志望区分:通－1

コンピュータ工学講座　論理回路分野

http://www.lab2.kuis.kyoto-u.ac.jp

研究室構成

教員　　LE GALL François 特定准教授，玉置卓 助教

研究テーマ

理論計算機科学は基本的な計算技術とそれらの限界のより良い理解を探求する．アルゴリズムと計算複雑性理論はこの分野の中核であり，それらが多数の応用を持つことは言うまでもない．我々はアルゴリズムと計算複雑性に関すること全て，特に以下に述べる話題に興味がある．

1. アルゴリズムの設計と解析

幅広い種類のアルゴリズムに取り組んでいる．我々の主要な興味の1つに代数的問題，特に行列の乗法がある．行列乗法は当然ながら数学と計算機科学における最も基本的な処理の1つである．いくつかの大きな進歩がこの分野で過去5年間に起こり，特に行列乗法に対するより高速なアルゴリズムが発見されている（20年以上最良であった行列乗法の初めての改良である）．我々はこのような最近の発展に積極的な貢献をしている．他の話題として，我々はグラフ理論的な問題や分散計算における問題に対するアルゴリズム，ストリーミングアルゴリズムや性質検査にも注目している．学生は上に挙げたごく一部の例に限定されず，各自で問題を選択することが推奨される．

2. 計算複雑性理論

計算複雑性理論には2つの主要な目標，つまり，計算問題を困難性（解くために必要な資源量）に応じて分類すること，及び，計算模型の能力を解析すること，がある．我々は多くの模型（有限オートマトン，非決定性Turing機械やさらに強力な計算模型など）や様々な資源（時間複雑性，領域複雑性，通信複雑性など）に取り組んで来た．計算複雑性理論の分野は，有名なP対NP問題のような手強い未解決問題で良く知られているが，適切な道具を用いて研究することで進展が見込まれる興味深い問題も多数存在する．

3. 量子計算

量子計算は量子力学の法則に基づく新しい計算パラダイムである．量子計算の有名な成功例として，完璧に安全な暗号系（量子鍵配送）の開発，及び，素因数分解や他の数論的計算問題に対する，現在最良のアルゴリズムより高速な量子アルゴリズムの設計がある．我々の主な研究分野は，量子アルゴリズム（量子計算機に対するアルゴリズムの研究）と量子計算複雑性理論（量子計算機が伝統的な計算機より強力である理由の探求）である．量子計算の研究は，十分な意欲さえあれば，量子力学や量子計算に馴染みがない学生でも取り組むことができる．

Application Code: CCE- 1

Logic Circuits, Algorithms, and Complexity Theory Group, Computer Engineering Division

http://www.lab2.kuis.kyoto-u.ac.jp

Laboratory Members

Teaching Staff	Associate Professor LE GALL François, Assistant Professor TAMAKI Suguru

Research Topics

Theoretical computer science seeks better understanding of fundamental computing techniques and their limitations. Algorithms and complexity theory are core areas in this field, and needless to say have a multitude of applications. We are interested in everything related to algorithms and complexity, and especially in the topics described below.

1. Algorithm design and analysis

We are currently working on a wide variety of algorithms. One of our main interests is algorithms for algebraic problems, in particular algorithms for multiplying matrices, a very fundamental task in mathematics and computer science. Several breakthroughs happened in this field during the past five years, including the discovery of faster algorithms for matrix multiplication (the first improvements for matrix multiplication in more than twenty years!) -- we are working actively on such recent developments. Other subjects we are focusing on are algorithms for graph-theoretic problems, distributed algorithms (i.e., algorithms for problems in distributed computation), as well as streaming algorithms or property testers. Students are not limited to this short list of examples. On the contrary, they are encouraged to choose themselves their problem.

2. Complexity theory

Complexity theory has two main goals: classifying computational problems according to their difficulty by investigating the amount of resource needed to solve them, and analyzing the computational power of models of computation. We have been working on complexity theory for many models of computations, from finite automata to non-deterministic Turing machines (and often even much stronger models of computation), and many kinds of resource (time complexity, space complexity, communication complexity…). While the field of complexity theory is well known for its intimidating open problems, like the celebrated P vs. NP problem, there do exist many accessible interesting questions just waiting to be tackled with the appropriate tools.

3. Quantum computation

Quantum computation is a new computation paradigm based on the laws of quantum mechanics. Among the most celebrated achievements of quantum computations are the development of perfectly secure cryptosystems (quantum key distribution) and the design of quantum algorithms for integer factoring and other number-theoretic computational problems faster than the best current algorithms. Our main areas of research are quantum algorithms, which studies algorithms for quantum computers, and quantum complexity theory, which seeks to understand how quantum computers are more powerful than traditional computers. Research on quantum computation is accessible to students who do not have any background in quantum mechanics or any prior exposure to quantum computation but do have enough motivation.