, ASME/ISCIE 2006 International Symposium on Flexible Automation, pp. 503-509, 2006）．しかし，この問題においては，閾値による探索切替が有効に機能した問題例とそうでない問題例が観察された．タイムラグを考慮した古典的 2 機械フローショップでは，重み付き完了時間和最小化問題に対する理論的成果が殆どなく，この問題の特徴を生かした閾値の導出方法を検討することが課題として残った．

5　食品の袋詰め問題

ピーマン，スナック菓子，冷凍食品，漬物などの食品を袋詰めするために，数十台程度のホッパからなる自動組合せ計量装置がしばしば用いられる．n 台のホッパを備えた自動組合せ計量装置の仕組みはつぎのように説明することができる．なお，ここでいう品物とは，ピーマン 1 個や一掴みのポテトチップスなど，一つのホッパに一回あたり投入される食品を指す．まず，未計量の品物がベルトコンベヤなどによって自動組合せ計量装置まで運ばれてくる．運ばれてきた品物は，一つずつ空いているホッパに投入され，その重量が測定される．なお，すべてのホッパが埋まっているとき，品物の投入は中断される．測定値は，自動組合せ計量装置の演算部へ送られる．演算部は，ホッパに入っている n 個の品物からいくつかを選んで，一袋あたりの目標重量を下回らない範囲で（お客からのクレームを避けるために，実際に袋に詰められた品物の合計重量が，袋の表示量より少なくなることがあってはならない），それらの合計重量を目標重量にできるだけ近づけなければならない．選ばれた品物はホッパから排出され，袋に詰められて自動組合せ計量装置から搬出される．空となったホッパには新たな品物が投入され，それらの重量が測定される．そして，演算部によって再びいくつかの品物が選ばれて，次の袋詰めがおこなわれる．

毎回の袋詰めにおける品物の選択の問題は，0-1 変数 x_i $(i = 1, 2, \ldots, n)$ によって，ホッパ i の品物が袋に入れられるのか，あるいはそうでないのかを表せば，一つの離散最適化問題として定式化できる．問題の最も重要な目的は，前述の通り，選んだ品物の合計重量が目標重量を下回らず，かつ，最もそれに近くなるようにすることである．合計重量を目標重量に近づけるだけならば，この袋詰めの問題はよく知られた 0-1 ナップサック問題として定式化できる．しかし，品物の重量のみを考慮して袋詰めをおこなった場合，いつまでも選ばれないで長期間ホッパに滞留する品物を発生させる可能性がある．自動組合せ計量装置では品物として食品を扱っているので，例えば，空気に触れている時間が短ければ短いほど良いといった食品を扱うような場合は，合計重量を目標重量に近づける過程で，ホッパにおける滞留期間に対しても何らかの最適化を図ることが望ましい．

本研究では，ホッパ内の品物に対して，それが選ばれなかった袋詰めの回数に応じて，品物の優先度というパラメータを定義した．そして，合計重量が目標重量を下回らない範囲で，最もそれに近くなる品物の組合せを計算するが，そのような組合せが複数あるときには，それらのうちで優先度の合計値が最も大きくなる品物の組合せを最適解とする袋詰め最適化問題を考察した．本研究では，これを 0-1 変数を用いた辞書式二目的離散最適化問題として定式化し，動的計画法に基づいた厳密アルゴリズムを提案した（軽野・永持・大嶋，食品の袋詰め最適化問題に対する動的計画法，日本機械学会論文集（C 編），vol. 72，pp. 1390-1397，2006）．また，計算実験を行って，繰り返し行われる一連の袋詰め操作における提案アプローチの滞留期間短縮効果を確かめた．

6　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ことが知られている最長路問題は, 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のが現状である.

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することはせず, 厳密解法の開発をも目指す.

6.1 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. この方向の研究としてはこれまで, わずかに木に対する線形時間の厳密アルゴリズムが知られる程度であり, これ以外に主たる先行研究は見当たらなかった. そこでわれわれは, それ以外にも自明でないグラフクラスに対して効率的に (たとえば多項式時間で) 最長路を計算するアルゴリズムの開発を試みた.

まずはじめに, 木の最長路を求める線形時間アルゴリズムである Dijkstra のアルゴリズムを一般化し, その正当性を示した上で, 木と同様の構造を持ついくつかのグラフクラスに対して, 効率的な最長路計算アルゴリズムを提案した. 具体的には, 点・枝重みつき木, ブロックグラフ, カクタスに対するそれぞれ $O(n), O(n+m), O(n^2)$ 時間アルゴリズムなどである (ただし n は点数, m は枝数). このとき, これらのアルゴリズムのうちの一部は, 必ずしも理論上達成可能な最速のアルゴリズムであるとは限らないが, ここでは Dijkstra のアルゴリズム (の一般化) の適用を目的としている.

つづいて, 最長路問題が自明ではないグラフクラスとして, 自然な交モデルを持ついくつかのクラスを提案し, それらに対する最長路問題を解決している. 具体的には, 包含関係の意味で interval graph と threshold graph の中間に位置する proper interval biconvex graph ならびに interval biconvex graph とよぶクラスを新たに導入し, 前者に対する $O(n^3(m+n\log n))$ 時間の計算量を持つアルゴリズムを設計している.

これらの結果ならびに考察は, いまだに未解決である interval graph に対する最長路問題を解く大きな手がかりになると考え, 次年度以降の解決が期待できる.

6.2 分枝限定法によるアプローチ

同じく, 困難な組合せ最適化問題に対する厳密解法の一つに, 分枝限定法がある. 分枝限定法は, 本質的には実行可能解の全探索であり, 理論的には必ずしも指数時間の計算量を改善できるものではないが, その探索を効果的に行うことにより, 計算時間を劇的に減少できる場合がある.

いま最長路問題は組合せ最適化問題 (整数計画問題) として定式化することができ, 厳密解法としての分枝限定法を適用することができる. このとき, もちろん汎用の整数計画問題ソルバを用いて解くアプローチもあり得るが, 本研究では入力のグラフが疎であるとき, そのグラフの構造的な特徴を利用して最長路を効率的に求める専用解法の開発を目指す.

より具体的には, われわれはまず最長路問題を始点固定最長路問題に帰着する. すなわち, 始点固定最長路問題とは路の始点を制約条件に加えたものであり, 最長路問題の最適解は, すべての点を始点とする始点固定最長路問題を解くことで求められる. そこで本研究では, 始点固定最長路問題の厳密解を, 分枝限定法を用いて計算する方法を設計する.

本年度はその端緒として, 入力となるグラフの 2 連結成分分解を行い, 2 連結成分とカット点を利用して部分的な最長路の情報 (最適値および最適解) を点の情報として集約・保持することを行っ

た．この処理により, 対象とするグラフの規模を縮小させるだけではなく, 分枝の際に重複して現れる最長路計算を省略することができ, それらによる分枝限定法の効率化を達成することが期待できる． その結果, CPU: Celeron 1GHz, メモリ: 256MB の計算機環境で, 100 枝 (58 点) 程度の比較的疎なグラフに対して, 約 1 秒程度の計算時間で最長路を計算することが可能となっている．

今後の方針として, 部分問題となるグラフが最長路を容易に計算できるようなグラフクラス (たとえば固定木幅のような) に属することが判定できたときには, 計算の上ただちにその問題を終端させることが挙げられる．この特殊な場合として, 隣接点数が 2 以下の点を効率的に処理した上で最長路を計算する方法を考案しており, これにより生成される部分問題数を減らし, 全体の計算が高速化できるのではないかと考えている．

7 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, それればかりではなく, 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/枝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．

8 ファイアウォール高速化のためのデータ構造

ファイアウォールは，通信ネットワーク上に流れるパケット（宛先と送信元のアドレス等のような制御情報を付加されたデータ通信の単位）に対し，与えられたルール（パケットの特徴とそれに対応する動作の対を記述したもの）に従って通過させたり破棄したりするようなネットワーク機器またはソフトウェアのことを言う．このようなファイアウォールは，インターネットなど，安全な通信を必要とするネットワークにとって必須なものになっており，Unix/Linux はもちろん，Windows でも XP SP2 から有効になった．また，専用装置や商用ソフトウェアも開発されている．

一方，通信中のパケットに対して照合作業（フィルタリングともいう）を行うため，ファイアウォールの導入によって通信の遅延が増大してしまう問題がある．従って，ファイアウォールの最適化，すなわち平均処理時間の最小化が望まれる．特に近年，物理的に高速な通信が可能になった一方，ファイアウォールによる遅延が目立つようになった．そのため，ここ数年ファイアウォールの高速化に関する研究が注目されるようになった．本研究は，従来の研究成果を踏まえ，ファイアウォー

ルの処理に適したルール集合の構造（線形木と呼ぶ）を提案する．以下具体的に説明する．

ファイアウォールのルールは，「パターン」部と「アクション」部からなっており，パターン部はパケットの特徴（アドレスやサービスなど）を記述し，アクション部は，パターン部に合致するパケットに対して行なわれる操作（通過や破棄など）を規定している．現行のファイアウォールは，合致するパターンが見つかるまで与えられたルールの線形リストを順番に調べていく，という単純な線形探索法を採用している．従って，リストの後ろにあるルールほど，それに合致するパケットの処理時間が長い．容易にわかるように，ルール間に先行制約（順番を変えたら異なる機能を持つファイアウォールになってしまうようなルール集合）がなければ，合致パケットの出現確率の高い順にルールを並べ変えると平均処理時間が最小化されるが，先行制約がある場合は，最適なルールの順番を求めるのが NP 困難となる．さらに後者に対して，いくつのヒューリスティックが提案されている．実データを用いてシミュレーション実験をした結果，おおむね数十パーセントの改善が報告されている．

先行研究は，ルールの記述を変えないという前提において行われている．本研究は，さらに平均処理時間を短縮するために，機能を壊さずにルールの記述を変える方法を検討してみた．その結果として階層的なルールの記述法を提案する．すなわち，従来の線形リストの代わりに「木構造」を用いて，木のノードは，あるグループのパケットの特徴（例えばアドレス空間やサービス番号等）を表し，各ルールは，木の根ノードからある葉までのパスに対応する．ただし，一つのノードは複数個の部分ルールを含むことが可能とし，その場合は，含まれる部分ルールの集合に対して従来通りの線形探索を行う．これは，単語を調べる辞書の構造に似ていて，線形リストより効率がよい．

今回の成果として，実際のファイアウォールを調べ，サービス番号によって第一レベルの木ノードを作るのが有効であることが分かった．さらに本学情報学科の場合をシミュレーションし，従来提案された高速化の手法で改善できないが，二レベルの木構造を組み合わせることにより平均処理時間が大幅に短縮できることを示した (L. Zhao, A. Shimae, H. Nagamochi, Linear-tree rule structure for firewall optimization, 6th IASTED Intl. Conf. on Communications, Internet, and Information Technology, July 2-4, 2007)．ただし，シミュレーションでは先行制約なしの場合のみを考えたが，今後の課題として，先行制約ありの場合についてさらに詳しく考察していくことが考えられる．

9 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近似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，ファイアウォール問題など多岐にわたる．今年度は，グラフ連結度に関する近似アルゴリズムに対し，set connector を定義し，広いクラスの問題を統一的に扱える理論的な基盤を得ることができた．また，これまでグラフ連結度を保存するグラフ変形操作として知られていたデタッチメント操作が化学グラフ推定問題を解くアルゴリズムの設計へ利用できることを発見した．デタッチメント操作は理論的には興味深い結果であったが，これまで実用的な問題への応用は知られていなかったことから今回の結果により，今後，さらにグラフ理論の実用問題への新しい適用が期待される．図形処理に関する問題としては，昨年度に引き続き，グラフ描画問題，図形の充填問題を取り扱った．今年度は，グラフ描画問題において，面 (face) の面積が指定された問題を取り扱い，必要な描画の複雑度に対する理論的な解析を行った．図形の充填問題においては，これまでの矩形ピースの配置問題を拡張した非凸図形の配置問題を取り扱い，非線形最適化問題を利用するアルゴリズムを設計した．また，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についても昨年度からの研究を継続し，新たな知見を積み重ねることができた．この他，食品の袋詰め問題やファイアウォール高速化のためのデータ構造など応用に直結する課題についても研究を行い一定の成果を収めることができた．

次年度は，これまで得られた種々の結果において，再度アルゴリズムがうまく設計されているメカニズムを詳細に検討し，アルゴリズムの一般化

や新しい問題への適用を進める予定である.

研究業績一覧

学術論文

1. Takuro Fukunaga, Hiroshi Nagamochi:
"Approximating minimum cost multigraphs of specified edge-connectivity under degree bounds", Journal of the Operations Research Society of Japan, (掲載決定).
概要: In this paper, we consider the problem of constructing a minimum cost graph with a specified edge-connectivity under a degree constraint. For a set V of vertices, let $r : \binom{V}{2} \to \mathbb{Z}_+$ be a connectivity demand, $a : V \to \mathbb{Z}_+$ be a lower degree bound, $b : V \to \mathbb{Z}_+$ be an upper degree bound, and $c : \binom{V}{2} \to \mathbb{Q}_+$ be a metric edge cost. The problem (V, r, a, b, c) asks to find a minimum cost multigraph $G = (V, E)$ with no self-loops such that $\lambda(u, v) \geq r(u, v)$ holds for each vertex pair $u, v \in V$ and $a(v) \leq d(v) \leq b(v)$ holds for each vertex $v \in V$, where $\lambda(u, v)$ (resp., $d(v)$) denotes the local-edge-connectivity between u and v (resp., the degree of v) in G. We reveal several conditions on functions r, a, b and c for which the above problem admits a constant-factor approximation algorithm. For example, we give a $(2 + 2/k)$-approximation algorithm to (V, r, a, b, c) with $r(u, v) \geq 2$, $u, v \in V$ and a uniform $b(v)$, $v \in V$, where $k = \min_{u,v \in V} r(u, v)$. To design the algorithms in this paper, we derive new results on splitting and detachment, which are graph transformations to split vertices into several copies of them while preserving edge-connectivity.

2. Hiroshi Nagamochi, Kengo Iwata, Toshimasa 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 $[1, |V|]$.

3. Peter Eades, Qingwen Feng, Xuemin Lin, Hiroshi 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 visu-

alization, 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.

4. Toshimasa Ishii, Hiroshi Nagamochi, Toshihide 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 $n = |V|$.

5. Hiroshi 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.

6. Toshimasa Ishii, Shigeyuki Yamamoto, Hiroshi Nagamochi:
"Augmenting forests to meet odd diameter requirements", Discrete Optimization, 3, 2006, 154-164.
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.

7. Hiroshi Nagamochi, Taizo Kawada:
"Minmax subtree cover problem on cacti", Discrete Applied Mathematics, 154, 1254-1263, 2006.
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.

8. 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", 日本機械学会論文集 (C 編), 72, 1390-1397, 2006.
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.

9. Hiroshi Nagamochi:
"A fast edge-splitting algorithm in edge-weighted graphs", Inst. Electron. Inform. Comm. Eng. Trans. Fundamentals, E89-A, 1263-1268, 2006.
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.

10. Hiroshi Nagamochi:
"Sparse connectivity certificates via MA orderings in graphs", Discrete Applied Mathematics, 154, 2411-2417, 2006.
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.

11. Hiro Ito, Hiroshi Nagamochi:
"Two equivalent measures on weighted hypergraphs", Discrete Applied Mathematics, 154, 2330-2334, 2006.
概要: Let H be a hypergraph with a node set $N = \{0, 1, \ldots, n-1\}$. Given an n-gon P with a vertex set $\{x_0, x_1, \ldots, x_{n-1}\}$ in the plane, we define a projection of H on P by mapping each node $i \in N$ to the vertex x_i and drawing each hyperedge e in H by the convex hull of the vertices x_j such that j is an end node of e, where we say that e covers every point p in the interior of the convex hull. We say that H *covers* P if any point in the interior of P is covered by at least one hyperedge of H. In this paper, we consider the problem of determining whether or not a given hypergraph H with an ordered node set covers *every* convex polygon and give a polynomial time algorithm to the problem. We also consider the problem of computing the smallest thickness of a point p (i.e., the smallest number of hyperedges that cover p) in a projection of H on all n-gons P, and solve the problem by a reduction to the maximum flow problem.

12. Hiroshi Nagamochi:
"Packing soft rectangles", International Journal of Foundations of Computer Science, 17, 1165-1178, 2006.
概要: Let R be a rectangle with given area $a(R)$, height $h(R)$ and width $w(R)$, and $r_1, r_2, \ldots, r_n$ be n soft rectangles, where we mean by a soft rectangle a rectangle r whose area $a(r)$ is prescribed but whose aspect ratio $\rho(r)$ is allowed to be changed. In this paper, we consider the problem of packing n soft rectangles $r_1, r_2, \ldots, r_n$ into R. We prove that, if $a(R) \geq \sum_{1 \leq i \leq n} a(r_i) + 0.10103 a_{max}$ and $a_{max} \leq 3(\min\{h(R), w(R)\})^2$ hold for $a_{max} = \max_{1 \leq i \leq n} a(r_i)$, then these n soft rectangles can be packed inside R so that the aspect ratio of each rectangle r_i is at most 3.

13. Yoko Kamidoi, Noriyoshi Yoshida, Hiroshi Nagamochi:
"A deterministic algorithm for finding all minimum k-way cuts", SIAM J. Computing, 36, 943-955, 2006.
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. Our algorithm is a divide-and-conquer method based on 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. With a slight modification, the algorithm can find all minimum k-way cuts in $O(n^{4k/(1-1.71/\sqrt{k})-16})$ time.

14. Hiroshi Nagamochi, Yuusuke Abe:
"An approximation algorithm for dissecting a rectangle into rectangles with specified areas", Discrete Applied Mathematics, 155, 523-537, 2007.
概要: Given a rectangle R with area α and a set of n positive reals $A = \{a_1, a_2, \ldots, a_n\}$ with $\sum_{a_i \in A} a_i = \alpha$, we consider the problem of dissecting R into n rectangles r_i with area a_i $(i = 1, 2, \ldots, n)$ so that the set $\mathcal{R}$ of resulting rectangles minimizes an objective function such as the sum of the perimeters of the rectangles in $\mathcal{R}$, the maximum perimeter of the rectangles in $\mathcal{R}$, and the maximum aspect ratio of the rectangles in $\mathcal{R}$, where we call the problems with these objective functions PERI-SUM, PERI-MAX and ASPECT-RATIO, respectively. We propose an $O(n \log n)$ time algorithm that finds a dissection $\mathcal{R}$ of R that is a 1.25-approximate solution to PERI-SUM, a $\frac{2}{\sqrt{3}}$-approximate solution to PERI-MAX, and has an aspect ratio at most

$\max\{\rho(R), 3, 1 + \max_{i=1,\ldots,n-1} \frac{a_{i+1}}{a_i}\}$, where $\rho(R)$ denotes the aspect ratio of R.

15. Hiroshi Nagamochi, Yoko Kamidoi:
"Minimum cost subpartitions in graphs", Information Processing Letters, 102, 79-84, 2007.
概要: Given an edge-weighted graph $G = (V, E)$, a subset $S \subseteq V$, an integer $k \geq 1$ and a real $b \geq 0$, the minimum subpartition problem asks to find a family of k nonempty disjoint subsets $X_1, X_2, \ldots, X_k \subseteq S$ with $d(X_i) \leq b$, $1 \leq i \leq k$ so as to minimize $\sum_{1 \leq i \leq k} d(X_i)$, where $d(X)$ denotes the total weight of edges between X and $V - X$. In this paper, we show that the minimum subpartition problem can be solved in $O(mn + n^2 \log n)$ time. The result is then applied to the minimum k-way cut problem and the graph strength problem to improve the previous best time bounds of 2-approximation algorithms for these problems to $O(mn + n^2 \log n)$.

16. Hiroshi Nagamochi, Katsutoshi Kuroya:
"Drawing c-planar biconnected clustered graphs", Discrete Applied Mathematics, (掲載決定).
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.

17. Hiroshi Nagamochi, Kohei Okada:
"Approximating the minmax rooted-tree cover in a tree", Information Processing Letters, (掲載決定).
概要: Given an edge-weighted rooted tree T and a positive integer p ($\leq n$), where n is the number of vertices in T, we cover all vertices in T by a set of p subtrees each of which contains the root r of T. The minmax rooted-tree cover problem asks to find such a set of p subtrees so as to minimize the maximum weight of the subtrees in the set. In this paper, we propose an $O(n)$ time $(2 + \varepsilon)$-approximation algorithm to the problem, where $\varepsilon > 0$ is a prescribed constant.

18. Hiroshi Nagamochi:
"Computing a minimum cut in a graph with dynamic edges incident to a designated vertex", Inst. Electron. Inform. Comm. Eng. Trans. Fundamentals, (掲載決定).
概要: We consider an edge-weighted graph G with a designated vertex v_0 such that weights of edges incident to v_0 may increase or decrease. We show that, with an $O(mn+n^2 \log n)$ time preprocessing, a minimum cut of the current G can be computed in $O(\log n)$ time per update of weight of any edge $\{v_0, u\}$.

19. Takuro Fukunaga, Hiroshi Nagamochi:
"Approximating a generalization of metric TSP", Inst. Electron. Inform. Comm. Eng. Trans. Fundamentals, (掲載決定).
概要: We consider a problem for constructing a minimum cost r-edge-connected multigraph in which degree $d(v)$ of each vertex $v \in V$ is specified. In this paper, we propose a 3-approximation algorithm for this problem under the assumption that edge cost is metric, $r(u, v) \in \{1, 2\}$ for each $u, v \in V$, and $d(v) \geq 2$ for each $v \in V$. This problem is a generalization of metric TSP. We also propose an approximation algorithm for the digraph version of the problem.

20. Takuro Fukunaga, Hiroshi Nagamochi:
"Generalizing the induced matching by edge capacity constraints", Discrete Optimization, (掲載決定).
概要: Given an edge-weighted graph, the induced matching problem is an edge packing problem, which asks to find a maximum weight edge set such that every edge in the graph is adjacent to at most one edge in the set. In this paper, we generalize this problem by introducing edge capacities and propose an approximation algorithm to the problem. The analysis of this algorithm is based on a relationship between two polytopes for an LP relaxation of the above problem and the capacitated b-matching problem.

21. Ehab Morsy, Hiroshi Nagamochi:
"Approximation algorithms for multicast routings in a network with multi-sources", IEICE Transactions, (掲載決定).
概要: We consider the capacitated multi-source multicast tree routing problem (CMMTR) in an undirected graph $G = (V, E)$ with a vertex set V, an edge set E and an edge weight $w(e) \geq 0$, $e \in E$. We are given a source set $S \subseteq V$ with a weight $g(e) \geq 0$, $e \in S$, a terminal set $M \subseteq V - S$ with a demand function $q : M \to R^+$, and a real number $\kappa > 0$, where $g(s)$ means the cost for opening a vertex $s \in S$ as a source in a multicast tree. Then the CMMTR asks to find a subset $S' \subseteq S$, a partition $\{Z_1, Z_2, ..., Z_\ell\}$ of M, and a set of subtrees $T_1, T_2, ..., T_\ell$ of G such that, for each i, $\sum_{t \in Z_i} q(t) \leq \kappa$ and T_i spans $Z_i \cup \{s\}$ for some $s \in S'$. The objective is to minimize the sum of the opening cost of S' and the constructing cost of $\{T_i\}$, i.e., $\sum_{s \in S'} g(s) + \sum_{i=1}^{\ell} w(T_i)$, where $w(T_i)$ denotes the sum of weights of all edges in T_i. In this paper, we propose a $(2\rho_{\rm UFL} + \rho_{\rm ST})$-approximation algorithm to the CMMTR, where $\rho_{\rm UFL}$ and $\rho_{\rm ST}$ are the best achievable approximation ratios for the uncapacitated facility location and Steiner tree problems, respectively. When all terminals have unit demands, we give a $((3/2)\rho_{\rm UFL} + (4/3)\rho_{\rm ST})$-approximation algorithm.

22. Toshimasa Ishii, Hitoshi Fujita, Hiroshi Nagamochi:
"Minimum cost source location problem with local 3-vertex-connectivity requirements", Theoretical Computer Science, (掲載決定).
概要: Let $G = (V, E)$ be a simple undirected graph with a set V of vertices and a set E of edges. Each vertex $v \in V$ has a demand $d(v) \in Z_+$ and a cost $c(v) \in R_+$, where Z_+ and R_+ denote the set of nonnegative integers and the set of nonnegative reals, respectively. The source location problem with vertex-connectivity in a given graph G asks to find a set S of vertices minimizing $\sum_{v \in S} c(v)$ such that there are at least $d(v)$ pairwise vertex-disjoint paths from S to v for each vertex $v \in V - S$. It is known that if there exists a vertex $v \in V$ with $d(v) \geq 4$, then the problem is NP-hard even in the case where every vertex has a uniform cost. In this paper, we show that the problem can be solved in polynomial time.

23. Yoshiyuki Karuno, Hiroshi Nagamochi, Jun Uchida:
"Selective vehicle scheduling on paths with a due date involving criterion", 日本機械学会論文集 (C 編), (掲載決定).
概要: In this paper, we consider a selective scheduling problem of minimizing a due date involving criterion for a single uncapacitated vehicle. Let $G = (V, E)$ be a path with a set $V = \{v_i \mid i = 1, 2, \ldots, n\}$ of vertices and a set $E = \{\{v_i, v_{i+1}\} \mid i = 1, 2, \ldots, n-1\}$ of edges. The vehicle is initially situated at v_1. There is a job i at each vertex $v_i \in V$, which has its own handling time h_i and due date d_i. Travel

times $w_{i,i+1}$ of the vehicle are associated with edges $\{v_i, v_{i+1}\} \in E$. A schedule of the vehicle is called *1-way* if it visits every edge $\{v_i, v_{i+1}\}$ exactly once, that is, it simply moves from v_1 to v_n on G. In this paper, the vehicle is assumed to move according to a 1-way schedule. But a choice still remains for each job whether it is processed at the time of the visit, since a certain penalty α (≥ 1) is required if some job is not processed by the vehicle. If a processed job i is completed by its due date d_i, no penalty is required. Othewise, the unit penalty is paid. The objective is to minimize the total penalty over all n jobs. We show that, if α is given as a positive integer, the selective vehicle scheduling problem can be solved in polynomial time by a dynamic programming approach.

24. Yoshitaka Nakao, Hiroshi Nagamochi:
"A DP-based heuristic algorithm for the discrete split delivery vehicle routing problem", Journal of Advanced Mechanical Design, Systems, and Manufacturing, (掲載決定).
概要: We propose a fast and effective algorithm for a discrete-type split delivery vehicle routing problem. The feature of this problem is that a demand for each customer is large and each demand consists of a set of items whose sizes are various. A demand of a customer can be serviced by more than one vehicle, while each item is serviced by exactly one vehicle. We propose a DP-based construction algorithm to solve the problem. The effectiveness of our algorithm is supported by eraborated route evaluation scheme to select a route. We report computational results for real-world instances and also artificial instances. The results show that our algorithm is fast and highly effective comparing to representative construction algorithms and representative improvement heuristics for the VRP and the SD-VRP algorithm.

25. Ryuhei Uehara, Yushi Uno:
"On Computing Longest Paths in Small Graph Classes", International Journal of Foundations of Computer Science, (掲載決定).
概要: The longest path problem is the one that finds a longest path in a given graph. While the graph classes in which the Hamiltonian path problem can be solved efficiently are widely investigated, few graph classes are known to be solved efficiently for the longest path problem. Among those, for trees, a simple linear time algorithm for the longest path problem is known. We first generalize the algorithm, and show that the longest path problem can be solved efficiently for some tree-like graph classes by this approach. We next propose two new graph classes that have natural interval representations, and show that the longest path problem can be solved efficiently on these classes.

26. Kazuhisa Makino, Yushi Uno, Toshihide Ibaraki:
"Minimum Edge Ranking Spanning Trees of Split Graphs", Discrete Applied Mathematics, 154, pp. 2373–2386, 2006.
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. Takuro Fukunaga, Hiroshi Nagamochi:
"Some theorems on detachments preserving local-edge-connectivity", Proceedings of 5th Cracow Conference on Graph Theory, Electronic Notes in Discrete Mathematics, 24, pp. 173-180, 2006.
概要: A detachment operation transforms a given graph by splitting some vertices into several their copies while maintaining the original set of edges, whose end vertices may change after the operation. A graph obtained by such an operation is called a detachment of the graph. Although necessary and sufficient conditions for a graph to have a k-edge-connected detachment are known, it is left open to derive a necessary and sufficient condition for a graph to admit a detachment which has a specified local-edge-connectivity. In this paper, we show our recent results on related problems such as the problem of finding an Eulerian detachment of a graph that maximizes the local-edge-connectivity, and the problem of splitting a vertex s into two vertices of degree 3 and $d(s) - 3$ preserving the local-edge-connectivity.

2. Takuro Fukunaga, Hiroshi Nagamochi:
"Network design with edge-connectivity and degree constraints", Proceedings of Fourth Workshop on Approximation and Online Algorithms, Lecture Notes in Computer Science, 4368, pp. 188-201, 2006.
概要: We consider the following network design problem; Given a vertex set V with a metric cost c on V, an integer $k \geq 1$, and a degree specification b, find a minimum cost k-edge-connected multigraph on V under the constraint that the degree of each vertex $v \in V$ is equal to $b(v)$. This problem generalizes metric TSP. In this paper, we propose that the problem admits a ρ-approximation algorithm if $b(v) \geq 2$, $v \in V$, where $\rho = 2.5$ if k is even, and $\rho = 2.5 + 1.5/k$ if k is odd. We also prove that the digraph version of this problem admits a 2.5-approximation algorithm and discuss some generalization of metric TSP.

3. Takuro Fukunaga, Hiroshi Nagamochi:
"The set connector problem in graphs", Proceedings of the 12th Conference on Integer Programming and Combinatorial Optimization, (発表決定).
概要: Given a graph $G = (V, E)$ with an edge cost and families $\mathcal{V}_i \subseteq 2^V$, $i = 1, 2, \ldots, m$ of disjoint subsets, an edge subset $F \subseteq E$ is called a set connector if, for each $\mathcal{V}_i$, the graph $(V, F)/\mathcal{V}_i$ obtained from (V, F) by contracting each $X \in \mathcal{V}_i$ into a single vertex x has a property that every two contracted vertices x and x' are connected in $(V, F)/\mathcal{V}_i$. In this paper, we introduce a problem of finding a minimum cost set connector, which contains several important network design problems such as the Steiner forest problem, the group Steiner tree problem, and the NA-connectivity augmentation problem as its special cases. We derive an approximate integer decomposition property from a fractional packing theorem of set connectors, and present a strongly polynomial 2α-approximation algorithm for the set connector problem, where $\alpha = \max_{1 \leq i \leq m}(\sum_{X \in \mathcal{V}_i} |X|) - 1$.

4. Takashi Imamichi, Mutsunori Yagiura, Hiroshi Nagamochi:
"An iterated local search algorithm based on nonlinear programming for the irregular strip packing problem", The 19th conference of the European Chapter on Combinatorial Optimization (ECCO XIX) and the International Symposium on Combinatorial Optimisation 2006 (CO 2006), 2006.
概要: The irregular strip packing prob-

lem is a combinatorial optimization problem that asks to place a set of 2-dimensional polygons within a rectangular container so that no two polygons overlap each other and no polygon protrudes from the container, where each polygon is not necessarily convex. The container has a fixed width, while its length can change so that all polygons are placed in it. The objective is to find a layout that minimizes the length of the container. This problem has many applications in material industry such as paper and textile industries, where raw materials are usually given in rolls. We propose a new separation algorithm based on nonlinear programming, which moves all polygons simultaneously and minimizes the total amount of overlap and protrusion. We formulate the overlap minimization problem as an unconstrained nonlinear programming problem in which we define the amount of overlap by using the penetration depth. We show that it is possible to compute the amount of overlap and its gradient efficiently, and applies the quasi-Newton method to the overlap minimization problem as our separation algorithm. We also propose an algorithm that swaps two polygons in a sophisticated way; it tries to find their positions with the least overlap among the vertices and the edge intersections of the no-fit polygons

5. Seok-Hee Hong, Hiroshi Nagamochi:
"Convex drawings with non-convex boundary", 32nd International Workshop on Graph-Theoretic Concepts in Computer Science (WG 2006) Bergen, Norway June 22-24, 2006, Lecture Notes in Computer Science, 4271, pp. 113–124, 2006.
概要: In this paper, we study a new problem of finding a convex drawing of graphs with a *non-convex* boundary. It is proved that every triconnected plane graph whose boundary is fixed with a star-shaped polygon admits a drawing in which every inner facial cycle is drawn as a convex polygon. Such a drawing, called an *inner-convex drawing*, can be obtained in linear time.

6. Mutsunori Yagiura, Toshihide Ibaraki, Takashi Imamichi, Y. Koga, Hiroshi Nagamochi, K. Nonobe:
"Efficient branch-and-bound algorithms for weighted MAX-2-SAT", The 21st European Conference on Operational Research (EURO XXI) Reykjavik, Iceland, July 2-5, 2006, 2006.
概要: Given a set of clauses on 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. We propose branch-and-bound algorithms for solving weighted MAX-2-SAT exactly. Our algorithms feature 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.

7. Takuro Fukunaga, Hiroshi Nagamochi:
"Approximating minimum cost multigraphs of specified edge-connectivity under degree bounds", Proceedings of the 9th Japan-Korea Joint Workshop on Algorithm and Computation (WAAC06) July 4-5, 2006, Hokkaido University, Sapporo, Japan, pp. 25–32, 2006.
概要: In this paper, we consider the problem of constructing a minimum cost graph with a specified edge-connectivity under a degree constraint. For a set V of vertices, let $r : \binom{V}{2} \to \mathbb{Z}_+$ be a connectivity demand, $a : V \to \mathbb{Z}_+$ be a lower capacity, $b : V \to \mathbb{Z}_+$ be an upper capacity and $c : \binom{V}{2} \to \mathbb{Q}_+$ be a metric edge cost. The problem (V, r, a, b, c) asks to find a minimum cost

multigraph $G = (V, E)$ with no self-loops such that $\lambda(u, v) \geq r(u, v)$ for each pair $u, v \in V$ and $a(v) \leq d(v) \leq b(v)$ for each $v \in V$, where $\lambda(u, v)$ (resp., $d(v)$) denotes the local-edge-connectivity between u and v (resp., the degree of v) in G. We reveal several conditions on functions r, a, b and c for which the above problem admits a constant-factor approximation algorithm. For example, we give a $(2 + 1/\lfloor k/2 \rfloor)$-approximation algorithm to (V, r, a, b, c) with $r(u, v) \geq 2$, $u, v \in V$ and a uniform $b(v)$, $v \in V$, where $k = \min_{u,v \in V} r(u, v)$. To design the algorithms in this paper, we use our new results on edge-splitting and detachment, which are graph transformations to split vertices while preserving edge-connectivity.

8. Seok-Hee Hong, Hiroshi Nagamochi:
"Convex drawings of hierarchical plane graphs", 17th Australasian Workshop on Combinatorial Algorithms (AWOCA 2006) Uluru, NT, Australia, July 13-16, 2006, 2006.
概要: This paper proves that every internally triconnected hierarchical plane graph with the outer facial cycle drawn as a convex polygon admits a *convex* drawing. We present an algorithm which constructs such a drawing. This extends the previous known result that every hierarchical plane graph admits a *straight-line* drawing.

9. Takashi Imamichi, Hiroshi Nagamochi, Mutsunori Yagiura:
"An iterated local search algorithm based on nonlinear programming for the irregular strip packing problem", Proc. of International Symposium on Scheduling 2006 (ISS2006) July 18-20, 2006 in Arcadia Ichigaya, Tokyo, Japan, pp. 132–137, 2006.
概要: The irregular strip packing problem is a combinatorial optimization problem that asks to place a set of 2-dimensional polygons within a rectangular container so that no two polygons overlap each other and no polygon protrudes from the container, where each polygon is not necessarily convex. The container has a fixed width, while its length can change so that all polygons are placed in it. The objective is to find a layout that minimizes the length of the container. This problem has many applications in material industry such as paper and textile industries, where raw materials are usually given in rolls. We propose a new separation algorithm based on nonlinear programming, and an algorithm that swaps two polygons in a sophisticated way; it tries to find their positions with the least overlap. We incorporate these algorithms as components in an iterated local search algorithm for the overlap minimization problem and then develop an algorithm for the irregular strip packing problem using the iterated local search algorithm. Computational comparisons on representative instances disclose that our algorithm is competitive with other existing algorithms. Moreover, our algorithm updates several best known results.

10. Toshihide Ibaraki, Akihiro Ishikawa, Hiroshi Nagamochi, Koji Nonobe, Mutsunori Yagiura:
"An iterated local search algorithm for the multi-resource generalized assignment problem with flexible assignment cost", Proc. of International Symposium on Scheduling 2006 (ISS2006) July 18-20, 2006 in Arcadia Ichigaya, Tokyo, Japan, pp. 160–165, 2006.
概要: We propose an iterated local search algorithm for the multi-resource generalized assignment problem (MRGAP) with flexible assignment cost. This problem generalizes the MRGAP so that the assignment cost function defined for each agent can be in any form. While this flexibility achieves a wide applicability, the computation of the assignment cost can be computationally expensive, Our algorithm features

two types of oracles to evaluate this cost approximately; i.e., quick-evaluation oracle and accurate-evaluation oracle. In our computational experiments on the parallel machine scheduling and the capacitated vehicle routing, the algorithm combining two oracles performs well and is sometimes competitive with other existing algorithms tailored for the specific problem.

11. Yashitaka Nakao, Hiroshi Nagamochi:
"A DP-based heuristic algorithm for the discrete split delivery vehicle routing problem", Proc. of International Symposium on Scheduling 2006 (ISS2006) July 18-20, 2006 in Arcadia Ichigaya, Tokyo, Japan, pp. 42–47, 2006.
概要: We propose a construction algorithm for a discrete-type split delivery vehicle routing problem. In this problem, delivery goods for a customer consist of a set of items. Each customer can be visited more than once, while each item is serviced by exactly one vehicle. This algorithm builds routes sequentially by iterating constructing routes by dynamic programming and selecting one. In order to select a route, this algorithm uses an elaborate evaluate function that estimates residual distance of routes to service all unrouted items. Experimental results on real-world and artificial instances are reported.

12. Ehab Morsy, Hiroshi Nagamochi:
"An improved approximation algorithm for capacitated multicast routings in networks", Proc. of International Symposium on Scheduling 2006 (ISS2006) July 18-20, 2006 in Arcadia Ichigaya, Tokyo, Japan, pp. 12–17, 2006.
概要: Let $G = (V, E)$ be a complete graph such that each edge $e \in E$ is weighted by nonnegative real $w(e)$. Let s be a vertex designated as a source, k be a positive integer, and $S \subseteq V$ be a set of terminals. The capacitated multicast routing problem (CMRP) asks to find a partition $\{Z_1, Z_2, ..., Z_\ell\}$ of the terminal set S and a set of subtrees $T_1, T_2, ..., T_\ell$ of G such that Z_i consists of at most k terminals and each T_i spans $Z_i \cup \{s\}$. The objective is to minimize $\Sigma_{i=1}^{\ell} w(T_i)$, where $w(T_i)$ is defined to be the sum of weights of all edges in T_i. In this paper, we propose a $(3/2 + (4/3)\rho)$-approximation algorithm to the CMRP, where ρ is the best achievable approximation ratio for the Steiner tree problem. Our approximation improves the previous best ratio for the case of $S = V$ from 2.9 to $17/6 \simeq 2.83$.

13. Hiroshi Nagamochi:
"A detachment algorithm for inferring a graph from path frequency", The Twelfth Annual International Computing and Combinatorics Conference (COCOON'06) Taipei, Taiwan, August 15-18, 2006, Lecture Notes in Computer Science, Editors: Danny Z. Chen, D. T. Lee, 4112, pp. 274–283, 2006.
概要: Inferring a graph from path frequency has been studied as an important problem which has a potential application to drug design. Given a multiple set g of strings of labels with length at most K, the problem asks to find a vertex-labeled graph G that attains a one-to-one correspondence between g and the set of sequences of labels along all paths of length at most K in G. In this paper, we prove that the problem with $K = 1$ can be reduced to a problem of finding a connected and loopless detachment, based on which an efficient algorithm for solving the problem is derived. Our algorithm also solves the problem even for the case where any vertex with the same label is required to have a degree specified for the label.

14. Mariko Sakashita, Kazuhisa Makino, Hi-

roshi Nagamochi, Satoru Fujishige:
"Minimum transversals in posi-modular systems", ESA 2006 14th Annual European Symposium on Algorithms 11-13 September 2006 ETH Zurich, Zurich, Switzerland, Lecture Notes in Computer Science, 4168, pp. 576–587, 2006.
概要: Given a system (V, f, d) on a finite set V consisting of two set functions $f : 2^V \to \mathbb{R}$ and $d : 2^V \to \mathbb{R}$, we consider the problem of finding a set $R \subseteq V$ of the minimum cardinality such that $f(X) \geq d(X)$ for all $X \subseteq V - R$, where the problem can be regarded as a natural generalization of source location problems and external network problems in (undirected) graphs and hypergraphs. We give an interesting structural characterization of minimal deficient sets of (V, f, d). We show that all such sets form a tree hypergraph if f is posi-modular and d is modulotone (i.e., each nonempty subset X of V has an element $v \in X$ such that $d(Y) \geq d(X)$ for all subsets Y of X that contain v), and that conversely any tree hypergraph can be represented by minimal deficient sets of (V, f, d) for a posi-modular function f and a modulotone function d. By using this characterization, we present a polynomial-time algorithm if f is in addition submodular and d is given by either $d(X) = \max\{p(v) \mid v \in X\}$ for a function $p : V \to \mathbb{R}_+$ or $d(X) = \max\{r(v, w) \mid v \in X, w \in V - X\}$ for a function $r : V^2 \to \mathbb{R}_+$. Our result provides first polynomial-time algorithms for source location problem in hypergraphs and external network problems in graphs and hypergraphs. We also show that the problem is intractable, even if f is submodular and $d \equiv \mathbf{0}$.

15. Kouji Hirata, Takahiro Matsuda, Hiroshi Nagamochi, Tetsuya Takine:
"Contention-Free λ-Planes in Optically Burst-Switched WDM", IEEE GLOBECOM 2006 Advanced Technologies and Protocols for Optical Networks, 27 November - 1 December 2006, San Francisco, California, USA, 2006.
概要: This paper proposes a contention-free burst scheduling scheme in optically burst-switched WDM networks. We construct contention-free wavelength planes (λ-planes) by assigning dedicated wavelengths to each ingress node. Bursts are transmitted to their egress nodes on λ-planes, along routes forming a spanning tree. As a result, contention at intermediate core nodes is completely eliminated, and contention at ingress nodes is resolved by means of electric buffer. This paper develops a spanning tree construction algorithm, aiming at balancing input loads among output ports at each ingress node. Further a wavelength assignment algorithm is proposed, which is based on the amount of traffic lost at ingress nodes. We show that the proposed scheme can decrease the burst loss probability drastically, even if traffic intensities at ingress nodes are different.

16. Morihiro Hayashida, Tatsuya Akutsu, Hiroshi Nagamochi:
"A novel clustering method for analysis of biological networks using maximal components of graphs", The Fifth Asia-Pacific Bioinformatics Conference, APBC2007, Hong Kong, pp. 257–266, 2007.
概要: This paper proposes a novel clustering method for analyzing biological networks. In this method, each biological network is treated as an undirected graph and edges are weighted based on similarities of nodes. Then, maximal components, which are defined based on edge connectivity, are computed and the nodes are partitioned into clusters by selecting disjoint maximal components. The proposed method was applied to clustering of protein sequences and was compared with conventional clustering

methods. The obtained clusters were evaluated using P-values for GO (GeneOntology) terms. The average P-values for the proposed method were better than those for other methods.

17. 上道 明生, 宇野 裕之, 永持 仁:
"最長路問題に対する 2 連結成分分解にもとづく分枝限定法による厳密解法", 日本オペレーションズ・リサーチ学会 秋季研究発表会 アブストラクト集, 2006.
概要: 最長路問題とは, 枝に重みのあるグラフを入力とし, グラフのすべての単純路の中で最長のものを出力する問題であり, NP 困難な問題として知られている. 類似の問題に巡回セールスマン問題 (TSP) があり, 現実の問題への応用も多く盛んに研究されているが, 一般に実行可能解であるハミルトン閉路が必ず存在する完全グラフのような密なグラフを対象にすることが多い. これに対して, 必ずしもハミルトン閉路が存在するとは限らない疎なグラフでは, 現実にはできる限り多くの点を通るような路 (最長路) が代替の解として必要になることも多い. 本稿では, 分枝限定法を用いて最長路問題を解く. とくに, 入力のグラフが疎であるとき, その特性を利用して最長路を効率的に求める方法を示している.

18. Yushi Uno, Yoshinobu Ota, Akio Uemichi and Motohide Umano:
"Mining communities and detecting link farms in the Web by isolated cliques", Proc. 2nd International Conference on Knowledge Engineering and Decision Support (ICKEDS06), pp. 179–187, 2006.
概要: Web structure mining is a research area that aims to find hidden communities that share common interests in specific topics in the Web, clustering the Web, and so on, by focusing on the link structure among web pages. The structure of the Web is generally viewed as the webgraph, and communities or their cores are supposed to constitute dense subgraphs. Thus, structure mining can be realized by enumerating those substructures. As an example of such substructures, a biclique model proposed by Kleinberg is well-known, however, not so many effective results have been seen so far that found useful information. In this paper, we afresh pick up some candidate substructures, including bicliques, and attempt to find useful information from the real web data. Especially, we exploit isolated cliques for our experiments of structure mining. As a result, we discovered that most of isolated cliques in the Web correspond to menu structures and are inherent in single domains, and that isolated cliques can be quite useful for detecting harmful link farms. On the other hand, although the number is not necessarily large, we discovered that isolated cliques that lie over multiple domains sometimes imply useful communities. By these observations, we can confirm the validity of isolated clique as candidate substructure for structure mining. We also propose, through our experiments, the undirected webgraph and the isolated clique contracted webgraph.

19. Yushi Uno, Yoshinobu Ota, Akio Uemichi and Motohide Umano:
"Web Structure Mining by Isolated Stars", Proc. 4th WAW Conference, 2006.
概要: Web structure mining is a research area that aims to find hidden communities in the Web, and so on, by focusing on the webgraph. In this paper, by observing the webgraph, we newly identify a frequent substructure and define it as an isolated star (i-star). We propose an efficient enumeration algorithm of i-stars, and try structure mining by enumerating them from the real web data. As a result, we observed that most of i-stars correspond to index structures in single domains, while some of them are verified to stand for useful communities, which implies the validity of i-stars as candidate

substructure for structure mining.

20. Akifumi Kawaguchi, Hiroshi Nagamochi: "Orthogonal drawings for plane graphs with specified face areas", The 4th Annual Conference on Theory and Applications of Models of Computation (TAMC07) Shanghai, China, 2007, (発表決定).
概要: We consider orthogonal drawings of a plane graph G with specified face areas.For a natural number k, a k-gonal drawing of G is an orthogonal drawing such that the outer cycle is drawn as a rectangle and each inner face is drawn as a polygon with at most k corners whose area is equal to the specified value. In this paper, we show that several classes of plane graphs have a k-gonal drawing with bounded k; A slicing graph has a 10-gonal drawing, a rectangular graph has an 18-gonal drawing and a 3-connected plane graph whose maximum degree is 3 has a 34-gonal drawing. Furthermore, we showed that a 3-connected plane graph G whose maximum degree is 4 has an orthogonal drawing such that each inner facial cycle c is drawn as a polygon with at most $10p_c + 34$ corners, where p_c is the number of vertices of degree 4 in the cycle c.

21. Liang Zhao, Akira Shimae, Hiroshi Nagamochi:
"Linear-tree rule structure for firewall optimization", 6th IASTED Intl. Conf. on Communications, Internet, and Information Technology, July 2-4, 2007, (発表決定).
概要: Given a list of filtering rules with individual hitting probabilities, it is known that the average processing time of a linear-search based firewall can be minimized by searching rules in some appropriate order. This paper proposes a new yet simple technique called the *linear-tree* rule structure. It utilizes an advanced feature of modern firewalls, the "goto"-like statement, to transform given rule list into a rule set that is functionally equivalent to the original but organized in a more efficient tree-like structure. We show it is possible to achieve much more performance improvement than the previous rule-reordering based studies. To demonstrate this, we study by both simulation experiment and test with real firewall.

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

‖ 小樽商科大学商学部社会情報学科
〒 047-8501 小樽市緑 3 丁目 5 番 21 号
ishii@res.otaru-uc.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。

I. 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

II. 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

平成１８年度に得られた主な成果は以下のとおりである。

I. 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

テキストマイニングに関して，新聞記事コーパスから交通事故原因表現を抽出する手法を提案した．テキストコーパスから所要の表現を抽出するタスクは，テキストマイニングにおける重要課題のひとつである。従来，個々の応用ごとに，人手で作成したルールに基づくか、または，学習データを人手で用意し，教師あり学習を用いて情報を抽出していた。本研究では、まず、「が原因」などの少数の手がかり表現を修飾している、「居眠り運転」などの事故原因表現を獲得する．次に，これらの事故原因表現が多く修飾してい表現を手がかり表現として取得するというプロセスをくり返すという、ブートストラップ的手法を提案した．この手法は，最初に極少数の手がかり表現を人手で用意するだけで，後は，自動的に実行されるので，人間の労力をほとんど要しないのが特徴である．ここで開発した手法は，事象の原因表現抽出にかなり汎用的に応用できるものと思われる．

テキスト自動要約に関する研究では，検索結果から成る文書集合を対象として，ユーザの興味に適合するため，文書集合から抽出したキーワードをユーザに提示し選択させることで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開発した．更に，テキスト自動要約の応用として，論文からの発表用スライド自動生成の研究でも各セクションをひとつの文書と見ることで，上述の複数文書要約手法を応用し，更に，箇条書きの自動生成を試みるなどの成果を得た．

II. 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

枝ランキングとは，与えられたグラフに，同じラベルを持つ枝どおしを結ぶ任意の路上に少なくともひとつそれより大きいラベルをもつ枝が存在するような枝へのラベル付けをいう。最小枝ランキング問題とは，グラフ G で枝ランキングで付されたラベルの最大値を最小にする問題で あり一般のグラフに対しては，NP-hard であることが知られている． 2 連結外平面グラフに対して，多項式時間のアルゴリズムを考案した．

一方、節点ランキングとは，与えられたグラフに，同じラベルを持つ節点どおしを結ぶ任意の路上に少なくともひとつそれより大きいラベルをもつ節点が存在するような節点へのラベル付けをいう。最小節点ランキング問題とは，グラフ G で節点ランキングで付されたラベルの最大値を最小にする問題であり, その値を $\chi(G)$ とする。最小節点ランキング全域木問題 (MVRST) とは，グラフ G の全域木 T の中で $\chi(T)$ が最小となるものを求める問題である。MVRST が NP 困難であることを証明し，また、外平面グラフに対して効率の良いアルゴリズムを得た.

また、グラフ理論における連結度の概念は, 種々のネットワークの制御・設計において, 耐故障性に関する基本的な評価尺度として用いられる. 所望の連結度を保証するネットワークを最適構成する問題として, 連結度増大問題と供給点配置問題についても成果を得た.

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 1]

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.

ここで開発した手法は，事象の原因表現抽出にかなり汎用的に応用できるものと思われる.

2.2 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 2]

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

[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.

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なることが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] http://research.nii.ac.jp/ntcir/workshop/work-ja.html

2.3 文章閲覧における読者の操作行動からの興味の推定 [学術論文 6]

文章情報を対象とし、「興味の程度」を推定することを試みた．推定の手がかりとして，文章閲覧時のユーザの挙動データ、具体的には画面を送るためのスクロール操作の時間情報、を用い，ユーザの興味を推定する問題として設定した．従来，興味の程度と閲覧時間が相関することから，閲覧時間によって興味を推定していた（この特徴量を速度指標と呼ぶ)。しかし、文の難易度などによっても閲覧時間が影響されるため，速度指標のみでは推定精度と安定性の面で不十分と考え，それを補間する新たな指標として，文の言語情報から標準的な閲覧時間を推定し，それと実測閲覧時間の乖離の程度を指標化（乖離指標）した．その結果，興味の推定における正解率に関し，乖離指標単体で速度指標と同等の性能を示した．また、乖離指標と速度指標の相関が低いことも確認した．

2.4 LaTeX 原稿からのプレゼンテーションスライド自動生成

研究のプレゼンテーションでは、限られた時間の中で，聴衆に研究成果をよく理解してもらうためにプレゼンテーションスライドの作成が必要不可欠である．しかし、スライドの作成には多くの時間と手間を擁する．そのため、多くの研究者がスライド作成を望んでいる．本研究では，研究者の負担を軽減することを目的として，論文 LaTeX 原稿からスライドを自動生成する手法を提案する．本手法では，LaTeX ファイルの解析，スライドへの内容の割り当て，接続詞を利用した箇条書き生成を行う．LaTeX ファイルの解析では，スライド生成に必要な情報は残し，不要な情報の削除を行う．LaTeX ファイルの定型的な性質を利用すれば，必要な情報を特定することが可能である．スライド割り当てにおいては，論文中の名詞の出現頻度，エントロピー、idf 値に基づいて名詞の重要度を計算する．その重要度に基づいて，各セクションに対して，スライド枚数の割り当て，重要文の抽出を行う．接続詞を利用した箇条書き生成においては、並列関係表す接続詞を利用する．なぜなら、並列関係を表す接続詞を含む文には，その文と対になる文が存在することが多いからである．評価の結果，本手法は，論文に忠実なスライド生成に有効であることが分かった．

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 4]

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、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。

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]

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 グラフの連結度増大問題と供給点配置問題

I. 連結度増大問題

$(k-1)$ 枝連結グラフ G が、最適な場合に比べて $\max\{\ell+1, 2k-4\}$ 個の余分な枝を付加することで ℓ 枝連結、かつ、k 節点連結に、$O(\min\{k,\sqrt{n}\}kn^3+n^4)$ 時間，但し，$n=|V|$、でできることを示した [学術論文 8].

グラフ $G=(V,E)$ と整数 $D\geq 1$ が与えられたとき，G に最小個数の枝を付加して， 直径が高々 D と成るようにする問題を考える．任意のグラフ G に対して定数近似アルゴリズムは，$P=NP$ でない限り存在しないことが知られている．森 G と奇数 $D\geq 3$ に対して, 定数近似アルゴリズムが存在するかどうかは未解決であったが、それを肯定的に解決した．考案したアルゴリズムは，$O(|V|^3)$ 時間で 8-近似解を求める．さらに，与えられたグラフが 2 連結のときは，4-近似解が 与えられたグラフ G と奇数 D に対し，線形時間で求まることを示した [文献 9].

無向多重グラフ $G=(V,E)$, 節点集合 $W\subseteq V$ の族 $\mathcal{W}$，及び，要求関数 $r:\mathcal{W}\to Z^+$ (ここで、Z^+ は非負整数の集合), が与えられたとき，得られるグラフが任意の v, W 間，但し，$v\in V$, $W\in\mathcal{W}$、に少なくとも $r(W)$ 個の枝素な路を持つように最小個数の枝を G に付加する問題を考える． 任意の $W\in\mathcal{W}$ に対し $r(W)=1$ である場合に NP 困難であること，また、任意の $W\in\mathcal{W}$ に対し $r(W)=r\geq 2$ である場合に対し多項式時間で解けることが知られていた．今回，任意の $W\in\mathcal{W}$ に対して $r(W)\geq 2$ であっても、$O(m+pn^4(r^*+\log n))$ 時間で解けることを示した．但し，$n=|V|$, $m=|\{\{u,v\}|(u,v)\in E\}|$, $p=|\mathcal{W}|$, かつ、$r^*=\max\{r(W)\mid W\in\mathcal{W}\}$ である [文献 10].

有限台集合 V に対し，集合関数 $r:2^V\to Z^+$ が単調であるとは、任意の $X'\subseteq X\subseteq V$, 但し，Z^+ は，非負整数の集合，に対し，$r(X')\geq r(X)$ が成り立つことである．無向多重グラフ $G=(V,E)$ と単調要求関数 $r:2^V\to Z^+$ が与えられたとき，G に最小個数の枝を付加して、得られたグラフ G' が任意の $\emptyset\neq X\subset V$ に対して $d_{G'}(X)\geq r(X)$ を満たすようにする問題を考える．但し，$d_G(X)$ は G の節点集合 X の次数である． この問題は枝連結増大問題を含み，一般には，r に対する多項式時間オラクルが利用可能な場合でも NP 困難である。任意の $\emptyset\neq X\subset V$ が $r(X)>0$ ならばいつでも $r(X)\geq 2$ を満たすならば,$O(n^4(m+n\log n+q))$ 時間で解けることを示した．但し，$n=|V|$, $m=|\{\{u,v\}\mid(u,v)\in E\}|$ であり、また、q は各 $X\subseteq V$ に対し $\mathrm{br}(X)$ を計算する時間である [文献 13].

II. 供給点配置問題，その他

$G=(V,E)$ を節点集合と枝集合 E を持つ単純無向グラフとする．各節点 $v\in V$ は要求 $d(v)\in Z_+$ とコスト $c(v)\in R_+$ を持つとする。但し，Z_+ と R_+ は、それぞれ、非負整数の集合と非負実数の集合である．与えられたグラフ G の節点連結要求を持つ供給点配置問題とは、S から任意の節点 $v\in V-S$ まで少なくとも $d(v)$ 個の枝素な路が存在するような S で $\sum_{v\in S}c(v)$ を最小にするものを見つける問題である。もし $d(v)\geq 4$ であるような節点 $v\in V$ が存在するならばすべての節点が一様なコストを持つ場合でも NP 困難であることが知られている．任意の $v\in V$ に対して $d(v)\leq 3$ が成り立つならばこの問題が $O(|V|^4(\log|V|)^2)$ 時間で解けることを示した [文献 11].

$G=(V,E)$ が節点集合 V、枝集合 E を持つ無向グラフとする．G は k 個のお互いに素な節点集合 $T_1,T_2,\ldots,T_k$(資源集合と呼ぶ)、但し，$|T_i|$ は任意の i に対し偶数である．k 個の資源集合を持った 2 分割問題とは，節点集合 V の分割 V_1、V_2 で V_1 と V_2 により誘導される部分グラフはそれぞれ連結であり，かつ、任意の $i=1,2,\ldots,k$ に対して $|V_1\cap T_i|=|V_2\cap T_i|=|T_i|/2$ が成り立つことをいう．2 分割問題は，$k=1$ でも NP 困難であることが知られている．一方，G が $(k+1)$ 連結, $k=1,2$, なら、任意の与えられた資源集合に対して G の 2 分割が存在することが知られている．$k\geq 3$ に対しある $(k+1)$ 連結グラフに対して 2 分割が存在するとの仮説が知られている．$k=3$ に対して仮説が成り立たないこと，一方， G が 4 連結で，かつ K_4 を部分グラフとしてもつならば，2 分割が存在し， $O(|V|^3\log|V|)$ 時間で求まることを示した．更に，節点を枝とした問題では，$k=1,2,3.$ に対し $(k+1)$ 枝連結が十分であることも示した [文献 12].

研究業績一覧

学術論文

1. 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, 13 巻 2 号, pp.99-123, 2006 年 4 月.
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交通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して定義して人手でひとつ与え，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、更に，取得した種表現からふたたび、交通事故表現を取得する．　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．

2. 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”, 知能と情報 (日本知能情報ファジィ学会誌), Vol.18, No.2, pp.265-279, 2006 年 4 月.
概要: 本論文では，ユーザの要約要求を反映させ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，主として単一文書からひと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，ある事柄に関連した複数の文書からひと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，検索結果等で得られた多くの文書を読むのに多大な時間が必要であり，それらをひとつの要約に，まとめることで読む時間の大幅な削減が可能となるからである．しかしながら、ユーザによって興味等が異なるため，ユーザごとに必要な要約は異なる．本論文では，ユーザにキーワードを提示し，それらの中からキーワードを選択させることでユーザ適合した要約の生成を実現した．

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スライド自動生成”, 知能と情報 (日本知能情報ファジィ学会誌), Vol.18, No.5, pp.752-760, 2006 年 10 月.
概要: 研究のプレゼンテーションでは、限られた時間の中で，聴衆に研究成果をよく理解してもらうためにプレゼンテーションスライドの作成が必要不可欠である．しかし、スライドの作成には多くの時間と手間を擁する．そのため、多くの研究者がスライド作成を望んでいる．本研究では，研究者の負担を軽減することを目的として，論文 LaTeX 原稿からスライドを自動生成する手法を提案する．本手法では，LaTeX ファイルの解析，スライドへの内容の割り当て，接続詞を利用した箇条書き生成を行う．LaTeX ファイルの解析では，スライド生成に必要な情報は残し，不要な情報の削除を行う．LaTeX ファイルの定型的な性質を利用すれば，必要な情報を特定することが可能である．スライド割り当てにおいては，論文中の名詞の出現頻度，エントロピー、idf 値に基づいて名詞の重要度を計算する．その重要度に基づいて，各セクションに対して，スライド枚数の割り当て，重要文の抽出を行う．接続詞を利用した箇条書き生成においては、並列関係表す接続詞を利用する．なぜなら、並列関係を表す接続詞を含む文には，その文と対になる文が存在することが多いからである．評価の結果，本手法は，論文に忠実なスライド生成に有効であることが分かった．

4. 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, Vol.154, Issue 16, pp.2402-2410, 2006年11月.
概要: The minimum vertex spanning tree problem (MVRST) is to find a spaning 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. More over, we present a $(\lceil D_s/2 \rceil + 1)/(\lfloor \log_2(D_s+1) \rfloor + 1)$-approximation algorithm for MVRST where D_s is the minimum diameter of spanning trees of G.

5. Shin-ichi Nakayama, shigeru Masuyama:
"A Polynomial Time Algorithm for Obtaining a Minimum Vertex Ranking Spanning Tree in Outerplanar Graphs(invited paper)", IEICE Trans. Information and Systems, Vol.E89-D, No.8, pp.2357-2363, 2006年8月.
概要: The minimum vertex ranking spanning tree is to find a spanning tree of G whose 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 the class of interval graphs. This paper proposes a polynomial time algorithms for solving the minimum vertex ranking spanning tree problem on outerplanar graphs.

6. 梅村祥之, 増山 繁:
"文章閲覧における読者の操作行動からの興味の推定", ヒューマンインターフェース学会誌, Vol.3, No.3, pp.435-444, 2006年8月.
概要: A number of methods of user profiling for imformation recommendation and information filtering are studied that assist users to read many documents in the Web. It is considered that the methods to estimate user's interest are important and difficult. Most previously proposed methods simply focus on reading time to estimate user's interest based on the hypothesis that reading time correlates interest. This paper presents a method to estimate user's interest by user's time lapse data to page in reading documents. Our method focuses on the relation of reading time and the language information of the reading sentance. We developed an index that reflects the degree of the difference between actual reading time and estimated reading time based on language information of the sentence. We collected subjective ratings of interest about 300 articles from 6 subjects, and we measured the accuracies of estimation of interest. As a result, our index performed about the same of the previous index. Moreover, the accuracy of estimation using indices combined our index and previous index exceeded accuracy of extimation by previous index.

7. Shin-ichi Nakayama, Shigeru Masuyama:
"A Polynomial Time Algorithm for Obtaining Minimum Edge Ranking on Two-connected Outerplanar Graphs", Information Processing Letters, (掲載予定).
概要: An edge ranking of a graph G is a labeling r of its edges with positive integers such that every path between different edges e_u, e_v with the same rank $r(e_u) = r(e_v)$ contains an intermediate edge e_w) with rank $r(e_w) > r(e_u)$. An edge ranking of G is *minimum* if the largest rank k assigned is the smallest among all rankings of G. The *edge ranking problem* is to find a minimum edge ranking of given graph G. This problem is NP-hard and no polynomial time algorithm for solving it is known for non-trivial classes of graphs other than than the class of trees. In this paper, we first show, on a generaql graph G, a relation between a minimum edge ranking of G and its minimal cuts, which ensures

that we can obtain a polynomial time algorithm for obtaining minimum edge ranking of a given graph G if minimal cuts for each subgraph of G can be found in polynomial time and the number of those is polynomial. Based on this relation, we develop a polynomial time algorithm for finding a minimum edge ranking on a 2-connected outerplanar graph.

8. 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, vol.44, no.3, pp.257-280, 2006年4月.
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 $n = |V|$.

9. Toshimasa Ishii, Shigeyuki Yamamoto and Hiroshi Nagamochi:
"Augmenting Forests to Meet Odd Diameter Requirements", Discrete Optimization, vol.3, pp.154-164, 2006年6月.
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.

10. Toshimasa Ishii, Masayuki Hagiwara:
"Minimum augmentation of local edge-connectivity between vertices and vertex subsets in undirected graphs", Discrete Applied Mathematics, vol.154, issue 16, pp.2307-2329, 2006年11月.
概要: Given an undirected multigraph $G = (V, E)$, a family $\mathcal{W}$ of sets $W \subseteq V$ of vertices (areas), and a requirement function $r : \mathcal{W} \to Z^+$ (where Z^+ is the set of nonnegative integers), we consider the problem of augmenting G by the smallest number of new edges so that the resulting graph has at least $r(W)$ edge-disjoint paths between v and W for every pair of a vertex $v \in V$ and an area $W \in \mathcal{W}$. So far this problem was shown to be NP-hard in the uniform case of $r(W) = 1$ for each $W \in \mathcal{W}$, and polynomially solvable in the uniform case of $r(W) = r \geq 2$ for each $W \in \mathcal{W}$. In this paper, we show that the problem can be solved in $O(m + pn^4(r^* + \log n))$ time, even if $r(W) \geq 2$ holds for each $W \in \mathcal{W}$, where $n = |V|$, $m = |\{\{u, v\} | (u, v) \in E\}|$, $p = |\mathcal{W}|$, and $r^* = \max\{r(W) \mid W \in \mathcal{W}\}$.

11. Toshimasa Ishii, Hitoshi Fujita, Hiroshi Nagamochi:
"Minimum cost source location problem with local 3-vertex-connectivity requirements", Theoretical Computer Science, vol.372, pp.81-93, 2007年3月.
概要: Let $G = (V, E)$ be a simple undirected graph with a set V of vertices and a set E of edges. Each vertex $v \in V$ has a demand $d(v) \in Z_+$ and a cost $c(v) \in R_+$, where

Z_+ and R_+ denote the set of nonnegative integers and the set of nonnegative reals, respectively. The source location problem with vertex-connectivity requirements in a given graph G asks to find a set S of vertices minimizing $\sum_{v\in S} c(v)$ such that there are at least $d(v)$ pairwise vertex-disjoint paths from S to v for each vertex $v \in V - S$. It is known that if there exists a vertex $v \in V$ with $d(v) \geq 4$, then the problem is NP-hard even in the case where every vertex has a uniform cost. In this paper, we show that the problem can be solved in $O(|V|^4(\log|V|)^2)$ time if $d(v) \leq 3$ holds for each vertex $v \in V$.

12. Toshimasa Ishii, Kengo Iwata, Hiroshi Nagamochi:
"Bisecting a four-connected graph with three resource sets", Discrete Applied Mathematics, (掲載予定).
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 $k = 1, 2, 3$.

13. Toshimasa Ishii:
"Minimum augmentation of edge-connectivity with monotone requirements in undirected graphs", Proceedings of the 13th Computing Theory: The Australian Theory Symposium (CATS'07), Ballarat, Australia, pp.91-100, 2007年1月.
概要: For a finite ground set V, we call a set-function $r : 2^V \to Z^+$ monotone, if $r(X') \geq r(X)$ holds for each $X' \subseteq X \subseteq V$, where Z^+ is the set of nonnegative integers. Given an undirected multigraph $G = (V, E)$ and a monotone requirement function $r : 2^V \to Z^+$, we consider the problem of augmenting G by a smallest number of new edges so that the resulting graph G' satisfies $d_{G'}(X) \geq r(X)$ for each $\emptyset \neq X \subset V$, where $d_G(X)$ denotes the degree of a vertex set X in G. This problem includes the edge-connectivity augmentation problem, and in general, it is NP-hard even if a polynomial time oracle for r is available. In this paper, we show that the problem can be solved in $O(n^4(m + n\log n + q))$ time, under the assumption that each $\emptyset \neq X \subset V$ satisfies $r(X) \geq 2$ whenever $r(X) > 0$, where $n = |V|$, $m = |\{\{u, v\} \mid (u, v) \in E\}|$, and q is the time required to compute $r(X)$ for each $X \subseteq V$.

研究会等

1. Toshimasa Ishii:
"Minimum augmentation of edge-connectivity with monotone requirements in undirected graphs", 電子情報通信学会報告書, vol. 106, no. 63, COMP2006-10, pp. 1-8, 2006年5月.
概要: For a finite ground set V, we call a set-function $r : 2^V \to Z^+$ monotone, if $r(X') \geq r(X)$ holds for each $X' \subseteq X \subseteq V$,

where Z^+ is the set of nonnegative integers. Given an undirected multigraph $G = (V, E)$ and a monotone requirement function $r : 2^V \to Z^+$, we consider the problem of augmenting G by a smallest number of new edges so that the resulting graph G' satisfies $d_{G'}(X) \geq r(X)$ for each $\emptyset \neq X \subset V$, where $d_G(X)$ denotes the degree of a vertex set X in G. This problem includes the edge-connectivity augmentation problem, and in general, it is NP-hard even if a polynomial time oracle for r is available. In this paper, we show that the problem can be solved in $O(n^4(m + n \log n))$ time under the assumption that each $\emptyset \neq X \subset V$ satisfies $r(X) \geq 2$ whenever $r(X) > 0$, where $n = |V|$ and $m = |\{\{u, v\} \mid (u, v) \in E\}|$.

2. 石井利昌:
"連結度要求を持つネットワーク構成問題", オペレーションズリサーチ学会北海道支部研究会, 2006 年 7 月.
概要: グラフ理論における連結度の概念は, 種々のネットワークの制御・設計において, 耐故障性に関する基本的な評価尺度として用いられる. 所望の連結度を保証するネットワークを最適構成する問題の一つである, 連結度増大問題を中心に最近の研究結果を紹介する.

3. 石井利昌:
"連結度要求を持つネットワーク構成問題", 第 18 回ＲＡＭＰシンポジウム論文集, pp.13-27, 2006 年 10 月.
概要: グラフ理論における連結度の概念は, 種々のネットワークの制御・設計において, 耐故障性に関する基本的な評価尺度として用いられる. 所望の連結度を保証するネットワークを最適構成する問題として, 連結度増大問題と供給点配置問題を取り上げる. 近年, これらの問題に対し, 効率的なアルゴリズムの研究が盛んに行われており, また劣モジュラ関数を用いて一般化された離散最適化問題の研究もされてきている. 本稿では, これらの問題に対する最近の研究結果を紹介する.

学会大会等

1. 増山　繁:
"最小節点ランキング全域木問題について (招待講演)", 科研費特定領域「新世代の計算限界－その解明と打破－」平成 18 年度第 1 回全体集会, 2006 年 6 月.

2. Shin-ichi Nakayama, Shigeru Masuyama:
"A Polynomial Time Algorithm for Obtaining the Minimum Vertex Ranking Spanning Tree on Outerplanar Graphs", INFORMS International Meeting Hong Kong 2006, 2006 年 6 月.

3. Toshimasa Ishii and Masahiro Oshita:
"Augmenting Cacti to Meet Diameter Requirements", INFORMS International Meeting Hong Kong 2006, 2006 年 6 月.

4. 鈴木　琢也, 関根　聡, 増山　繁:
"百科事典を対象とした属性値抽出", 言語処理学会第 13 回年次大会発表論文集, pp.123-126, 2007 年 3 月.

5. 酒井　浩之、増山　繁:
"企業の業績発表記事からの業績要因の抽出", 言語処理学会第 13 回年次大会発表論文集, pp.436-439, 2007 年 3 月.

6. 山本悠二、増山　繁:
"構文木情報を用いた機械可読辞書からの類義語および上位・下位語の抽出", 言語処理学会第 13 回年次大会ワークショップ「言語的オントロジーの構築・連携・利用」
論文集, pp.39-42, 2007 年 3 月.

7. 小泉　賢司, 増山　繁:
"AGV システムのデッドロックに関する研究", 日本オペレーションズ・リサーチ学会春季研究発表会アブストラクト集, pp.12-13, 2007 年 3 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 ‡　小野　孝男 †　和田 幸一 §

† 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 大学院 工学研究科
〒 466-8555 名古屋市昭和区御器所町
wada@nitech.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、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。また、頂点彩色問題に対して高性能の発見的アルゴリズムを設計した。さらに、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。集合被覆問題に関しては、重みつき集合被覆問題に関して成果を得た。この他, 画像処理で有用な距離変換を効率よく求めるシストリックアルゴリズムの提案を行った．また、センサーネットワークのプロトコルや無線ネットワークの初期化アルゴリズムについて研究を行った。

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　最小木状被覆問題の近似アルゴリズム

無向グラフ $G = (V, E)$ において，G の各辺がいずれかの端点を頂点集合 $C \subseteq V$ 内にもつとき，C を G の**頂点被覆**という．また辺集合 D は，D に含まれない G の各辺が D 内の辺に隣接するとき，**辺支配集合**と呼ばれる．連結グラフ G における木 T は，その辺集合が G の辺支配集合を構成するとき，G の**木状被覆**（あるいは**連結辺支配集合**）といわれる．なお，この条件を，T の頂点集合が G の頂点被覆を構成する，と換言することもできる．**木状被覆問題**とは，各辺に非負コスト l_e が割当られた連結グラフ G が与えられたときに，G の木状被覆の中で，そのコスト（つまり，辺コストの総和）が最小となるものを計算する最適化問題である．

最小コストの頂点被覆を計算する問題である**頂点被覆問題**は，NP 困難な基本問題の一つであるが，連結グラフを誘導するような頂点被覆が求められる**連結頂点被覆問題**もまた NP 困難であり，後者の多項式時間近似計算は前者のそれ以上に困難であることも知られている [16]．ところが一様コストの場合，木のもつ辺数と頂点数の関係から，木状被覆問題と連結頂点被覆問題は同じ問題と見なすことができ，これより木状被覆問題

の多項式（近似）計算が頂点被覆問題のそれ以上に困難であることがいえる．頂点被覆問題の近似精度の多項式時間保証については，2 倍以下とすることが可能である [29, 2, 33, 22] その一方で，$10\sqrt{5} - 21 \approx 1.36067$ 以下を保証することは NP 困難となってしまうことが知られている [8].

元々グラフの木状被覆問題は，グラフの各頂点に隣接するように施設を木状配置する問題との関連から，Arkin らによって導入された問題である [1]．と同時に彼らは，一様コストの場合に 2 倍近似保証アルゴリズムを，一般コストの場合に 3.55 倍近似保証をを提示している．実のところ一様コストの場合には，より早くからより簡単な 2 倍近似アルゴリズムが，Savage により開発されている [37]（もっとも，同アルゴリズムは頂点被覆問題用として提案されたものである）．一方，一般コストの場合は，その後アルゴリズムの改善が見られ，近似保証は $3 + \epsilon$ まで下げられている [31, 12]．この時点では，頂点被覆問題や辺支配集合問題，更にそれらの関連問題の多くが，付随コストの何如んによらず 2 という近似保証が得られている [13, 35] のに対し，木状被覆問題では，一様コストと一般コストの場合で，保証できる近似精度に差があることを意味する．更に悪いことには，上述の $(3+\epsilon)$ 倍近似アルゴリズム [31, 12] 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代物である．というのも，そこでは指数関数オーダーの規模をもつ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．

このような状況を背景に，一般コストをもつ木状被覆問題に対し，より良い近似アルゴリズムを開発し，近似保証ならびに計算時間をともに向上させることを本研究の目標とした．得られた成果を要約すると，以下の通りである：

1. まず，与えられるコストは 2 倍以上の開きがある 2 種類だけの場合に制限して検証した．その結果，線形計画の主双対法に基づいて設計された近似アルゴリズムにより，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. 上記制限下での成功を基に，一般の場合について検討した結果，高速な組合せアルゴリズムにより，この場合も 2 倍近似保証することが可能であることを示した．一般コスト用にこれまでに開発された，いずれのアルゴリズムもが，まず頂点被覆 C を計算してから，C の頂点をシュタイナー木で連結させるという方法をとっていたのに対し，同アルゴリズムの特徴は，最小全域木に枝刈りを施すことで木状被覆を構成するところにある．

2.2 頂点彩色問題の発見的アルゴリズム

無向グラフ $G = (V, E)$（$n = |V|$，$m = |E|$）に対し，関数 $c\colon V \to \{1, 2, \ldots\}$ は全ての $(i, j) \in E$ に対して $c(i) \neq c(j)$ ならば G の**頂点彩色**と呼ぶ．全ての $i \in V$ に対して $c(i) \leq k$ ならこの c は G の k **彩色**であり，k 彩色が存在するとき G は k **彩色可能**といわれる．グラフ G が与えられたときに，色数 k が最小となる k 彩色を求める問題を**頂点彩色問題**と呼ぶ．可能な色数の最小値を G の**彩色数**と呼び $\chi(G)$ で表す．

頂点彩色問題は NP-困難であることが知られており，さらに，P $\neq$ NP を仮定すると，一般のグラフに対し多項式時間で $O(n^{1/7-\epsilon}) \cdot \chi(G)$ 彩色を見付けることはできない（$\epsilon > 0$ は任意）[3]．一般の場合に対して現在知られている最良の結果は，$O(n(\log\log n)^3/(\log n)^2) \cdot \chi(G)$ 彩色 [19] である．ここで，グラフ G の彩色数を制限するとより良い結果が得られており，例えば半定値計画法を用いることにより 3 彩色可能なグラフに対する $\tilde{O}(n^{3/14})$ 彩色 [4] や 4 彩色可能なグラフに対する $\tilde{O}(n^{7/19})$ 彩色 [23] は多項式時間で求まることが知られている（$\tilde{O}()$ は $\log n$ の多項式を無視することを示す）．但し，このようにグラフを制限しても定数倍での近似は困難であり，k 彩色可能なグラフに対する $5k/3 - 1$ 彩色を見つけることは NP-困難 [30] である．

一方この問題はコンパイラにおけるレジスタ割当や無線基地局に対する周波数割当など，多くの資源配分問題に適用することができるため，発見的手法に基づくアルゴリズムについても研究されている．DIMACS 2nd Implementation Challenge では，高性能なアルゴリズムとして**繰り返し貪欲法**（iterated greedy）[7] や**タブー分枝限定法**（tabu branch-and-bound）[17] などが挙げら

れている．

本研究では，頂点彩色問題を 2 次元に制限した半定値計画法に変換して解く発見的アルゴリズムを提案した．半定値計画法に基づく従来のアルゴリズムでは，各頂点に対して n 次元の単位ベクトルを割当てて半定値計画法に変換し，これを解いて得られたベクトル配置から頂点彩色を求めている．これに対し，本手法では各頂点に 2 次元の単位ベクトルを割当て 2 次元上でのベクトル配置問題に変換し，これを解いて得られるベクトル配置を頂点彩色に変換する．

半定値計画法を用いるアルゴリズムは，理論上は多項式時間で実行できるが，半定値計画法を解くために多くの時間とメモリが必要であるため，大規模な問題に対しては実用的ではない．また，半定値計画法の解を元のグラフに対する彩色に変換するときにも，得られる結果が良い彩色であることを保証するのは簡単ではない．これに対し，本手法で用いた，2 次元に制限した半定値計画法そのものは頂点彩色問題と等価であることがわかり，従って（P $\neq$ NP を仮定すると）多項式時間で最適解を求めることはできない．しかし，得られる解は元のグラフに対する彩色に容易に変換することができる．特に，各頂点に対応するベクトルが与えられたときに，これらのベクトルに対し最適な頂点彩色は**円弧グラフのクリークカバー問題**[26] を通して $O(m + n \log n)$ 時間で見付けることができる．

今回提案したアルゴリズムでは，ランダムなベクトル配置から始め，各ベクトルに対し「現在の配置のもとでそのベクトルにとって最適な位置」へ移動させるという探索を繰り返すことによって良いベクトル配置を求めることとした．このアルゴリズムをいくつかのグラフに対し実行したところ，密なランダムグラフに対しては DSATUR[5] や単純なタブー探索 [25] よりも性能が良いことがわかった．

本研究で用いた「半定値計画法を 2 次元に制限する」手法は，2 次元の単位ベクトルが偏角のみで定まることから「新しい解の表現方法を与えている」と解釈することもできる．このように考えた場合，隣接する頂点に対応するベクトル同士が全く同じベクトルにならない限り必ず正しい頂点彩色になっている．頂点彩色問題に対して遺伝的アルゴリズムを適用すると，単純な方法では遺伝的操作を行ったときに頂点彩色にならないことがあるため修正を加えなければならないが，本研究で用いた解の表現を遺伝子として用いればそのような修正はほぼ不要である．そのため，遺伝的アルゴリズムを含め，他の発見的手法に応用することでより良いアルゴリズムを与えるものと考えている．

2.3 一般化彩色問題の近似アルゴリズム

通常の頂点彩色問題に対するアルゴリズムと **defective coloring** に対するアルゴリズムとの関係について，以下の問題が提起されている：n 頂点のグラフを $O(n^\epsilon)$ 色で彩色可能な頂点彩色アルゴリズムが与えられたとする．このアルゴリズムに基づいて $(O(n/d)^\epsilon, d)$-defective coloring を行うことは常に可能だろうか．ここで，(k, d)-**defective coloring** とは，与えられたグラフの頂点の，k 個の d-**defected 独立集合**（最大次数が高々 d の部分グラフを誘導するような頂点の部分集合）への分割である．0-defected 独立集合とは通常の独立集合のことであり，従って (k, d)-defective coloring は通常の k 彩色を一般化した概念である．(k, d)-**defective coloring 問題**，すなわちグラフが与えられたときに (k, d)-defective coloring が存在するかどうかを判定する問題は，$k \geq 3$ かつ $d \geq 0$ ならば NP-完全であることが知られている．

本研究では，先の問題に対する解答の一部として，「最大次数 Δ のグラフに対する $O(\Delta^\alpha)$ 彩色アルゴリズムが存在すれば，同じく最大次数 Δ のグラフに対して $(O((\Delta/d)^\alpha), d)$-defective 彩色可能である」ことを示した．これは，「($\Delta+1$ 色で彩色可能である) 最大次数 Δ のグラフが $(\lceil \Delta/d \rceil, d)$-defective 彩色可能である」という Lovász の結果を一般化するものである．さらに，通常の頂点彩色問題に対しては「頂点数 n，最大次数 Δ，彩色数 k のグラフに対し $O(\Delta^{1-x/k})$ 色で彩色可能なら $O(n^{\epsilon(k)})$-彩色可能」であることがわかっているが，これを defective 彩色に拡張可能である，つまり同じ $\epsilon(k)$ により「頂点数 n，最大次数 Δ，彩色数 k のグラフに対し $O(\Delta^{1-x/k})$ 色で彩色可能なら $(O(n^{\epsilon(k)}), d)$-defective 彩色可能」である

ことを示した.

3 集合問題

3.1 集合被覆問題の近似アルゴリズム

集合被覆問題（*SC*）は，よく知られた組合せ最適化問題で，これまでに多くの研究成果が得られている．ここでは，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，$\bigcup_{S\in\mathcal{F}'} S = U$ となるような部分集合族 $\mathcal{F}'$ の中で最小コストのもの，つまり，含まれる部分集合のコスト和 $\sum_{S\in\mathcal{F}'} c_S$ が最小であるもの，が求められる．また，与えられた部分集合の位数がいずれも k 以下であるとき，それを k **集合被覆問題（*k*-*SC*）**と呼ぶ．同問題は $k \geq 3$ であれば NP 困難であり，APX 困難でもある [34].

SC に対するヒューリスティックの中で，貪欲法は直感的に最も自然かつ単純である．U の要素 u は，u を要素とする部分集合をもつ集合族により**被覆される**というが，貪欲法は部分集合を集合族に順次追加することで，すべての要素を被覆するような集合族を最終的に構成する．部分集合 S の選択基準は**コスト効率**で，新たに被覆するのに要する 1 要素当りのコスト（つまり，S 内で未被覆な要素数で c_S を割ったもの）が最小なものが選ばれる．SC に対する貪欲法は，$H(n) = \sum_{i=1}^{n}(1/i) = O(\log n)$ の近似精度を保証し，k-SC に対しては $H(k)$ を保証する [27, 32, 6]．更に一様コストをもつ SC の場合（つまり $c_S = 1, \forall S \in \mathcal{F}$），より精密な近似保証の $\ln n - \ln\ln n + \Theta(1)$ が示されている [38]．その一方で，対話証明による近似困難性の結果より，SC に対し多項式時間内に保証できる近似精度が，貪欲法の与える近似保証にほぼ一致することもわかっており [11, 36]，SC に対しては貪欲法が漸近的に最良の近似アルゴリズムであるといえる．

一方 k-SC に対しては，貪欲法を改良することで，一様コストの場合に $H(k)-1/6$ の近似保証が示された [18]．更に様々な局所探索の手法を取り入れることで，$H(k)-11/42, H(k)-1/3$ [20, 21] へと改善され，現在のところ $H(k)-1/2$ まで知られている [9]. 残念ながら，一様コスト k-SC における，これらの改良方法は，一般コストの場合には通用せず，貪欲法の $H(k)$ を改善できるか否かは未解決問題として残されていた．本研究では，この未解決問題に対する最初の回答を，次のように条件付ながら，肯定的に与える：一般コスト 3-SC において，異なる部分集合コストには 2 倍以上の開きがある場合には，貪欲法を改良することで $H(3)-1/6$ の近似保証が得られる．アルゴリズムは，Goldschmidt らによる貪欲法の変形版 [18] を一般化したものである．ただし，貪欲法より優れたアルゴリズム [20, 21, 9] がすべて組合せ論的に解析されているのに対し，本研究では 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 [14, 15] と Edmonds [10] によるグラフの分割定理がキーとなっている．

その後，同未解決問題には更なる進展が見られ，一般コスト k-SC に対して $H(k) - \frac{k-1}{8k^9}$ の近似保証を有し，貪欲法よりも真に高精度な近似アルゴリズムの存在が初めて確認された [24].

参考文献

[1] 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.

[2] R. Bar-Yehuda, S. Even, “A local-ratio theorem for approximating the weighted vertex cover problem,” *Annals of Discrete Mathematics*, Vol. 25, pp. 27–46, North-Holland, 1985.

[3] M. Bellare, O. Goldreich, M. Sudan, “Free bits, PCPs and non-approximability — towards tight results,” *SIAM J. Comput.*, Vol. 27, pp. 804–915, 1998.

[4] A. Blum, D. Karger, “An $\tilde{O}(n^{3/14})$-coloring Algorithmfor 3-colorable Graphs,” *Information Processing Letters*, Vol. 61, pp. 49–53, 1997.

[5] D. Brélaz, "New methods to color vertices of a graph," *Communications of the ACM*, Vol. 22, pp. 251–256, 1979.

[6] V. Chvátal, "A greedy heuristic for the set-covering problem," *Math. Oper. Res.*, Vol. 4, No. 3, pp. 233–235, 1979.

[7] J. C. Culberson and F. Luo, "Exploring the k-colorable landscape with iterated greedy," In David S. Johnson and Michael A. Trick, editors, *Cliques, Coloring, and Satisfiability: Second DIMACS Implementation Challenge*, Vol. 26 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pp. 245–284. American Mathematical Society, 1993.

[8] I. Dinur, S. Safra, "The Importance of Being Biased," in *Proc. 34th Annual ACM Symp. Theory of Computing*, pp. 33–42, 2002.

[9] 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.

[10] J. Edmonds, "Paths, trees and flowers," *Canad. J. Math.*, Vol. 17, pp. 449–467, 1965.

[11] U. Feige, "A threshold of $\ln n$ for approximating set cover," *J. ACM*, Vol. 45, No. 4, pp. 634–652, 1998.

[12] T. Fujito, "On approximability of the independent/connected edge dominating set problems," *Inform. Process. Lett.*, Vol. 79, No. 6, pp. 261–266, 2001.

[13] 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.

[14] T. Gallai, "Kritische Graphen II," *Magyar Tud. Akad. Mat. Kutató Int. Közl.*, Vol. 8, pp. 373–395, 1963.

[15] T. Gallai, "Maximale Systeme unabhängiger Kanten," *Magyar Tud. Akad. Mat. Kutató Int. Közl.*, Vol. 9, pp. 401–413, 1964.

[16] M.R. Garey, D.S. Johnson, "The rectilinear Steiner-tree problem is NP-complete," *SIAM J. Appl. Math.*, Vol. 32, No. 4, pp. 826–834, 1977.

[17] F. Glover, M. Parker and J. Ryan, "Coloring by Tabu Branch and Bound," In David S. Johnson and Michael A. Trick, editors, *Cliques, Coloring, and Satisfiability: Second DIMACS Implementation Challenge*, Vol. 26 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pp. 285–307. American Mathematical Society, 1993.

[18] 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.

[19] M.M. Halldórsson, "A still better performance guarantee for approximate graph coloring," *Inform. Process. Lett.*, Vol. 45, pp. 19–23, 1993.

[20] M.M. Halldórsson, "Approximating discrete collections via local improvements," in *Proc. 6th Annual ACM-SIAM Symp. Discrete Algorithms*, pp. 160–169, 1995.

[21] M.M. Halldórsson, "Approximating k-set cover and complementary graph coloring," in *Proc. IPCO V*, pp. 118–131, 1996.

[22] 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.

[23] E. Halperin, R. Nathaniel, U. Zwick, "Coloring k-colorable graphs using smaller palettes," in *Proceedings of the 12th Annual*

ACM-SIAM Symposium on Discrete Algorithms, pp. 319–326, 2001.

[24] R. Hassin, A. Levin, “A better-than-greedy approximation algorithm for the minimum set cover problem,” *SIAM J. Comput.*, Vol. 35, No. 1, pp. 189–200, 2005.

[25] A. Hertz and D. de Werra, “Using tabu search techniques for graph coloring,” *Computing*, Vol. 39, pp. 345–351, 1987.

[26] W.L. Hsu and K.H. Tsai, “Linear time algorithms on circular-arc graphs,” *Information Processing Letters*, Vol. 40, pp. 123–129, 1991.

[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*, Vol. 45, No. 2, pp. 246–265, 1998.

[29] G. Karakostas, “A better approximation aatio for the vertex cover problem,” in *Proc. 32nd ICALP*, pp. 1043–1050, 2005.

[30] S. Khanna, N. Linial, S. Safra, “On the hardness of approximating the chromatic number,” *Proc. Israel Symposium on Theory of Computing Systems*, pp. 250–260, 1993.

[31] J. Könemann, G. Konjevod, O. Parekh, A. Sinha, “Improved approximations for tour and tree covers,” *Algorithmica*, Vol. 38, No. 3, pp. 441–449, 2003.

[32] L. Lovász, “On the ratio of optimal integral and fractional covers,” *Discrete Math.*, Vol. 13, pp. 383–390, 1975.

[33] B. Monien, E. Speckenmeyer, “Ramsey numbers and an approximation algorithm for the vertex cover problem,” *Acta Informat.*, Vol. 22, pp. 115–123, 1985.

[34] C. Papadimitriou, M. Yannakakis, “Optimization, approximation and complexity classes,” *J. Comput. System Sci.*, Vol. 43, pp. 425–440, 1991.

[35] O. Parekh, “Edge dominating and hypomatchable sets,” in *Proc. 13th SODA*, pp. 287–291, 2002.

[36] R. Raz, S. Safra, “A sub-constant error-probability low-degree test, and sub-constant error-probability PCP characterization of NP,” in *Proc. 29th Annual ACM Symp. Theory of Computing*, pp. 475–484, 1997.

[37] C. Savage, “Depth-first search and the vertex cover problem,” *Inform. Process. Lett.*, Vol. 14, No. 5, pp. 233–235, 1982.

[38] P. Slavík, “A tight analysis of the greedy algorithm for set cover,” *J. Algorithms*, Vol. 25, pp. 237–254, 1997.

研究業績一覧

著書

1. 情報システムと情報技術事典編集委員会編: “情報システムのための情報技術辞典”, 培風館, 2006 年 7 月.
   概要: 近似アルゴリズムに関する 5 中項目 (近似アルゴリズム，近似精度保証の近似アルゴリズム，近似アルゴリズムの設計法，線形計画緩和に基づく方法，半正定値計画緩和に基づく方法）を執筆担当 (藤戸).

学術論文

1. M. Miyazawa, P. F. Zeng, N. Iso, T. Hirata: “A Systolic Algorithm for Euclidean Distance Transform”, Trans. of IEEE on Pattern Analysis and Machine Intelligence, 28(7), 1127–1134, 2006 年 7 月.
   概要: Distance maps of binary images

contain, for each pixel, the distance between that pixel and the pixel of value 0 closest to it. The distance transform is to compute the distance map for a binary image. It finds various applications in many fields such as computer vision, pattern recognition, morphological filtering, and robotics. Several distances such as the city-block (L_1), the chess-board (L_∞), the octagonal and the Euclidean (L_2) distances are used in image processing. Among them, the Euclidean distance is the most natural one and appropriate for many applications. In some cases, however, the Euclidean distance transform takes much processing time and thus other distances such as the city-block or chess-board were often used as its approximations. Recently, several linear time algorithms for the Euclidean distance transform were reported. However, in real-time applications of image processing such as robotics, less and less computation time is required. In this paper, we propose a systolic algorithm that computes the Euclidean distance map of an $N \times N$ binary image in $3N$ clocks on $2N^2$ processing cells. The algorithm is designed so that the hardware resources are reduced; especially no mulitipliers are used, and thus it facilitates VLSI implementation.

2. H. Otsuki and T. Hirata:
"Inapproximability of the edge contraction problem", Trans. of IEICE on Fundamentals, 89A(5), 1425–1427, 2006年5月.
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 cardinarity whose contraction results in agraph satisfying the property π. This paper gives a lower bound for the approximation ration for the problem for any property π that is hereditary on contractions and determined by biconnected components.

3. T. Fujito, T. Okumura:
"A Modified Greedy Algorithm for Dispersively Weighted 3-Set Cover", Discrete Applied Mathematics, 154(9), 1392–1400, 2006年6月.
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.

4. T. Fujito:
"How to trim an MST: A 2-approximation algorithm for minimum cost tree cover", Lecture Notes in Computer Science (Proc. 33rd ICALP), 4051, 431–442, 2006年7月.
概要: The *minimum cost tree cover* problem is to compute a minimum cost tree T in a given connected graph G with costs on the edges, such that the vertices of T form a vertex cover for G. The problem is supposed to arise in applications of vertex cover and edge dominating set when connectivity is additionally required in solutions. Whereas a linear-time 2-approximation algorithm for

the unweighted case has been known for quite a while, the best approximation ratio known for the weighted case is 3. Moreover, the known 3-approximation algorithm for such case is far from practical in its efficiency. In this paper we present a fast, purely combinatorial 2-approximation algorithm for the minimum cost tree cover problem. It constructs a good approximate solution by trimming some leaves within a minimum spanning tree (MST), and to determine which leaves to trim, it uses both of the primal-dual schema and the local ratio technique in an interlaced fashion.

5. T. Doi, T. Fujito:
"A Primal-Dual Method for Approximating Tree Cover with Two Weights", Discrete Optimization, 3(3), 230–237, 2006 年 9 月.
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.

6. W. Chen, A.K.M.M. Islam, M. Malkani, A. Shirkhodaie, K. Wada, M. Zein-Sabatto:
"Novel broadcast/multicast protocols for dynamic sensor networks", 9th Workshop on Advances in Parallel and Distributed Computational Models(in 21st IEEE International Parallel and Distributed Processing Symposium), (発表予定).
概要: In this paper, we propose time efficient, energy saving and robust broadcast/multicast protocols in a reconfigurable cluster-based network sensor network. In our broadcast protocol, a broadcast can be executed in $O(hd^2 + D^2)$ rounds and each node needs to be awake in $O(D^2)$ rounds, where D and d are the degrees of the sensor network G and the sub-network induced by G's backbone, respectively, and h is the height of the backbone. When k channels are available, a broadcast can be executed in $O((hd^2 + D^2)/k)$ rounds and each node needs to be awake only in $O(D^2/k)$ rounds. We show that our broadcast protocol can be easily modified for multicast. The cluster-based architecture used in this paper is self-constructible and reconfigurable by using two topology management operations: node-move-in and node-move-out. We also show the algorithms for these two operations.

7. Naoki Inaba, Koichi Wada:
"Efficient Initialization Algorithms on Single-hop Radio Networks", IEICE Transactions on Information and Systems, (掲載予定).
概要: We consider an initialization problem in single-hop radio networks. The initialization is the task of assigning distinct ID numbers to nodes in a network. We have greatly improved the previous results for the initialization in an n-node network. We propose randomized initialization algorithms in two cases. The first case is that n is known to all the nodes and the

second case is that n is unknown to all the nodes. The algorithm for the first case completes in $en + \ln n + O(1)$ expected time slots, and the algorithm for the second case completes in $en + O(\sqrt{n})$ expected slots.

8. Jiro Uchida, Wei Chen, Koichi Wada:
"Acknowledged Broadcasting and Gossiping in ad hoc radio networks", Theoretical Computer Science, （掲載予定）.
概要: A radio network is a collection of transmitter-receiver devices (referred to as nodes). Acknowledged Radio Broadcasting(ARB) means transmitting a message from one special node called source to all other nodes and informing the source about its completion. In our model each node takes a synchronization per round and performs transmission or reception at one round. Each node does not have a collision detection capability and knows only own ID. In [B.S. Chlebus, L. Ga, sieniec, A.M. Gibbons, A. Pelc, W. Rytter, Deterministic broadcasting in ad hoc radio networks, Distributed Computing 15 (2002) 27.38], it is proved that no ARB algorithm exists in the model without collision detection. In this paper, we show that if $n \geq 2$, where n is the number of nodes in the network, we can construct ARB algorithms in $O(n)$ rounds for bidirectional graphs and in $O(n^{4/3} \log^{10/3} n)$ rounds for strongly connected graphs and construct Acknowledged Radio Gossiping(ARG) algorithms in $O(n \log^3 n)$ rounds for bidirectional graphs and in $O(n^{4/3} \log^{10/3} n)$ rounds for strongly connected graphs without collision detection.

9. W. Chen, A.K.M.M. Islam, Y. Katayama, J. Uchida, K. Wada:
"Construction and maintenance of a novel cluster-based architecture for ad hoc sensor networks", the Journal of Ad Hoc and Sensor Wireless Networks, （掲載予定）.
概要: 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 operations. When nodes in the network are organized with total 1-hop data, these operations work in expected $O(q)$ 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 show that if nodes in the network know partial 1-hop data (i.e., incomplete knowledge about the neighbors in the network), node-move-in can be done in expected $O(\log q)$ rounds and node-move-out can have a similar performance as the case of the total 1-hop data. Finally, we demonstrate some simulation results for the operations, where we show that in our proposed design the number of clusters increases very slowly w.r.t the increasing number of nodes in the network.

10. Y. Katayama, Y. Tomida, H. Imazu, N. Inuzuka, K. Wada:
"Dynamic Compass Models and Gathering Algorithms for Autonomous Mobile Robots", 14th Colloquium on Structural Information and Communication Complexity, （発表予定）.
概要: This paper studies a gathering problem for a system of asynchronous autonomous mobile robots that can move freely in a two-dimensional plane. We consider robots equipped with an inaccurate (incorrect) compass which may point a different direction from other robots' com-

passes. A gathering problem is that the robots are required to eventually gather at a single point which is not given in advance from any initial configuration. In this paper, we propose several inaccurate compass models and give two algorithms which solve a gathering problem on these models. One algorithm is the very first result treating the compass whose indicated direction may change in every beginning of execution cycles of robots. It solves the problem when compasses have difference at most $\pi/8$ from the (absolute) north. The other one solves the problem when the difference is at most $\pi/3$ relatively to each other robot where the compasses are never changed.

研究会等

1. 藤戸敏弘:
"最小コスト木状被覆問題の 2 倍近似アルゴリズム", 情報処理学会 アルゴリズム研究会, 2006-AL-107, 13–20, 2006 年 7 月.
概要: 辺コストをもつ連結グラフ G において，その頂点集合が G の頂点被覆を成す木を木状被覆，そのような木の中からコスト最小のものを計算する問題を木状被覆問題という． NP 困難である同問題に対し，辺コストが一定の場合，線形時間 2 倍近似アルゴリズムが従来から知られていたが，任意コストの場合，3 倍近似アルゴリズムがベストで，しかもそれらは（多 項式時間とはいえ）非効率的である．本稿では，最小スパンニング木の葉を刈ることで，高速な 2 倍近似アルゴリズムが得られることを示す.

2. Xuzhen Xie，Takao Ono，Tomio Hirata:
"An Argument on Approximate Defective Coloring for k-colorable Graphs", The 9th Japan-Korea Joint Workshop on Algorithms and Computation, 41–48, 2006 年 7 月.
概要: David Karger has asked the following question: Is there a universal argument that shows for a class of approximation algorithms using $O(n^\epsilon)$ colors for proper vertex coloring, we can always achieve an $(O((n/d)^\delta), d)$-defective coloring? We partially answer his quetion by assuming that there were an algorithm that properly colors an graph with maximum degree Δ using $O(\Delta^\alpha)$ colors. Specifically, we will prove that for any k-colorable graphs with $k \geq 3$, most of the known approximation algorithms using $O(n^\epsilon)$ colors can be used to derive an $(O((n/d)^\epsilon), d)$-defective coloring as David Karger asked.

3. 小野孝男，柳浦睦憲，岩城正哉，平田富夫:
"半定値計画法にもとづく彩色問題の発見的解法", 情報処理学会 アルゴリズム研究会, 2006-AL-108, 65–72, 2006 年 9 月.
概要: 本論文では頂点彩色問題に対する新しい発見的アルゴリズムを提案する．このアルゴリズムでは, 各頂点に平面上の単位ベクトルを割当ることにより頂点彩色問題をベクトル配置問題に還元する．このベクトル配置問題は半定値計画問題ではあるが, 求める半正定値行列のランクに制約があるため, NP-困難である．このため発見的手法により可能解を見付ける．得られたベクトル配置からは簡単に実行可能な彩色が得られる．計算機実験により, 密なグラフにおいては提案するアルゴリズムがタブー探索や DSATUR よりも色数の少ない彩色を見付けることがわかった.

4. 松浦勇、安藤正好、平田富夫:
"長目綜絖を用いた場合の織物組織数の増加", 電子情報通信学会技術報告, COMP2006-37, 49–56, 2006 年 10 月.
概要: 織物はたて糸とよこ糸から構成され, 織物組織のパターンは製織の際のたて糸の動き方で生成される．ドビー織機を使った場合, たて糸の動きの種類は綜絖枠の枚数に依存する．そのため，製織可能な織物組織の数は、綜絖枠枚数により決まる．ドビー織機に長目綜絖を使用すると，同じ綜絖枠枚数であっても，製織可能な織物組織数が増加する．本論文では，たて糸 4 本，よこ糸 4 本からなる織物組織で，綜絖枠 3 枚を用いた場合の製織可

能な織物組織数を評価する．普通綜絖のみを使う場合に比べ，長目綜絖を併用すると，製織可能な織物組織数が約 2 倍に増えることを示す．

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 18 年度の結果を述べる．

2 安定結婚問題に対する近似アルゴリズムの改良とその厳密な解析

安定結婚問題とは，N 人の男性と N 人の女性と各個人が持つ希望リストが与えられたときに安定なマッチングを求める問題である．希望リストとは，異性全員の全順序である．この問題に対して，不完全リストと同順位リストという拡張を許した場合の問題を考える．この場合，異なるサイズの安定マッチングが存在する可能性があり，その中で最大サイズの安定マッチングを求める問題 (MAX SMTI) は NP 困難であることが知られている．

この問題では，最大サイズと最小サイズの安定マッチングでは比が高々2 倍しか違わない．また，サイズを考慮しなければ，安定マッチングは多項式時間アルゴリズムで求めることができる．従って，2-近似アルゴリズムは自明である．これまで知られている最良の近似度は $2 - c\frac{1}{\sqrt{n}}$ であったが，我々は初めて 2 よりも厳密によい近似度である 1.8-近似アルゴリズムを達成した．このアルゴリズムは局所探索に基づくもので，局所探索により改善が可能な領域をより厳密に解析することにより得られたものである．

3 クラスタリングにおける合意最大化問題の近似アルゴリズム

合意最大化問題は，相関クラスタリング上で定義された最適化問題であり，クラスタリング後の合意数を最大にするようなクラスタリングを求める問題である．この問題は NP 困難であることが知られているため，近似アルゴリズムによる解法の研究がされてきた．半正定値計画法への緩和を利用した近似アルゴリズムにより近似比 0.7666 が Swamy らにより得られている．

本研究では既知の近似アルゴリズムよりもよい近似比を得られるアルゴリズムを提案した．我々の手法は，半正定値計画問題への緩和の方法を改善することによって，近似比を 0.777 に改善できることを十分な精度の数値実験に基づいて示した．緩和の方法は，Frieze らにより考案されたランダ

ムな k 個のベクトルを利用する手法を用い，4 つのランダムなベクトルによる緩和と 5 つのランダムなベクトルによる緩和を合わせるというものである．我々の手法によって得られるクラスタの数は高々5 個である．また，クラスタを k 個以下に制限した合意最大化問題に対しても近似比の改善を行った．

4 頂点被覆問題に対するリストヒューリスティックの解析

本研究では，頂点被覆問題に対する一種の貪欲アルゴリズムであるリストヒューリスティックについて近似度の解析を行った．リストヒューリスティックは，特にジョブスケジューリング問題に対して良い性能を発揮するアルゴリズムである．このアルゴリズムでは，まず頂点の操作順序を頂点次数に基づいて決定し，その後その順序に従って頂点を処理していく．本研究の結果，次数が非減少となるように並べた頂点順序に対し，リストヒューリスティックの近似度が高々$\sqrt{\Delta}/2 + 3/2$ となることを示した．ただし，Δ は入力グラフの最大次数である．また，どんな頂点順序でも近似度は $\sqrt{\Delta}/2$ より小さくならないことを示した．

5 目標枝連結度 3 の最大被覆供給点配置問題

グラフが与えられたとき，ある節点の組 v, w の枝連結度が k であるとは，どの $k-1$ 本の枝を削除しても v と w の間にパスが存在し，かつこのような k の中で最大なものを言う．また，ある節点集合 S とある節点 v の枝連結度が k 以上である場合に，S が v を被覆すると呼び，この S のことを供給点集合と呼ぶ．最大被覆供給点配置問題は，被覆できる節点集合 (の重みの和) が最大となるような p 個以下の供給点集合を求める問題である．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な問題である．

本研究では，本問題に対して $k = 3$ の場合における多項式時間アルゴリズムを与えた．また本問題が，入力グラフの節点重みと枝容量が全ての節点や枝で一定の場合でも，NP 完全問題となることを示した．

6 有向グラフにおける k 枝連結性の検査

有向グラフ $G = (V, E)$ が k 枝連結であるとは，任意の $u, v \in V$ に対して u から v への k 本の辺素な道が存在することをいう．本研究では，次数の上限が d の有向グラフが k 枝連結であるか，または k 枝連結から ϵ-far であるかを検査する $O(\frac{k2^k \log^2(k/(\epsilon d))}{\epsilon})$ 時間アルゴリズムを示した．本アルゴリズムの計算量はグラフの頂点数および辺の数によらない．

頂点数が n，頂点次数の上限が d の有向グラフ G が k 枝連結から ϵ-far であるとは，次数の上限を保ったまま G を k 枝連結にするのに少なくとも ϵdn 本の辺の追加および削除が必要であることをいう．

本研究で示した検査アルゴリズムは，Property Testing と呼ばれる検査手法に従っている．これは入力グラフが k 枝連結であれば 2/3 以上の確率で受理し，k-枝連結から ϵ-far であれば 2/3 以上の確率で拒否するアルゴリズムとして定義される．

頂点次数を制限した無向グラフにおける k 枝連結の検査については既に結果が知られているが，この手法を有向グラフにそのまま適用することはできない．無向グラフにおいて成り立つカットに関する性質の多くが，有向グラフでは成り立たないからである．よって本研究では，新しいアイデアを用いてアルゴリズムを構築した．実際の計算機実験においても，n が十分に大きければ，決定性の $O(kn^2d)$ アルゴリズムに比べて本アルゴリズムが十分に実用的であるという結果が得られた．

7 3 次元 strip パッキング問題に対する Harmonic アルゴリズム

3 次元 strip パッキング問題では，3 次元直方体のアイテム $I = \{(x_i, y_i, z_i) : i = 1, \ldots, n\}$ と 3 次元の箱 B が与えられる．制約は重なることなしに全てのアイテムを箱 B にパッキングすることであり，目的はパッキングされた部分の高さを最小に

することである．本研究では，最も基本的な問題である，アイテムを回転させることなくアイテムの辺と箱 B の辺とが並行になるようにパッキングする場合について扱う．本研究では，2 次元ビンパッキングに対する Caprara のアルゴリズムを改良して，同様の性能保証である $T_\infty \approx 1.69$ の近似アルゴリズムを得た．ただし，T_∞ はよく知られている Harmonic 数という値であり，ビンパッキング問題において自然に現れる数である．これまで知られていた近似アルゴリズムは $2, 2.64, 2.67, 2.89, 3.25$ の最悪近似保証であった．また本研究では，全てのアイテムの底面が正方形の場合に漸近的 PTAS を得た．

8 2 点同時要求 k-サーバ問題

k-サーバ問題は Mark Manasse, Lyle A. McGeoch, Daniel Sleator によって提起された有名なオンライン問題のひとつである．距離空間上に k 個のサーバが存在し，要求点が順に与えられたときにいずれかのサーバが要求点に移動する．移動距離の総和をなるべく小さくすることが問題の目的となる．

従来の k-サーバ問題では要求点は常に 1 点であり，要求点にサーバが移動するまで次の要求点は与えられない．しかし，実用上の問題では要求点が 1 つずつ来るとは限らない．本研究では要求点が同時に 2 つ与えられる問題を対象に解析を行い，この問題の下界が $k-1$ であることを示した．また，2 点同時要求 m 点 k サーバ問題の競合比が $\binom{m}{k} - 1$ であることを証明した．

9 正直なオークションにおける入札者の談合

一般的に知られているオークションは，ある商品を購入する権利を複数の買い手が競い合うものである．本研究では，音楽ファイルやコンピュータ・ソフトウェアのように複製により無限に供給可能な商品を扱う 1 回秘密入札オークションを議論の対象とする．1 回秘密入札オークションとは，次のようなものである．入札は 1 度だけ行われ，その入札額は公開されない．競売人は全員の入札額から落札者と落札価格を決定する．このオークションで最も重要なのは，落札者が複数存在し得て，落札額がそれぞれ異なるということである．すべての入札者は落札者と落札価格の決定方法を知っており，それに合わせて自信の利得が最大になるような入札をする．

本研究ではオークションに談合の概念を定義し，既存のオークションであるコストシェアリング (CS)，サンプルコストシェアリング (SCS) における談合者の行動について解析し，どちらのオークションにおいても決定性の支配戦略が得られないことを示した．

10 入札額の範囲が制限された正直なオークション

本研究では，1 回のみの秘密入札で行われる正直なオークションについて扱う．ここでのオークションは競売人の立場に立って構成し，その利得の最大化を目的とする．また，販売する商品は複製にコストがかからず無限に供給できるものとし，入札者はそれぞれの商品を 1 個購入したいと考えているとする．正直なオークションとは，正直に入札することが入札者にとってそれぞれの最良の利得が得られるようなオークションのことである．設計する正直なオークションの評価には，正直ではないが単一価格全知のオークションとの利得の比で定義される競合比を用いる．任意の正直なオークションの競合比の下界は 2.42 であることが示されており，CORE オークションが競合比 3.39 を達成することが知られている．

本研究では，入札額の最大値が最小値の高々 r 倍という条件の下で，オークションのアルゴリズムを提案し，競合比の改善を図った．入札者に対する提示額の種類を確率分布に従って決定する手法と，入札者をランダムに 2 つの集合に分割する手法を組み合わせ，競合比 $\ln r + 1$ を達成した．これは $r < 10$ の範囲において，従来の CORE オークションの競合比の上界を改善している．

11 誤りを含むパリティ関数の量子アルゴリズムにおけるクエリ計算量

ブラックボックスモデルにおいて論理関数 OR や AND のクエリ計算量は $\Theta(N)$ である．一方，量子計算においては，Grover の探索アルゴリズムを用いることで $O(\sqrt{N})$ で実現できる．また，OR や AND の量子アルゴリズムの下界は $\Omega(\sqrt{N})$ であることも証明されている．しかし，すべての論理関数でクエリ計算量の減少が見込める訳ではない．多数決関数とパリティ関数は古典・量子ともにクエリ計算量が $\Theta(N)$ であることが証明されており，OR や AND のような高速化は期待できない．

本研究では，パラメータを持つ誤りを含むパリティ関数を定義し，クエリ計算量の上界が下がることを示した．また，この上界が下界と一致することを示し，アルゴリズムが最適であることを証明した．

12 いくつかのグラフにおける離散時間量子ウォークについて

量子計算とは，量子力学に基づいた量子ビットの特性を利用して考えられた計算機である．量子計算モデルにより，Shor の因数分解や Grover のデータベース探索などで，従来の計算機よりも高速に問題を解くことができるアルゴリズムが考案されている．

ランダムウォークを利用したアルゴリズムは古典計算モデルにおいて有用であり，様々な探索問題において使用されている．このことから，量子計算モデルにおいてもランダムウォークを利用した有効なアルゴリズムを設計できる可能性が高い．実際に，量子ウォークを用いて一部の探索問題については古典計算より指数的に高速なものも見つかっている．

本研究では，代表的な NP 完全問題である 3-SAT を離散時間量子ウォークアルゴリズムによって解くことを目標に，いくつかのグラフ上での量子ウォークの性質とその有効性を調べた．対象としたグラフは，Clever らの Glued-graph, n 次元 Hypercube グラフ，3-SAT の古典ランダムウォークを利用して作った 3-SAT グラフの 3 種類である．計算機シミュレーションによって，これらのウォークの分布や解に到達するまでの様子を確認した．

13 (4,1)-量子ランダムアクセス符号化の非存在性について

$(n, 1, p)$-量子ランダムアクセス符号化 (QRA) とは，Ambainis らによって導入された次のような通信システムである．送信者は n ビットの情報を 1 量子ビットに符号化し，受信者に送る．このとき受信者は，ある種の正作用素値測度を用いて，元の n ビットのうち任意の 1 ビットを確率 p で復元できる．Ambainis らは (2,1,0.85)-QRA が存在することを示し，古典ビットでは同じ符号化は行えないことを示した．Chuang はこの結果を拡張して (3,1,0.79)-QRA の存在を示した．それ以来，さらなる拡張である (4,1,p)-QRA ($p > 1/2$) が存在するかは未解決であった．本研究では，この未解決問題を否定的に解決した．すなわち $p > 1/2$ について (4,1,p)-QRA は存在しないことを示した．さらに，より一般的な複数量子ビットへの符号化に関しても，否定的な結果を導いた．

14 MAX-2SAT 問題の平均時間計算量の解析

2CNF 論理式の最大充足可能性問題 (MAX-2SAT) とは，和積形のブール論理式で各節に含まれるリテラルの数が高々2 個であるものが与えられた時，できるだけ多くの節を真にする真理値割り当てを求める最適化問題である．本研究では MAX-2SAT の平均時間計算量を解析するために，入力例題を生成する確率分布として，埋め込み解モデルを提案した．節数の密度をパラメータに取ると，パラメータの広い範囲で生成された例題は埋め込まれた解を最適解として持つ確率が高いことを示した．また，メッセージ伝播法に基づく線形時間アルゴリズムの解析を行い，このモデルに対して高い確率で最適解が得られることも示した．

15 SAT充足解の偏りを利用した局所探索の高速化

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．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．Schöningは3SATに対して時間計算量が1.334^nである単純な局所探索アルゴリズムを与えた．本研究では，充足解にある種の偏りがあるときにアルゴリズムを修正して高速化できることを示した．修正されたアルゴリズムは，充足解の0の個数と1の個数が偏っている場合，すなわち解が$p_0 n$の0と$p_1 n$の1を含む場合，例えば$p_0 = 1/3$ならば1.260^n時間で，$p_0 = 0.1$ならば1.072^n時間で解を見つけることができる．そのような偏りは他の組合せ問題からSATに還元した例題によく見られるため，この種の改良は実用的であると言える．本研究では具体例として，3次元マッチングから変換した例題を取り上げ，修正されたアルゴリズムが，総当たり法よりも高速に動作することを示した．また，いくつかのベンチマーク例題に対して計算機実験を行い，既存のアルゴリズムと比較した．

16 対称関数を実現する定数段数回路について

計算量理論は理論計算機科学分野において重要な研究のひとつである．計算機を用いて問題を解くときに，計算量理論は必要な時間やメモリの領域量の重要な指標となる．この分野においては様々な研究がなされているが，本研究ではその中でも回路計算量に焦点をあてる．

回路計算量とは，具体的な論理関数を計算する回路の段数や素子数に関する研究である．回路計算量の研究を行うことはその具体的な論理関数を計算する回路の効率のよい構築法を考えることを暗に意味している．しかし，それが全てではなく，さらに重要な意義が存在している．

回路計算量はTuring機械における計算複雑さと密接に関係している．Turing機械における計算量の分野には長年にわたる大きな未解決問題として，P対NP問題がある．ある明示的な論理関数における回路計算量の下限の研究は，P対NP問題の解決のための有望な手段のひとつである．

本研究では，対称関数，特に閾値関数や多数決関数を計算する定数段数回路の構成法を考える．最近まで，n変数多数決関数を計算する3段回路について，素子数が高々$2^{O(\sqrt{n \log n})}$となる構成法が知られていた．これに対して，G.Wolfovitsは2006年に，素子数が$2^{O(\sqrt{n})}$の3段回路の存在を示した．しかし，彼の証明には致命的な誤りが含まれていた．本研究ではまず，これらの誤りを指摘し，その構成法の修正と解析をおこない，その構成法で構成される対称関数を実現する回路の素子数を示した．また，この構成法を元に新たな構成法を与えることで，任意の対称関数について素子数$2^{O(\sqrt{n \log n})}$の回路が存在することを示した．さらに段数dの定数段数回路において，任意の対称関数について素子数$2^{O(n^{\frac{1}{d-1}} (\log n)^{\frac{d-2}{d-1}})}$の回路が存在することを示した．

17 単調論理回路における還元

0-1ソートや0-1マージ等のブール関数を含む大きな計算量クラスであるNLOGは，単調回路のサイズに対して$O(n \log n)$の上界が示されている．つまり，NLOGが含む関数は，$O(n \log n)$個のファンイン数2のAND/ORゲートで構成される回路を持つ．今，AND/OR以外にr (≥ 2)個の入力とr' (≥ 1)個の出力をもち，単調ブール関数Fを実現する“F-ゲート”を使えると仮定する．ただし，AND/ORゲートのコストを1とするのに対し，F-ゲートのコストはrであるとする．NLOGに属す関数fを，合計コスト$o(n \log n)$のAND/OR/Fゲートからなる回路で計算可能なとき，F-容易と呼ぶことにする．本研究では，0-1マージが$r' \leq r/\log r$となる任意のFに対してF-容易とはならないことを証明した．

18 論理式における非線形下界証明手法の回路への拡張

論理関数の回路計算量とは，その関数を計算する論理回路を構成するのに必要な素子数のことである．明示的な関数に対して良い回路計算量の下界を示すことは，計算機科学における重要な研究の一つである．一般的な回路に対して，ほぼ全ての関数は非常に大きい下界 (超多項式程度の下界) を持つことが示されている．この事実の証明は数え上げ論法によるもので，明示的な関数に対して良い下界を示すのは非常に難しく，現在知られている最も良い下界は線形程度 $(5n - o(n))$ である．従って，回路に様々な制約を付けて下界を考えるのは自然なアプローチである．そのような制約の代表例として論理式がある．論理式においてはある程度良い非線形の下界 $(\Omega(n^{3-o(1)}))$ が得られている．本研究では，論理式における非線形下界証明手法を回路に拡張することを目的として，一般の回路と論理式の間のモデルとなるカクタス回路を定義し，このカクタス回路に対して非線形下界証明手法を拡張した．カクタス回路とは，どの二つの閉路も高々一つの接点しか共有しないような回路のことである．カクタス回路においては，出力 3 以上の素子は存在せず，また一度出力 2 の素子が表れると，閉路が閉じるまで再び出力 2 の素子が表れることは無い．また論理回路では各素子が一つの論理関数を計算するが，ここで使える論理関数の種類 (基底) によってその性質が大きく異なる．本研究では，基底が任意の有限基底である場合と，U_2 である場合の二つの場合について考察を行った．結果として，基底が全ての有限基底である場合では $\Omega(n^2/\log n)$ の下界を証明し，基底が U_2 である場合には $\Omega(n^{13/6-o(1)})$ の下界を証明した．

19 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）通信が多く用いられている．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，帯域の利用率の低い，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た．

本研究では，距離 2 の彩色の結果を利用した，帯域の利用率が高い 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．さらに提案手法の帯域利用率について，シミュレーションにより既存の TDMA スケジューリングである Ramanathan の手法に対しては 38.9 ∼ 9.2% の改善，神崎らの手法に対しては 7.4 ∼ 3.9% の改善を実現し，これにより既存手法に対して帯域の高い利用率を達成していることを示した．

20 P2P システムの適応乱択探索プロトコル

P2P のファイル共有システムにおいて，目標となるファイルを持つピアを探す問題は重要である．P2P システムは巨大で動的なピアを維持するため，探索プロトコルはスケーラブルで適応性のあることが望まれる．

本研究では，適応乱択探索プロトコル（ARSP）と呼ばれる新しい P2P 探索プロトコルを提案した．本プロトコルは，コーラムベースプロトコルの効率的な拡張である．ARSP では，対象の人気度次第で通信コストが最小となる．また興味深いことに，ARSP は自己適応性をもち，ネットワーク環境の動的変化に自動的に適応することができる．

研究業績一覧

著書

1. 岩間一雄:
   “アルゴリズム・サイエンス: 出口からの超入門”, 共立出版, 2006 年 10 月.

学術論文

1. H. Kakugawa, and T. Masuzawa:
"A Self-Stabilizing Minimal Dominating Set Algorithm with Safe Convergence", Proc. the 8th Workshop on Advances on Parallel and Distributed Processing Symposium (APDCM) (Workshop of the 20th IEEE International Parallel and Distributed Processing Symposium), no.103, pp.8, 2006 年 4 月.
概要: A self-stabilizing distributed system is a fault-tolerant distributed system that tolerates any kind and any finite number of transient faults, such as message loss and memory corruption. In this paper, we formulate a concept of safe convergence in the framework of self-stabilization. An ordinary self-stabilizing algorithm has no safety guarantee while it is in converging from any initial configuration. The safe convergence property guarantees that a system quickly converges to a safe configuration, and then, it gracefully moves to an optimal configuration without breaking safety. Then, we propose a minimal independent dominating set algorithm with safe convergence property. Especially, the proposed algorithm computes the lexicographically first minimal independent dominating set according to the process identifier as a priority. The priority scheme can be arbitrarily changed such as stability, battery power and/or computation power of node.

2. Y. Nakaminami, H. Kakugawa, and T. Masuzawa:
"An Advanced Performance Analysis of Self-Stabilizing Protocols: Stabilization Time with Transient Faults During Convergence", Proc. the 8th Workshop on Advances on Parallel and Distributed Processing Symposium (APDCM) (Workshop of the 20th IEEE International Parallel and Distributed Processing Symposium), no.106, pp.8, 2006 年 4 月.
概要: A self-stabilizing protocol is a brilliant framework for fault tolerance. It can recover from any number and any type of transient faults and eventually converge to its intended behavior. Performance of a self-stabilizing protocol is usually measured by stabilization time: the time required to complete the convergence to its intended behavior under the assumption that no new fault occurs during the convergence. But a self-stabilizing protocol has no guarantee to complete the convergence if faults are frequently occurred. This paper brings new light to efficiency analysis of stabilization. The efficiency is evaluated with consideration for faults occurring during the convergence. To show the feasibility and effectiveness of the approach, this paper applies the approach to the maximal matching protocol.

3. 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.E89-A, no.5, pp.1292–1298, 2006 年 5 月.
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 fragments 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.

4. K. Sugihara, and H. Ito:
"Maximum-Cover Source-Location Problems", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.E89-A, no.5, pp.1370–1377, 2006 年 5 月.
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.

5. S. Kato, S. Miyazaki, Y. Nishimura, and Y. Okabe:
"Cheat-Proof Serverless Network Games", 5th International Conference on Computers and Games (CG 2006), 2006 年 5 月.
概要: We consider playing online games on peer-to-peer networks, without assuming servers that control the execution of a game. In such an environment, players may cheat the opponent by, for example, illegally replacing the cards in their hands. The aim of this paper is to examine a possibility of excluding such cheatings. We show that by employing cryptographic techniques, we can exclude some types of cheating at some level. Finally, based on our discussion, we implement cheat-proof network "Gunjin-Shogi", which is a variant of Japanese Chess.

6. H. Ito:
"Harary's Generalized Ticktacktoe", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.J89-A, no.6, pp.458–469, 2006 年 6 月.
概要: The generalized ticktacktoe, presented by F. Harary, is a game that two players put a stone on a given square grid board alternately and one who make a given animal (figure) by his or her stones first is the winner. For any animal, if the both players play optimally, the first player wins (the animal is a winner) or the game is brought to a draw (the animal is a loser). The problem which animals are winners or losers have been investigated and have been solved for many animals. This paper surveys the results, techniques, and open problems of the game, and discusses directions of feature work.

7. F. Ooshita, S. Matsumae, and T. Ma-

suzawa:
"Scheduling Independent Tasks on Heterogeneous Parallel Computing Environments under the Unidirectional One-Port Model", Proc. the 2006 International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'06), vol.2, pp.690–696, 2006年6月.
概要: For execution of computation-intensive applications, one of the most important paradigms is to divide the application into a large number of small independent tasks and execute them on heterogeneous parallel computing environments (abbreviated by HPCEs). In this paper, we aim to execute independent tasks efficiently on HPCEs. We consider the problem to find a schedule that maximizes the throughput of task execution for a huge number of independent tasks. First, we show that we can find, in polynomial time, a schedule that attains the optimal throughput. This algorithm, however, uses the ellipsoid method, hence it is very time-consuming. Therefore, secondly, we propose a fast $(3/2+\epsilon)$-approximation algorithm for any constant ϵ $(0 < \epsilon < 1)$. In addition, we also show that the framework of our approximation algorithm can be applied to other collective communications such as the gather operation.

8. K. Sugihara, and H. Ito:
"Maximum-Cover Source-Location Problem with Object Edge-Connectivity Three", Proc. Cologne-Twente Workshop on Graphs and Combinatorial Optimization (CTW 2006), pp.131–136, 2006年6月.
概要:

9. X. Han, K. Iwama, R. Klein, and A. Lingas:
"Approximating the Maximum Independent Set and Minimum Vertex coloring on box graphs", Proc. the 9th Japan-Korea Joint Workshop on Algorithms and Computation (WAAC 2006), pp.33–60, 2006年6月.
概要: A box graph is the intersection graph of a finite set of orthogonal rectangles in the plane. The problem of whether or not the maximum independent set problem (MIS for short) for box graphs can be approximated within a substantially sublogarithmic factor in polynomial time has been open for several years. We show that for box graphs on n vertices which have an independent set of size $\Omega(n/\log^{O(1)} n)$ the maximum independent set problem can be approximated within $O(\log n/\log\log n)$ in polynomial time. Furthermore, we show that the chromatic number of a box graph on n vertices is within an $O(\log n)$ factor from the size of its maximum clique and provide an $O(\log n)$ approximation algorithm for minimum vertex coloring of such a box graph. More generally, we can show that the chromatic number of the intersection graph of n d-dimensional orthogonal rectangles is within an $O(\log^{d-1} n)$ factor from the size of its maximum clique and obtain an $O(\log^{d-1} n)$ approximation algorithm for minimum vertex coloring of such an intersection graph.

10. K. Iwama:
"Classic and Quantum Network Coding (Invited Talk)", Proc. 10th Scandinavian Workshop on Algorithm Theory (SWAT 2006), LNCS 4059, pp.3–4, 2006年6月.
概要:

11. A. Ambainis, K. Iwama, A. Kawachi, R. Raymond, and S. Yamashita:
"Improved Algorithms for Quantum Identification of Boolean Oracles", Proc. 10th Scandinavian Workshop on Algorithm Theory (SWAT 2006), LNCS 4059, pp.280–291, 2006年6月.
概要: The oracle identification problem (OIP) was introduced by Ambainis et al.

[3]. It 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 improve the algorithms in [3] by providing a mostly optimal upper bound of query complexity for this problem: (i) For any oracle set S such that $|S| \leq 2^{N^d}$ $(d < 1)$, we design an algorithm whose query complexity is, $O(\sqrt{N \log N / \log N})$ matching the lower bound proved in [3]. (ii) Our algorithm also works for the range between 2^{N^d} and $2^{N/\log N}$ (where the bound becomes $O(N)$), but the gap between the upper and lower bounds worsens gradually. (iii) Our algorithm is robust, namely, it exhibits the same performance (up to a constant factor) against the noisy oracles as also shown in the literatures [2, 11, 18] for special cases of OIP.

12. M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita:
"(4,1)-Quantum Random Access Coding Does Not Exist", Proc. of IEEE International Symposium on Information Theory (ISIT 2006), pp.446–450, 2006年6月.
概要: An $(n, 1, p)$-Quantum Random Access (QRA) coding, introduced by Ambainis, Nayak, Ta-shma and Vazirani in ACM Symp. on Theory of Computing 1999, is the following communication system: The sender which has n-bit information encodes his/her information into one qubit, which is sent to the receiver. The receiver can recover any one bit of the original n bits correctly with probability at least p, through a certain decoding process based on positive operator-valued measures. Actually, Ambainis et al. shows the existence of a (2,1,0.85)-QRA coding and also proves the impossibility of its classical counterpart. Chuang immediately extends it to a (3,1,0.79)-QRA coding and whether or not a $(4, 1, p)$-QRA coding such that $p > 1/2$ exists has been open since then. This paper gives a negative answer to this open question.

13. Y. Nakaminami, T. Masuzawa, and T. Herman:
"Linear-State-Transition Protocols: Asynchronous Protocols with Ease of Efficiency Evaluation", Journal of Aerospace Computing, Information, and Communication (JACIC), vol.3, no.6, pp.281–293, 2006年6月.
概要: Distributed systems are commonly modeled by asynchronous models where no assumption is made about process execution speed. The asynchronous model is preferable to the synchronous one because the model reflects the fact that a distributed system consists of heterogeneous computers and their performance varies with time depending on their loads. However, the asynchrony of the system makes it difficult to evaluate efficiency (performance) of distributed protocols.To diminish the difficulty, this paper introduces a class of distributed protocols called linear-state-transition protocols (LST protocols) in the shared-state model and shows that efficiency of the LST protocols in the asynchronous distributed model can be derived from analysis of their synchronous execution where all processes are synchronized in the lock-step fashion. This provides an effective method for evaluating efficiency of the LST protocols in the asynchronous distributed model. The paper also demonstrates the effectiveness of the method by applying it to the self-stabilizing alternator.

14. T. Izumi, and T. Masuzawa:
"Condition Adaptation in Synchronous Consensus", IEEE Transactions on Com-

puters, vol.55, issue 7, pp.843–853, 2006年7月.

概要: The condition-based approach is one of the sophisticated methods used to overcome several impossibility results in the 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 introduce the new 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. The execution time of adaptive condition-based algorithms depends on the legality level of input vectors. We propose two adaptive condition-based algorithms for synchronous consensus. The first algorithm requires that the majority of processes be correct, and terminates within $\min\{f+2, t+1\}-l$ rounds if $l < f$, where f and t are the actual and the maximum numbers of faults, respectively, and l is the legality level of the input vector. Moreover, the algorithm terminates in one round if $l \geq t$ and $f = 0$ and terminates within two rounds if $l \geq f$ holds. Compared with previous algorithms, this algorithm achieves the best time complexity. The second algorithm can tolerate any number of faults, and terminates within $\max\{3, \min\{f+3, t+2\}-l\}$ rounds if $l < f$ holds, terminates in one round if $l \geq t$ and $f = 0$, and terminates within three rounds if $l \geq f$ holds.

15. Y. Kiyonari, E. Miyano, and S. Miyazaki: "Computational Complexity Issues in University Interview Timetabling", Proc. the 6th International Conference on the Practice and Theory of Automated Timetabling (PATAT 2006), pp.448–453, 2006年8月.

    概要: This paper introduces a new timetabling problem on universities, called interview timetabling. In this problem, some constant number, say, three, of referees are assigned to each of $2n$ graduate students. It requires to assign these students to an $n \times 2$ array, consisting of n timeslots and two rooms, so that two students sharing the same referee must be assigned to different timeslots. Furthermore, we want to minimize the total number of movements of all referees between two rooms. This is a problem actually having arisen in the interview timetabling in Kyoto University. We propose two restricted models of this problem, and investigate their time complexities.

16. K. Iwama, and H. Morizumi: "Reductions for Monotone Boolean Circuits", Proc. the 31st International Symposium on Mathematical Foundations of Computer Science (MFCS 2006), LNCS 4162, pp.540–548, 2006年8月.

    概要: The large class, say *NLOG*, of Boolean functions, including 0-1 Sort and 0-1 Merge, have an upper bound of $O(n \log n)$ for their monotone circuit size, i.e., have circuits with $O(n \log n)$ AND/OR gates of fan-in two. Suppose that we can use, besides such normal AND/OR gates, any number of more powerful "F-gates" which realize a monotone Boolean function F with $r(\geq 2)$ inputs and $r'(\geq 1)$ outputs. Note that the cost of each AND/OR gate is one and we assume that the cost of each F-gate is r. Now we define: A Boolean function f in NLOG is said to be F-Easy if f can be

constructed by a circuit with AND/OR/F gates whose total cost is $o(n \log n)$. In this paper we show that 0-1 Merge is not F-Easy for an arbitrary monotone function F such that $r' \leq r/\log r$.

17. M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita:
"(4,1)-Quantum Random Access Coding does not Exist — One Qubit is not Enough to Recover One of Four Bits", New Journal of Physics, vol.8, no.129, 2006年8月.
概要: An $(n, 1, p)$-quantum random access (QRA) coding, introduced by Ambainis et al (1999 *ACM Symp. Theory of Computing* p 376), is the following communication system: the sender which has n-bit information encodes his/her information into one qubit, which is sent to the receiver. The receiver can recover any one bit of the original n bits correctly with probability at least p, through a certain decoding process based on positive operator-valued measures. Actually, Ambainis et al shows the existence of a (2,1,0.85)-QRA coding and also proves the impossibility of its classical counterpart. Chuang immediately extends it to a (3,1,0.79)-QRA coding and whether or not a (4,1,p)-QRA coding such that $p > 1/2$ exists has been open since then. This paper gives a negative answer to this open question. Moreover, we generalize its negative answer for one-qubit encoding to the case of multiple-qubit encoding.

18. K. Iwama, S. Miyazaki, and K. Okamoto:
"A $(2 - c \log N/N)$-Approximation Algorithm for the Stable Marriage Problem", IEICE Transactions on Information and Systems, vol.E89-D, no.8, pp.2380–2387, 2006年8月.
概要: An instance of the classical stable marriage problem requires all participants to submit a strictly ordered preference list containing all members of the opposite sex. However, considering applications in real-world, we can think of two natural relaxations, namely, incomplete preference lists and ties in the lists. Either variation leaves the problem polynomially solvable, but it is known that finding a maximum cardinality stable matching is NP-hard when both variations are allowed. It is easy to see that the size of any two stable matchings differ by at most a factor of two, and so, an approximation algorithm with a factor two is trivial. A few approximation algorithms have been proposed with approximation ratio better than two, but they are only for restricted instances, such as restricting occurrence of ties and/or lengths of ties. Up to the present, there is no known approximation algorithm with ratio better than two for general inputs. In this paper, we give the first nontrivial result for approximation of factor less than two for general instances. Our algorithm achieves the ratio $2 - c\frac{\log N}{N}$ for an arbitrarily positive constant c, where N denotes the number of men in an input.

19. T. Imamura, K. Iwama, and T. Tsukiji:
"Approximated Vertex Cover for Graphs with Perfect Matchings", IEICE Transactions on Information and Systems, vol.E89-D, no.8, pp.2405–2410, 2006年8月.
概要: Chen and Kanj considered the VERTEX COVER problem for graphs with perfect matchings (VC-PM). They showed that: (i) There is a reduction from general VERTEX COVER to VC-PM, which guarantees that if one can achieve an approximation factor of less than two for VC-PM, then one can do so for general VERTEX COVER as well. (ii) There is an algorithm for VC-PM whose approximation factor is given as $1.069 + 0.069d$ where d is the average degree of the given graph. In this paper we improve (ii). Namely we give a new VC-PM algorithm which greatly outperforms the above one and its approximation factor is roughly

$2-6.74/d+6.28$. Our algorithm also works for graphs with "large" matchings, although its approximation factor is degenerated.

20. T. Izumi, and T. Masuzawa:
"One-Step Consensus Solvability", Proc. the 20th International Symposium on Distributed Computing (DISC 2006), LNCS 4167, pp.224–237, 2006 年 9 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 an 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 an 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 vectors for which the consensus can be solved in one step 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 an instance of the sufficient condition sequences. Compared with existing constraints for inputs this instance is more relaxed.

21. Y. Sakurai, F. Ooshita, and T. Masuzawa:
"A Self-Stabilizing Link-Coloring Protocol in Tree Networks with Permanent Byzantine Faults", Journal of Aerospace Computing, Information, and Communication (JACIC), Vol.3, No.9, pp.424–437, 2006 年 9 月.
概要: Self-stabilizing protocols can tolerate any type and any number of transient faults. But self-stabilizing protocols have no guarantee of their behavior against permanent faults. Thus, investigation concerning self-stabilizing protocols resilient to permanent faults is important. This paper proposes a self-stabilizing link-coloring protocol resilient to permanent Byzantine faults in tree networks. The protocol assumes the central daemon, and uses $\Delta+1$ colors where Δ is the maximum degree in the network. This protocol guarantees that, for any non-faulty process v, if the distance from v to any Byzantine ancestor of v is greater than two, v reaches its desired states within three rounds and never changes its states after that. Thus, it achieves fault containment with radius of two. Moreover, we prove that the containment radius becomes $\Omega(\log n)$ when we use only Δ colors, and prove that the containment radius becomes $\Omega(n)$ under the distributed daemon. These lower bound results prove necessity of $\Delta+1$ colors and the central daemon to achieve fault containment with a constant radius.

22. 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, vol.154/16, pp.2247–2262, 2006 年 11 月.
概要: In this paper, we study how to collect n balls moving with a fixed constant velocity 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;

(iii) minimizing the number of the robots to collect all n balls. The situations considered in this paper 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.

23. Y. Hanatani, T. Horiyama, and K. Iwama: "Density Condensation of Boolean Formulas", Discrete Applied Mathematics, vol.154/16, pp.2263–2270, 2006 年 11 月.
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.

24. H. Ito, and H. Nagamochi:
"Two Equivalent Measures on Weighted Hypergraphs", Discrete Applied Mathematics, vol.154/16, pp.2330–2334, 2006 年 11 月.
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 $0 \leq i < j < k \leq n-1$, 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 eE 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:
· $A_P(H) \leq A_P(H')$ for all convex n-gons P.
· $c_H(i,j,k) c'_H$ (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 "$A_P(H) \leq A_P(H')''$ for all convex n-gons P'' is immediately obtained.

25. T. Masuzawa, and S. Tixeuil:
"Bounding the Impact of Unbounded Attacks in Stabilization", Proc. the 8th International Symposium on Stabilization, Safety and Security of Distributed Systems (SSS 2006), LNCS 4280, pp.440–453, 2006 年 11 月.
概要: As a new challenge of containing the unbounded influence of Byzantine processes in self-stabilizing protocols, this paper introduces a novel concept of strong stabilization. The strong stabilization relaxes the requirement of strict stabilization so that processes beyond the containment radius are allowed to be disturbed by Byzantine processes, but only a limited number of times. A self-stabilizing protocol is (t, c, f)-strongly stabilizing if any process more than c hops away from any Byzantine process is disturbed at most t times in a distributed system with at most f Byzantine processes. Here c denotes the containment radius and t denotes the containment times. The pos-

sibility and the effectiveness of the strong stabilization is demonstrated using tree orientation. It is known that the tree orientation has no strictly stabilizing protocol with a constant containment radius. This paper first shows that the problem has no constant bound of the containment radius in a tree with two Byzantine processes even when we allow processes beyond the containment radius to be disturbed any finite number of times. Then we consider the case of a single Byzantine process and present a $(1, 0, 1)$-strongly stabilizing protocol, which achieves optimality in both containment radius and times.

26. T. Masuzawa, and S. Tixeuil:
"On Bootstrapping Topology Knowledge in Anonymous Networks", Proc. the 8th International Symposium on Stabilization, Safety and Security of Distributed Systems (SSS 2006), LNCS 4280, pp.454–468, 2006 年 11 月.
概要: In this paper, we quantify the amount of " practical " information (i.e. views obtained from the neighbors, colors attributed to the nodes and links) to obtain " theoretical " information (i.e. the local topology of the network up to distance k) in anonymous networks. In more details, we show that a coloring at distance $2k + 1$ is necessary and sufficient to obtain the local topology at distance k that includes outgoing links. This bound drops to $2k$ when outgoing links are not needed. A second contribution of this paper deals with color bootstrapping (from which local topology can be obtained using the aforementioned mechanisms). On the negative side, we show that (i) with a distributed daemon, it is impossible to achieve deterministic color bootstrap, even if the whole network topology can be instantaneously obtained, and (ii) with a central daemon, it is impossible to achieve distance m when instantaneous topology knowledge is limited to m . 1. On the positive side, we show that (i) under the k-central daemon, deterministic self-stabilizing bootstrap of colors up to distance k is possible provided that k-local topology can be instantaneously obtained, and (ii) under the distributed daemon, probabilistic self-stabilizing bootstrap is possible for any range.

27. Y. Yamauchi, S. Kamei, F. Ooshita, Y. Katayama, H. Kakugawa, and T. Masuzawa:
"Composition of Fault-Containing Protocols Based on Recovery Waiting, Fault-Containing Composition Framework", Proc. the 8th International Symposium on Stabilization, Safety and Security of Distributed Systems (SSS 2006), LNCS 4280, pp.516–532, 2006 年 11 月.
概要: Self-stabilizing protocols provide autonomous recovery from finite number of transient faults. Fault-containing self-stabilizing protocols promise not only self-stabilization but also quick recovery from and small effect of a small number of faults. However, existing composition techniques of self-stabilizing protocols (e.g. fair composition) cannot preserve the fault-containment property when composing fault-containing protocols. In this paper, we present *Recovery Waiting Fault-containing Composition* (*RWFC*) framework that preserves the fault-containment property of the composed protocol. We show an example of fault-containing composition of a minimum spanning tree protocol on arbitrary weighted graphs and a median finding protocol on trees via *RWFC*.

28. Y. Wu, T. Izumi, F. Ooshita, H. Kakugawa, and T. Masuzawa:
"An Adaptive Randomised Searching Protocol in Peer-to-Peer Systems Based on

Probabilistic Weak Quorum System", Proc. the 8th International Symposium on Stabilization, Safety and Security of Distributed Systems (SSS 2006), LNCS 4280, pp.586–587, 2006年11月.
概要: In this paper we propose a new Peer-to-peer searching protocol called Adaptive Randomised Searching Protocol (ARSP) which is an efficient extension of the searching protocol based on Probabilistic Weak Quorum System (PWQS). ARSP has good characteristics such as scalability, load balance and self-stabilization inherited from the original protocol. In addition, it achieves better message complexity which is self-optimized to the minimum according to network environment.

29. K. Iwama:
"Stable Matching Problems (Invited Talk)", Proc. International Symposium on Symbolic and Algebraic Computation (ISAAC 2006), LNCS 4288, pp.1, 2006年12月.
概要:

30. T. Horiyama, K. Iwama, and J. Kawahara:
"Finite-State Online Algorithms and Their Automated Competitive Analysis", Proc. the 17th Annual International Symposium on Algorithms (ISAAC 2006), LNCS 4288, pp.71–80, 2006年12月.
概要: In this paper we study the Revocable Online Knapsack Problem (ROKP) which is an extension of the Online Knapsack Problem. We prove an optimal upper bound of $1/t$ for the competitive ratio of ROKP, 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 base algorithm that is designed in a conventional manner, 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+.

31. K. Iwama, H. Morizumi, and J. Tarui:
"Negation-Limited Complexity of Parity and Inverters", Proc. the 17th Annual International Symposium on Algorithms (ISAAC 2006), LNCS 4288, pp.223–232, 2006年12月.
概要: We give improved lower bounds for the size of negation-limited circuits computing Parity and for the size of negation-limited inverters. An inverter is a circuit with inputs $x_1, \ldots, x_n$ and outputs $\neg x_1, \ldots, \neg x_n$. We show that (1) For $n = 2^r - 1$, circuits computing Parity with $r-1$ NOT gates have size at least $6n - \log_2(n+1) - O(1)$ and (2) For $n = 2^r - 1$, inverters with r NOT gates have size at least $8n - \log_2(n+1) - O(1)$. We derive our bounds above by considering the minimum size of a circuit with at most r NOT gates that computes Parity for *sorted* inputs $x_1 \geq \cdots \geq x_n$. For an *arbitrary* r, we completely determine the minimum size. For odd n, it is $2n-r-2$ for $\lceil \log_2(n+1) \rceil - 1 \leq r \leq n/2$, and it is $\lfloor 3/2\, n \rfloor - 1$ for $r \geq n/2$. We also determine the minimum size of an *inverter for sorted inputs* with at most r NOT gates. It is $4n-3r$ for $\lceil \log_2(n+1) \rceil \leq r \leq n$. In particular, the negation-limited inverter for sorted inputs due to Fischer, which is a core component in all the known constructions of negation-limited inverters, is shown to have the minimum possible size. Our fairly simple lower bound proofs use gate elimination arguments.

32. T. Izumi, and T. Masuzawa:

"A Weakly-Adaptive Condition-Based Consensus Algorithm in Asynchronous Distributed Systems", Information Processing Letters, vol.100, issue 5, pp.199–205, 2006 年 12 月.

概要: The condition-based consensus is one of sophisticated approaches to circumvent the insolvability of the consensus problem in asynchronous distributed systems prone to crash faults. It is specified by conditions on input vectors, and condition-based consensus algorithms can correctly solves the consensus if actual input vectors satisfy a particular condition. In this paper, we study about the feasibility of the adaptive condition-based consensus in asynchronous systems. In the adaptive condition-based consensus, all possible input vectors are classified into hierarchical conditions according to their difficulty. We consider consensus algorithms as the following form: They are instantiated by a condition sequence of $t+1$ hierarchical conditions, where t is the maximum number of crash faults, and guarantee to solve the consensus problem if the input vector belongs to the k-th class in the hierarchy and at most k processes crash. This paper proposes the notion of legality, which completely characterinzes the property of condition sequences for which adaptive condition-based consensus algorithms exist. In addition, we also show an instance of legal condition sequences. It is defined for a threshold value k. If the actual number of crash faults is smaller than k, the example for this condition sequence solves the consensus problem for a larger set of input vectors than the non-adaptive algorithm. However, if more than k processes crash, this algorithm solves the consensus only for a small set of input vectors than the existing one. In this sense, this algorithm is weakly-adaptive.

33. T. Suzuki, T. Izumi, F. Ooshita, and T. Masuzawa:
"Self-Adaptive Mobile Agent Population Control in Dynamic Networks Based on the Single Species Population Model", IEICE Transactions on Information and Systems, vol.E90-D, no.1, pp.314–324, 2007 年 1 月.

概要: Mobile-agent-based distributed computing is one of the most promising paradigms to support autonomic computing in a large-scale of distributed system with dynamics and 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 the application on the mobile-agent-based system. This paper considers the mobile agent population control problem in dynamic networks: it requires adjusting the number of agents to a constant fraction of the current network size. This paper proposes algorithms inspired by the single species population model, which is a well-known population ecology model. These two algorithms are different in knowledge of networks each node requires. The first algorithm requires global information at each node, while the second algorithm requires only the local information. This paper shows by simulations that the both algorithms realize self-adaptation of mobile agent population in dynamic networks, but the second algorithm attains slightly lower accuracy than the first one.

34. 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 スケジュール法", 情報処理学会論文誌, 第 48 巻, no.1, pp.327–341, 2007 年 1 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，帯域の利用率が高い 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り，提案手法の帯域利用率についても測定し，既存の TDMA スケジューリングである Ramanathan の手法に対しては 38.9 ～ 9.2% の改善，神崎らの手法に対しては 7.4 ～ 3.9% の改善を実現し，既存手法に対して帯域の高い利用率を達成していることを示す．

35. N. Bansal, X. Han, K. Iwama, M. Sviridenko, and G. Zhang:
"Harmonic Algorithm for 3-Dimensional Strip Packing Problem", Proc. 18th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2007), pp.1197–1206, 2007 年 1 月.
概要: In the three dimensional strip packing problem, we are given a set of three-dimensional rectangular items $I = \{(x_i, y_i, z_i) : i = 1, \ldots, n\}$ and a three dimensional box B. The goal is to pack all the items in the box B without any overlap, such that the height of the packing is minimized. We consider the most basic version of the problem, where the items must be packed with their edges parallel to the edges of B and cannot be rotated. Building upon Caprara's work for the two dimensional bin packing problem we obtain an approximation algorithm with a similar performance guarantee of $T_\infty \approx 1.69$ where T_∞ is the well known Harmonic number that occurs naturally in the context of bin packing. The previously known approximation algorithms for this problem had worst case performance guarantees of 2, 2.64, 2.67, 2.89 and 3.25. Our second algorithm is an asymptotic PTAS for the case in which all items have *square* bases.

36. K. Iwama, S. Miyazaki, and N. Yamauchi:
"A 1.875-Approximation Algorithm for the Stable Marriage Problem", Proc. 18th ACM-SIAM Symposium on Discrete Algorithms (SODA 2007), pp.288–297, 2007 年 1 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 known to be APX-hard, and the current best known approximation algorithm achieves the approximation ratio $2 - c\frac{1}{\sqrt{N}}$, where c is some positive constant. In this paper, we give a 1.875–approximation algorithm, which is the first result on the approximation ratio better than two.

37. Y. Asahiro, E. Miyano, S. Miyazaki, and T. Yoshimuta:
"Weighted Nearest Neighbor Algorithms for the Graph Exploration Problem on Cycles", Proc. 33rd Conference on Current Trends in Theory and Practice of Informatics (SOFSEM 2007), LNCS 4362, pp.164–175, 2007 年 1 月.
概要: In the graph exploration problem, a searcher explores the whole set of nodes of an unknown graph. The searcher is not aware of the existence of an edge until he/she visits one of its endpoints. The searcher's task is to visit all the nodes and go back to the starting node by traveling as a short tour as possible. One of the simplest strategies is the nearest neighbor algorithm (NN), which always chooses the unvisited node nearest to the searcher's current po-

sition. The weighted NN (WNN) is an extension of NN, which chooses the next node to visit by using the weighted distance. It is known that WNN with weight 3 is 16-competitive for planar graphs. In this paper we prove that NN achieves the competitive ratio of 1.5 for cycles. In addition, we show that the analysis for the competitive ratio of NN is tight by providing an instance for which the bound of 1.5 is attained, and NN is the best for cycles among WNN with all possible weights. Furthermore, we prove that no online algorithm is better than 1.25-competitive.

38. F. Ooshita, S. Matsumae, and T. Masuzawa:
"Scheduling for Independent-Task Applications on Heterogeneous Parallel Computing Environments under the Unidirectional One-Port Model", IEICE Transactions on Information and Systems, vol.E90-D, no.2, pp.403–417, 2007年2月.
概要: For execution of computation-intensive applications, one of the most important paradigms is to divide the application into a large number of small independent tasks and execute them on heterogeneous parallel computing environments (abbreviated by HPCEs). In this paper, we aim to execute independent tasks efficiently on HPCEs. We consider the problem to find a schedule that maximizes the throughput of task execution for a huge number of independent tasks. First, for HPCEs where the network forms a directed acyclic graph, we show that we can find, in polynomial time, a schedule that attains the optimal throughput. Secondly, for arbitrary HPCEs, we propose an $(3/2 + \epsilon)$-approximation algorithm for any constant $\epsilon(\epsilon > 0)$. In addition, we also show that the framework of our approximation algorithm can be applied to other collective communications such as the gather operation.

39. H. Fujiwara, K. Iwama, and K. Yonezawa:
"Online Chasing Problems for Regular n-Gons", The 5th International Conference on Research, Innovation and Vision for the Future (RIVF2007), pp.36–41, 2007年3月.
概要:

40. Y. Wu, T. Izumi, F. Ooshita, H. Kakugawa, and T. Masuzawa:
"An Adaptive Randomized Searching Protocol in Peer-to-Peer Systems", Proc. the 22nd Annual ACM Symposium on Applied Computing, 2007年3月.
概要: Search problem, which is to identify the peer that has a target resource object, is an important problem in Peer-to-Peer (P2P) file sharing systems. Since P2P systems maintain large and dynamic sets of peers, the search protocol is desired to be scalable and adaptive. In this paper we propose a new Peer-to-peer search protocol, called Adaptive Randomized Search Protocol (ARSP), which is an efficient extension of the Quorum-Based Protocol for Searching Objects in Peer-to-Peer Networks. ARSP minimizes the communication cost of the protocol according to objects' popularity. Interestingly, the protocol works in the self-adaptive manner: it can automatically adapt to the dynamics of network environments.

41. T. Izumi, A. Saitoh, and T. Masuzawa:
"Adaptive Timeliness of Consensus in Presence of Crash and Timing Faults", Journal of Parallel and Distributed Computing, (掲載予定).
概要: The Δ-timed uniform consensus is a stronger variant of the traditional consensus and it satisfies the following additional property: Every correct process terminates its execution within a constant time Δ (Δ-timeliness), and no two processes decide differently (Uniformity). In this paper, we consider the Δ-timed uniform consen-

sus problem in presence of f_c crash processes and f_t timing-faulty processes, and propose a Δ-timed uniform consensus algorithm. The proposed algorithm is adaptive in the following sense: It solves the Δ-timed uniform consensus when at least $f_t + 1$ correct processes exist in the system. If the system has less than f_t+1 correct processes, the algorithm cannot solve the Δ-timed uniform consensus. However, as long as $f_t + 1$ processes are non-crashed, the algorithm solves (non-timed) uniform consensus. We also investigate the maximum number of faulty processes that can be tolerated. We show that any Δ-timed uniform consensus algorithm tolerating up to f_t timing-faulty processes requires that the system has at least $f_t + 1$ correct processes. This impossibility result implies that the proposed algorithm attains the maximum resilience about the number of faulty processes. We also show that any Δ-timed uniform consensus algorithm tolerating up to f_t timing-faulty processes cannot solve the (non-timed) uniform consensus when the system has less than $f_t + 1$ non-crashed processes. This impossibility result implies that our algorithm attains the maximum adaptiveness.

42. K. Iwama, and S. Tamaki:
"Exploiting Partial Knowledge of Satisfying Assignments", Discrete Applied Mathematics, (掲載予定).
概要: Recently Schoning has shown that a simple local-search algorithm for 3SAT achieves the currently best upper bound, i.e., an expected time of 1.334^n. In this paper, we show that this algorithm can be modified to run much faster if there is some kind of imbalance in satisfying assignments and we have a (partial) knowledge about that. Especially if a satisfying assignment has imbalanced 0's and 1's, i.e., $p_1 n$ 1's and $(1 - p_1)n$ 0's, then we can find a solution in time 1.260^n when $p_1 = 1/3$ and 1.072^n when $p_1 = 0.1$. Such an imbalance often exists in SAT instances reduced from other problems. As a concrete example, we investigate a reduction from 3DM and show our new approach is nontrivially faster than its direct algorithms. Preliminary experimental results are also given.

43. H. Ito, M. Kobayashi, and G. Nakamura:
"Semi-Distance Codes and Steiner Systems", Akiyama-Chvatal Festschrift, Supplement of Graphs and Combinatorics, (掲載予定).
概要:

44. H. Ito, G. Nakamura, and S. Takata:
"Winning Ways of Weighted Poset Games", Akiyama-Chvatal Festschrift, Supplement of Graphs and Combinatorics, (掲載予定).
概要:

45. X. Han, K. Iwama, D. Ye, and G. Zhang:
"Strip Packing vs. Bin Packing", AAIM 2007, (掲載予定).
概要: In this paper we establish a general algorithmic framework between bin packing and strip packing, with which we achieve the same asymptotic bounds by applying bin packing algorithms to strip packing. More precisely we obtain the following results: (1) Any offline bin packing algorithm can be applied to strip packing maintaining the same asymptotic worst-case ratio. Thus using FFD (First Fit Decreasing Height) as a subroutine, we get a practical (simple and fast) algorithm for strip packing with an upper bound 11/9. (2) A class of Harmonic-based algorithms for bin packing can be applied to online strip packing maintaining the same asymptotic competitive ratio. It implies online strip packing admits an upper bound of 1.58889 on the asymptotic competitive ratio. This significantly improves the previously best bound of 1.6910 and affirmatively answers an open question.

46. J. Akiyama, H. Fukuda, H. Ito, and G. Nakamura:
"Infinite series of generalized Gospher space filling curves", Proc. the China-Japan Joint Conference on Discrete Geometry and Graph Theory (CJCDGCGT2005), (掲載予定).
概要:

47. H. Ito:
"Impossibility of transformation of vertex labeled simple graphs preserving the cut-size order", Proc. the China-Japan Joint Conference on Discrete Geometry and Graph Theory (CJCDGCGT2005), (掲載予定).
概要:

48. M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita:
"Quantum Network Coding", Proc. 24th International Symposium on Theoretical Aspects of Computer Science (STACS 2007), (掲載予定).
概要:

研究会等

1. 高橋佑典，泉泰介，増澤利光:
"P2P ネットワークにおけるブルームフィルタを利用したインデックス情報散布法の改良", 電子情報通信学会技術研究報告（ネットワークシステム，NS2006-21），vol.106, no.41, pp.1–4, 2006 年 5 月.
概要: ブルームフィルタは，データアイテム集合のインデックス情報を効果的に表現するための一つの手法である．ブルームフィルタは誤検出を生じる可能性があるが，一方で少ないメモリ領域で実現可能という利点がある．そのため，P2P ネットワークにおいて，各ノードが自分の所持するデータアイテム集合に対するブルームフィルタを近隣ノードに散布することで，検索効率を上げる手法が提案されている．本稿では，従来のブルームフィルタを改良した，決定性減衰型ブルームフィルタ，および，それに基づく検索手法を提案する．従来のブルームフィルタでは，散布半径の増加に伴い，1 フィルタが表すデータアイテム数が増えるため，誤検出確率が増加するという問題が存在するが，決定性減衰型ブルームフィルタでは，ノードが散布するフィルタ構成のための情報量を距離に応じて減衰させることで，1 ノードが収集する情報の量を削減し，誤検出確率の増加を抑える．また，提案手法が従来手法よりも効率的な検索が実現できていることを，シミュレーションにより示す.

2. K. Iwama, and H. Morizumi:
"Reductions for Monotone Boolean Circuits", 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.106，no.128, COMP2006-19, pp.15–19, 2006 年 6 月.
概要: The large class, say *NLOG*, of Boolean functions, including 0-1 Sort and 0-1 Merge, have an upper bound of $O(n \log n)$ for their monotone circuit size, i.e., have circuits with $O(n \log n)$ AND/OR gates of fan-in two. Suppose that we can use, besides such normal AND/OR gates, any number of more powerful "F-gates" which realize a monotone Boolean function F with $r(\geq 2)$ inputs and $r'(\geq 1)$ outputs. Note that the cost of each AND/OR gate is one and we assume that the cost of each F-gate is r. Now we define: A Boolean function f in NLOG is said to be F-Easy if f can be computed by a circuit with AND/OR/F gates whose total cost is $o(n \log n)$. In this paper we show that 0-1 Merge is not F-Easy for an arbitrary monotone function F such that $r' \leq r/\log r$.

3. 清成悠貴，宮野英次，宮崎修一:
"試問予定表作成問題の計算複雑さ", 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.106, no.128, COMP2006-18, pp.7–14, 2006 年 6 月.
概要: 本稿では，試問予定表作成問題と呼ばれる大学における時間割表作成問題を導入す

る．この問題では，ある決まった数の審査員，例えば 3 人の審査員が $2n$ 人の学生にそれぞれ割り当てられる．それらの学生と担当審査員の組は，n 個の時刻と 2 つの部屋から成る $n \times 2$ 行列に割り当てられる必要がある．ここで，同じ審査員が担当する異なる 2 人の学生は異なる時刻に 割り当てられなければならない．さらに，すべての審査員が 2 つの部屋を移動する回数の合計をできるだけ少なくした．これは，実際に京都大学の試問予定表作成において発生した問題である．この問題について 2 つの制約付きモデルを提案し，それらの計算複雑さについて調査する．

4. T. Horiyama, K. Iwama, and K. Seto:
"Constant Depth Circuits for Symmetric Boolean Functions", 夏の LA シンポジウム, pp.20.1–20.4, 2006 年 8 月.
概要: We consider Σ_d circuits of unbounded fan-in, whose depth is constant d and the top gate is an OR. We prove that any symmetric Boolean function has a Σ_d circuit of size at most $2^{O(n^{1/(d-1)})}$ where n is the number of the variables. This result is obtained by showing the upper bound $2^{k^{1/(d-2)}}(1+1/k)^{n+O(\log n)}$ on Σ_d^k circuits, in which the bottom fan-in is bounded by k.

5. 吉牟田拓朗, 宮野英次, 宮崎修一:
"オンライン TSP アルゴリズムに対する下限について", 平成 18 年度 第 59 回電気関係学会九州支部連合大会, 10-2A-07, pp.342, 2006 年 9 月.
概要: 本稿では，代表的な最適化問題の 1 つである巡回セールスパーソン問題（Traveling Salesperson Problem，以下 TSP）のオンライン版であるオンライン TSP を考える．通常の TSP は，入力であるグラフ $G = (V, E, w)$（V は頂点集合，E は辺集合，w は辺重み）が予め与えられたとき，全ての頂点を最低一回ずつ訪問し，出発点に戻る巡回路で辺重みの総和を最小にするものを求めることを目的とする．オンライン TSP では，新しい頂点を訪れると，その頂点と隣接する全ての頂点間の辺とそれらの辺重みの情報が新たに分かる．このような条件の下で巡回路の辺重みの総和をできるだけ小さくすることを目的とする．オンラインアルゴリズムは競合比によって評価される．任意の入力 G に対するオンラインアルゴリズム ALG の出力を $ALG(G)$，オフラインアルゴリズムの最適解を $OPT(G)$ としたとき，$\frac{ALG(G)}{OPT(G)} \leq \alpha$ が成り立つとき，ALG の競合比が α であると言う．すなわち，α の値が 1 に近いほど良いアルゴリズムになる．オンライン TSP に対しては，競合比が 16 のアルゴリズム（ShortCut）が知られているが，下限例に関してはあまり議論されていない．本稿では，ShortCut に対する 6 競合比の下限例を示し，さらにはオンライン TSP に対する 1.25 競合比の下限例を示す.

6. 高橋佑典，泉泰介，増澤利光:
"P2P ネットワークにおける決定性減衰型ブルームフィルタの提案と検索効率の評価", 電子情報通信学会技術研究報告 (ネットワークシステム, NS2006-133) (奨励講演), vol.106, no.355, pp.55–60, 2006 年 11 月.
概要: ブルームフィルタは，データアイテム集合のインデックス情報を効果的に表現するための一つの手法である．ブルームフィルタは誤検出を生じる可能性があるが，一方で少ないメモリ領域で実現可能という利点がある．そのため，P2P ネットワークにおいて，各ノードが自分の所持するデータアイテム集合に対するブルームフィルタを近隣ノードに散布することで，検索効率を上げる手法が提案されている．我々は以前の報告において，従来のブルームフィルタを改良した，決定性減衰型ブルームフィルタ (DDBF)，および，それに基づく検索手法を提案した．従来のブルームフィルタでは，散布半径の増加に伴い，1 フィルタが表すデータアイテム数が増えるため，誤検出確率が増加するという問題が存在するが，DDBF では，ノードが散布するフィルタ構成のための情報量を距離に応じて減衰させることで，1 ノードが収集する情報の量を削減し，誤検出確率の増加を抑えることができる．本稿では，従来の DDBF による検索手法において，データアイテムの検索頻度に応じて散布半径を変更する手法を併せて

用いることで，更なる検索効率の向上を達成することが可能であることをシミュレーションにより示す．

7. 乾広二，鈴木朋子，大下福仁，角川裕次，増澤利光:
“分散ハッシュテーブル Chord における故障耐性向上のための経路の多重化手法”, 電子情報通信学会技術研究報告 (ネットワークシステム, NS2006-146) , vol.106, no.418, pp.39–44, 2006 年 12 月.
概要: P2P システムにおいて資源の効率的な配置と検索を実現する手法として，分散ハッシュテーブル (DHT) がよく用いられている．DHT の故障耐性を高める方法としてマルチパスおよびワイドパスと呼ばれる経路の多重化がある．マルチパスは低コストで実現できるが故障耐性が十分でなく，ワイドパスは高い故障耐性を有する反面，高コストである．そこで本研究では，これらの手法を組み合わせた手法を提案し，DHT の一種である Chord に対して適用する．また，解析とシミュレーションによる性能評価を行い，提案手法では既存手法に比べて低コストで故障耐性が向上することを示す．

8. 朝廣雄一, 宮野英次, 宮崎修一, 吉牟田拓朗:
“サイクルグラフ上での地図作成問題に対する重み付き最近傍アルゴリズム”, 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.106, no.405, COMP2006-43, pp.15–22, 2006 年 12 月.
概要: グラフ上での地図作成問題とは，探索者が未知のグラフの全ての頂点を訪問することによりグラフ構造を調査する問題である．探索者は辺の存在とその長さをその端点を訪れるまで判らないとする．探索者は，できるだけ短い経路を通ることにより全ての頂点と辺を調査して，出発点まで戻って来なければならない． 本問題に対する最も単純な方法の一つは，最近傍アルゴリズム (NN) であり，まだ訪れていない頂点の中で探索者の現在の場所から最も近い場所に移動す る戦略である．重み付き最近傍アルゴリズム (WNN) は，NN の拡張であり，ある重み付きの距離により次の移動場所を決める．平面グラフにおいては，重み 3 である WNN が 16 競合であることが知られている．本稿ではサイクルグラフについては，NN の競合比が 1.5 となること，その解析が厳密であることを示す．また，サイクルグラフに対しては WNN の中で NN が最適であることを示す．さらに，本問題に対しては，1.25 競合よりも良いアルゴリズムが存在しないことを示す．

9. 山内直哉, 宮崎修一, 岩間一雄:
“安定結婚問題に対する 1.875-近似アルゴリズム”， 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.106，no.405, COMP2006-48, pp.49–56, 2006 年 12 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，現在知られている中で最も良い近似アルゴリズムは, $(2-c\frac{1}{\sqrt{N}})$-近似アルゴリズムである．(ここで，c は $c \leq \frac{1}{4\sqrt{6}}$ を満たす正定数であり，N は入力中の男性の数である．) 本論文では，この近似度を 1.875 に改良した．

10. H. Morizumi, and J. Tarui:
“Linear-Size Log-Depth Negation-Limited Inverter for k-tonic 0/1 Sequences”, 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.106, no.405, COMP2006-49, pp.57–60, 2006 年 12 月.
概要: A binary sequence $x_1, \ldots, x_n$ is called k-tonic if for $1 \leq i \leq n-1$ the number of i's such that $x_i \neq x_{i+1}$ is at most k. In this paper, we give the construction of a circuit inverting k-tonic sequences, which has size $O((\log k) \cdot n)$ depth $O((\log k) \cdot \log\log n + \log n)$ and contains $\log_2 n + O(\log\log n)$ NOT gates. Our construction improves all parameters of the construction by Sato, Amano and Maruoka, whose size is $O(kn)$ and depth is $O(k\log^2 n)$ using $O(k\log n)$ NOT gates. If $k = O(1)$, the previous construction needs $O(\log^2 n)$ depth, but our inverter has linear size and log depth using

$O(\log n)$ NOT gates. Beals, Nishino and Tanaka have shown the construction of a size $O(n \log n)$ depth $O(\log n)$ inverter for all sequences with $\lceil \log_2(n+1) \rceil$ NOT gates. If $k = n^{o(1)}$, our construction reduces the size to $o(n \log n)$ with the same depth and only $O(\log \log n)$ increase of the number of ! NOT gates. Our idea on the construction of an inverter for k-tonic sequences also give an improvement for a circuit sorting k-tonic sequences from the construction by Sato, Amano and Maruoka.

11. 森住 大樹, 垂井 淳, 岩間 一雄:
"Negation-Limited Complexity of Parity and Inverters", 冬の LA シンポジウム, 京都大学数理解析研究所講究録, pp.21.1–21.9, 2007 年 1 月.
概要: In *negation-limited* complexity, one considers circuits with a limited number of NOT gates, being motivated by the gap in our understanding of monotone versus general circuit complexity, and hoping to better understand the power of NOT gates. We give improved lower bounds for the size (the number of AND/OR/NOT) of negation-limited circuits computing Parity and for the size of negation-limited inverters. An *inverter* is a circuit with inputs $x_1, \ldots, x_n$ and outputs $\neg x_1, \ldots, \neg x_n$. We show that (a) For $n = 2^r - 1$, circuits computing Parity with $r - 1$ NOT gates have size at least $6n - \log_2(n+1) - O(1)$, and (b) For $n = 2^r - 1$, inverters with r NOT gates have size at least $8n - \log_2(n+1) - O(1)$. We derive our bounds above by considering the minimum size of a circuit with at most r NOT gates that computes Parity for *sorted* inputs $x_1 \geq \cdots \geq x_n$. For an *arbitrary* r, we completely determine the minimum size. It is $2n - r - 2$! for odd n and $2n - r - 1$ for even n for $\lceil \log_2(n+1) \rceil - 1 \leq r \leq n/2$, and it is $\lfloor 3/2\, n \rfloor - 1$ for $r \geq n/2$. We also determine the minimum size of an *inverter for sorted inputs* with at most r NOT gates. It is $4n - 3r$ for $\lceil \log_2(n+1) \rceil \leq r \leq n$. In particular, the negation-limited inverter for sorted inputs due to Fischer, which is a core component in all the known constructions of negation-limited inverters, is shown to have the minimum possible size. Our fairly simple lower bound proofs use gate elimination arguments in a somewhat novel way.

12. 中島拓也, 岩間一雄:
"Improvement of the Algorithm for the Traveling Salesman Problem on Cubic Graphs", 冬の LA シンポジウム, 京都大学数理解析研究所講究録, pp.23.1–23.8, 2007 年 1 月.
概要: 本発表では, n 頂点の cubic graphs, あるいは次数 3 以下のグラフにおいて巡回セールスマン問題が $O(1.2569^n)$ 時間で解く事ができることを示す. これは同じく n 頂点 cubic graphs における TSP が $O(2^{n/3}) \approx 1.2599^n$ で解けることを示した Eppstein の論文の改良である. 探索中における内部の状態を考慮にいれ, 最悪の場合が高々$7n/24$ 回しかおきないように Eppstein のアルゴリズムを変更することで計算量を改善した.

13. 伊藤亮太, 長瀧寛之, 大下福仁, 角川裕次, 増澤利光:
"アルゴリズム学習における誤りからの学習を実現する演習課題の自動生成手法", 電子情報通信学会技術研究報告 (教育工学, ET2006-97), vol.106, no.507, pp.81–86, 2007 年 1 月.
概要: 本研究では,「誤りからの学習」に基づくアルゴリズム学習のための演習問題の自動生成手法を提案する. ここでの演習問題とは, あるアルゴリズムを実装したソースコードに誤りを含ませたものであり, 誤りの修正及び考察を通じてアルゴリズムの理解を深める形式を想定している. 演習問題の自動生成においては, 演習を通じてアルゴリズムの理解を深められるような誤りの自動挿入を実現することを目標とし, これを実現するシステムを試作した. また, 提案手法の評価として, 教員等が学習効果を考えて挿入した誤りと提案手法で自動的に挿入される誤りを比較した

結果，高い割合で学習効果のある誤りを自動挿入できていることがわかった．加えて，実際の講義において演習を実施した結果も報告する．

14. 西川元，山内由紀子，大下福仁，角川裕次，増澤利光:
“トポロジ変化の影響を抑えたモバイルアドホックネットワーク向け自己安定相互排除プロトコル”, 情報処理学会研究報告（マルチメディア通信と分散処理, 2007-DPS-130(30)), vol.2007，no.16, pp.177–182, 2007 年 3 月.
概要: 自己安定プロトコルとは，任意の初期状況から実行を開始し，いずれ正しい状況に収束するという性質を持つ故障耐性に優れたプロトコルである．しかし，モバイルアドホックネットワークのようなトポロジ変化が頻発する環境においては，正しい状況に収束する前に新たな状況変化が発生し，プロトコルが永久に安定できなくなる可能性が存在する．そのため，モバイルアドホックネットワークに自己安定プロトコルを適用するには，トポロジ変化に対する対応が必要となる．モバイルアドホックネットワーク上での自己安定相互排除プロトコルの既存研究に Chen らの手法が存在する．この手法はノードの移動によるトポロジ変化に対して優れた適応性を持つが，ノードの離脱によるトポロジ変化に対する適応能力は十分ではない．本論文では Chen らの手法を改善し，ノードの移動，離脱の両方に対して優れた適応性を持つ自己安定相互排除プロトコルを提案する．

15. 森川雅和，鈴木朋子，大下福仁，角川裕次，増澤利光:
“領域被覆のためのセンサネットワークアルゴリズム”, 情報処理学会研究報告（マルチメディア通信と分散処理, 2006-DPS-130(61)), vol.2007，no.16, pp.357–362, 2007 年 3 月.
概要: センサネットワークの利用例の多くに，ある特定の領域の監視を行い，得られた情報を収集したいという要求がある．各センサの検知領域で監視を行いたい領域 (要求領域) を被覆する連結なセンサの集合を連結センサカバーとよび，センサ数が最小の連結センサカバーを求めることは NP 困難であると知られている．分散環境において，少数のセンサで構成される連結センサカバーを求める手法が既に提案されているが，既存手法ではアルゴリズムを開始するのはただ 1 つのセンサであり，広大な要求領域に対し連結センサカバーを求めるには非常に長い時間を要する．そこで本研究では，分散環境において要求領域の被覆を複数センサで平行に行う手法を提案する．また実験により，提案手法を用いて短時間で十分に少ないセンサ数の連結センサカバーが得られることを示す．

16. 古川正広，鈴木朋子，大下福仁，角川裕次，増澤利光:
“類似実行に基づく耐故障分散アルゴリズム理解支援システムの提案”, 情報処理学会研究報告（数理モデル化と問題解決，2007-MPS-63(10)）, vol.2007, no.19, pp.37–40, 2007 年 3 月.
概要: f-耐故障分散アルゴリズムとは，高々 f 個の計算機が故障しても正しく問題を解くアルゴリズムである．本研究では，f-耐故障分散アルゴリズムの理解を支援するために，$f+1$ 個の故障のもとで正しい解を出力しない実行と，その実行に類似した f 個または $f+1$ 個の故障のもとで正しい解を出力する実行を生成するシステムを提案する．これらの実行を比較することで，故障が問題を解けなくした原因を利用者は考察でき，f-耐故障分散アルゴリズムの理解に繋がる．さらに，本研究では，２つの実行の生成に必要な計算時間を削減する仕組みについて考察と実験を行なう．その結果，類似度の高い２つの実行を実用的な時間で生成できることを示す．

17. Y. Yamauchi, T. Masuzawa, and D. Bein:
“Emulation of Ring Protocols on Trees Preserving Fault-Containment”, 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.106, no.566, COMP2006-52, pp.13–20, 2007 年 3 月.
概要: A desired property of a distributed, self-stabilizing protocol is to minimize the impact of faults that can corrupt the data

stored locally at some process(es), called *fault-containment*. We consider emulation of fault-containing ring protocols on tree networks. We propose a novel ring embedding on an arbitrary tree in which each process in the tree appears on the virtual ring as a single virtual process. We also propose a self-stabilizing protocol RET that emulates ring protocols on the embedded ring with preserving the fault-containment property. The notion of emulation is more general than the notion of simulation, defined by Lynch over the set of configurations of two different protocols.

18. T. Suzuki, T. Izumi, F. Ooshita, H. Kakugawa, and T. Masuzawa:
"Move Complexity of Gossiping among Mobile Agents", 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.106, no.566, COMP2006-54, pp.29–36, 2007 年 3 月.
概要: Mobile-agent-based distributed systems are attracting widespread attention as the adaptive and flexible systems: mobile agents traverse the distributed system and carry out a task at each node. In such mobile-agent-based systems, *gossip* is the most fundamental scheme supporting cooperation among mobile agents. It requires to accomplish all-to-all information exchange over all agents so that each agent can obtain the all informations each agent initially has. Rendezvous algorithms, which require that all the agents rendezvous on a node at a time, can achieve this requirement, however it takes excessive cost for our objective. In this paper, we newly introduce the mobile agent gossip problem. In this problem, an agent can obtain the information of another agent by meeting the agent itself or the agent that has already got the information. The gossip scheme is expected to accomplish the all-to-all information exchange with a smaller number of agents' moves than the rendezvous algorithms. We propose mobile agent gossip algorithms on several network topologies, and prove that all proposed algorithms are asymptotically optimal in term of the number of moves.

学会大会等

1. 宮崎修一:
"ルータ上のバッファ管理問題に対するオンラインアルゴリズム", 電子情報通信学会誌, vol.89, no.4, pp.299–303, 2006 年 4 月.

2. 堀山貴史:
"3 彩色不能な平面グラフの構成", 列挙アルゴリズム合宿, 2006 年 9 月.

3. H. Ito, M. Paterson, and K. Sugihara:
"Multicommodity Source Location Problems and Price of Greed", Research Seminar on Connectivity of Graphs and Its Applications, 2007 年 1 月.

4. 山内直哉, 宮崎修一, 岩間一雄:
"安定結婚問題に対する 1.8-近似アルゴリズム", 電子情報通信学会 総合大会, DS-1-3, 2007 年 3 月.

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 § 巳波 弘佳 † 野々部 宏司 ¶
梅谷 俊治 ‖ 藤原 洋志 † 千葉 英史 †

† 関西学院大学理工学部
〒 669-1337 三田市学園 2-1
{ibaraki, miwa, h-fujiwara, e-chiba}@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
〒 102-8160 東京都千代田区富士見 2-17-1
nonobe@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. 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. 組合せ最適化問題を解決するためのアルゴリズムの研究,
2. 社会のさまざまな現象を数理的にモデル化する研究,
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 のタイプの研究は柳浦, 野々部, 梅谷, 千葉が重点的に進めており, 第 2 のタイプは, 巳波が中心になり, 第 3 のタイプは藤重, 藤原が主に担当している. 茨木はこのグループ全体の総括とともに, 主に第 1 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. それぞれを厳密に分類することは困難であるが, しいて述べれば, 第 2〜8 章はタイプ 1 の研究, 第 9 章はタイプ 3, 第 10 章はタイプ 2 に分類される.

2 集合被覆問題

集合被覆問題は，複数の要素と要素集合の族, および各集合のコストが与えられたとき，全ての

要素をカバーするように要素集合をいくつか選び，選ばれた集合のコストの総和を最小化する問題である．この問題に対する，大きな近傍を利用した局所探索に基づくメタ戦略アルゴリズムを提案した．

この問題は，たとえば，飛行機や列車の乗務員スケジューリング問題などの重要な実用問題を解く際の部分問題として利用されるなど，実用上重要な基本問題である．このような実用の場面においては，問題サイズが極めて大きくなる傾向にあり，要素集合族の大きさが 100 万を越えることも少なくない．実際，そのような大規模な問題例がベンチマークとして公開されている．そのような大規模な問題例に対してもアルゴリズムが効率よく動作するように注意を払いつつ，メタ戦略アルゴリズムの設計・開発を進めた．

大規模な問題を扱うためのアイデアのひとつとして，集合被覆問題のラグランジュ緩和問題から得られる情報を利用しつつ，問題サイズを適応的に縮小する工夫を行った．具体的には，よい解に含まれる集合については，ラグランジュ緩和問題を解くことによって得られる相対コストの値が小さい傾向にあることに着目し，そのような集合に絞って探索を行うようにしている．ただし，探索対象の集合の絞り方が適切でないと，解の精度が落ちることが懸念される．そのため，探索状況に応じて探索対象の集合の選択を時々修正するという工夫を加えている．

また，メタ戦略の基本となる局所探索法において，大きな近傍を効率よく探索する工夫を行うことで，解の質と求解のスピードの両面における改善を図っている．具体的には，近傍操作において，3 つ以下の集合を入れ替えるというものを考えた．このように近傍を拡大することで，解の精度の向上が期待できるが，このような近傍操作に基づく近傍の中から改善解を探索するアルゴリズムを単純に実装してしまうと，集合族の大きさを n として $O(n^3)$ 時間を要する．n は 100 万を越えることもあるので，このような実装では現実的な時間では探索が終了しない．そこで，問題のコスト構造をうまく利用することで，改善の望みのない解への探索を省略する工夫を加え，改善解の探索の計算手間を大幅に改善している．

さらに，探索中に実行不可能解を探索することを許容し，制約違反をペナルティとして評価するという方針を取った．制約違反のペナルティに対する重みの適正値は，問題例に大きく依存し，その値を手動で調整することは現実的でないため，ペナルティ重みを探索中に適応的に調整するメカニズムを導入した．これにより，実行可能領域と実行不可能領域を交互に行き来するように探索を誘導する戦略的振動を実現している．

以上のような工夫を総合した結果，大規模なベンチマーク問題に対してこれまで知られていた最良の解よりもよい解を発見するなど，大きな成功を収めることができた．

3　割当型問題に対する汎用解法

複数のエージェントに幾つかの仕事を割当てる問題など，あるものを何かに割当てるタイプの問題は世の中に数多く存在する．組合せ最適化の分野においても，割当問題，一般化割当問題，2 次割当問題などが代表的な割当型問題として古くから研究されてきたが，これらの問題では割当てコストが線形もしくは 2 次に限定されており，その応用範囲はあまり広範なものではなかった．そこで本研究では，より汎用性の高い形で問題の定式化を行い，問題の適用範囲を拡げるとともに，メタヒューリスティクスに基づく発見的解法を提案した．

本研究における割当型問題の定式化は以下の通りである．仕事集合 J とエージェント集合 I が入力として与えられ，各仕事に対して，どれか 1 つのエージェントを割当てなくてはならない．ここで，エージェント i が割当てられた仕事の集合を J_i としたとき，i に対して，J_i に応じて定まる割当てコスト $f_i(J_i)$ が発生するものとする．そして，すべてのエージェントに対する割当てコストの合計 $\sum_i f_i(J_i)$ を最小化することが目的である．ただし，エージェント i を仕事 j に割当てるためには a_{ij} の資源が必要である．各エージェント i には容量 b_i が定められており，仕事集合 J_i に対して，$\sum_{j \in J_i} a_{ij} \leq b_i$ でなくてはならない．なお，本研究の定式化では，割当てコスト $f_i(J_i)$ は効率的に計算可能である必要はなく，その計算自体が NP 困難であってもよい．これにより，並列機械スケジューリング問題や容量制約つき配送

計画問題なども割当型問題として捉えることが可能になる．

この割当型問題に対して，反復局所探索法によるアルゴリズムを実装した．すべての割当てからなる集合を探索空間とし，近傍として，シフト近傍（現在の割当てから，ある1つの仕事の割当てを変更して得られる割当て集合）とスワップ近傍（ある2つの仕事に対して，割当てられているエージェントを交換することで得られる割当て集合）を用いた．

ところで，局所探索においては，現在の割当てや近傍内の割当てに対してそれらの割当てコストを計算する必要がある．しかし，本研究の定式化では割当てコストを効率よく計算できるとは限らないため，割当てコストとして近似値を用いることを許可し，計算時間の短縮を行っている．ただし，このとき，割当てコストの計算をどの程度正確に行うかが問題となる．一般に，コストの計算を正確に行えば，より効果的な探索が期待される反面，多くの計算時間が必要となり，逆に，コストの計算にあまり時間をかけなければ，局所探索の反復を数多く実行できるが，最終的に得られる解の精度はあまり望ましいものではなくなる．そこで本研究では，割当てコストの近似値を，あまり正確ではないが高速に計算するルーチン（高速ルーチン）と，比較的多くの計算時間をかけ，より正確な値を計算するルーチン（精密ルーチン）の2種類のルーチンを併用して局所探索を行う方法を提案した．なお，割当てコストの計算を行うこれらのルーチンは問題依存であるが，それ以外のルーチンは，汎用的なものであり，さまざまな割当型問題に対して同様に適用可能である．したがって，ユーザが開発すべきルーチンは，割当てコストの計算ルーチン（高速ルーチンおよび精密ルーチン）のみである．

提案手法の有効性を評価するため，並列機械スケジューリング問題と容量制約つき配送計画問題を対象に計算実験を行った．ともに割当型問題として定式化した場合，割当てコストの計算が NP 困難になる問題である．例えば，容量制約つき配送計画問題の場合，エージェント i の割当てコスト $f_i(J_i)$ を計算することは都市数 $|J_i|$ の巡回セールスマン問題を解くことと同値であり，割当てコストの近似値の計算は，実行可能な巡回路を1つ生成することで実現できる．また，局所探索において近傍解評価のために $f_i(J_i)$ を計算するとき，J_i は現在の割当て J_i' との共通部分が多いため，$f(J_i')$ の計算のために生成した巡回路を活用することができる．この性質を利用し，高速ルーチンでは，J_i' 用の巡回路に対し新たな都市を挿入するなどの軽微な修正を行い，J_i 用の巡回路を生成している．一方，精密ルーチンでは，高速ルーチンと同様の操作を行った後，単純な局所探索法を実行している．

計算実験の結果，高速ルーチンと精密ルーチンの2種類を使い分けることで，両方の利点を活かした効率的な探索が実現できることが分かった．また，並列機械スケジューリング問題や容量制約つき配送計画問題専用に設計されたアルゴリズムと比較しても，解の質に関しては遜色のない結果が得られており，とくに並列機械スケジューリング問題に対しては，計算時間の面でも専用アルゴリズムと同等であることが確認できた．

4 可変形状長方形詰込み問題

与えられた n 個の長方形をできるだけ小さな領域に重ならないように詰め込む問題はこれまで詳しい研究がある．本研究では，これらの長方形の形状 (高さと幅) があらかじめ決まっているのではなく，指定された範囲内で可変であるという想定の下で詰め込み問題を考えた．この種の問題はVLSIのフロアプランや建築設計に応用がある．本論文で開発した局所探索法のアルゴリズムは，順列対によって長方形の相対位置を定めたのち，具体的な配置を数理計画法を用いて決定する．長方形の形状に周長一定という制約を加える場合は線形計画問題に，面積一定の場合は非線形計画問題となる．良い解を与える順列対は，局所探索によって探索するが，効果的な近傍を計算実験によって定めた．計算実験の結果，長方形の個数が数十程度ならば実用的に十分使えることが判明した．

n 個の長方形の相対位置関係を順列対 $\sigma = (\sigma_+, \sigma_-)$ で表すことができる．σ_+, σ_- はそれぞれ集合 $\{1, 2, \ldots, n\}$ の順列である．ただし，n 個の長方形からなる順列対は全部で $(n!)2$ 通り存在し，全探索により厳密解を求めるのは困難であるため，良い結果を与える順列対を局所探索を用い

て近似的に求める．

長方形 i の横幅と高さを w_i, h_i とする．ただし，w_i, h_i はそれぞれ下限値，上限値の区間で可変とする．長方形 i の幅と高さの合計値を L_i (すなわち $L_i = w_i + h_i$), 各長方形の配置を決定するため長方形 i の左下隅の座標を (x_i, y_i) とする．また，これらの長方形を詰め込む長方形領域の幅と高さを W, H とする．順列対 σ が定める相対位置制約の下で，周長条件を考慮した長方形詰め込み問題は以下の線形計画問題に定式化される．

$$
\begin{aligned}
P(\sigma): \quad & \text{minimize } H + W \\
& \text{subject to } 0 \le x_i \le W - w_i, \forall i \\
& 0 \le y_i \le H - h_i, \forall i \\
& w_i + h_i = L_i, \forall i \\
& (\sigma\text{によって下の一つが定まる}) \\
& x_i + w_i \le x_j,\ x_j + w_j \le x_i, \\
& y_i + h_i \le y_j,\ y_j + h_j \le y_i, \forall i, j
\end{aligned}
$$

同様に, 長方形 i の面積を A_i 以上に制限し, 詰め込む領域の高さを H^* と固定し, 横幅 W を最小化する長方形詰め込み問題は非線形計画問題 $Q(\sigma)$ に定式化される．制約条件の形から, 凸形計画問題である．線形計画問題も凸形計画問題も適当なアルゴリズムを用いて効率よく解くことができる．本論文ではソフトウエア NUOPT を用いて, 前者はシンプレックス法で, 後者は直線探索法により解を求めた．

上記の $P(\sigma)$ あるいは $Q(\sigma)$ を解くと一つの長方形配置が求まるが，その良さは σ によって変化する．良い配置を与える σ を局所探索法を用いて求める．標準的な局所探索では, 注目する順列対数も多く, 計算時間もその分多くかかってしまう．そのため，探索の際に注目する長方形を限定して近傍サイズを下げる工夫を行った．

一つの配置が決まると, 左右関係 (あるいは上下関係) によって最長路を構成する臨界路が定まる．臨界路を短くすることが詰め込む領域を小さくすることに繋がるため，臨界路上に位置する長方形に注目する．その中でも下限値をとる長方形はこれ以上短くできないため，その移動は大きな影響を与える．また, 縦と横の両軸の臨界路の交差点に位置する長方形は，両方の軸から押し込まれるため下限値を取ることは難しいが，解の改良の鍵を握っている場合がある．そこで，そのような長方形を移動させることも考える．さらに, 大きな隙間の近くにある長方形に注目し, 微小に変化させることで隙間を埋める動作を通して, 全体の領域を詰めることを考える．

以上のアイデアに基づいて, 数種類の近傍を定義し, 計算実験によって, 妥当な近傍を選択した．

最終的に, 得られた近傍に基づく局所探索のアルゴリズムを構築し, 実験した結果, 長方形の数が 50 程度までならば数分の計算で高い品質の配置が得られることが分かった．下図は, 同じ方法で，長方形数 100 個のベンチマーク rp100 を解いた結果であるが, 3 時間程度もかかった．計算時間を短縮するために更なるアルゴリズムの改良が必要である．

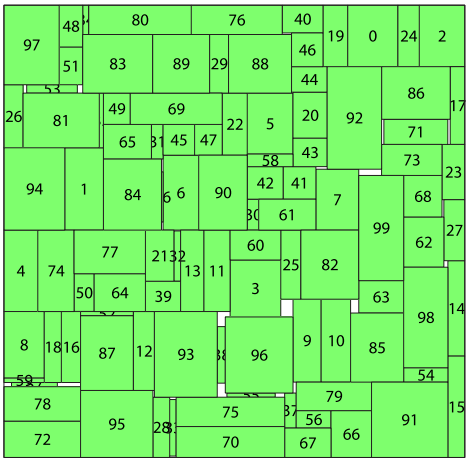


図 2.1: 面積最小化の例 rp100 ($H^* = 450$)

5 重量付モジュール詰込最適化

従来からの 2 次元，3 次元詰め込みは複数の長方形，直方体モジュールを重なりなく配置するときに必要な面積，体積の最小化を目的とするものが多い．各モジュールが持つ情報には重量がなく，配置したときの全体の重量の偏り，ばらつきなどは考慮されていなかった．しかし，配置した複数のモジュールを運搬することを考えると，全体の重心が中央にありかつ慣性モーメントが小さければ，持ちやすく，運びやすく，回転させやすいなどのメリットがある．応用例として，自動車の車体上の部品配置などが考えられる．本研究では 2 次元

の長方形詰め込み問題をベースに重量付モジュールの配置問題を扱った．

モジュール集合 $M = \{m_1, m_2, \ldots, m_n\}$ が与えられ，それぞれのモジュール $m_i \in M$ には幅，高さの 2 種類の寸法 s_i, t_i がある．各モジュールは配置する方向が決まったとき，その幅を w_i，高さを h_i とする．つまり，初期状態で s_i が幅であり，t_i が高さのとき，最終的に 90 度回転された状態で配置されたとすると $h_i = s_i,\ w_i = t_i$ となる．また，各モジュールの重さを g_i とする．すべてのモジュールを収めるべき領域の大きさを幅 W と高さ H とする．出力として，m_i の配置されたときの中央座標 (x_i, y_i) と配置の方向を示す (w_i, h_i) を得る．

このとき以下の問題を考える．

$$\text{minimize } \alpha \sum_{i=1}^{n} g_i(x_i^2 + y_i^2) + \beta \sum_{i=1}^{n} P_i + \gamma G_x^2 + \delta G_y^2 \tag{2.24}$$

$$\text{subject to } \begin{pmatrix} x_i + w_i/2 & \leq & x_j - w_j/2 & \text{or} \\ x_i - w_i/2 & \geq & x_j + w_j/2 & \text{or} \\ y_i + h_i/2 & \leq & y_j - h_j/2 & \text{or} \\ y_i - h_i/2 & \geq & y_j + h_j/2 & \end{pmatrix} \quad \forall (m_i, m_j) \tag{2.25}$$

ただし，

$$\begin{aligned} P_i =& \max(x_i - w_i/2 + W/2, 0) \\ &+ \max(x_i + w_i/2 - W/2, 0) \\ &+ \max(y_i - h_i/2 + H/2, 0) \\ &+ \max(y_i + h_i/2 + H/2, 0) \\ G_x =& \frac{\sum_{i=1}^{n} g_i x_i}{\sum_{i=1}^{n} g_i} \\ G_y =& \frac{\sum_{i=1}^{n} g_i y_i}{\sum_{i=1}^{n} g_i} \end{aligned}$$

ここで，目的関数は，慣性モーメント，領域からのはみ出し，重心の領域中心からのずれに対するペナルティの和である．

制約式 (2.25) は or 条件であるため，sequence pair を用いて，この部分を任意の 2 モジュール間で一意的に決定する．つまり，一つの sequence pair σ を決めると，上記の問題 $P(\sigma)$ は非線形計画問題となるために解くことができ，すべてのモジュールの座標が決定する．

そこで，アルゴリズムの枠組みとして，局所探索によって sequence pair を探索することにする．その際，各 sequence pair σ に対する目的関数値は，非線形計画問題 $P(\sigma)$ を解くことで得る．

本研究では，まず，非線形計画問題 $P(\sigma)$ に対する近似アルゴリズムを設計し，その近似解を用いても解の質は大きく落とさずに計算時間は大幅に短縮できることを示した．

次に，局所探索における様々な近傍の違いにおける性能の違いを評価し，近傍の探索能力を調べた．

これらの結果に基づき，複数の近傍を組み合わせ，かつ $P(\sigma)$ の近似解を用いるアルゴリズムを提案し，良好な性能が得られることを確認した．

図 2.2，図 2.3は，重量無し詰込問題のベンチマークである ami33，rp100 に対して，提案アルゴリズムを適用した配置である．黒いモジュールほど重く，白いモジュールほど軽いことを表している．外側の枠がすべてのモジュールを収めるべき領域を表しており，中央の縦線と横線の交点が領域の中心であり，中央付近の白点が全体の重心を表している．

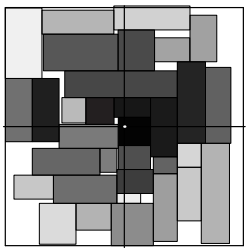


図 2.2: ami33

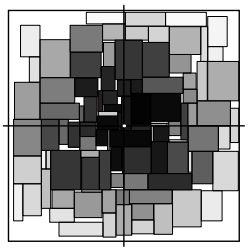


図 2.3: rp100

6 段取り替え数制約付き 1 次元資材切出し問題

1 次元資材切出し問題は，定型の母材から様々な長さの板材を顧客の注文に応じて切出す計画を求める問題であり，鉄鋼・製紙・繊維などの素材産業をはじめとする多くの分野に応用を持つ代表的な組合せ最適化問題の一つとして知られている．

素材産業では，歩留まりの向上，つまり余剰素材の削減が最も重要な課題である．古典的な 1 次元資材切出し問題は，使用する母材の本数を最小

にする板材の組合せを求める問題として定式化され，列生成法によって，大規模問題の良い近似解が短時間で求まることが知られている．しかし，実際の素材産業では，単に余剰素材の削減だけで製造コストが抑えられるわけではない．近年では，切出し工程の段取り替え作業にともなうコストや，切出された製品を一時的に積み上げておく空間の削減が重要な課題として注目されつつある．

本研究では，与えられた段取り替え数の下で，使用する母材の本数を最小化する段取り替え数制約付き 1 次元資材切出し問題に対して, メタ戦略と線形計画法を組み合わせたハイブリッド解法を提案した．

1 次元資材切出し問題では，1 本の母材から切出される板材の組合せはパターンと呼ばれる．提案解法では，現在の解のあるパターン p にある板材 i を追加した後に別の板材 i' を削除して新たなパターン p' を生成する操作と，現在の解のある板材 i をパターン p_1 から別のパターン p_2 に移動した後に，別の板材 i' をパターン p_2 からパターン p_1 に移動，もしくはパターン p_2 から削除して新たなパターン p'_1, p'_2 を生成して得られる解の集合を近傍とする局所探索法を用いた．また，使用するパターン集合が与えられた際に，各パターンの切出し回数を求める問題は整数計画問題として定式化できるが，整数条件を緩和して得られる線形計画問題を解いて，得られた実数最適解を適当な方法で丸めて整数解を求めている．

提案解法では，探索中に生じる微少に異なる多くの線形計画問題を独立に解くのではなく，現在の解における線形計画問題の最適解を基に，感度分析を適用して，これらの問題の最適解を高速に求めている．最後に，板材が 38 種類の 1 次元資材切出し問題に対する，列生成法と提案手法の実行結果を図 2.4, 2.5に示す． 図 2.4, 2.5における使用母材数は，405.922(実数最適値)，410，段取り替え数は 38，12 となっている．このように提案解法では，使用母材本数をほとんど増やすことなく，段取り替え数を大幅に削減していることが確かめられる．

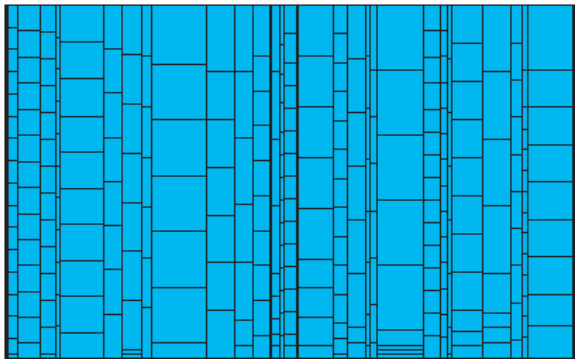


図 2.4: 1 次元資材切出し問題に対する列生成法の適用結果

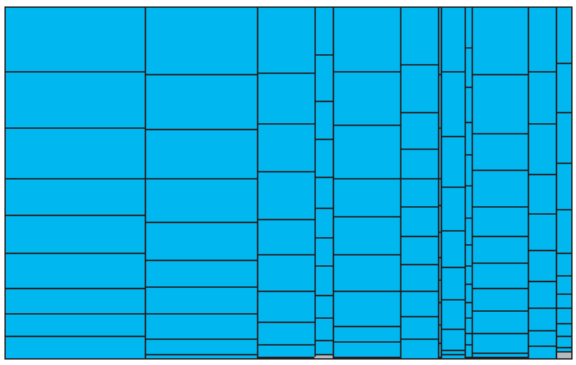


図 2.5: 1 次元資材切出し問題に対する提案解法の適用結果

7　可変移動時間をもつ配送計画問題

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．また，移動距離を短くすることは輸送費用削減につながり，間接的には CO_2 削減にも寄与するなど，環境問題への取り組みへの貢献も期待できる．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を行ってきた．

本年度は，このモデルの拡張のひとつとして，客間の移動時間にも柔軟性を持たせた非常に汎用性の高い定式化を行い，局所探索法に基づく近似解法を開発した．車両が客間を移動するのに要する時間（荷下ろしなど客のサービスに要する時間も含む）は，既存の研究では定数として扱われてきたが，本研究では，移動時間に伴うコスト関数を導入することで，問題の汎用性を高めている．現実の配送計画では，人手を増やすことでサービス時間を短縮する，有料道路を使って移動時間を減らすなど，コストを伴うことで移動時間に自由度を持たせられるケースは多く見受けられるため，このような柔軟性を取り入れたモデルに対する性能の高いソルバがあれば，非常に有用であると考えられる．

アルゴリズムの設計方針は，すべての制約条件を考慮制約として扱い，得られたペナルティ関数を最小化するというものである．1 つの車両の客の訪問順序が与えられたとき，各客におけるサービス開始時刻を決定するという部分問題を解く必要が生じるが，この部分問題の計算の複雑さを理論的に解析し，

- 客間の移動時間コストが一般の場合には NP 困難であることを示し，
- 移動時間に対するコストが凸関数の場合にはこれを厳密に解く動的計画法を考案した

ところが独創的な点である．さらに，この動的計画法の計算を高速化するために，精密なデータ構造に基づく様々な工夫を加え，実用性の高いアルゴリズムに仕上げることに成功した．

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た．また，移動時間の短縮を考慮した問題例に対する計算実験を行い，そのようなコストを支払うことで，移動時間が固定された定数である場合よりも時間枠による制限を緩める効果が生じ，車両台数を減らしたり，移動距離を小さくしたりできることを確認した．このような柔軟な配送スケジュールを提示できることで，ユーザの選択肢が増え，利便性の向上が期待できる．

8　生産ラインにおける衝突確率に関する研究

近年，液晶テレビ，プラズマテレビ，ノートパソコンなどに用いられる平面ディスプレイ（FPD）の需要が高まってきており，効率の良い製造方法が求められている．元となるガラス基板の大型化や技術進歩に伴い，生産効率も良くなってきているが，一方で生産ラインも日々変化し，新たな課題も生じている．最近，Crystal Flow のような高度なシステムが開発されているが，これは既存ラインだけでなく，次世代生産工程におけるより高度なライン制御を目指して，進化していくものである．

FPD の生産システムは，タクトタイム方式で稼動するものが多い．これは，システムへのガラス基板の投入間隔を一定にすることで，制御が簡単になるばかりでなく，単位時間当たりの生産数の正確な見積もりをすることができるという利点がある．機械の処理時間は，様々な原因（例えば，熱処理，薬品処理などの影響）で一定とならず，そのときの状況によって変化する．それゆえ，システム稼動中に，ガラス基板同士の衝突が起こる可能性があるが，ガラス基板は高価でもろいので，衝突はできるだけ避けることが求められている．

生産効率をよくするには，タクトタイムをできるだけ短く設定すればよいが，その分だけ衝突確率はあがる．一方，衝突確率を下げるには，タクトタイムをできるだけ長く設定すればよいが，そうすると生産効率が悪くなる．これが，タクトタ

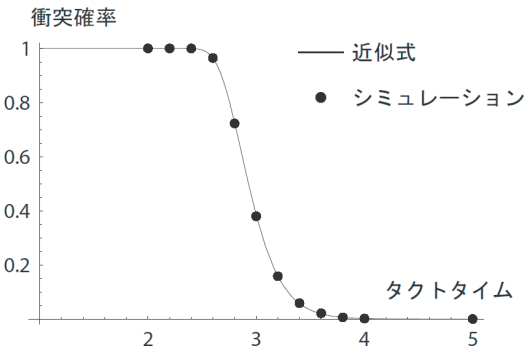


図 2.6: 近似式とシミュレーションによる衝突確率の例.

イムと衝突確率のトレード・オフである．このトレード・オフを考察するには，与えられたタクトタイムに対して衝突確率を評価することが重要である．

本研究では，FPD などの製造装置を簡単化したモデル上で，処理時間を確率変数とみなす場合に近似衝突確率の解析を行った．これまで，処理時間が正規分布，および指数分布に従う場合の解析結果が知られている．指数分布を仮定すると，正規分布の場合と違って，解析結果は閉じた形で表されるが，指数分布は実際の処理時間を必ずしも正確に表現していない．一方，正規分布は負の値も取り得るという欠点がある．そこで，指数分布をアーラン分布に一般化して解析した結果，衝突確率を閉じた形で表すことに成功した．

数値結果を図 2.6に示しておく．ここでは，機械数が 2，ジョブ数が 1000，各機械で処理時間は平均値が 1 分散が 0.1 のアーラン分布に従うと仮定した．図 2.6から，近似式とシミュレーションによる評価結果がほぼ同じになり，タクトタイムが増えるに従って，衝突確率が下がることが見てとれる．

また，バッファを考慮した直列システム上での衝突確率に関する研究も行った．具体的には，ジョブの衝突確率を α (> 0) 以下にするには各機械にどのくらいのバッファを持たせればよいかを検討した．最適なバッファ配置は各機械における処理時間の確率分布に大きく依存する．そこで，衝突確率 α をパラメータとして最適なバッファ配置を計算するために，シミュレーションに基づく実用的な近似解法を提案し，計算実験によりその効果を確かめた．

9　オンライン領域追跡問題

有名なオンライン問題の 1 つに k サーバ問題がある．プレーヤーには平面上の k 個のサーバが与えられ, 要求として与えられた点に k 個のうちのいずれかのサーバを移動させるということを繰り返す．問題の目的は一連の要求列に対するサーバの移動距離の総和を小さくすることである．これまでに競合比の下界が k であることが知られている．本研究ではサーバが 1 個の場合を取り上げる．サーバが 1 個では上で述べた k 個の中から選ぶという選択の可能性がなくなってしまうので問題として成立しない．しかし, サーバの移動を要求点そのものでなく, その「近く」でも良いとするなら話は違ってくる．具体的には, 要求に対して一定の領域を対応させ, サーバはその領域内のどこかに移動させれば良いとする．つまりプレーヤーは単一のサーバをもって要求領域を「追跡」するのである．例えば移動無線中継車を使って次々と発生する事件を追跡する問題や, 進入制限のある旧市街のホテルからタクシーを呼ぶ場合等への応用が考えられる．既存結果は, 要求領域が凸である場合に, 有界な競合比を持つアルゴリズムが存在することのみであった．

我々は, プレーヤーが要求領域の形状を事前に知っている場合にその形状情報を利用してどのように巧い追跡ができるかという点に興味がある．本研究では要求領域としては正多角形を選んだ．そしてプレーヤーのアルゴリズムとしては貪欲アルゴリズムに注目し性能解析を行った．貪欲アルゴリズムとは, 現在サーバのいる地点から最短距離で要求領域へと移動させるアルゴリズムである．性能尺度である競合比の解析に際しては償却解析と呼ばれる技法を用いる．解析の鍵は, 償却解析で適用するポテンシャル関数の選択である．試行錯誤の後, 正多角形の各辺の方向に関してマンハッタン距離を一般化したものがポテンシャル関数として有効であることを発見した．そしてこれを適用した結果, 正 n 角形に対して貪欲アルゴリズムの競合比が, n が奇数ならば $1/\sin(\pi/2n)$, 偶数ならば $1/\sin(\pi/n)$ となることを証明した．さらに

表 2.1: 正 n 角形を追跡する貪欲アルゴリズムの競合比

n	3	4	5	6	7	8
競合比	2.00	1.41	3.24	2.00	4.49	2.61

この解析はタイトである. 即ちこの値になるような要求領域列を実際に生成可能である．また, 別のアルゴリズムとして仕事関数アルゴリズムについての考察と, 凹領域の場合における競合比下界も与えた.

10 現実のネットワークの特性に関する研究

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，まず，複雑ネットワークに関する研究動向をサーベイした．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を整理し，今後の方向性を示した．

次に，複雑ネットワークの生成モデルである閾値モデルの性質を詳しく調べた．現実世界に存在するネットワークの中には，次数分布がべき則に従うという性質（スケールフリー）や，クラスター係数や隣接点平均次数などに関しても特徴的な性質を持つものもある．このような特徴を持つネットワークの生成モデルとして，各点に重みが確率的に与えられており，点 v_i と v_j の間には，v_i と v_j の重みの和や積（一般的には 2 点の重みの関数）がある閾値を越える時，またその時に限って辺が張られるという原理で生成される閾値モデルというものがある．この閾値モデルにおいて，特に重みがガウス分布に従う場合を調べ，数値実験によりスケールフリー性に近い性質を持つことを示した．

さらに，通信ネットワークにおける P2P(peer-to-peer) 通信に関して，効率の良い制御方式を検討した．効率よく目的のデータを取得するためには，実際のネットワーク上に仮想的に構成するオーバレイネットワーク（P2P ネットワーク）の構造が非常に重要である．そこで，頂点数が大きくても，次数と直径が小さい de Bruijn グラフを用いることによって，ルーティングに必要な次数を最悪 4 に抑えつつ，目的ノードまでのホップ数を最悪 $\lceil \log_2 n \rceil$（n はノード数）に抑えることができるオーバレイネットワークの構成法について述べ，その構成法に基づいて構成したネットワークの性能をシミュレーションによって評価した．

研究業績一覧

著書

1. 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．

2. K. Nonobe and T. Ibaraki（分担執筆）：
“A metaheuristic approach to the resource constrained project scheduling with Variable activity durations and Convex Cost Functions”, in: J. Jozefowska and J. Weglarz, eds., Perspectives in Modern Project Scheduling, Springer Science+Business Media, 2006.
概要: We introduce a generalized model of the resource constrained project scheduling problem (RCPSP). It features that (i) the duration of an activity is not constant, but can vary in a specified range, 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 start/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.

3. 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. S. Fujishige, G. A. Koshevoy, and Y. Sano: “Matroids on convex geometries”, Discrete Mathematics, (to appear).
概要: 効率的なアルゴリズムを支えるマトロイド的な構造が, 凸幾何という離散構造の上にどのように拡張されるかを詳細に吟味し, 独立集合族, 基族, 階数関数の特徴付けを与えた．このように一般化された凸幾何-マトロイド上での最適化問題に対するアルゴリズムの研究をさらに進めている．効率的なアルゴリズムに導く有効な離散構造に関する新たな知見が得られると期待される．

2. H. Hashimoto, T. Ibaraki, S. Imahori and M. Yagiura:
“The vehicle routing problem with flexible time windows and traveling times”, Discrete Applied Mathematics, 154, 2271–2290, 2006.
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 and K. Nakamura:
"Packing problems with soft rectangles", Springer LNCS, Hybrid metaheuristics, 4030, 13–27, 2006.
概要: We consider the problems of packing rectangles, whose shapes are adjustable within given perimeter and area constraints. Using "sequence pairs" to specify relative positions of rectangles, we solve the resulting linear or convex programming problem to determine sizes and locations of all rectangles. To find good sequence pairs, we then resort to local search techniques. This is therefore a hybrid of local search and mathematical programming. The resulting algorithm can solve problem instances with $30 \sim 50$ rectangles in reasonable amount of time.

4. T. Ishii, H. Nagamochi and 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 $k, l > 0$ and an undirected graph $G = (V, E)$, 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-verstex-connected by adding at most $\max\{l + 1, 2k - 4\}$ surplus edges over the optimum in $O(\min\{k, \sqrt{n}\}kn^3 + n^4)$ time.

5. K. Makino, Y. Uno and T. Ibaraki:
"Minimum edge ranking spanning trees of split graphs", Discrete Applied Mathematics, 154, 2373–2386, 2006.
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. This problem is known to be NP-hard for general graphs. In this paper, we show that MERST has a polynomial time algorithm for split graphs, which have useful applications in practice. We also show that MERST for threshold graphs can be solved in linear time.

6. 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, 2-16, 2006.
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.

7. 巳波弘佳:
"グラフ理論の基礎", 数理科学（特集・ネットワーク科学の数理）サイエンス社, 518, 5-11, 2006.
概要: 複雑ネットワークの研究に関する特集号において, この分野においてよく使われる基本的なグラフの諸概念とアルゴリズムについて解説した.

8. M. Nishihara, M. Yagiura and T. Ibaraki:
"Duality in option pricing based on prices of other derivatives", Operations Research Letters, 35, 165–171, 2007.
概要: We clarify a financial meaning of duality in the semi-infinite programming problem which emerges in the context of deter-

mining a derivative price range based only on the no-arbitrage assumption and the observed prices of other derivatives. The interpretation links studies in the above context to studies in stochastic models.

9. 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, 5, 43–64, 2006.
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 minimize 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.

10. S. Umetani and M. Yagiura:
"Relaxation heuristics for the set covering problem", Journal of the Operations Research Society of Japan, （掲載予定）.
概要: The set covering problem (SCP) is one of representative combinatorial optimization problems, which has many practical applications. The continuous development of mathematical programming has derived a number of impressive heuristic algorithms as well as exact branch-and-bound algorithms, which can solve huge SCP instances of bus, railway and airline crew scheduling problems. We survey heuristic algorithms for SCP focusing mainly on contributions of mathematical programming techniques to heuristics, and illustrate their performance through experimental analysis.

11. 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 per-

forms quite effectively for various types of problems, especially for very large-scale instances.

12. 柳浦睦憲, 野々部宏司:
“分枝限定法 — さらなる計算効率の希求”, システム/制御/情報, Vol. 50, No. 9, 350–356, 2006 年 9 月.
概要: 組合せ最適化問題に対する数理計画アプローチとして, 分枝限定法・分枝カット法の最新動向を紹介するとともに, 一般化割当問題を例として, アルゴリズムを構成する場合のガイドライン・勘所について解説した. また, 巡回セールスマン問題, 矩形パッキング問題など, いくつかの具体的な適用例を紹介した.

研究会等

1. E. Chiba, H. Fujiwara and T. Ibaraki:
“A new approach to approximate the collision probability in an automated production line”, The 8th Workshop on Models and Algorithms for Planning and Scheduling Problems (MAPSP 2007), （発表予定）.
概要: In this paper, we give a simpler expression of the collision probability by a new approximation approach, which enables us to easily compute numerical values of the collision probability over a wider range of parameter values. We also carry out some simulations to evaluate the exact probabilities and confirm that our approximation approach yields reasonable results compared to the simulated results.

2. E. Chiba, H. Fujiwara, Y. Sekiguchi and T. Ibaraki:
“Collision probability in an automated production line under Erlang distribution”, Proceedings of the 5th International Conference on Research, Innovation and Vision for the Future (RIVF 2007), 42–49, 2007.
概要: Flat Panel Displays (FPDs) are manufactured through many different processing equipments arranged sequentially in a line. Although the constant inter-arrival time (i.e., the tact time) of glass substrates in the line should be kept as short as possible, the collision probability between glass substrates increases as the time becomes shorter. Since the glass substrate is expensive and fragile, the collision should be avoided. In this paper, we derive a closed form formula of the collision probability for a model, in which the processing time on each equipment is assumed to follow the Erlang distribution. We also show some numerical results and computer simulation results of the collision probability.

3. 千葉英史，浅野哲夫，茨木俊秀:
“衝突確率を考慮したバッファ配置問題に対する計算機シミュレーションを利用した手法”, 情報処理学会研究報告（アルゴリズム, 2006 – AL – 108）, 57–63, 2006.
概要: 液晶や半導体の製造装置には，衝突回避のために，製造ライン上に通常十分にバッファが装備されているが, 実際には余分なバッファも少なくない．一方，コスト面から見ると，できるだけバッファ数を減らすことが求められている．本論文では，ジョブの投入間隔が一定の直列システムにおいて，各機械のバッファ数を任意に設定できるとき，計算機シミュレーションにより衝突確率を求める手法を提案する．この手法を利用することで，与えられた衝突確率を満たすようなバッファ配置の中で，総バッファ数ができるだけ少ない配置を実時間内で求めることができる．また，代表的な数値結果も与える．

4. H. Fujiwara, K. Iwama, K. Yonezawa:
“Online chasing problems for regular n-gons”, Proceedings of the 5th International Conference on Research, Innovation and Vision for the Future (RIVF 2007), pp. 36–41, 2007 (Best Paper Award).
概要: We consider a server location prob-

lem with only one server to move. If each request must be served on the exact position, there is no choice for the online player and the problem is trivial. In this paper we assume that a request is given as a region and that the service can be done anywhere inside the region. Namely, for each request an online algorithm chooses an arbitrary point in the region and moves the server there. Our main result shows that if the region is a regular n-gon, the competitive ratio of the greedy algorithm is $\frac{1}{\sin\frac{\pi}{2n}}$ for odd n and $\frac{1}{\sin\frac{\pi}{n}}$ for even n. Especially for a square region, the greedy algorithm turns out to be optimal.

5. K. Haraguchi and M. Yagiura:
"A randomness based analysis on the data size needed for generating reliable rules", Proceedings of the Second International Conference on Knowledge Engineering and Decision Support (ICKEDS 2006), 75–82, 2006年5月.
概要: We consider a two-labeled data set $X = X_1 \cup X_0$ in which each xample is a Boolean vector. A pattern is a co-occurrence of a particular value combination of some variables. If a pattern appears frequently in X_1 and infrequently in X_0, we call it a good pattern. In this article, we discuss the data size needed for removing "deceptive" good patterns; if X is small, many good patterns may appear independently of the underlying structure. We hypothesize that X should contain more number of examples than that at which a random data set contains few good patterns. We justify this hypothesis by computational studies, and derive a theoretical upper bound on the needed data size in view of our hypothesis.

6. T. Ibaraki, A. Ishikawa, H. Nagamochi, K. Nonobe and M. Yagiura:
"An iterated local search algorithm for the multi-resource generalized assignment problem with flexible assignment cost", Proceedings of the Third International Symposium on Scheduling, 160–165, 2006.
概要: We propose an iterated local search algorithm for the multi-resource generalized assignment problem (MRGAP) with flexible assignment cost. This problem generalizes the MRGAP so that the assignment cost function defined for each agent can be in any form. While this flexibility achieves a wide applicability, the computation of the assignment cost can be computationally expensive, Our algorithm features two types of oracles to evaluate this cost approximately; i.e., quick-evaluation oracle and accurate-evaluation oracle. In our computational experiments on the parallel machine scheduling and the capacitated vehicle routing, the algorithm combining two oracles performs well and is sometimes competitive with other existing algorithms tailored for the specific problem.

7. T. Imamichi, M. Yagiura and H. Nagamochi:
"An iterated local search algorithm based on nonlinear programming for the irregular strip packing problem", Proceedings of the Third International Symposium on Scheduling, 132–137, 2006.
概要: The irregular strip packing problem is a combinatorial optimization problem that asks to place a set of 2-dimensional polygons within a rectangular container so that no two polygons overlap each other and no polygon protrudes from the container, where each polygon is not necessarily convex. The container has a fixed width, while its length can change so that all polygons are placed in it. The objective is to find a layout that minimizes the length of the container. This problem has many applications in material industry such as paper and textile industries, where raw materials are usually given in rolls. We propose a new sep-

aration algorithm based on nonlinear programming, and an algorithm that swaps two polygons in a sophisticated way; it tries to find their positions with the least overlap. We incorporate these algorithms as components in an iterated local search algorithm for the overlap minimization problem and then develop an algorithm for the irregular strip packing problem using the iterated local search algorithm. Computational comparisons on representative instances disclose that our algorithm is competitive with other existing algorithms. Moreover, our algorithm updates several best known results.

8. Y.Kurebe, H.Miwa, and T.Ibaraki:
"Weighted module placement based on rectangle packing", 4th ESICUP meeting (EURO Special Interest Group on Cutting and Packing), 2007 年 3 月.
概要: 2D rectangle packing problems ask to pack several modules in the minimum area without overlap. In this research, we consider the weight of a module in addition to its area. For a placement of the modules in the engine room of a car, and so on, it is important to pack the modules not only in the small area, but also with the low inertia moment and with the small gap between the center of gravity of the modules and the center of the area. Using sequence pairs to specify relative positions of rectangles, we solve the resulting nonlinear programming problems to determine the locations of all rectangles. To find good sequence pairs, we then resort to local search techniques. A local search algorithm is in general defined by the neighborhood (a subset of the set of all sequence pairs) of the current sequence pair. We popose a hybrid algorithm of local search and mathematical programming by combining some specialaized neighborhoods to this problem and using an approximation algorithm to solve the nonlinear programming problems. The proposed algorithm can solve problem instances with up to 50 rectangles in reasonable amount of time.

9. K. Matsumoto, H. Miwa, and T. Ibaraki:
"Scheduling of corrugated paper production", Proceedings of the Third International Symposium on Scheduling, 2006.
概要: Corrugated paper is produced by gluing three types of papers. Given a set of orders, we first assign each order to one of the rolls with standard breadths, and then sequence the orders assigned to each roll so that they are continuously manufactured by the machine called corrugator. Here we are asked to minimize the total length of roll papers, total loss of papers caused by the differences between the standard breadths and breadths of orders, and the number of machine stops needed during production. We use integer programming to assign orders to standard breadths, and then develop a special purpose algorithm to sequence the orders assigned to each standard breadth.

10. 巳波弘佳, 増田直紀, 今野紀雄:
"スケールフリー性を持つ閾値モデルの諸特性量の解析", 信学技報, Vol. 106, No. 42, IN2006-13, 73-78, 2006 年 5 月.
概要: 現実世界に存在するネットワークの中には，次数分布がべき則に従うという性質（スケールフリー）を持つものも多い．他にもクラスター係数や隣接点平均次数などに関しても特徴的な性質を持つものもある．このような特徴を持つネットワークの生成モデルとして，各点に重みが確率的に与えられており，点 v_i と v_j の間には，v_i と v_j の重みの和や積（一般的には 2 点の重みの関数）がある閾値を越える時，またその時に限って辺が張られるという原理で生成される閾値モデルというものがある．本研究では，この閾値モデルにおいて，特に重みがガウス分布に従う場合を調べ，数値実験によりスケールフリー性に近い性質を持つことを示した．

11. 佐々木裕介，巳波弘佳:
"P2P における次数・直径の小さいオーバレ

イネットワーク構成法", 信学技報, Vol. 106, No. 42, IN2006-11, 61-66, 2006 年 5 月.
概要: 近年，クライアント/サーバ型に取って代わるネットワーク形態として P2P(Peer-to-Peer) 型のネットワークが注目されている．P2P ネットワークはファイル共有，分散ストレージ，コンテンツ配信等，様々な分野での応用が期待されている．この P2P ネットワークにおいて，いかに効率よく確実に目的のデータを取得するかについて，様々な研究が行われてきた．効率よく目的のデータを取得するには，実際のネットワーク上に仮想的に構成するオーバレイネットワークの構造が重要である．本研究では，頂点数が大きくても，次数を小さく保ちつつ，直径が小さい de Bruijn グラフを用い，ノード数 n としたとき，ルーティングに必要な次数を最悪 4 に抑えつつ，目的ノードまでのホップ数を最悪 $\lceil \log_2 n \rceil$ に抑えることができ，さらに，ノードの参加・離脱に対しても安定性を有するオーバレイネットワークの構成法について提案した．

12. 佐々木裕介，巳波弘佳:
"次数・直径の小さい P2P ネットワーク構成法とその評価", 信学技報, Vol. 106, No. 578, IN2006-240, 357-362, 2007 年 3 月.
概要: 本研究では，頂点数が大きくても，次数と直径が小さい de Bruijn グラフを用いることによって，ルーティングに必要な次数を最悪 4 に抑えつつ，目的ノードまでのホップ数を最悪 $\lceil \log_2 n \rceil$（n はノード数）に抑えることができるオーバレイネットワークの構成法について述べ，その構成法に基づいて構成したネットワークの性能をシミュレーションによって評価した．

13. S. Umetani, M. Yagiura, T. Imamichi, S. Imahori, K. Nonobe and T. Ibaraki:
"A guided local search algorithm based on a fast neighborhood search for the irregular strip packing problem", Proceedings of the Third International Symposium on Scheduling, 126–131, 2006.
概要: The irregular strip packing problem asks to place a set of polygons within a rectangular strip of fixed height without overlap, so as to minimize the strip width required. We consider an overlap minimization problem which minimizes the amount of overlap penalty for all pairs of polygons within a given bound of strip width. We propose a local search algorithm which translates a polygon in horizontal and vertical directions iteratively, and incorporate it in metaheuristic approaches called the iterated local search and the guided local search. Computational results show that our algorithm is competitive with other existing algorithms.

学会大会等

1. 千葉英史，茨木俊秀:
"衝突確率を考慮したバッファ配置問題に対する近似解法", 日本オペレーションズ・リサーチ学会春季研究発表会, 2007.

2. 千葉英史, 藤原洋志, 関口良行, 茨木俊秀:
"生産ラインにおける衝突確率: 処理時間がアーラン分布に従う場合", 日本オペレーションズ・リサーチ学会秋季研究発表会, 116–117, 2006.

3. H. Fujiwara, K. Iwama, K. Yonezawa:
"Online chasing problems for regular n-gons", 日本オペレーションズ・リサーチ学会春季研究発表会, 2007.

4. 暮部裕介，巳波弘佳，茨木俊秀:
"重量付モジュール詰め込みの最適化", 日本オペレーションズリサーチ学会 2007 年春季研究発表会, 2-C-7, 2007 年 3 月.

5. 原口和也，柳浦睦憲，Endre Boros, 茨木俊秀:
"ルール生成に必要なデータ量に関するランダム性に基づいた解析", 信学技報, Vol. 106, No. 289 (COMP2006-38), 57–64, 2006 年 10 月.

6. 橋本英樹，柳浦睦憲:
"時間依存配送計画問題に対する反復局所探

索法", ミニシンポジウム: 新世代計算限界と地球環境問題, 15–23, 2006 年 12 月.

7. H. Hashimoto, T. Ibaraki, S. Imahori and M. Yagiura:
"Generalizations of the vehicle routing problem with time windows", The 1st Workshop on Mathematical Contributions to Metaheuristics (Matheuristics 2006), 2006 年 8 月.

8. T. Ibaraki, A. Ishikawa, H. Nagamochi, K. Nonobe, M. Yagiura:
"An iterated local search algorithm for the multi-resource generalized assignment problem with flexible assignment cost", The 19th International Symposium on Mathematical Programming (ISMP 2006), 2006 年 8 月.

9. T. Imamichi, M. Yagiura, H. Nagamochi:
"An iterated local search algorithm based on nonlinear programming for the irregular strip packing problem", The 19th conference of the European Chapter on Combinatorial Optimization (ECCO XIX) and the International Symposium on Combinatorial Optimisation 2006 (CO 2006), 2006 年 5 月.

10. 野々部宏司:
"スケジューリング最適化ソルバ", 日本オペレーションズ・リサーチ学会 第 3 回関西支部講演会, 「スケジューリング設計法 – 離散最適化アプローチを中心として –」, 2006 年 11 月.

11. 小野孝男, 柳浦睦憲, 岩城正哉, 平田富夫:
"半定値計画法に基づく彩色問題の発見的解法", 第 108 回アルゴリズム研究会, 2006 年 9 月.

12. T. Ono, M. Ygiura, M. Iwaki and T. Hirata:
"Graph coloring via vector assignment in the plane", The 19th International Symposium on Mathematical Programming (ISMP 2006), 2006 年 8 月.

13. S. Umetani, M. Yagiura, T. Imamichi, S. Imahori, K. Nonobe and T. Ibaraki:
"A guided local search based on a fast neighborhood search for the irregular strip packing problem", INFORMS International Conference, 2006 年 6 月.

14. S. Umetani, M. Yagiura, T. Imamichi, S. Imahori, K. Nonobe and T. Ibaraki:
"A guided local search based on a fast neighborhood search for the irregular strip packing problem", The 1st Workshop on Mathematical Contributions to Metaheuristics (Matheuristics 2006), 2006 年 8 月.

15. M. Yagiura, T. Ibaraki, T. Imamichi, Y. Koga, H. Nagamochi and K. Nonobe:
"Efficient branch-and-bound algorithms for weighted MAX-2-SAT", The 21st European Conference on Operational Research (EURO XXI), 2006 年 7 月.

16. 柳浦睦憲:
"組合せ最適化問題に対する実用的解法", 日本オペレーションズ・リサーチ学会 平成 18 年度第 1 回 OR セミナー『最適化の各論』, 1–10, 2006 年 6 月.

17. 柳浦睦憲:
"離散最適化問題に対するメタヒューリスティクス", OR 学会第 56 回シンポジウム — ここまで使える数理計画法, 33–40, 2006 年 9 月.

18. 柳浦睦憲:
"割当型問題に対する汎用解法構築の試み", 日本オペレーションズ・リサーチ学会 第 3 回関西支部講演会, 「スケジューリング設計法 – 離散最適化アプローチを中心として –」, 7–13, 2006 年 11 月.

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 システム情報科学研究院
〒 819-0395 福岡市西区元岡 744
{sada,mak,ono}@csce.kyushu-u.ac.jp

1　今年度の研究活動

本研究課題では領域効率の良いアルゴリズムの開発を行っている．大量のデータを扱う場合には，そのデータを格納するメモリ量の問題が発生する．その問題を解決するために，本研究では 2 つのアプローチを取っている．

1. データおよびデータ構造を圧縮する
2. ランダムアルゴリズムを用いてデータの一部のみをメモリに格納して問題を解く．

1 つ目のアプローチでは，簡潔データ構造およびそれをさらに圧縮した超簡潔データ構造の開発を行っている．これまでに多くのデータ構造を開発しているが，今年度はその効率の良い実装にも取り組んでいる．2 つ目のアプローチでは，スケールフリーグラフの性質を利用した，効率の良いグラフ探索アルゴリズムを開発した．

2　研究成果の概要

2.1　順序木の新しい表現法

簡潔データ構造 (succinct data structures) はある要素を情報理論的下界に近い大きさの空間に格納し，かつ，要素に対する多くの原始的操作を定数時間で行えるデータ構造である．ここで情報理論的下界とは，位数 L の集合の中のある 1 つの要素を格納する場合のデータ構造サイズの下界であり，$\log L$ ビットである．対数の底は 2 とする．また，$0 \log 0 = 0$ とする．なぜならば 2 つの異なる要素を区別するには最悪の場合はこのビット数が必要だからである．例えば，順序集合 $\{1, 2, \ldots, n\}$ の部分集合の場合，2^n 個の異なる部分集合が存在するため，情報理論的下界は n ビットとなる．また，n ノードの順序木の場合，木は $\binom{2n-1}{n-1}/(2n-1) = 2^{2n}/\Theta(n^{\frac{3}{2}})$ 種類存在するため，下界は $2n - \Theta(\log n)$ となる．

データ構造のサイズは一般には $(1+\mathrm{o}(1)) \log L$ ビットとなるが，いくつかのデータ構造では $\mathrm{O}(\log L)$ ビットを用いている．要素に対する多くの基本的演算は語長 $\Theta(\log n)$ の word RAM モデル上で定数時間で行える．演算の例としては，集合中である指定された値よりも小さい値の数を数えるものや，木のノードの親を求めるものなどがある．

本論文では順序木に対する簡潔データ構造を考える．過去に多くのデータ構造が提案されているが，それらには以下のような欠点が存在する．

1. 全ての基本演算を定数時間で実行できるデータ構造は存在しない．例えば，括弧列表現 (BP) は i 番目の子を求める演算ができず，DFUDS (depth-first unary degree sequence) は *lca* (lowest common ancestor) を計算できない．
2. データ構造のサイズは最悪の場合には最適だが，あるクラスに入る木のみを格納する場合は最適ではない．例えば，n ノードの木で，全ての内部ノードがちょうど 2 つの子を持つような場合，そのような木は n ビットで表現できる (深さ優先探索の順で内部ノードに対して 1 を出力し，葉に対して 0 を出力すればいい) が，BP と DFUDS では共に $2n$ ビット必要である．

これらの欠点は大量文書処理などでは致命的である．現在 Web ページやゲノム配列などの大量の文書が存在するが，これらを検索しようとした場合，高速に検索するためにデータ構造として接尾

辞木 や圧縮接尾辞木 を用いる．圧縮接尾辞木では木構造を表現するために BP を用いているがこれは接尾辞木において *lca* 演算が必要だからである．接尾辞木は最大 $2n-1$ 個のノードを持つため，BP のサイズは $4n+\mathrm{o}(n)$ ビットとなる．一方，接尾辞木をパトリシア木で表現すると $2n$ ビットで十分であるが，効率的な問い合わせができない．従って効率的な問い合わせを行うためにデータ構造のサイズが $2n$ ビット大きくなっている．これは大量の文書を扱う場合には無視できない．

もちろん，任意の n ノードの木を cn ビット以下 $(c<2)$ で表現することはできない．なぜなら情報理論的下界は $2n$ ビットだからである．しかし，もし n ノードの木全体ではなく，そのうちのある部分クラスだけを表現する場合には，情報理論的下界よりも小さくできる可能性はある．これがデータ圧縮の概念である．本論文ではある要素に対するデータ構造のサイズが，その要素のエントロピーであらわされるようなものを扱う．そのようなデータ構造を本論文では超簡潔データ構造 (ultra-succinct data structures) と呼ぶ．そのようなデータ構造としては，文字列に対するものや順序集合に対するものが存在するが，順序木に対するものは存在しない．

本論文は順序木に対する超簡潔データ構造を提案する．特徴は以下の点である．

1. 知られている全ての基本演算を定数時間で実行できる
2. データ構造のサイズは以下で定義する順序木のエントロピーを達成する．

順序木の **木形状エントロピー** を次のように定義する．

Definition 1 (木形状エントロピー) n ノードの順序木 T において，i 個の子を持つノードの数を n_i で表すとする $(0 \le i < n)$．このとき，T の木形状エントロピー $H^d(T)$ を以下のように定義する．

$$H^d(T) = \sum_i \frac{n_i}{n} \log \frac{n}{n_i}.$$

この定義は自然である．なぜならこの値は順序木でノードの次数の分布を固定した場合の情報理論的下界と一致するからである．

Lemma 1 (Rote 96) n ノードの木で，i 個の子を持つノードの数が n_i のとき，そのような木の数は

$$\frac{1}{n}\binom{n}{n_0\ n_1\ \cdots\ n_{n-1}}$$

である．ただし $\sum_{i\ge 0} n_i(i-1) \neq -1$ の場合は木の数は 0 である． □

この数を L とすると，$\log L \approx nH^d(T)$ となる．

本論文の主な貢献は，データ構造のサイズが木形状エントロピーに漸近的に一致するような，順序木の超簡潔データ構造の提案である．データ構造のサイズが既存のものよりも小さいだけでなく，木に対する操作の計算量も他のデータ構造と同じである．我々の証明技法は，個々の操作に対して証明を行うのではなく，より一般的な事実を示すものである．具体的には，DFUDS の瞬時復号可能性を示す．

Theorem 1 任意の n ノードの根付き順序木 T に対し，サイズが $nH^d(T) + \mathrm{O}(n(\log\log n)^2/\log n)$ ビットで，T の *DFUDS* 表現の任意の部分の連続する $\log n$ ビットを *word RAM* モデル上で定数時間で復元できるデータ構造が存在する． □

この定理は，このデータ構造を用いると，DFUDS 表現をそのまま格納していると仮定できることを意味する．よって，DFUDS で実現可能な演算は全て我々のデータ構造でも同じ計算量で実行できることは明らかである．さらに，たとえ DFUDS に対する新しい操作が提案されたとしても，それは我々のデータ構造の上でも同じ計算量で実行できる．

本論文のもう 1 つの貢献は，DFUDS の上で *lca*, *depth*, *level-ancestor* を求めるための $\mathrm{o}(n)$ ビットの補助データ構造の提案である．なお，*depth* と *level-ancestor* を求める簡潔データ構造は既に存在するが，これは BP や DFUDS とは異なる表現で汎用性がない．よって，DFUDS で実現可能な演算がこのデータ構造の上でも行えるという保障はない．また，*lca* は計算できない．さらに，このデータ構造のサイズは $2n+\mathrm{o}(n)$ ビットであり，これをさらに圧縮することは難しい．よって，DFUDS の上で上記の演算を実現することは価値がある．本論文では以下の定理を示す．

Theorem 2 任意の 2 つのノードの最近共通祖先 *(lca)*, 各ノードの深さと深さ指定先祖 *(level-ancestor)* は，*DFUDS* 表現と $O(n(\log\log n)^2/\log n)$ ビットの補助データ構造を用いて定数時間で計算できる． □

本論文で提案する新しい補助データ構造は既存のものよりも小さい．従来は $O(n\log\log n/\sqrt{\log n})$ ビットであった．

n ノードの根付き順序木を考える．そのような木は $\binom{2n+1}{n}/(2n+1)$ 個存在する．従ってデータ構造サイズの情報理論的下界は $2n-\Theta(\log n)$ ビットである．サイズがこれに漸近的に一致するデータ構造は多く提案されている．

順序木の表現で最もよく知られたものはバランスした括弧列表現である．本論文ではこれを BP と呼ぶ．n ノードの木は長さ $2n$ の括弧列 P で表される．1 つのノードは `(` と `)` のペアで表され，そのノードを根とする全ての部分木はこの括弧のペアの間に符号化される (図 2.1参照)．

木の巡回を行うために，以下の操作を定数時間で行う補助データ構造が提案されている:

- $findclose(P,x), findopen(P,x)$: $P[x]$ にある開き (閉じ) 括弧に対応する閉じ (開き) 括弧の位置を返す．
- $enclose(P,x)$: $P[x]$ にある括弧を囲む括弧で最もタイトなものの位置を返す．

これらの操作を用いて，以下の操作が実現される:

- $parent(x), firstchild(x), sibling(x)$: x の親，最初の子，次の弟
- $depth(x)$: x の深さ
- $desc(x)$: x の子孫の数
- $\mathbf{rank}(x)$: x の通りがけ順
- $\mathbf{select}(i)$: 通りがけ順が i であるノードの開き括弧の位置
- $LA(x,d)$: x の祖先で深さが d のもの (*level-ancestor*),
- $lca(x,y)$: ノード x と y の最近共通祖先
- $degree(x)$: x の子の数
- $child(x,i)$: x の左から i 番目の子
- $childrank(x)$: x がその親の左から何番目の子であるか

これらの操作は $o(n)$ ビットの補助データ構造を用いて定数時間で実現される．ただし *child* と *childrank* は $O(i)$ 時間かかる．

DFUDS 表現

順序木の DFUDS 表現 (depth-first unary degree sequence representation) は以下のように定義される．1 つの葉のみからなる木は `()` で表現される．これは BP と同じである．ある木 T が k 個の部分木 $T_1,\ldots,T_k$ を持つ場合，T の DFUDS 表現は $k+1$ 個の `(`，1 つの `)`，$T_1,\ldots,T_k$ の DFUDS 表現 (ただし各部分木の DUFDS 表現の最初の `(` を削除したもの) を順に連結したものと定義する．このときできあがった DFUDS 表現はバランスした括弧列表現となっている (図 2.1参照)．DFUDS 表現の括弧列は，先頭の `(` を架空の根ノードとみなすと，全ノードを通りがけ順に並べ，各ノードは次数が k の場合に k 個の `(`と，それに続いて 1 つの `)`を出力したものと解釈できる．各ノードはそれに対応する 1 番左の括弧の位置によって表される．その括弧は内部ノードの場合は `(` であり，葉の場合は`)` である．1 番左の括弧列の位置を 0 とする．その位置の括弧は架空の根を表すため，通常の根ノードの位置は 1 となる．DFUDS 表現は BP 表現と同じ大きさの空間を用い上述の操作のうち *lca*, *depth*, *LA* 以外を定数時間で計算できる．*depth* と *LA* を計算できるデータ構造も存在するが，それは DFUDS とは異なる．

本節では DFUDS の上で *lca*, *depth*, *level-ancestor*, *childrank* を求めるシンプルなアルゴリズムとデータ構造を提案する．*lca* を求めるアルゴリズムは今まで知られていない．*depth* と *level-ancestor* は Geary らによって提案されているが，これらは DFUDS とは異なる表現の上で実現されており，データ構造は複雑でそれを圧縮することは難しい．一方，本論文のデータ構造は DFUDS の上で *depth* と *level-ancestor* を求めるもので

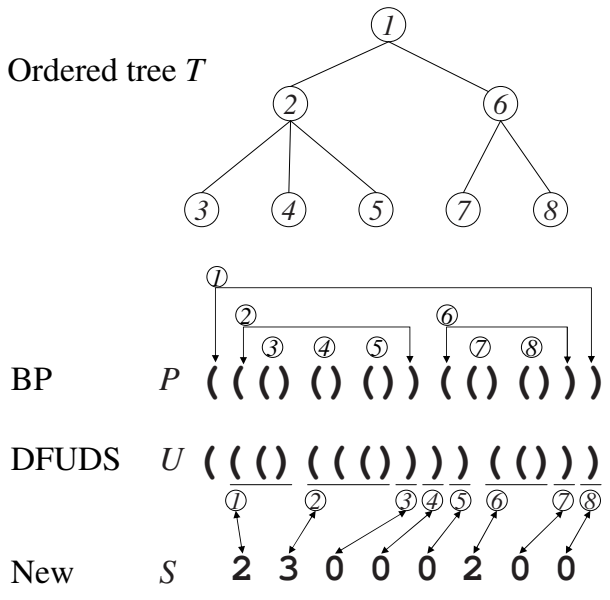


図 2.1: 木の簡潔データ構造.

あり，既存のものよりもシンプルである．本論文のデータ構造はシンプルなだけでなく，データ構造のサイズの低次項を改善している．従来のものは $\mathrm{O}(n \log\log n/\sqrt{\log n})$ ビット使用していたが，本論文では $\mathrm{O}(n(\log\log n)^2/\log n)$ ビットである．*childrank* のデータ構造も既に提案されているが，本論文では DFUDS において同じ演算を実現するアルゴリズムを提案する．

LCA T の DFUDS 表現を U とする．U の超過数列 E を $E[i] =$ ($U[0..i]$ 中の $\boxed{(}$ の数) − ($U[0..i]$ 中の $\boxed{)}$ の数) と定義する．なお，BP 表現では超過数はノードの深さに対応するが，DFUDS では直接は対応しない．

T のある内部ノード v を考える．そのノードの子として k 個の部分木 $T_1, \ldots, T_k$ があるとする．U の部分列 $U[l_0..r_0]$ が v を表すとする．また，$U[l_i..r_i]$ $(1 \le i \le k)$ はそれぞれ T_i の DFUDS 表現とする．なお，$l_i = r_{i-1}+1$ である．$d = E[r_0]$ とする．すると超過数について以下の性質が成り立つ．

Lemma 2

$$\begin{aligned} E[r_i] &= E[r_{i-1}] - 1 = d - i \quad (1 \le i \le k) \\ E[j] &> E[r_i] \quad (l_i \le j < r_i) \end{aligned}$$

□

Lemma 3 順序木のノード x, y の最近共通祖先は木の *DFUDS* 表現と $\mathrm{O}(n(\log\log n)^2/\log)$ ビットの補助データ構造を用いて定数時間で計算できる． □

証明: $z = lca(x, y)$ $(x < y)$ は以下のように計算できる．

$$\begin{aligned} w &= RMQ_E(x, y-1) + 1 \\ z &= parent(w) \end{aligned}$$

ここで x と y は DFUDS 中でのノードの位置である．$RMQ_E(x, y-1)$ は区間最小値問い合わせと呼ばれ，$E[x..y-1]$ 中の最小値の位置を返す演算である．もし最小値が複数ある場合は RMQ は最も左にある最小値の位置を返す．RMQ は $\mathrm{O}(n(\log\log n)^2/\log n)$ ビットの補助データ構造を用いて定数時間で計算できる． □

n ノードの木 T の DFUDS 表現 U を圧縮することを考える．T の最大次数を σ で表す．基本的な考えは，DFUDS での 1 進数符号化を 2 進数にするというものである．T のノードの次数を通りがけ順に格納した整数配列を $S[1..n]$ とする．S の各要素は $\log\sigma$ ビットで符号化される．なお，各 $S[i]$ を $S[i]$ 個の開き括弧と 1 つの閉じ括弧に置き換えると，S と U は等しくなる．従って，S と U の間の変換が $\mathrm{O}(n)$ 時間で行えるのは自明である (図 2.1参照)．本論文では S は $nH^d(T) + \mathrm{o}(n)$ ビットに圧縮でき，かつ，その圧縮された S の表現から U の任意箇所の連続する $\log n$ ビットを定数時間で復元できることを示す．

同様の手法は DFUDS 表現でラベル付き木を表すために持ちられている．その論文では $\sigma = 4$ の場合にノードの次数をある符号で符号化している．本論文では一般のアルファベットの場合に順序木のエントロピーを達成するデータ構造を提案する．

まず，木の最大次数が定数である場合に木を符号化する方法を考える．つまり，S のアルファベットサイズが定数の場合である．S は $nH_k(S) + \mathrm{O}(n\log\log n/\log n)$ ビットに圧縮でき，S の連続する $\log n$ 個の値を定数時間で復元できる．よって，S は圧縮されていない状態で格納されていると仮定しても良い．

任意の i に対し，$U[i..i+w-1]$ $(w = \frac{1}{2}\log n)$ を S から定数時間で求めるデータ構造を考える．U から S への写像 f を $S[i]$ の 1 進数符号が $U[l_i..r_i]$ に格納されているとしたときに $f(j) = i$ $(l_i \leq j \leq r_i)$ と定義する．各 $U[jw]$ $(j = 1, 2, \ldots, n/w)$ に対し，S 中の位置 $m_j = f(jw)$ に印をつける．これは FID で表現でき，$\mathrm{O}(n \log\log n / \log n)$ ビットを用いる．また，各 $U[jw]$ に対し，$S[m_j]$ の 1 進数表現の開始位置と jw の差を格納する．つまり，もし $d = S[m_j]$ が $U[l..l+d]$ $(l \leq jw \leq l+d)$ に格納されているとき，格納する差の値は $jw - l$ である．これは $\mathrm{O}(\log w) = \mathrm{O}(\log\log n)$ ビットで格納できる．

一般性を失うことなく，i は w の倍数と仮定してよい．$U[i..i+w-1]$ を復元するためには，まず $U[i]$ の周辺に符号化されている $S[m_j]$ $(j = i/w)$ を求める．長さ w の U の部分文字列に対応する S の要素数は高々 w 個であり，それらは $\mathrm{O}(\log n)$ ビットで表現できる．よってそれらを 1 進数符号 (DFUDS) に変換することは表引きで定数時間で行える．データ構造のサイズは全ての $0 \leq k \leq \mathrm{O}(\log\log n)$ に対して $nH_k(S) + \mathrm{O}(n(k + \log\log n)/\log n)$ ビットである．$H_0(S) = H^d(T)$ であるため，これは $nH^d(T) + \mathrm{O}(n \log\log n / \log n)$ ビットと表現できる．DFUDS での任意の操作は，このデータ構造の上でも同じ計算量で実行できる．

一般の木の場合，S のアルファベット $\mathcal{A}$ を 2 つの集合に分割する．$\mathcal{A}_1$ は値が $\log n$ 以上のものの集合，$\mathcal{A}_2$ はそれ以外とする．そして文字列 S_1 と S_2 をそれぞれ S 中の文字から $\mathcal{A}_1$ のものだけと $\mathcal{A}_2$ のものだけを取り出したものとする．S_2 のアルファベットサイズは $\sigma = |\mathcal{A}_2| \leq \log n$ であり，各値は $\log\log n$ ビットで表現される．文字列 S_1 と S_2 は異なる符号化をする．U の部分文字列を求める場合は，S_1 と S_2 から部分文字列を求め，それらを併合する．

2.2 単純な Rank/Select 辞書

Rank/Select 辞書とは，順序集合 $S \in \{0, 1, ..., m-1\}$ において $rank(x, S) = |\{y \in S | y \leq x\}|$ と $select(i, S)$ (S の中で i 番目に小さい要素) を返すデータ構造である．これは文字列，木，グラフなどの圧縮データ構造の基本構成要素であり，多くのデータ構造が提案されている．しかしそれらは漸近的な性能のみを考えており，実データに対する性能は良くない．本研究では単純な Rank/Select 辞書を提案する．特徴としては，集合 S の要素数が小さい場合にデータ構造のサイズを縮小できることと，データ構造が単純であるために実装が容易で，実データに対する性能 (データ構造のサイズと問い合わせ時間) が良い．実験により，既存の実装よりも速度，サイズともに優れていることを示す．

集合 S は長さ m の $\{0,1\}$ のベクトル $B[0, m-1]$ を用いて表現できる．すると $\mathbf{rank}(x, S)$ は $B[0, x]$ 内の 1 の数，$\mathbf{select}(i, S)$ は B 内で左から i 番目の 1 の位置となる．Rank/Select は，m ビットの B と，$\mathrm{O}(m \log\log m / \log m)$ ビットの補助的なデータ構造を用いて定数時間で計算できる．ベクトル B をそのまま格納するデータ構造は，S の要素数 n が小さい場合，または多い場合にはサイズに無駄が多い．なぜなら B は $\binom{m}{n}$ 通りしかないため，$B(n, m) = log\binom{m}{n} \approx n \log \frac{m}{n} + (m-n) \log \frac{m}{m-n}$ ビットで表現できるからである．Raman ら **rank** と **select** を定数時間で求める $B(n, m) + \mathrm{O}(m \log\log m / \log m)$ ビットのデータ構造を提案している．

本研究で提案するデータ構造は，疎なベクトルに対してデータ構造のサイズが小さくなり，問い合わせ時間は既存のどのデータ構造よりも高速である．

2.3 スケールフリーグラフの効率の良い探索アルゴリズム

スケールフリーグラフとは，ノードの次数分布がべき乗則を満たすグラフのことであり，Web グラフのような実際に現れる大規模グラフのいくつかはスケールフリーであることが知られている．一般に，グラフのノードを探索する場合には同じノードを複数回訪れないように各ノードにフラグが必要である．しかし大規模グラフでは全ノードに対してフラグを用意することは計算機のメモリ量の制限により困難である．本研究ではスケールフリーグラフの性質を利用して，少ないメモリでノードの重複無くグラフを探索するアルゴリズム

を提案する．

探索アルゴリズムは Avis, Fukuda の逆探索に基づいている．逆探索ではグラフの各ノードに対して親ノードを定義し，グラフ内に木を定義する．そしてその木の枝のみを用いてグラフを探索する．本研究ではスケールフリーグラフにおける親ノードを新たに定義する．あるノードの親ノードは，そのノードとその全隣接ノードのうち次数の最も大きいものとする．もしそのようなノードが複数ある場合はノードの ID の最も小さいものとする．あるノードの次数がその隣接ノードのどれよりも大きい場合は，そのノードは親ノードを持たない．つまり木の根ノードとなる．

上記の方法で親ノードを定義すると，根ノードが複数現れる．つまりグラフが木ではなく森として表現されることになる．そこで逆探索アルゴリズムを変更し，1 つの木の中での逆探索と，複数の根ノード間の通常の深さ優先探索を行うようにする．深さ優先探索では各根ノードを既に訪れたかどうかのフラグを用いる．

根ノードの数をさらに削減するために，親ノードの定義を変更する．上の定義での根ノードに対しては，そのノードから距離 2 の全ノードの中で次数が最大のものを根ノードの親ノードとする．

このアルゴリズムの必要とするメモリは，根ノードの数に比例する．ランダムに作成したスケールフリーグラフにおいて実験を行うと，100 万ノードの場合に根ノードの数は平均して 4 ないし 5 個になる．つまり数十バイトのメモリのみを用いて全ノードを重複無く列挙することができる．

研究業績一覧

学術論文

1. Jesper Jansson, Kunihiko Sadakane, and Wing-Kin Sung:
   “Ultra-succinct Representation of Ordered Trees”, Proc. ACM-SIAM SODA, pp. 575–584, Jan. 2007.
   概要: There exist two well-known succinct representations of ordered trees: BP (balanced parenthesis) [Munro, Raman 2001] and DFUDS (depth first unary degree sequence) [Benoit et al. 2005]. Both have size $2n + o(n)$ bits for n-node trees, which asymptotically matches the information-theoretic lower bound. Many fundamental operations on trees can be done in constant time on word RAM, for example finding the parent, the first child, the next sibling, the number of descendants, etc. However there has been no single representation supporting every existing operation in constant time; BP does not support i-th child, while DFUDS does not support lca (lowest common ancestor). In this paper, we give the first succinct tree representation supporting every one of the fundamental operations previously proposed for BP or DFUDS along with some new operations in constant time. Moreover, its size surpasses the information-theoretic lower bound and matches the entropy of the tree based on the distribution of node degrees. We call this an ultra-succinct data structure. As a consequence, a tree in which every internal node has exactly two children can be represented in $n+o(n)$ bits. We also show applications for ultra-succinct compressed suffix trees and labeled trees.

2. Kunihiko Sadakane:
   “Compressed Suffix Trees with Full Functionality”, Theory of Computing Systems, Online First, DOI:10.1007/s00224-006-1198-x, Feb. 2007.
   概要: We introduce new data structures for compressed suffix trees whose size are linear in the text size. The size is measured in bits; thus they occupy only $O(n \log |\mathcal{A}|)$ bits for a text of length n on an alphabet A. This is a remarkable improvement on current suffix trees which require $O(n \log n)$ bits. Though some components of suffix trees have been compressed, there is no linear-size data structure for suffix trees with full functionality such as computing suffix links, string-depths and lowest com-

mon ancestors. The data structure proposed in this paper is the first one that has linear size and supports all operations efficiently. Any algorithm running on a suffix tree can also be executed on our compressed suffix trees with a slight slowdown of a factor of polylog(n).

3. Daisuke Okanohara and Kunihiko Sadakane:
"Practical Entropy-Compressed Rank/Select Dictionary", Proc. Workshop on Algorithm Engineering and Experiments (ALENEX), Jan. 2007.
概要: Rank/Select dictionaries are data structures for an ordered set $S \subset \{0, 1, \ldots, n-1\}$ to compute **rank**(x, S) (the number of elements in S which are no greater than x), and **select**(i, S) (the i-th smallest element in S), which are the fundamental components of *succinct data structures* of strings, trees, graphs, etc. In those data structures, however, only asymptotic behavior has been considered and their performance for real data is not satisfactory. In this paper, we propose novel four Rank/Select dictionaries, **esp**, **recrank**, **vcode** and **sdarray**, each of which is small if the number of elements in S is small, and indeed close to $nH_0(S)$ ($H_0(S) \leq 1$ is the zero-th order *empirical entropy* of S) in practice, and its query time is superior to the previous ones. Experimental results reveal the characteristics of our data structures and also show that these data structures are superior to existing implementations in both size and query time.

4. 定兼 邦彦:
"圧縮データ構造", 電子情報通信学会論文誌, vol. J89-A, no. 6, pp. 470–475, 2006 年 6 月.
概要: 大量のデータからの検索を行う場合にはデータ構造を用いることが多いが，そのデータ構造のサイズが問題となっている．圧縮データ構造はデータ構造の機能や問合せ時間を保ったままサイズを小さくするものである．これまでに集合，文字列，木などを表現する圧縮データ構造が多く提案されている．本論文ではそれらのデータ構造を解説する．

5. Yuichi Kurumida, Hirotaka Ono, Kunihiko Sadakane, and Masafumi Yamashita:
"Forest Search: A Paradigm for Faster Exploration of Scale-Free Networks", Proc. of the 4th International Symposium on Parallel and Distributed Processing and Applications (ISPA), LNCS 4330, pp. 39–50, Dec. 2006.
概要: Scale-free networks naturally model wide area networks like the WWW. We consider the problem of fast exploration of huge scale-free networks using small memory space. Although there are many search algorithms for exploring an unknown graph, they require much space or time. For example, the depth first search requires some memory for all the nodes in the worst case, and the random walk requires an $O(n^3)$-time in average, where n is the size of the graph. Under assumptions reflecting WWW applications, we propose a new exploration paradigm called *forest search* particularly designed for scale-free networks, and theoretically evaluate its space complexity. We also demonstrate its superiority over random walk based search algorithms by conducting simulations.

6. Diego Arroyuelo, Gonzalo Navarro, and Kunihiko Sadakane:
"Reducing the space requirement of LZ-index", Proc. Combinatorial Pattern Matching, LNCS 4009, pp. 307–318, Jul. 2006.
概要: The LZ-index is a *compressed full-text self-index* able to represent a text $T_{1...u}$, over an alphabet of size σ and with k-th order empirical entropy $H_k(T)$,

using $4uH_k(T) + o(u \log \sigma)$ bits for any $k = o(\log_\sigma u)$. It can report all the *occ* occurrences of a pattern $P_{1...m}$ in T in $O(m^3 \log \sigma + (m + occ) \log u)$ worst case time. This is the only existing data structure of size $O(uH_k(T))$ able of spending $O(\log u)$ time per occurrence reported. Its main drawback is the factor 4 in its space complexity, which makes it larger than other state-of-the-art alternatives. In this paper we present two different approaches to reduce the space requirement of LZ-index. In both cases we achieve $(2 + \epsilon)uH_k(T) + o(u \log \sigma)$ bits of space, for any constant $\epsilon > 0$, and we simultaneously improve the search time to $O(m^2 \log m + (m + occ) \log u)$. Both indexes support displaying any subtext of length ℓ in optimal $O(\ell / \log_\sigma u)$ time. In addition, we show how the space can be squeezed to $(1+\epsilon)uH_k(T)+o(u \log \sigma)$ to obtain a structure with $O(m^2)$ average search time for $m \geq 2 \log_\sigma u$.

7. Masashi Shiozaki, Hirotaka Ono, Kunihiko Sadakane, and Masafumi Yamashita:
"A Probabilistic Model of the DNA Conformational Change", Proc. DNA, LNCS 4287, pp. 274–285, Jun. 2006.
概要: Predicting the behavior of DNA molecules in vitro is one of the most fundamental issues on DNA computing, but is also known to be quite difficult. Shiozaki et al. proposed a probabilistic model that can simulate many features of biochemical experiments in terms of the reaction rate, although there are several differences between the biochemical experiments and the computational simulations on the model. In this paper, we extend the model to support base pairs construction among k DNA sequences, which plays an essential role in realizing branch migrations. The simulation results have much more similarities to the biochemical experiments results than ones on the previous model, which implies that the analysis of the model may give some insight about the reaction rate. Through the analysis, we conclude this paper by giving a guideline for designing DNA sequences that can quickly react.

8. Suguru Kawashimo, Hirotaka Ono, Kunihiko Sadakane, and Masafumi Yamashita:
"DNA Sequence Design by Dynamic Neighborhood Searches", Proc. DNA, LNCS 4287, pp. 157–171, Jun. 2006.
概要: We propose a local-search based algorithm to design DNA sequence sets that satisfy several combinatorial constraints about hamming-distance criteria. To deal with the constraints in the local search, we adopt elaborate (and dynamic) neighborhood search frameworks called the Variable Neighborhood Search (VNS) and the Variable Depth Search (VDS). Although our algorithm can deal with many types of hamming distance-based constraints and is easy to extend (e.g., also applicable for other constraints), in computational experiments, we succeeded in generating better sequence sets than the ones generated by exiting methods of more specified constraints.

9. Yuichi Kurumida, Tsukasa Ogata, Hirotaka Ono, Kunihiko Sadakane, and Masafumi Yamashita:
"A generic search strategy for large-scale real-world networks", Proc. of the 1st international conference on Scalable information systems (INFOSCALE), ACM International Conference Proceeding Series; Vol. 152, May 2006.
概要: We consider the following situation for a given large-scale network: Starting from an initial node we move to its neighbor node and repeat that until reaching a target node. How fast can we do this without any global topological information? This problem is considered "searching networks", and

several approaches have been proposed. In this paper, we present a general framework of search strategies, under which all of these existing approaches can be formalized. Our framework characterizes random search strategies by the following three parameters: memory for previously-visited nodes, look-ahead property and transition probability. Through computational simulations for large-scale networks with small-worldness and scale-freeness, we investigate the relationship between the effect of parameters of the strategies and the coefficients of networks such as the clustering coefficient. The comparison result provides a guideline to obtain good parameters of the strategies according to the diameter and the clustering coefficients of networks.

研究会等

1. 原田 雄太, 小野 廣隆, 定兼 邦彦, 山下 雅史: “負荷分散セミマッチングにおける最適性について”, コンピュテーション研究会, vol. 106, no. 29, pp. 1–8, 2006 年 4 月.
   概要: 本研究で扱う問題は 2 部グラフにおけるセミマッチング問題である．セミマッチングとは，2 部グラフ $G = (U \cup V, E)$ において各 U の頂点が 1 つの V の頂点と対を成す枝の集合である．これまで，各 V の頂点の次数が最も均等化されるようなセミマッチングを求める問題 (負荷分散セミマッチング問題) の研究が行われている．それに対し，本研究では重み付き 2 部グラフにおける最小重み負荷分散セミマッチング問題を定式化し，アルゴリズムを提案する．

2. 前村 一哉, 小野 廣隆, 定兼 邦彦, 山下 雅史: “隠れマルコフモデルを用いた DNA 配列設計”, コンピュテーション研究会, vol. 106, no. 63, pp. 39–46, 2006 年 5 月.
   概要: DNA コンピューティングとは，DNA 同士の反応過程を計算として見なした新しい計算パラダイムである．DNA コンピューティングでは，計算に使用する DNA 分子の塩基配列設計することが重要な研究テーマのひとつとなっている．DNA 分子が意図したように反応するには，様々な制約をできるだけ満たす配列を準備する必要がある．このため従来様々な塩基配列の設計手法が研究されてきたが，本研究では隠れマルコフモデルを用いた配列設計を提案する．隠れマルコフモデルはマルコフ過程を利用した確率モデルである．本論文では，試験的な配列設計として行った，DNA のもつ最小自由エネルギーが小さい配列の設計の実験と結果について述べる．

3. 川下 優, 小野 廣隆, 定兼 邦彦, 山下 雅史: “動的近傍操作を用いた DNA 塩基配列設計”, コンピュテーション研究会, vol. 106, no. 63, pp. 47–54, 2006 年 5 月.
   概要: 近年，DNA 塩基配列集合を利用したナノコンピューティング・ナノテクノロジーが注目されている．これらの技術に用いられる塩基配列集合は，利用目的に応じた制約を満たす必要がある．いくつかの制約は組合せ的であるので，本論文では塩基配列集合問題を組合せ最適化問題と捉える．さらに，他の制約より組合せ的なオーバーラップ指標に着目し，局所探索法に基づくアルゴリズムを提案する．このアルゴリズムでは組合せ的制約を局所探索法で充足させるために，可変近傍探索法・可変深度探索近傍法と呼ばれる動的近傍操作を採用する．計算機実験において，提案手法は同様の制約を満たす他の手法と同等以上の配列集合の設計に成功した．

4. 定兼 邦彦:
   “単純な Rank/Select 辞書”, コンピュテーション研究会, vol. 106, no. 128, pp. 43–48, 2006 年 6 月.
   概要: Rank/Select 辞書とは，順序集合 $S \in \{0, 1, ..., m-1\}$ において $rank(x, S) = |\{y \in S | y \leq x\}|$ と $select(i, S)$ (S の中で i 番目に小さい要素) を返すデータ構造である．これは文字列，木，グラフなどの圧縮データ構造の基本構成要素であり，多くのデータ構造が提案されている．しかしそれらは漸近的な性能のみを考えており，実データに対する性能は良くない．本研究では単純な Rank/Select

辞書を提案する．特徴としては，集合 S の要素数が小さい場合にデータ構造のサイズを縮小できることと，データ構造が単純であるために実装が容易で，実データに対する性能 (データ構造のサイズと問い合わせ時間) が良い．実験により，既存の実装よりも速度，サイズともに優れていることを示す．

5. Jesper Jansson, 定兼 邦彦, Wing-Kin Sung: “順序木の新しい表現法”, コンピュテーション研究会, vol. 106, no. 258, pp. 31–37, 2006 年 9 月.
概要: 順序木を表現する簡潔データ構造として有名なものは 2 つ存在する．BP (balanced parenthesis) [Munro, Raman 2001] と DFUDS (depth first unary degree sequence) [Benoit et al. 2005] である．これらは n ノードの木を $2n + o(n)$ ビットで表現するものであり，この大きさは情報理論的下界と一致する．これらのデータ構造の上では多くの基本的演算 (親, 最初の子, 次の弟) への移動，子孫の数など) を word RAM モデル上で定数時間で行える．しかし知られている基本的演算の全てを定数時間で行えるデータ構造は知られていない．BP では i 番目の子を求めることができず，DFUDS では lca (lowest common ancestor) を求めることができない．本論文は，BP または DFUDS で実行できる基本的操作の全てを定数時間で実行可能な新しい順序木の表現法を提案する．このデータ構造のサイズは $2n$ ビットより小さく，木のノードの次数の分布から定義されるエントロピーまで圧縮できる．その結果，全ての内部ノードがちょうど 2 つの子を持つような木の場合，サイズは $n + o(n)$ まで圧縮される．

学会大会等

1. 前村 一哉, 小野 廣隆, 定兼 邦彦, 山下 雅史: “ボトムアップ手法を用いた系統樹構築の近似アルゴリズム”, 冬の LA シンポジウム, 2007 年 1 月.

2. 後藤 隆元, 小野 廣隆, 定兼 邦彦, 山下 雅史: “部分文字列の高速復元に適した圧縮データ構造に関する研究”, 冬の LA シンポジウム, 2007 年 1 月.

3. 川下 優, 小野 廣隆, 定兼 邦彦, 山下 雅史: “局主探索法に基づく DNA 配列設計手法”, 冬の LA シンポジウム, 2007 年 1 月.

4. 佐薙 光樹, 小野 廣隆, 定兼 邦彦, 山下 雅史: “センサーネットワークにおける省電力高信頼なデータ伝送”, 冬の LA シンポジウム, 2007 年 1 月.

5. 坂田 敦, 小野 廣隆, 定兼 邦彦, 山下 雅史: “k-set Agreement を解く故障検知器”, 冬の LA シンポジウム, 2007 年 1 月.

6. 原田 雄太, 小野 廣隆, 定兼 邦彦, 山下 雅史: “負荷分散枝被覆問題に対する最適性とアルゴリズム”, 冬の LA シンポジウム, 2007 年 1 月.

7. 原田 雄太, 小野 廣隆, 定兼 邦彦, 山下 雅史: “負荷分散枝被覆問題に対する最適性とアルゴリズム”, 冬の LA シンポジウム, 2007 年 1 月.

8. 深見 浩和, 小野 廣隆, 定兼 邦彦, 山下 雅史: “境界上を移動可能なロボット 2 台による多角形探索”, 冬の LA シンポジウム, 2007 年 1 月.

9. 原田 雄太, 小野 廣隆, 定兼 邦彦, 山下 雅史: “負荷分散枝被覆問題とその解法”, 夏の LA シンポジウム, 2006 年 8 月.

10. 坂田 敦, 小野 廣隆, 定兼 邦彦, 山下 雅史: “k-set Agreement を解く故障検知器”, 夏の LA シンポジウム, 2006 年 8 月.

11. 来見田 裕一, 小野 廣隆, 定兼 邦彦, 山下 雅史:
“スケールフリーネットワークにおける次数情報を用いた探索手法”, 夏の LA シンポジウム, 2006 年 8 月.