科学研究費補助金 新学術領域研究

多面的アプローチの統合による計算限界の解明

平成24年度 成果報告書

平成25年6月

領域代表者　渡辺 治
東京工業大学 大学院 情報理工学研究科　教授

目 次

1. 研究活動 **1**

1.1. チュートリアル・学校 3

電子情報通信学会コンピュテーション研究会 特別企画計算限界解明入門講義 (招待チュートリアル講演) 3

計算量理論の秋学校 5

暗号理論秋学校 7

1.2. ELC Tokyo Complexity Workshop 8

ELC Tokyo Complexity Workshop 8

Satellite Mini-Workshop, Shinagawa 14

Mini-Workshop on Geometric Complexity Theory (GCT) 15

Satellite Mini-Workshop, Kyoto 16

1.3. ELC Mini-Workshop 17

ELC Mini-Workshop (B01) 17

ELC Mini-Workshop (B02, B03) 19

ELC Mini-Workshop (C02) 21

ELC Mini-Workshop (暗号理論) 22

ELC Mini-Workshop (A01) 24

ELC Mini-Workshop (C03) 25

ELC Mini-Workshop (C01) 27

1.4. ELC Seminar 29

ELC Seminar (Lance Fortnow, Benjamin Rossman, Kazuhisa Seto) 29

ELC Seminar (Laszlo Egri, Yuichi Yoshida, Kazuhisa Seto) 30

ERATO 河原林巨大グラフプロジェクト & ELC 合同講演会 (Arnab Bhattacharyya & Mikkel Thorup) 31

ELC セミナー (萩原 学) 32

ELC セミナー (河内亮周) 33

ELC セミナー (A01) 34

2. 研究課題別活動報告 **35**

A01: 数理論理学からの計算限界解析

牧野 和久，河村 彰星，垣村 尚徳，小林 佑輔，Suppakitpaisarn Vorapong 37

A02: 情報理論・符号理論からの計算限界研究

河原林 健一，伊藤 大雄，玉置 卓，吉田 悠一，脊戸 和寿，Skip Jordan 40

A03：記憶領域制限シナリオにおける計算限界の解明

浅野 哲夫，垂井 淳，上原 隆平，小野 廣隆，清見 礼，Guenter Rote，Wolfgang Mulzer，Ovidiu Daescu，小長谷 松雄 44

B01: 最適化技法との融合による計算限界解析法の深化
加藤 直樹，岩田 覚，岡本 吉央，来嶋 秀治，神山 直之 48
B02: 大規模数理計画による計算限界解析法の展開
David Avis，天野 一幸，上野 賢哉，福田 公明，Antoine Deza，Oliver Friedmann，
Samuel Fiorini，Hans Raj Tiwary 53
B03: 計算限界解析法から革新的データ構造化技術への展開
徳山 豪，宇野 毅明，渋谷 哲朗，堀山 貴史，定兼 邦彦 56
C01: 統計力学からの計算限界解明へのアプローチ
渡辺 治，伊東 利哉，小柴 健史，山本 真基，樺島 祥介，福島 孝治 60
C02: 量子力学からの計算限界解明へのアプローチ
山下 茂，河内 亮周，中西 正樹，西村 治道，Le Gall Francois，小林 弘忠，谷 誠一郎，
根本 香絵，村尾 美緒 62
C03: 学習理論からの計算限界解明へのアプローチ
瀧本 英二，正代 隆義，畑埜 晃平，篠原 歩，内沢 啓，吉仲 亮，津田 宏治，Cuturi Marco 65

1. 研究活動

電子情報通信学会コンピュテーション研究会
特別企画計算限界解明入門講義
(招待チュートリアル講演)

1 概要

日本の理論計算機科学コミュニティの中核をなす組織の一つである電子情報通信学会コンピュテーション研究会の特別企画として，本プロジェクトより周辺分野の研究者・学生へのアウトリーチ及びプロジェクトの広報，及び人材交流の手掛かりの一環として計算の複雑さ理論の基本と最先端トピックについての講演を行った．

第一回は領域代表の渡辺治（東工大）による平均時計算複雑さの理論の基本から最先端まで，第二回は事務局メンバーの河内亮周（東工大）によるアルゴリズムの視点から見た計算限界証明手法についての解説が行われた．

講演時間内外で活発な質問・議論が行われ，周辺分野の研究者の計算限界解明というトピックおよび本プロジェクトへの興味の高さを伺い知ることができ，またそのような議論を通じて，多くの研究者と本プロジェクトとの研究交流の機会を設けることができた．

2 講演情報

2.1 第一回講演

タイトル:
計算複雑さへの招待 (1): 基本＋平均時計算複雑さ
Introduction to Computational Complexity Theory (1):
Basics and Average-Case Computational Complexity
講師: 渡辺 治 (東京工業大学)
場所: 九州大学
講演概要：
計算複雑さの理論の基本的な考え方とその最前線を紹介するシリーズ講演の第１回目として，計算複雑さの基本的な考え方を中心に説明する．また，最前線の研究の話として，NP 問題に対する平均時の計算複雑さの解析について述べる．

As the 1st lecture of the lecture series on computational complexity, I would like to explain key basic concepts in computational complexity theory. I also mention in this talk some interesting topics from the average-case complexity study of NP problems as an example of current advanced research.

2.2 第二回講演

タイトル:
計算複雑さへの招待 (2)：アルゴリズムから攻める計算複雑さの下界証明
Introduction to Computational Complexity Theory (2):
Algorithmic Approaches to Lower Bounds of Computational Complexity
講師: 河内 亮周 (東京工業大学)
場所: 岐阜大学
講演概要：
計算複雑さの理論の基本的な考え方とその最前線を紹介するシリーズ講演の第二回目として，計算複雑さの下界証明のための代表的な手法の一つであるアルゴリズム設計による証明手法を紹介する．

特に Kannan の 1984 年の結果である多項式時間階層における回路計算量の多項式下界（任意の定数 $c > 0$ に対して $\mathrm{PH} \not\subset \mathrm{SIZE}[n^c]$）の証明をはじめとして，そのアプローチでの発展（例えば，Koebler-Watanabe の 1994 年の結果など）についても解説する．また最近のブレイクスルーであっ

た 2011 年の Williams の結果（非決定性指数時間クラスにおける定数段剰余素子付回路の回路計算量の超多項式下界 NEXP $\not\subset$ ACC^0）もアルゴリズム的なアプローチの一つとして紹介する．

「アルゴリズムの限界を証明するためにアルゴリズムを設計する」というアプローチは 1980 年代から現代まで代表的な手法として活用されているが，このような手法がなぜ有効であるのかについて議論したい．

As the second lecture of the lecture series on computational complexity, I briefly survey algorithmic approaches to proving lower bounds of computational complexity.

Particularly, I review Kannan's result in 1984 of polynomial lower bounds of circuit complexity in the polynomial-time hierarchy (i.e., PH $\not\subset$ SIZE$[n^c]$ for any constant $c > 0$), and its improvements (e.g., Koebler and Watanabe's result in 1994). Also, I briefly mention the recent breakthrough by Williams in 2011 that shows a superpolynomial lower bounds of circuit complexity in the nondeterministic exponential-time class against constant-depth circuits with modulo gates (i.e., NEXP $\not\subset$ ACC^0) as one of the algorithmic approaches.

I would like to discuss why such approaches that "designing good algorithms implies proving limits of algorithms," which have been utilized as a typical approach to proving lower bounds since 80's, is quite effective.

計算量理論の秋学校

世話役: 玉置 卓 (京都大学)

1 概要

新学術領域研究「多面的アプローチの統合による 計算限界の解明 (ELC)」の活動の一環として，「計算量理論の秋学校」を開催した．概要は以下の通りである．

- 日時: 2012 年 9 月 24 日 (月)〜9 月 26 日 (水)
- 場所: かんぽの宿 熱海 (本館)，静岡県熱海市水口町 2-12-3
- 参加人数: 47 名 (一般 19，学生 26)
- 内容: 計算量理論の基礎から先端まで
- 講師: 渡辺 治 (領域代表者，東京工業大学)，天野 一幸 (B02 班，群馬大学)，垂井 淳（A03 班，電気通信大学）

図 1.1: 集合写真 (秋学校終了直後)

2 目的

本秋学校の目的は，ELC 構成員およびその周辺の研究者や学生に，計算量理論の中心的な話題を理解してもらうことである．ELC では，計算量理論に革新的な進展をもたらすために，計算量理論とは限らない様々な分野の研究者と連携して研究を推進する．そこで，計算量理論の基本的な知識を非専門家にも共有してもらうことが重要になる．

本秋学校では，理論計算機科学・数学・物理分野の研究者や学生を対象として，計算クラスや回路計算量など計算量理論の基礎的な知識について講義を行う．また，計算量理論の高度な話題についても概要を解説する．

3 詳細

講義のスケジュールと内容は以下の通りである．

- 9 月 24 日 14:00〜17:30 渡辺 治 「計算量クラス入門 〜 戸田の定理まで」
  チューリング機械に基づく計算量理論の入門として，以下の話題についての講義がなされた．(1) 計算量クラス，(2) 変な quantifiers，(3) 戸田の定理．
- 9 月 25 日 09:00〜12:30 天野 一幸 「回路計算量の基礎」
  論理回路に基づく計算量理論の入門として，以下の話題についての講義がなされた．(1) 回路計算量，(2) 限定された回路の下界，(3) 下界証明が難しい理由．
- 9 月 25 日 14:00〜17:30 垂井 淳 「高度な話題」
  計算量理論の先端的な話題として，以下のトピックについての解説がなされた．決定木計算量，通信計算量，論理関数の解析，証明計算量，可算の定数段数回路が無限偶奇関数を計算できないこと，困難性増幅，疑似乱数生成器，対話証明系，Karp-Lipton の定理，剰余素子付定数段数回路が非決定性指数時間を計算できないこと．

- 9 月 26 日 09:00〜12:00 「自由討論」
  徳山 豪 (B03 班，東北大学) から「幾何計算量理論」について，内沢 啓 (C03 班，東北大学) から「パーマネント計算の#P 完全性」について話題提供があり，それらに関して参加者で討論を行った．

4 総括

開催決定から開催日までの時間があまりなかったため，準備の都合上参加募集は広く行わず，ELC 構成員の周辺のみに留めた．それにもかかわらず多数の参加があったことから，専門家でない研究者や学生の計算量理論への関心の強さがうかがわれた．より広い範囲で参加募集を行えば，さらに多数の参加者が見込めそうである．同様の学校を次回開催する際には，準備と周知の時間を十分に取り，様々な分野から参加者を集めて ELC との交流を促進したい．

内容については，計算量理論の基礎から先端までを幅広く網羅しており，非専門家・専門家のどちらもが興味が持てる内容であったと思われる．非専門家にとっては難解な先端の話題もあったようであるが，雰囲気だけでも感じ取ってもらえていれば幸いである．

なお，本秋学校の講義はビデオ撮影を行っている．それらのビデオはだれでも視聴できるようにウェブ上で公開する．詳細は ELC のウェブページに掲載される．

最後に，講師を快く引き受けて下さった渡辺先生，天野先生，垂井先生，開催にあたってお世話になった ELC 関係各位，ご参加下さった皆様に感謝いたします．

図 1.2: 講義風景 (24 日午後)

図 1.3: 講義風景 (25 日午前)

図 1.4: 講義風景 (25 日午後)

暗号理論秋学校

世話役:　河内 亮周 (東京工業大学)

1　目的と概要

暗号分野における学生および若手研究者間の交流と，近年の暗号理論研究において重要な位置づけである各分野の若手研究者・学生の学習機会の提供を目的として，暗号理論秋学校を企画，実施した.

秋学校の実施にあたり，講師に草川恵太（NTT）, 西巻陵（NTT）, 安永憲司（金沢大学）の 3 氏を迎えた．草川氏には共通鍵による認証およびデジタル署名の構成について，西巻氏には ID ベース暗号の構成と応用について，初期から最先端までの研究成果を包括的に，安永氏にはゲーム理論と暗号理論の関係性をご講義いただいた.

2　実施内容

具体的な実施内容は以下の通りである.

日時　2012 年 9 月 24 日（月）13:00
～ 27 日（木）12:00

開催場所　河口湖セントビレッヂ

講師　草川恵太（NTT）, 西巻陵（NTT），
安永憲司（金沢大学）

参加者　31 名（うち学生 24 名）

講義概要

1 限 8:45-10:15
2 限 10:30-12:00
3 限 13:00-14:30
4 限 14:45-16:15
5 限 16:30-18:00

- 9 月 24 日（月）
  - 3 限 : IBE 1．IBE 概論，Boneh-Boyen（西巻）
  - 4 限 : IBE 2．Waters'05，Naor 変換（西巻）
  - 5 限 : ゲーム理論と暗号理論 1.（安永）
- 9 月 25 日（火）
  - 1 限:IBE 3．Gentry，CHK 変換（西巻）
  - 2 限 : IBE 4．Fuzzy IBE（FE 概論）（西巻）
  - 3 限 : MAC 1.（草川）
  - 4 限 : MAC 2.（草川）
  - 5 限 : ゲーム理論と暗号理論 2.（安永）
- 9 月 26 日（水）
  - 1 限 : 認証 1.（草川）
  - 2 限 : 認証 2.（草川）
  - 3 限 : IBE 5．Lewko-Waters（西巻）
  - 4 限 : IBE 6．DPVS，Lewko（西巻）
  - 5 限 : ゲーム理論と暗号理論 3.（安永）
- 9 月 27 日（木）
  - 1 限 : 署名 1.（草川）
  - 2 限 : 署名 2.（草川）

3　総括

今回ご講義いただいたそれぞれの分野は, 今日の暗号理論において重要な研究分野でありながら, 学習用の文献や講義等の不足により, 学生個人による主体的な学習が困難なのが現状である．よって，各分野のエキスパートに包括的な講義をしていただいたことは，参加者各人にとって有用な学習体験となった.

また，暗号理論の研究に携わる学生，若手研究者と交流をする貴重な機会であり，講義時間内外における討論等を通して，親睦を深めることができた.

ELC Tokyo Complexity Workshop

世話役:　渡辺 治 (東京工業大学), 垂井 淳 (電気通信大学)

1　会議概要

日時:　2013 年 3 月 14 日から 3 月 17 日
場所:　品川プリンスホテルメインタワー 8 階
　　ターコイズ
参加人数:　154 名

プログラム

3 月 14 日

1:20-1:30 開催の言葉

1:30-2:20 Umesh V. Vazirani:
Quantum Hamiltonian Complexity: through the computational lens

2:35-3:25 Rahul Jain:
Direct product theorems in communication complexity

3:40-4:30 Pavel Pudlak:
Polynomial Hierarchy and Bounded Arithmetic Hierarchy

4:45-5:35 Ryan O'Donnell:
Approximability and Proof Complexity

3 月 15 日

9:00-9:50 Noam Nisan:
Selling Two Objects (in Three Models)

10:15-11:05 Ketan Mulmuley:
The GCT Chasm

11:30-12:20 Joshua A. Grochow:
Geometric Complexity Theory Unifies and Generalizes Many Known Lower Bounds

2:00-2:50 Shachar Lovett:
The probabilistic method — new frontiers

3:15-4:05 Zeev Dvir:
Locally Decodable Codes: recent progress and open problems

4:30-5:20 Luca Trevisan:
Spectral Graph Theory

3 月 16 日

9:00-9:50 Raghu Meka:
Pseudorandomness: old problems, retrofit methods and current challenges

10:15-11:05 David Zuckerman:
Pseudorandomness from Shrinkage

11:30-12:20 Irit Dinur:
Direct products and PCPs

2:00-2:50 Rocco Servedio:
A Complexity-Theoretic View on Unsupervised Learning

4:30-5:20 Ran Raz:
Interactive Channel Capacity

3 月 17 日

9:00-9:50 Valentine Kabanets:
Yin and Yang of computing: From circuit lower bounds to compression and SAT algorithms, and back

10:05-10:55 Eric Allender:
Strengthening the Link between Complexity Classes and Kolmogorov Complexity

11:10-12:00 Yuichi Yoshida:
Robust approximation of CSPs: Universal algebra meets optimization

2　会議の目的

本領域課題に関わる世界のトップ研究者を計算量理論研究者を中心としつつ幅広い分野から集め，１９の招待講演および個別の研究ディスカッションからなる 4 日間にわたる集会を開いた。本領域課題のフロンティアと多様なアプローチの可能性に関する集中的検討により本領域内の研究を推進する起爆剤とするとともに，本領域課題に関係する世界の研究全体を推進する機会とすることを目的とした。また，本領域課題というプロジェクトがスタートしたことを世界的に広く知らしめて，今後国内外の研究者の幅広い交流促進をはかった。この研究集会の成果については，海外からの参参加者からも高い評価を受け，以上の目的は達成できたと思われる。

3 講演の内容

各講演の概要は以下の通りであった.

Umesh V. Vazirani

Much as probabilistic thinking did starting in the early 80s, quantum computing is expanding the core questions of complexity theory in fundamental new directions. For example, here is a list of three basic questions about quantum mechanics that are at their heart questions about computational complexity:

1. Do 'typical' quantum states that occur in Nature have succinct (polynomial) description?
2. Can quantum systems at room temperature exhibit exponential complexity?
3. Is the scientific method sufficiently powerful to comprehend general quantum systems?

Each of these issues is best studied through the computational lens as a question about computation. The resulting questions lie at the core of computational complexity theory. The first asks about the structure of solutions to the quantum analog of SAT. The second asks whether there is a quantum analog of the PCP theorem. And the third can be formulated as a question about interactive proof systems with quantum polynomial time provers. I will briefly outline these connections and the state of the art on these questions.

Rahul Jain

Given a model of computation, suppose solving one instance of a given problem f with probability of success p_1 requires c units of some resource. A natural question that may be asked is: how much resource is needed to solve f^k, k instances of the same problem, simultaneously. A naive way is by running the optimal protocol for f, k times in parallel, which requires ck units of resource, however the probability of overall success is p^k (exponentially small in k). A strong direct product conjecture for f states that this is essentially optimal, that is if only $o(kc)$ units of resource are provided for any protocol solving f^k, then the probability of overall success is at most $p^{\Omega(k)}$.

Proving or disproving strong direct product conjectures in various models of computation has been a central task in theoretical computer science, notable examples of such results being Yao's XOR lemma and Raz's theorem for two-prover games.

In this talk we investigate this question in the model of (two-party, public-coin) communication complexity. We do not know of any function (or more generally a relation) for which this conjecture is false in this model. Settling this conjecture for all functions and relations is a major open question. There has been some good progress towards this goal in some of the recent works. We present a survey of some of these results.

Pavel Pudlak

Using the relation of Bounded Arithmetic Hierarchy to Polynomial Hierarchy as a paradigm, I will explain some basic concepts, results and conjectures of proof complexity.

Ryan O'Donnell

In this talk I will give a survey of:

- The Positivstellensatz / Sum-of-Squares proof system;
- Its connection to the approximability of optimization problems;
- Recent works showing its power in this context for Unique-Games, Sparsest-Cut, Vertex-Cover, and Max-Cut.

Noam Nisan

As more economic activity is done by computing systems or *for* computing systems, CS-ey points of view on economic questions become needed. This talk will demonstrate this using a very simple type of economic problem: A single seller wants to sell two items to one or two possible buyers. One would think that we would know how to do this optimally for most natural goals, and in most natural scenarios and models. Yet, this talk will present three basic scenarios for which while economic theory knows essentially everything about selling a single item, it knows very little when it comes to selling two. We will not be able to provide the "answers" in any of these cases either, but will be able to shed some light on the difficulties involved and obtain some interesting approximation results.

The talk is based on joint works with Shahar Dobzinski, with Sergiu Hart, and with Avinatan Hassidim, Haim Kaplan and Yishay Mansour.

Ketan Mulmuley

It is shown that derandomization of Noether's Normalization Lemma (NNL) for explicit varieties is essentially equivalent to black-box derandomization of Polynomial Identity Testing (PIT). This and related results reveal that the fundamental problems in Geometry (classification of algebraic varieties) and Complexity Theory (derandomization and lower bounds) share a common root difficulty, namely the problem of overcoming the formidable EXPSPACE vs. P gap in the complexity of NNL for explicit varieties. We call this gap the GCT chasm.

Joshua A. Grochow

Geometric Complexity Theory (GCT) is an approach towards P versus NP and other lower bounds using algebraic geometry and representation theory. In this talk, we discuss how many known lower bounds can be viewed as following the part of the GCT approach outlined in [GCT I, II, SIAM J. Comput.], such as permanent versus determinant [Mignon-Ressayre, Landsberg-Manivel-Ressayre], the Razborov-Smolensky lower bound, the Nisan-Wigderson partial derivatives technique, and others. In particular, we expose the representation-theoretic content of these proofs. No knowledge of algebraic geometry or representation theory is assumed — in fact, we motivate the use of representation theory via these previous complexity-theoretic proofs.

図 1.1: 講演を行う Ketan Mulmuley 氏

Shachar Lovett

The probabilistic method is a widely used technique for establishing existence of mathematical objects with certain prescribed properties. It has numerous applications in computer science, combi- natorics, number theory, geometry and more. There are certain problems however on which it fails miserably. I will discuss several techniques that allow to extend the standard probabilistic method to some new frontiers; and many scenarios where we still don't know how to do so.

Zeev Dvir

Locally Decodable Codes (LDCs) are error correcting codes that allow for super efficient decod- ing of a single message symbol using only a small number of queries to a corrupted codeword. These codes and their variants have many theoretical applications and are also starting to appear in practical scenarios. Our understanding of these codes is quite limited and this talk will attempt to survey the state of the art both in term of constructions and lower bounds.

Luca Trevisan

Spectral graph theory is the study of the combinatorial graph properties that can be derived by considering the eigenvalues and eigenvectors of the adjacency matrix of the graph. Such study leads to fast (both in theory and practice) approximation algorithms for graph partitioning problems, and to sufficient conditions to prove that certain graphs are expanders and that certain random walks converge quickly. We survey recent progress in this area, and its applications to approximation algorithms for small-set expansion, sparsest cut, and clustering problems.

Raghu Meka

In this talk I will survey recent results related to two classical questions in complexity theory: derandomizing constant depth circuits and small space algorithms. Along the way, I will highlight some new techniques and retrofit adaptations of classical methods focusing on the following results:

1) Deterministic approximate counting for DNFs.

2) PRGs for "garbled" read-once branching prorgams.

3) PRGs for combinatorial rectangles.

I will also try and emphasize a few open problems and challenges (among many) that seem to test the limits of our knowledge and tools in derandomization.

David Zuckerman

One powerful theme in complexity theory and pseudorandomness in the past few decades has been the use of lower bounds to give pseudorandom generators (PRGs). However, the general results using this hardness vs. randomness paradigm suffer a quantitative loss in parameters, and hence do not give nontrivial implications for models where we don't know superpolynomial lower bounds but do know lower bounds of a fixed polynomial. We show that when such lower bounds are proved using random restrictions, we can construct PRGs that are essentially best possible without in turn improving the lower bounds.

More specifically, say that a circuit family has shrinkage exponent Γ if a random restriction leaving a p fraction of variables unset shrinks the size of any circuit in the family by a factor of $p^{\Gamma+o(1)}$. Our PRG uses a seed of length $s^{1/(\Gamma+1)+o(1)}$ to fool circuits in the family of size s. By using this generic construction, we get PRGs with polynomially small error for the following classes of circuits of size s and with the following seed lengths:

1. For de Morgan formulas, seed length $s^{1/3+o(1)}$;

2. For formulas over an arbitrary basis, seed length $s^{1/2+o(1)}$;

3. For read-once de Morgan formulas, seed length $s^{.234...}$;

4. For branching programs of size s, seed length $s^{1/2+o(1)}$.

The previous best PRGs known for these classes used seeds of length bigger than $n/2$ to

output n bits, and worked only when the size $s = \mathrm{O}(n)$.

Joint work with Russell Impagliazzo and Raghu Meka.

Irit Dinur

Probabilistically checkable proofs (PCPs) are proofs in which the distance between right and wrong is greatly amplified: a verifier needs read only O(1) bits of the proof to make its decision.

A PCP can be constructed by pushing any proof through a gap-amplifying transformation. One of the most basic ways to get gap-amplification is by parallel repetition, aka direct product. This is a very easy-to-define operation, yet its analysis leaves many open questions.

We will introduce PCPs and direct products and then survey existing results and describe some open questions.

Rocco Servedio

In the 1980s Valiant's PAC (Probably Approximately Correct) learning model brought a com- putational complexity perspective to the study of machine learning. The PAC framework deals with supervised learning problems, where data points are labeled by some target function and the goal is to infer a high-accuracy hypothesis that is close to the target function. The PAC learning model and its variants provide a useful setting for studying how the complexity of learning different types of Boolean functions scales with the complexity of the functions being learned.

A large portion of contemporary machine learning deals with *unsupervised* learning problems. In problems of this sort data points are unlabeled, so there is no "target function" to be learned; instead the goal is to infer some structure from a sample of unlabeled data points.

This talk will focus on the problem of learning an unknown *probability distribution* given access to independent samples drawn from it. Analogous to the PAC model for learning Boolean functions, the broad goal here is to understand how the complexity of learning different types of distributions scales with the complexity of the distributions being learned. We survey recent results in this area and identify questions for future work.

Pinyan Lu

The main theme of theoretical computer science is to classify various computational problems in terms of their inherent computational difficulty. In this talk, I will try to demonstrate this general theme by some cases study of my own research on the algorithms and complexity for counting problems.

Ran Raz

We study the interactive channel capacity of an ε-noisy channel. The interactive channel capacity $C(\varepsilon)$ is defined as the minimal ratio between the communication complexity of a problem (over a non-noisy channel), and the communication complexity of the same problem over the binary symmetric channel with noise rate ε, where the communication complexity tends to infinity.

Our main result is the upper bound $C(\varepsilon) \leq 1 - \Omega(\sqrt{H(\varepsilon)})$ (where H is the binary entropy function). This compares with Shannon's non-interactive channel capacity of $1 - H(\varepsilon)$. In particular, for a small enough ε, our result gives the first separation between interactive and non-interactive channel capacity, answering an open problem by Schulman.

We complement this result by the lower bound $C(\varepsilon) \geq 1 - \mathrm{O}(\sqrt{H(\varepsilon)})$, proved for the case where the players take alternating turns.

Valentine Kabanets

In this talk, we relate lower bounds and algorithms. We consider the problem of proving lower bounds for several models of computation (constant-depth Boolean circuits, Boolean formulas, etc.), the problem of compressing the truth tables of Boolean functions that are computable by small circuits, and the problem of deciding the satisfiability of circuits of restricted kind. We survey some known and present some new results showing that these three problems are intrinsically connected: making progress in one leads to progress for the others.

Eric Allender

This talk centers around some audacious conjectures that attempt to forge firm links between computational complexity classes and the study of Kolmogorov complexity.

More specifically, let R denote the set of Kolmogorov-random strings. Two familiar complexity classes are:

- BPP: the class of problems that can be solved with negligible error in polynomial-time, and
- NEXP: the class of problems solvable in nondeterministic exponential time.

Conjecture 1. $\mathsf{NEXP} = \mathsf{NP}^R$.

Conjecture 2. BPP is the class of problems non-adaptively polynomial-time reducible to R.

The first thing to note is that these conjectures are not only audacious; they are obviously false! R is not a decidable set, and thus it is absurd to suggest that the class of problems reducible to it constitutes a complexity class.

The absurdity fades if, for example, we interpret "NP^R" to be "the class of problems that are NP-Turing reducible to R, no matter which universal machine we use in defining Kolmogorov complexity". The lecture will survey the body of work (some of it quite recent) that suggests that, when interpreted properly, the conjectures may actually be true.

In particular, if one considers a time-bounded variant of Kolmogorov randomness, then the class of problems that are non-adaptively reducible in polynomial time to the set of random strings lies between BPP and $\mathsf{PSPACE} \cap \mathsf{P}/\mathrm{Poly}$.

Yuichi Yoshida

Universal algebra has been a standard tool to analyze computational complexity of CSPs, and it is now active to use universal algebra also for analyzing the optimization version of CSPs. As one such an example, we survey recent results on classifying robust approximability of CSPs. Here, an algorithm is said to robustly approximate a CSP if, given a $(1-\varepsilon)$-satisfiable instance, it outputs a $(1-f(\varepsilon))$-satisfying assignment, where $f(0)=0$ and $f(\varepsilon)$ tends to zero as ε goes to zero.

図 1.2: 休憩中の議論

Satellite Mini-Workshop, Shinagawa

世話役: 岡本 吉央 (電気通信大学), 玉置 卓 (京都大学), 垂井 淳 (電気通信大学)

3 月 14 日から 17 日にかけて開催された ELC Tokyo Complexity Workshop のサテライト・イベントとして，ミニワークショップを開催した．

- 開催地：京都大学品川オフィス
- プログラム：
  - 10:30–12:15 David Zuckerman (テキサス大学オースティン校)：Randomness Extraction: A Survey
  - 13:40–15:25 Ran Raz (ワイツマン科学研究所)：Parallel Repetition of Two Prover Games: A Survey
  - 15:45–17:30 Noam Nisan (エルサレム・ヘブライ大学，マイクロソフト研究所)：Algorithmic Mechanism Design: Multi-unit Auctions
- 参加者数：62 名

各講演の概要は以下の通りであった．

David Zuckerman

乱数抽出器とその応用に関する概要の紹介が行われた．特に，種を用いた乱数抽出器と種を用いない乱数抽出器に関する話題に触れ，それらと擬似乱数生成，暗号，乱択アルゴリズム，近似不可能性などに対する応用が議論された．

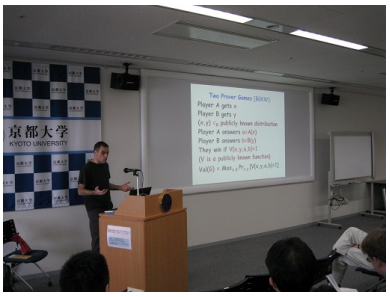


図 1.1: Ran Raz による講演．

Ran Raz

2 証明者ゲームの並列反復定理について知られている結果と関連する予想の紹介が行われた．まず，並列反復定理と強並列反復定理の内容が説明され，その後に，PCP 定理，近似不可能性，量子通信理論 (Bell の不等式)，幾何学 (泡の問題) との関連が議論された．

Noam Nisan

同種複数財オークションにおける勝者決定，価格決定に関して，そのアルゴリズム的側面が紹介された．特に，近似アルゴリズムによる決定に誘因両立性を持たせるという課題に関して知られている事項と未解決問題が議論された．

各講演に対して質疑応答も行われ，活発な議論が交わされた．

図 1.2: 聴衆．

Mini-Workshop on Geometric Complexity Theory (GCT)

世話役: 徳山 豪（東北大学），有木 進（大阪大学），垂井 淳 ，脊戸 和寿（電気通信大学）

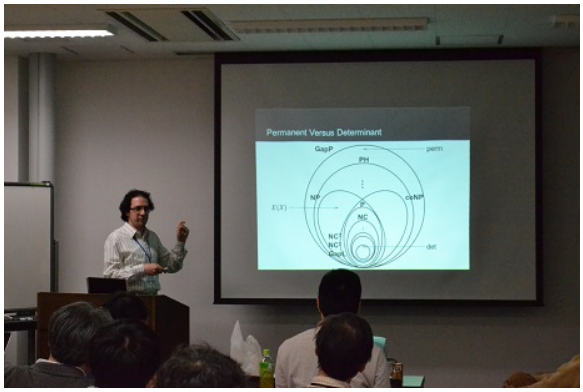
表現論を専門とする数学者と計算量理論の研究者を聴衆として，近年，非常に活発に研究されている幾何的計算量理論について，この分野の創始者である Ketan Mulmuley（シカゴ大）と若手研究者 Joshua A. Grochow（トロント大）にチュートリアル講演を行ってもらった．４時間半におよぶ講演の最初から最後まで聴衆との間で非常に活発な質疑が続いた．参加した数学者グループが取り組むべき複数の具体的問題を特定し，それらに対してまず試みるべきアプローチを具体化するところまで議論を進めることができた．PvsNP 問題をはじめとする未解決問題の解決に向けた幾何的計算量理論によるアプローチの発展を目指し，今後も更なる交流の場を設けることが期待される．

日時　2013 年 3 月 17 日（日）
場所　CELC（計算限界研究センター，田町）
参加者　35 名

講演内容
1.「The GCT Chasm」 Ketan Mulmuley (University of Chicago)

It is shown that derandomization of Noether's Normalization Lemma (NNL) for explicit varieties is essentially equivalent to black-box derandomization of Polynomial Identity Testing (PIT). This and related results reveal that the fundamental problems in Geometry (classification of algebraic varieties) and Complexity Theory (derandomization and lower bounds) share a common root difficulty, namely the problem of overcoming the formidable EXPSPACE vs. P gap in the complexity of NNL for explicit varieties. We call this gap the GCT chasm.

2.「Symmetry-Characterization in Geometric Complexity Theory」 Joshua A. Grochow（The University of Toronto）



Satellite Mini-Workshop, Kyoto

世話役: 谷川 眞一，玉置 卓 (京都大学)，垂井 淳 (電気通信大学)

1　概要

新学術領域研究「多面的アプローチの統合による 計算限界の解明 (ELC)」の活動の一環として，「Satellite Mini-Workshop, Kyoto」を開催した．概要は以下の通りである．

- 日時: 2013 年 3 月 19 日 (火)
- 場所: 京都大学数理解析研究所，京都市左京区北白川追分町
- 参加人数: 20 名 (一般 16，学生 4)
- 内容: ガウス的幾何による和集合限界の打破，局所復号可能符号，幾何学的複雑さの理論
- 講師: Raghu Meka (Institute for Advanced Study and DIMACS), Zeev Dvir (Princeton University), Ketan Mulmuley (University of Chicago)

2　目的

本ワークショップの目的は，理論計算機科学分野の研究者を主体とする ELC と数学分野の研究者の交流を図ることである．特に，3 番目の講演者 Mulmuley が提唱する幾何学的複雑さの理論は，表現論と代数幾何学を駆使して P vs. NP 問題の解決を目指すという壮大なプログラムであり，純粋数学者の関心と協力を得ることでプログラムの進展が早まることが期待できる．そこで，数学の一大拠点である京都大学数理解析研究所を会場とし，数学分野にも参加を呼びかけてワークショップを開催する．

3　詳細

講義のスケジュールと内容は以下の通りである．

- 13:15〜14:15 Raghu Meka, “Beating the Union Bound via Gaussian Geometry.”
- 14:30〜15:30 Zeev Dvir, “Locally Decodable Codes: recent progress and open problems.”
- 15:45〜17:15 Ketan Mulmuley, “The GCT chasm.”

図 1.1: 講義風景 (Ketan Mulmuley)

4　総括

講演の最中に活発な質疑応答がかわされたほか，Mulmuley と有木進 (大阪大学教授) ら表現論の研究者グループ，Meka, Dvir と谷川ら，などの組合せで個別議論を並行して行うなど，目的としていた交流を十分に達成できた．今後も同様の目的の企画が望まれる．

最後に，開催にあたり多大なご協力をいただいた京都大学数理解析研究所の谷川 眞一氏に感謝いたします．

(文責: 玉置)

ELC Mini-Workshop (B01)

世話役: 加藤直樹（京都大学）

1　会議概要

日時: 2012 年 9 月 5 日 (水) 〜 9 月 7 日 (金)
場所: 京都大学 桂キャンパス
参加人数: 11 名

プログラム
9 月 5 日
13:00–15:00 上野 賢哉（京都大）
「線形空間探索による計算限界解析」
15:30–17:30 内沢 啓（東北大）
「線形決定木の計算限界解明」
9 月 6 日
10:00–12:00 岡本 吉央（電気通信大）
「最適化×計算限界＝ (算法設計＋問題構造) × (計算上界＋計算下界)」
13:00–17:00 自由討論
9 月 7 日
9:30–17:00 自由討論

2　会議の目的

B01 班のテーマである「最適化 × 計算限界 =(算法設計 + 問題構造)×(計算上界 + 計算下界)」の遂行に向け，計算量理論分野における最適化問題，最適化分野における計算量理論の諸問題について勉強会を行った．特に B02 班を始めとする他班との連携に向けた情報交換が主要な目的である．

勉強会の前半は，班テーマの関連話題について，専門家をお招きしてご講演いただいた．上野先生には，論理回路サイズの下界証明に対する LP bound と呼ばれる証明技法について解説いただいた．内澤先生には，線形決定木サイズの下界に対する通信複雑度を用いた証明法について解説いただいた．岡本先生には，B01 班の研究の方向性について説明いただいた．

勉強会の後半は，前半の講演を踏まえ，現状の課題の洗い出しおよび今後の研究方針について議論した．また，Non-Negative Rank について,「これのマトロイドに対応するような抽象的な概念は作れないか？」といった問題について考えた．

3　議論の内容

3.1　論理回路サイズの下界と線形計画法

Karchmer, Kushilevitz, Nisan (SIAM J. Discrete Math. 1995) は，論理式サイズ下界証明について，LP Bound と呼ばれる一般的証明技法を開発した．LP bound では，論理式サイズの下界をある整数計画問題 (Rectangle Bound) として定式化し，その LP 緩和の双対問題に解を与えることで下界を証明する．近年，LP Bound が既存の証明手法の多くを包括することが示されている [Laplante, Lee, Szegedy (CCC 2005), Lee (STACS 2007)].

上野先生は，論理式サイズ下界を証明する一般的技法として，LP Bound の強化版として，
—LP Bound with Clique Constraints
—Sherali-Adams Bound
—Quasi-Additive Bound
の 3 つの手法を開発している．新しい技法により，多数決関数などの基本的な論理関数に対する下界値が改良されるなど，これらの技法は LP Bound の真の拡張になっている．講演では Quasi - Additive Bound が，Rectangle Bound を上回る例があることをお話いただいた．

3.2　線形決定木の下界と通信複雑度

線形決定義は，内部ノードでの分類が，線形しきい値関数で行われる 2 分決定木である．Gröoger, G. Turán (ICALP 1991) は，入力サイズ n の線

形決定木のサイズが $\Omega(n)$ となることを示している．実数関数版の線形決定木のサイズが $2^{\Omega(n)}$ となることは，Fleischer (Inf. Comput. 1999) によって示されたが，(ブール関数の) 線形決定木のサイズ下界として $\Omega(n)$ を超えるものは知られていなかった．

内澤先生は，(ブール関数の) 線形決定木のサイズ下界として，$2^{\Omega(\sqrt{n})}/w$ を与えている．ただし，w は線形しきい値関数の重みの最大値である．したがって，重み w が $2^{o(\sqrt{n})}$ のとき，入力 n の超多項式サイズとなる．この下界の導出には，通信複雑度の議論が用いられている．

3.3 最適化 × 計算限界 =(算法設計 + 問題構造)×(計算上界 + 計算下界)

岡本先生には，最適化 × 計算限界 =(算法設計 + 問題構造)×(計算上界 + 計算下界) の考え方について，4 通りの場合を豊富な例と共に説明いただいた．特に「最適化理論と計算量理論の融合」のショーケースとして Jain, Ji, Upadhyay, Watrous (STOC 2010, JACM 2011) による QIP=PSPACE の結果を解説していただいた．

3.4 非負階数

勉強会の後の自由討論では非負階数について議論した．

3.5 Extended formula

上野先生の講演を踏まえ，Goemans の論文を読んだ．

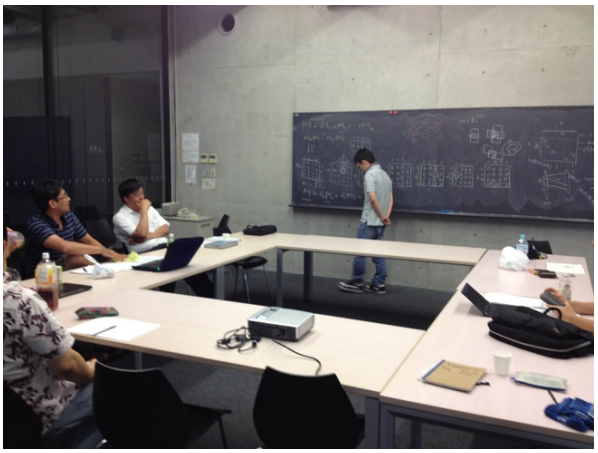


図 1.1: Non-negative rank に関する議論の風景

ELC Mini-Workshop (B02, B03)

世話役:　徳山 豪 (東北大学), David Avis (京都大学)

2012 年 10 月 28 日 (日), 29 日 (月) 両日に B02, B03 班を中心にして、新学術領域研究「多面的アプローチの統合による計算限界の解明」のワークショップを、宮城県仙台市秋保温泉で開催した。

参加者は徳山 豪 (東北大)、David Avis (京大)、Peter Eades (University of Sydney)、Hans Tiwary (ULB)、堀山 貴史 (埼玉大)、宇野 毅明 (NII)、渋谷 哲朗 (東大)、上野 賢哉 (京大)、塩浦 昭義 (東北大)、宮田 洋行 (東北大)、全 眞嬉 (東北大) 及び学生 12 名の計 22 名であった。

初日 (28 日) に、話題提供のための講演を 4 件 (それぞれ 45 分) 行い、そのあとで、討論と問題解決セッションを 4 時間 (内 2 時間は夕食後の自由討論) 取って共同研究を行った。講演タイトルは下記の通りである。

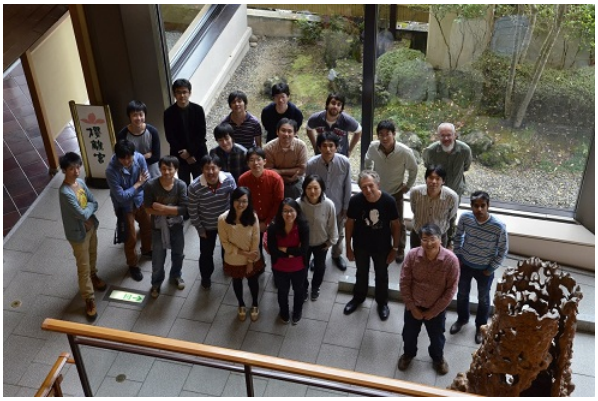
- 徳山 豪: “Matching, Determinant, Permanent, Pfaffian, Dimer, Squared Ice, and Tokuyama’s Formula”
- 上野 賢哉: “Basic Problems on Binary Matrix Factorization”
- Hans Tiwary: “Linear Programming Lower Bound for TSP”
- 堀山 貴史: “Tiling in between 2D and 3D”

徳山の講演は、計算理論の大きなテーマである代数的な計算限界へのアプローチの一端として、群論や熱物理学との関連を紹介したものである。上野の講演は、回路計算量の計算量を解析するために用いる行列分解に関する最新成果の紹介、Tiwary の講演は、巡回セールス問題を数理計画法を用いて解くときの計算限界の改良を与えたものである。堀山の講演は、タイリングの分類と数え上げに対する最新のデータ圧縮技法の利用について述べたものであり、いずれも本新学術領域のテーマの解明に深く関係するものであった。

2 日目 (29 日) には未解決問題の提示とそれに関する議論を行った。話題提供は以下の通りである。

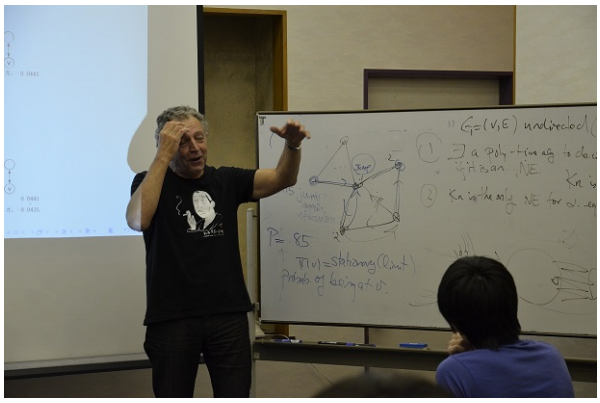
- 宇野 毅明: “Spanner of Visibility Graph”
- 渋谷 哲朗: “Local Alignment DAG Decomposition of Assembly Graphs”
- David Avis: “Equilibrium of Page Rank in Undirected Graph”
- Peter Eades: “Problems in Graph Drawing”

宇野は幾何学に関する問題と、列挙に関する問題の提供を行い、渋谷は計算生物学に関係する最適化の問題を提示した。Avis は WEB 検索でのラ



ンク付けアルゴリズムでのランダムウォークの改良についての提案を行い、Eades はグラフの描画における最適化基準をいくつか示し、未解決問題を提示した。これらの問題について 4 時間の議論を行った。

　宿泊合宿形式のワークショップならではの活発な質疑と交流が行われた。



ELC Mini-Workshop (C02)

世話役: 山下茂（立命館大学），河内亮周 (東京工業大学), 西村治道 (名古屋大学)

1 概要

本ミニワークショップはC02班（量子力学からの計算限界解明へのアプローチ）の年次集会であり，初年度である平成24年度は11月12日から13日にかけて名古屋大学情報科学研究科棟にて開催された．参加者は以下の通り．

山下茂（立命館大），河内亮周（東京工業大）
中西正樹（山形大），フランソワルガル（東京大）
西村治道（名古屋大），小林弘忠（NII）
谷誠一郎（NTT），小柴健史（埼玉大）
伊藤剛志（NEC ラボラトリーズ アメリカ）

小柴以外はC02班のメンバーである．小柴はC01班のメンバーであるが，量子計算の研究も行っているため今回オブザーバーとして参加した．各参加者が自身の研究あるいは最近の量子計算・量子情報に関して発表者が興味を持った研究の報告を行い，その内容について議論を行った．

2 内容

初日は山下，河内，小柴，小林の４名が以下のトピックについて報告を行った．

山下：量子回路のゲート数削減
河内：古典の計算量理論と量子計算量理論への応用
小柴：ancilla-driven 測定ベース量子計算
小林：量子対話型証明系の片側誤り化

２日目は谷，中西，ルガル，伊藤，西村の５名が以下のトピックについて報告を行った．

谷：量子通信計算量と fooling set methods
中西：非有界型誤り量子オートマトン
ルガル:ブール行列積に関する量子アルゴリズム
伊藤：多証明者量子対話型証明系
西村:証明長が指数的に短い量子非対話型証明系

特に伊藤の発表では，本年度の国際会議FOCS'12において最優秀論文に選ばれた

MIP* contains NEXP
Tsuyoshi Ito and Thomas Vidick

の内容が報告された．計算量クラスNEXPは，指数時間限定非決定性Turing機械によって認識可能な判定問題のクラスである．古典の計算量理論では，多証明者対話型証明系によって検証可能な問題のクラスMIPがNEXPと一致することは1991年にBabai, Fortnow, Lundによって示されていたが，複数いる証明者に量子的な相関（エンタングルメント）を許した場合の量子計算量クラスMIP*がどのような計算能力を持つのかは，１０年来の未解決問題であった．伊藤は，NEXP完全問題を検証するBabai-Fortnow-Lund型の検証プロトコルが，量子相関を証明者間に許したとしても依然として健全に働くことを明らかにし，この計算量理論的にも量子力学的にも重要な未解決問題に対して大きな進展を与えた．一方で，MIP*がNEXPに含まれる（すなわちMIP* = NEXP）かなど，まだこのクラスにまつわる未解決な問題は多く，それらの課題についても伊藤から報告された．

全体を通して，非常に活発に議論が行われ，各人の研究結果や問題に関して，より新しいモデルや問題，お互いの疑問点に対する情報やアイデアの提供，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．本ミニワークショップは参加者の研究を進める大きな力となるであろう．

ELC Mini-Workshop (暗号理論)

世話役: 河内亮周 (東京工業大学), 小柴健史 (埼玉大学)

本ワークショップは平成 24 年 12 月 4 日 - 6 日インド工科大学マドラス校の Pandu Rangan Chandrasekaran 教授が東京大学を訪問された際に開催されたミニワークショップである．暗号理論に関する様々な分野の研究者が集まり，議論と意見交換が行われた．

ワークショップには暗号プロトコルの安全性証明をはじめ理論的な結果から実用的な実装までの幅広い内容があり、合計 4 件の一般講演が行われた．詳細は以下の通りである．

日時 2012 年 12 月 6 日（木） 13:30 − 17:10

場所 Center for Exploring the Limits of Computation (CELC)
キャンパス・イノベーションセンター東京
5F 502 号室

参加者数 9 名（教員 4 名, 学生 5 名）

講演

1. “Symmetric-Key Encryption Scheme with Multi-Ciphertext Non-Malleability”

   竹部裕俊 (東京工業大学)

   要旨 : A standard notion of non-malleability is that an adversary cannot forge a ciphertext c' from a single valid ciphertext c for which a plaintext m' of c' is meaningfully related to a plaintext m of c. The *multi-ciphertext non-malleability* is a stronger notion; an adversary is allowed to obtain multiple ciphertexts $c_1, c_2, ...$ in order to forge c'. We provide an efficient symmetric-key encryption scheme with an information-theoretic version of the multi-ciphertext non-malleability in this paper by using ℓ-wise almost independent permutations of Kaplan, Naor, and Reingold.

2. “Generalized Analysis Methods for Efficiency of Representations for Elliptic Curve Scalar Multiplication”

   Vorapong Suppakitpaisarn (東京大学)

   要旨 : In this talk, we introduce the algorithmic analysis approach for elliptic curve scalar multiplication implemented using various kinds of number representations. Scalar multiplication is the bottleneck operation of elliptic curve cryptography, and there are many works proposed to speed-up the operation including the improvement on how we represent the scalar. Many number representations, which are designed to optimize the computation time in a specific type of elliptic curve implementation, are too complicated to be analyzed using mathematical approach. We devise the method based on dynamic programming scheme, automatically-generated Markov chain, and the generic property of most representations. Our focus in this presentation is the r-radix representation for $r > 2$, which is practically used in pairing-based cryptography. We found an interesting relationship between the memory usage and the average speed of optimal scalar multiplication.

3. “On Unidirectional Public Discussion in Secure Message Transmission”

   小柴健史 (埼玉大学)

   要旨 : We consider the possibility and the limitation of secure message transmission (SMT) in the ”unidirectional” public discussion (PD) model. Let epsilon be the privacy parameter and δ be the reliability parameter, where smaller values are better. [Koshiba, Sawada 2010] has shown that the privacy and the reliability are not compatible in the SMT-PD model when only backward public channel is avaiable. Roughly speaking, $\epsilon + \delta$ must be close to 1. Also, we have shown that δ must be larger than approximately $\frac{1}{2}$ when only foreward public channel is avaiable, while we provide an upper-bound protocol achieving approximately $\delta < \frac{t}{n}$, where n is the number of channels and t is the number of channels controlled by an adaptive adversary with unlimited computational resources.

4. “A Novel Digital Signature Scheme with Tight Reduction”

   Pandu Rangan Chandrasekaran (IIT, Madras)

   要旨 : We present a novel digital signature scheme and prove its security using formal reduction technique. The proof is presented in a random oracle model by relating forgeability of the scheme to solvability of a hard problem. We argue that our scheme is the most efficient one among all the systems known because our reduction is tight. We point out some important applications of our scheme in the context of ID based signature schemes and aggregate schemes.

ELC Mini-Workshop (A01)

世話役:　伊藤　大雄 (電気通信大学)

A02 班「情報理論・符号理論からの計算限界解明」のキックオフワークショップを行った．内容は班員の個々の研究成果だけではなく，既存研究から考えられる今後の研究課題，また A02 班としてどういった方向で研究を進めていくのかについて話合われた．

日時　2012 年 12 月 17 日（月）
場所　CELC（計算限界研究センター，田町）
参加者　8 名

講演内容

1.「Experimental Model Theory and Testing: Recent Directions」Skip Jordan (JST ERATO Minato Project & 北海道大学)

記述計算量の理解のための計算機援用の手法と Logic の性質検査についての講演であった．計算機援用は，SAT-solver や QBF-solver を用いて，効率のよい Reduction を探す手法について紹介された．性質検査は，First-Order Logic に対して，どのようなクラスであれば性質検査可能を示された．またグラフの性質検査でよく用いられる Regularity Lemma において，実用的な Regularity Lemma の紹介がされた．

2.「性質検査と CSP–今後の展望–」吉田 悠一（国立情報学研究所 & PFI & JST ERATO Kawarabayashi Project）

CSP を対象とした性質検査について既存結果と今後の課題について講演された．まず，関数の性質検査に関して，片側誤りで検査可能な性質と両側誤りで検査可能な性質の特徴付けについて紹介された．また定数時間近似アルゴリズムと LP 緩和の関係性について自身の結果を交え説明があった．最後に，Polymorphism という概念の紹介とそれから特徴づけられる CSP と計算量の関係が紹介され，さらに Polymorphism と性質検査の融合について結果を述べられた．

3.「回路計算量と通信複雑さ」脊戸 和寿（電気通信大学）

回路計算量と通信複雑さの survey を中心に紹介された．回路計算量は基本的な回路の計算量クラスの話から，有名な既存結果の紹介や次にターゲットとなる問題の説明がなされた．また通信複雑さにおいては，Interactive Proof における通信者間のプロトコルにおける通信量と回路計算量の関係を紹介し，未解決問題について述べられた．その中でも Set Disjointness Problem について，上界の改良における Exponential Time Hypothesis の障壁と下界の改良可能性について述べた．

4.「計算限界証明における障壁と性質検査アルゴリズム」玉置 卓（京都大学）

現在，計算量クラスの分離証明における有名な 3 つの障壁である，相対化 (relativization)，自然な証明 (natural proof)，代数化 (algebrization) について紹介された．これらの障壁がどのようにして下界の証明手法の障壁になっているかを実際の証明手法を例示し紹介された．また現時点では，これらの壁を打ち砕く証明手法が存在せず，これらのバリアを破るために，性質検査が利用できないかを論じた．

ELC Mini-Workshop (C03)

世話役：畑埜 晃平（九州大学），瀧本 英二（九州大学）

学習理論と計算複雑さに関する研究集会を，下記のように開催した．講演は，研究協力者も含めた C03 班のメンバー全員が行った．特に，内澤氏には，自身の研究成果に関する講演の他に，学習可能性と回路計算量の関係に関する最近の研究動向について，チュートリアル講演をお願いした．

C03 班は，計算論の立場から学習過程の複雑さについて論じる，いわゆる計算学習理論の研究者を中心に構成されているが，対象とする計算モデルや研究の方法論の違いにより，それぞれ少しずつ異なるコミュニティに属している．本研究集会は，C03 班のメンバーが一堂に会し，様々な視点から学習と計算複雑さの関係を俯瞰する良い機会を与えることとなった．

講演の途中でも自由に質問や議論ができるように，各講演の時間を十分長くとったが，実際には，ほとんどの講演で予定の時間を過ぎてしまうほど活発に議論が行われた．特に，C03 班と関係が深い B01 班から 2 名（来嶋氏，神山氏）の参加があり，組み合わせ最適化等の立場から深い議論が行われた．C03 班が掲げる目標の一つである，他の研究班への問題提起を含む境界領域分野の活性化は一部達成されたと言えよう．

日時： 2012 年 12 月 17 日（月）〜18 日（火）
会場： JR 博多シティ 9F 会議室

プログラム：

December 17

10:00〜10:20 Eiji Takimoto (Kyushu Univ.) “Opening address and some remarks on the mission of Group C03”

10:30〜12:00 Kei Uchizawa (Yamagata Univ.) [Tutorial] “Learning Algorithm and Circuit Lower Bounds”

Abstract: We mainly survey the following two papers concerning a relationship between learning algorithms and circuit lower bounds:

- Efficient Learning Algorithms Yield Circuit Lower Bounds, JCSS, 75, 27–36, 2009.
- Learning DNFs and Circuits using Teaching Assistants, Proc. COCOON, 188–197, 2004.

We then discuss future work and open problems along a line of research given by the latter paper.

14:00〜14:45 Kohei Hatano (Kyushu Univ.) “Combinatorial Online Prediction using Offline Approximation Algorithms”

Abstract: We consider online prediction problems of combinatorial concepts such as s-t paths, permutations, truth assignments, set covers. A generic approach to this problem is to design an “offline-online converter”, i.e., an online prediction algorithm using a corresponding offline (approximation) algorithm as an oracle. The current state-of-the art converter, however, is not efficient enough. In this talk, we show an promising approach to constructing more efficient offline-online converters.

14:45〜15:30 Marco Cuturi (Kyoto Univ.) “Transportation Distances and their Application in Machine Learning: New Problems”

Abstract: I will present two topics related to the optimal transportation distance and its application in machine learning to compare histograms of features. I discuss first the ground metric learning problem, which is the problem of tuning automatically the parameters of transportation distances using labeled histogram data. I will argue that learning transportation distances is akin to learning an L1 distance on the simplex, and then introduce our algorithm and more recent extensions. In the second part of my talk, I address the fact that transportation distances

are not Hilbertian by showing that they can be cast as positive definite kernels through the "generating function trick".

15:45〜16:30 Ayumi Shinohara (Tohoku Univ.) "Revisiting minimum consistency problem for DFA, and on the maximum number of runs in a string"

Abstract: We discuss two topics. The first one is about the computational complexity for soving a simple puzzle. It is NP-hard in general, since it contains the minimum consistency problem for DFAs as a special case. We are trying to analyze the complexity for a special case, which is also related to the problem of inferring graphs from walks. The second topic is concerning the combinatorial properties of maximal repetitions (runs) in strings. We give a new lower bound of maximal sum of exponents of runs in a string.

16:30〜17:15 Ryo Yoshinaka (Kyoto Univ.) "Distributional Learning of Context-Free Grammars"

Abstract: In Grammatical Inference, intensive research on learning regular languages has achieved a plenty of positive results so far. It had been thought to be quite a hard task to learn a considerably rich class of languages that handle context-free structures. In these years, a new line of research on learning context-free languages, called "distributional learning", has been proposed and has produced several fruitful results. Distributional learning algorithms model and exploit the distribution of substrings in grammatical sentences. This talk summarizes different approaches of distributional learning and presents some open problems on the efficiency of the learning algorithms.

17:30〜18:15 Kei Unizawa (Tohoku Univ.) "Output Patterns of Logic Circuits"

Abstract: Consider any combinatorial circuit C of logic gates. We define the output pattern of C for input x as a vector consisting of the output values of the gates in C for x, and say that C has a number p of output patterns if different p output patterns arise in C over all inputs. In this talk, we observe that the number of output patterns are strongly related to the size of C, and then present some lower bounds on the number of output patterns. We also give some dichotomy result on the problem of counting output patterns of a simple logic circuit.

December 18

10:00〜10:45 Takayoshi Shoudai (Kyushu Univ.) "Learning Unordered Tree Contraction Patterns in Polynomial Time"

Abstract: We present a concept of edge contraction-based tree-structured patterns as a graph pattern suited to represent tree-structured data. A tree contraction pattern (TC-pattern) is an unordered tree-structured pattern common to a given tree-structured data, which is obtained by merging every uncommon connected substructure into one vertex by edge contraction. In this talk, in order to establish an algorithmic foundation for the discovery of knowledge from tree-structured data, we show that TC patterns are learnable in polynomial time.

10:45〜11:30 Koji Tsuda (AIST) "Loss Minimization of Power Distribution Networks with Binary Decision Diagrams"

Abstract: Determining loss minimum configuration in a distribution network is a hard discrete optimization problem involving many variables. Existing fast methods employ local updates that gradually improve the loss to solve such an optimization problem. However, they finally get stuck at local minima, resulting in arbitrarily poor results. In contrast, we presents a novel optimization method that provides an error bound on the solution quality. Instead of using local updates, we construct a highly compressed search space using a binary decision diagram and reduce the optimization problem to a shortest path-finding problem. Optimization of a large-scale model network with 468 switches was solved in three hours with 1.56% relative error bound.

ELC Mini-Workshop (C01)

世話役:　渡辺 治（東京工業大学）

新学術領域研究「計算限界解明」Ｃ０１班では，今年度の主要行事として，海外の研究協力者を招いてのテーマ検討会議を計画し，2013 年 1 月 15 日〜 18 日の日程で，Lenka Zdeborova (CNRS, Institute of Theoret. Physics at CEA) と Haijun Zhou (Chinese Academy of Science) を招き，1 月 16 日，17 日に，班員（渡辺治（代表），小柴健史（分担者），山本真基（分担者））ならびに Benjamin Rossman（Ａ０１班研究協力者），河内亮周（Ｃ０３班分担者）とＣ０１班の研究テーマについて集中討議を行った．

その機会を利用して，Ｃ０１班主催のミニワークショップを 1 月 17 日午後，東工大 Campus Innovation Center の Cener for ELC（田町）にて行った．上記の Zdeborova, Zhou の講演に加え，Ｃ０１班研究協力者の樺島祥介（東工大），福島孝治（東大）が講演を行った．参加者は約 30 名だった．領域からは上記の討議参加者の他，牧野和久（Ａ０１班代表），天野一幸（Ｂ０１班分担者），脊戸和寿（Ａ０２班ＰＤ）が参加した．

講演風景

今回のミニワークショップでは,「統計力学の観点から計算複雑さにどのように挑んでいるか?」，そして「統計力学的手法とはどういうものなのか?」といった点を，計算理論の研究者に紹介することを目的とした．そのため，統計力学の専門家を講演者とし，彼らの考え方や方針の解説を中心に説明してもらった．

以下に講演者順に講演内容を簡単に紹介する．

１．福島孝治は，「The minimum vertex cover problem in random hypergraphs: replica-symmetric solution and a leaf removal algorithm」という題する講演で，random hypergraph の minimum vertex cover の大きさ（全頂点に対する平均比率）に対し，統計力学的手法で算出したものと leaf removal 法というヒューリスティクスで測った場合との比較を行ったという研究を紹介した．この話題を題材に,「レプリカ対称性の崩れ」とは，どういう現象で，それがどのような意味を持つのかを解説した．

福島孝治

2. Haijun Zhou は,「Searching for witness of unsatisfiability for a random 3-SAT formula」という題で講演した．この講演では，3SAT 問題の非充足解に対して非充足の（簡潔な）証拠を与えられるか？という課題に対する平均時の解析が取り上げられた．ランダム 3CNF 論理式では，節数が十分与えられれば簡潔な証拠を（高い確率で）与えられる，ということが示されている．その節

数の下界として，現在（変数数 n に対し）は Feige-Kim-Ofek らが示した $\Omega(n^{1.4})$ が最大だが，その改善を様々なヒューリスティクスで試みていることが紹介された．

Haijun Zhou

3. 樺島祥介は「Statistical mechanics approach to the sample complexity of dictionary learning」という講演を行った．dictionary learning とは，ある規則に従って生成される観測結果の解析技法の主要なステップであり，圧縮センシング問題にも密接に関連している．講演では，その計算ステップの正当性（一意性）を保証するために必要な観測事例数を統計力学的な観点から解析した研究が紹介された．

樺島祥介

4. 最後に，Lenka Zdeborva は「Where the really hard problems really are?」と題する講演で，これまでの講演を締めくくる形で,「計算複雑さを統計力学的に見る」とはどういうことなのかを解説した．

その中でとくに，uniquely extensible constraint satisfaction 問題の平均時複雑さの解析が，今後の重要な課題となる，との見解を具体的な例証をもとに示した．

Lenka Zdeborova

以上の講演で紹介された解析手法や研究テーマの中には，計算理論の立場からも取り掛かれそうなものも多かった．その中でも，uniquely extensible constraint satisfaction 問題や非充足性の簡潔証拠などの研究は，Ｃ０１班が中心となり，他班とも協力して進めることができる，という手ごたえが得られた．こうした点は今回の集中討議ならびに講演会の大きな成果だったといえるだろう．

ELC Seminar
(Lance Fortnow, Benjamin Rossman, Kazuhisa Seto)

世話役: 河内 亮周（東京工業大学）

1 概要

本領域「計算限界解明」プロジェクトのゲストとして東京工業大学を訪問されていた，計算量理論研究の第一人者のひとりである Lance Fortnow 氏を迎え，10 月 2 日にセミナーを行った．本セミナーでは Lance Fortnow 氏に加え，脊戸和久氏 (電通大) および Benjamin Rossman 氏 (東工大) にも講演をお願いし，この三名の各人が近年の重要な結果について，基礎的な部分から紹介し，参加者と様々な議論を行った．本セミナーには学生や若手研究者も多く参加しており，最新の結果を知ることで個々の研究についての知見を深めることに大きく役立ったであろう．

2 内容

日時　2012 年 10 月 2 日（火）
場所　東京工業大学
参加者　10 月 2 日（火）20 名

講演内容

1. "Poset Games are PSPACE-complete," Lance Fortnow (Northwestern University)

2. "Black-Box and Non-Adaptive Search-to-Decision Reductions," Benjamin Rossman (Tokyo Institute of Technology)

For any polynomial-time relation $L \subseteq \{0,1\}^m \times \{0,1\}^n$ where $n = m^{O(1)}$, the classic search-to-decision reduction of Ben-David, Chor, Goldreich and Luby gives a $\mathrm{BPP}_{||}^{\mathrm{NP}}$ algorithm which solves the search problem for L (given x, find w such that $(x,w) \in L$) with only $O(n^2)$ non-adaptive queries to the NP oracle. We begin by observing that this algorithm is *black-box* in the following sense: it can be implemented in the setting where the input x is unavailable and, instead, only the witness set $\{w \mid (x,w) \in L\}$ is provided as a black-box. Our main result is a tight lower bound in this black-box setting: we show that every such black-box $\mathrm{BPP}_{||}^{\mathrm{NP}}$ search-to-decision reduction requires $\Omega(n^2)$ non-adaptive queries to the NP oracle. As the framework for proving this lower bound, we introduce a general *witness finding problem* with respect to a class $\mathcal{W}$ of witness sets and a class $\mathcal{Q}$ of queries. In addition to NP-type queries, we prove lower bounds for monotone queries as well as for affine witness sets.

3. "A Satisfiability Algorithm and Average-Case Hardness for Formulas over the Full Binary Basis," Kazuhisa Seto (ELC & The University of Electro-Communications)

We present a moderately exponential time algorithm for the satisfiability of Boolean formulas over the full binary basis. For formulas of size at most cn, our algorithm runs in time $2^{(1-\mu_c)n}$ for some constant $\mu_c > 0$. As a byproduct of the running time analysis of our algorithm, we get strong average-case hardness of affine extractors for linear-sized formulas over the full binary basis.

ELC Seminar
(Laszlo Egri, Yuichi Yoshida, Kazuhisa Seto)

世話役:　河内 亮周 (東京工業大学)

国立情報学研究所に訪問されていた，Laszlo Egri 氏を迎え，11 月 2 日と 9 日の 2 週に渡ってセミナーを行った．各人が近年の自分の結果について，基礎的な部分から紹介し，参加者と様々なディスカッションを行った．本セミナーには学生も数名参加しており，若手研究者の最新の結果に触れることで，個々の研究意欲の増進や知見を深めるのに大いに役立ったであろう．

日時　2012 年 11 月 2 日（金），9 日（金）
場所　東京工業大学
参加者　11 月 2 日（金）8 名，9 日（金）6 名

講演内容（11 月 2 日）

1.「The Complexity of the List Homomorphism Problem for Graphs」Laszlo Egri (McGill University)

We completely classify the computational complexity of the list H-colouring problem for graphs (with possible loops) in combinatorial and algebraic terms: for every graph H, the problem is either NP-complete, NL-complete, L-complete or is first-order definable; descriptive complexity equivalents are given as well via Datalog and its fragments. Our algebraic characterisations match important conjectures in the study of constraint satisfaction problems.

2.「An Algebraic Characterization of Testable Boolean CSPs」Yuichi Yoshida（NII & PFI & JST ERATO Kawarabayashi Project）

Given an instance I of a CSP, a tester for I distinguishes assignments satisfying I from those which are far from any assignment satisfying I. The efficiency of a tester is measured by its query complexity, the number of variable assignments queried by the algorithm. In this paper, we characterize the hardness of testing Boolean CSPs in terms of the algebra generated by the relations used to form constraints. In terms of computational complexity, we show that if a non-trivial Boolean CSP is sublinear-query testable (resp., not sublinear-query testable), then the CSP is in NL (resp., P-complete, $\oplus$L-complete or NP-complete) and that if a sublinear-query testable Boolean CSP is constant-query testable (resp., not constant-query testable), then counting the number of solutions of the CSP is in P (resp., #P-complete).

Also, we conjecture that a CSP instance is testable in sublinear time if its Gaifman graph has bounded treewidth. We confirm the conjecture when a near-unanimity operation is a polymorphism of the CSP.

（11 月 9 日）

3.「An Introduction to Circuit Complexity and Satisfiability Algorithms on Formulas」Kazuhisa Seto（The University of Electro-Communications）

In this talk, we give a basic introduction to circuit complexity and satisfiability algorithms on formulas. At first, we show Subbotovskaya's technique for proving the lower bound of parity function on formulas. Next, we introduce Santhanam's satisfiability algorithm for de morgan formulas by using Subbotovskaya's technique. Finally, we give our satisifiablity algorithm for formulas over the full binary basis by extension of Santhanam's algorithm.

ERATO河原林巨大グラフプロジェクト & ELC合同講演会 (Arnab Bhattacharyya & Mikkel Thorup)

世話役: 河内 亮周 (東京工業大学)

ERATO河原林巨大グラフプロジェクトと新学術領域「多面的アプローチの統合による計算限界の解明」(通称:ELC) との合同セミナーとして，Arnab Bhattacharyya 氏と Mikkel Thorup 氏を招き，講演会が行われた．ERATO，ELC ともに本年度より開始され，今後数年にわたり，日本の理論計算機科学分野を牽引していくプロジェクトであり，今後のコラボレーションも視野にいれ，その第一回目として合同講演会が開催された．Arnab 氏は関数の性質検査に関する講演を行い，Mikkel 氏はデータ構造に関する講演を行った．両講演ともに理論計算機科学のトップカンファレンスである STOC に論文が採択される非常にレベルの高い内容であり，興味深い内容であった．ERATO と ELC 両チームから若手を中心に参加者が集まり，ハイレベルな議論が行われ，非常に実りのある講演会であった．本講演会のように，今後も両プロジェクトを横断するような講演会や研究集会の開催が期待される．

日時　2012 年 11 月 30 日（金）
場所　キャンパスイノベーションセンター東京（東工大田町キャンパス）
参加者　15 名

講演内容

1.「Every locally characterized affine-invariant property is testable」Arnab Bhattacharyya (DIMACS/Rutgers)

Let $F = F_p$ for any fixed prime $p \geq 2$. An affine-invariant property is a property of functions on F^n that is closed under taking affine transformations of the domain. We prove that all affine-invariant property having local characterizations are testable. In fact, we show a proximity-oblivious test for any such property P, meaning that there is a test that, given an input function f, makes a constant number of queries to f, always accepts if f satisfies P, and rejects with positive probability if the distance between f and P is nonzero. More generally, we show that any affine-invariant property that is closed under taking restrictions to subspaces and has bounded complexity is testable.（一部抜粋）

Joint work with Eldar Fischer, Hamed Hatami, Pooya Hatami, and Shachar Lovett.

2.「The Power of Tabulation Hashing」Mikkel Thorup (AT&T Labs Research)

Randomized algorithms are often enjoyed for their simplicity, but the hash functions used to yield the desired theoretical guarantees are often neither simple nor practical. Here we show that the simplest possible tabulation hashing provides unexpectedly strong guarantees. The scheme itself dates back to Carter and Wegman (STOC'77). Keys are viewed as consisting of c characters. We initialize c tables T1,⋯,Tc mapping characters to random hash codes. A key x=(x1,⋯,xc) is hashed to T1[x1]⊕⋯⊕Tc[xc], where ⊕ denotes xor. While this scheme is not even 4-independent, we show that it provides many of the guarantees that are normally obtained via higher independence, e.g., Chernoff-type concentration, min-wise hashing for estimating set intersection, and cuckoo hashing. We shall also discuss a twist to simple tabulation that leads to extremely robust performance for linear probing with small buffers.

ELC セミナー (萩原 学)

世話役:　河内 亮周 (東京工業大学)

1　概要

本セミナーでは符号理論の新進気鋭の若手研究者である産総研の萩原学氏をお招きし，フラッシュメモリなどの物理デバイスから由来する従来の古典的な符号理論とは大きく異なる新しい数理モデルに基づいた符号である置換符号とその解析に関する萩原氏自身の結果を講演していただいた．

符号理論は計算量理論をはじめとして理論計算機科学の基本的なツールとしてしばしば利用される重要な概念である．計算量理論では例えば確率的検査可能証明，リスト復号可能符号，局所復号可能符号，性質検査，などの多くの応用を持つ．本プロジェクトのメンバーがその最先端の知見を得るのは非常に有意義である．

特に萩原氏の新しい結果は置換符号という代数的な対象に対して最適化数理の基本技法である線形計画法を利用するこれまでにはないタイプの復号アルゴリズムを提案しており，符号理論に関連する計画研究班 A02 班だけではなく，最適化数理に深く関係する B01 班，B02 班のトピックにも関連性を見いだせる非常に分野縦断的な話題であった．

2　開催情報

日時: 2012 年 12 月 7 日（金）
タイトル:
コンパクトグラフと線形計画法による置換符号
Compact Graph and Linear Programming for Permutation Codes
講師: 萩原 学 (産総研)
場所: 計算限界研究センターセミナー室
参加者　10 名
講演概要：
置換符号は符号理論の話題の一つである．これまでこの符号は，電力線搬送通信向きとして研究されてきた．この符号の特別なケースである，ランク変調と呼ばれる方式は，近年，フラッシュメモリの誤り訂正に応用できる可能性が指摘され，注目が高まっている．本講演では，置換符号やランク変調のコンセプトについて解説する．また，それらの誤り訂正アルゴリズムとして線形計画法を適用する為の，置換符号とランク変調の構成法について議論したい．

Permutation codes are error-correcting codes and have been investigated mainly for study of power line communication. Rank modulation, which is a class of permutation codes, has recently attracted since the modulation might be applicable to an error-correction method for flash memories. In this talk, basic notion and idea will be introduced and some previous results on construction of the codes and the modulations suitable for linear programming method as decoding algorithm will be discussed.

ELC セミナー (河内亮周)

世話役:　河内亮周 (東京工業大学)

1　概要

本セミナーでは東京工業大学の河内による計算量理論の最先端の結果についての解説がなされた.

特に Ryan Williams の 2011 年の結果である回路クラス ACC^0 の NEXP における超多項式下界 (国際会議 Conference on Computational Complexity 2011 最優秀論文賞) および，その背景となる二つの結果，Ryan Williams の 2010 年の結果である回路充足可能性問題を解くアルゴリズムの高速化からの NEXP における回路計算量の超多項式下界 (国際会議 Symposium on Theory of Computing 2010 で発表)，そして Impagliazzo, Kabanets, Wigderson らによる NEXP における多項式サイズの証拠回路の存在性 (論文誌 Journal of Computers and System Sciences 掲載) の論文を中心に詳細な解説が与えられ，またその内容に関して今後の研究方針や可能性について深い議論・意見交換がなされた.

ACC^0 の NEXP における超多項式下界の論文は近年の計算量理論の中においても目覚ましい結果であり，計算限界の解明のための今後の大きな発展の原動力となり得る技法を数多く提供している. この技法を学び，メンバー間で共有していくことは本プロジェクトに大変有意義であると言える.

特にこの論文自体とその背景となる結果が与えている，ある種の回路の充足可能性問題を非自明に高速に解くアルゴリズムから回路計算量の下界という計算限界を明らかにする，という新しい手法は回路計算量の下界を直接証明するという困難な課題から，ある種の問題のアルゴリズムの計算時間の良い上界を得ることに目標を挿げ替えることのできる大変興味深い技法であり，計算量の上界へのアプローチと下界へのアプローチを橋渡しするという意味で本プロジェクトで情報共有することは非常に重要である.

2　開催情報

日時: 2012 年 12 月 28 日（金）
タイトル: ACC^0 回路の NEXP での超多項式下界の解説
講師: 河内 亮周 (東工大)
場所: 計算限界研究センターセミナー室
参加者　10 名
関連論文:

[Wil13] Ryan Williams: Natural Proofs versus Derandomization, manuscript (available at R. Williams' website).

[Wil11] Ryan Williams: Non-uniform ACC Circuit Lower Bounds. IEEE Conference on Computational Complexity 2011: 115-125

[Wil10] Ryan Williams: Improving exhaustive search implies superpolynomial lower bounds. STOC 2010.

[IKW02] Russell Impagliazzo, Valentine Kabanets, Avi Wigderson: In search of an easy witness: exponential time vs. probabilistic polynomial time. J. Comput. Syst. Sci. 65(4): 672-694 (2002)

ELCセミナー (A01)

世話役:　河村彰星 (東京大学)

A01 班「数理論理学からの計算限界解析」の研究課題である計算量と論理学のかかわりに位置する様々な話題について知るためのセミナーとして、各分野の専門家である照井一成氏 (京都大)、ゼバスティアン・ミュラー氏 (カレル大)、マルティン・ツィーグラー氏 (ダルムシュタット工科大) による講演会を平成 25 年 2 月 21 日 (木) 午後に東京大学理学部七号館 214 室にて開催した。なおツィーグラー氏は当班の研究協力者であり引続き 3 月 30 日まで河村との共同研究のため本領域で招聘して東大に滞在中である。

ツィーグラー教授の講演

13:50–14:50
Kazushige Terui (Kyoto University)
Type Theoretic Approaches to
Implicit Computational Complexity

15:10–16:10
Sebastian Müller (Charles University)
Short Refutations of Random 3CNF
in TC^0-Frege

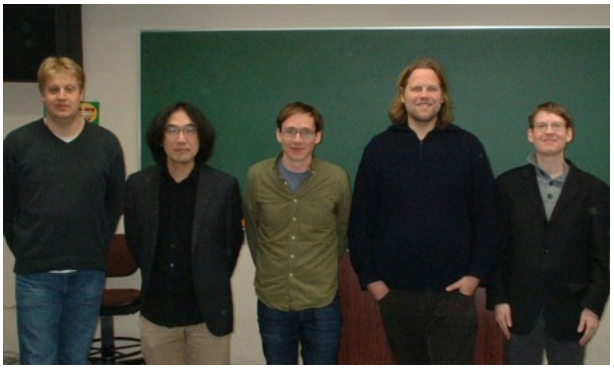
16:30–17:30
Martin Ziegler (TU Darmstadt)
Real Benefit of Promises and Advice

18:00–　Dinner

照井氏は陰計算量理論における安全再帰、型理論、線型論理、表示意味論についての概観、ミュラー氏は証明量の研究の概論からランダム CNF 充足不能証明における御自身の結果の紹介、ツィーグラー氏は実数値計算における離散的な情報と計算量の関係についての内容であった。それぞれ異なる研究分野の話題であるので、講師には予め多様な聴衆を想定して概論からじっくりとお話を頂くようお願いした。49 名の参加があり活発な議論がなされた。

本領域全体では理論情報学の研究者が多いが、当班の研究課題では数理論理学の専門家との連携が重要である。この分野からの参加者の便宜を図るため開催日を計算可能性と数学基礎論に関する研究集会 CTFM (2 月 18?20 日於東工大) の翌日とし、その開催事務局に広報の面でも御協力を頂いた。実際に論理学の他分野から多くの参加者があり本領域の周知にも効果があった。

また連続開催のセミナーとして同日午前にクリストファー・ハンセン氏 (オーフス大)、ミヒャエル・エルバーフェルト氏 (バークレー国際情報学研) の講演も行われた。これはそれぞれ閾値回路の下界、グラフ性質の記述量に関する講演であり、午前・午後合せて広く計算量の論理学関連分野の広い話題に触れるセミナーとなった。


ハンセン氏、照井氏、エルバーフェルト氏、
ミュラー氏、ツィーグラー氏

2.　研究課題別活動報告

文部科学省科学研究費補助金 新学術領域研究 (課題番号 24106002)

A01: 数理論理学からの計算限界解析

研究代表者：	牧野 和久	京都大学 数理解析研究所
研究分担者：	河村 彰星	東京大学 大学院 情報理工学系研究科
	垣村 尚徳	東京大学 教養学部附属教養教育高度化機構
	小林 佑輔	東京大学 大学院 情報理工学系研究科
特任研究員：	Suppakitpaisarn Vorapong	東京大学 大学院 情報理工学系研究科

開催した研究集会

1. ELC セミナー (A01)
   期間: 2012 年 12 月 15 日
   場所: 東京大学本郷キャンパス
   講演者: 山下 真 (東京工業大学), 永野 清仁 (東京大学)

2. ELC セミナー (A01)
   期間: 2013 年 2 月 2 日
   場所: 東京大学本郷キャンパス
   講演者: 小関 健太 (国立情報学研究所), 武田 朗子 (慶応義塾大学)

3. ELC セミナー (A01)
   期間: 2013 年 2 月 21 日
   場所: 東京大学本郷キャンパス
   講演者: 照井一成 (京都大学), ゼバスティアン・ミュラー (カレル大学), マルティン・ツィーグラー (ダルムシュタット工科大学)

4. ELC セミナー (A01)
   期間: 2013 年 2 月 27 日
   場所: 東京大学本郷キャンパス
   講演者: マイケル・ランピス (スウェーデン王立工科大学)

招聘研究者

1. マルティン・ツィーグラー (ダルムシュタット工科大学)
   期間: 2013 年 2 月 15 日〜3 月 30 日
   受入: 東京大学

2. マイケル・ランピス (スウェーデン王立工科大学)
   期間: 2013 年 2 月 25 日〜3 月 2 日
   受入: 東京大学

受賞

1. 太田浩行:
   LA/EATCS 学生発表論文賞, 2013 年 1 月.
   対数空間階層の相対化 (河村との共著).

2. 小林佑輔:
   日本オペレーションズ・リサーチ学会 研究賞奨励賞, 2012 年 9 月.
   (1) Y. Kobayashi and C. Sommer: On Shortest Disjoint Paths in Planar Graphs, Discrete Optimization, Vol.7 (2010), pp. 234–245. (2) K. Kawarabayashi and Y. Kobayashi: An Improved Algorithm for the Half-disjoint Paths Problem, SIAM Journal on Discrete Mathematics, Vol.25 (2011), pp. 1322–1330. (3) K. Kawarabayashi and Y. Kobayashi: Breaking $O(n^{1/2})$-approximation Algorithms for the Edge-disjoint Paths Problem with Congestion Two, Proceedings of the 43rd ACM Symposium on Theory of Computing (STOC 2011), 2011, pp. 81–88..

3. スッパキットパイサーン ウォラポン:
   タイ日国際学会　論文発表賞, 2012 年 10 月 20 日.

Optimal Elliptic Curve Cryptography Using Fibonacci Sequence.

4. 河瀬康志:
日本オペレーションズ・リサーチ学会「最適化の理論と応用」研究部会 SOTA 最優秀発表賞, 2012 年 7 月.
キャンセルコスト付きオンライン重みなしナップサック問題 (韓，牧野との共著).

5. 木村 慧:
電子情報通信学会 総合大会 COMP 学生シンポジウム（2013 年）最優秀論文賞, 2013 年 3 月 19 日.
整数線形不等式系の実行可能性問題に対する符号情報に基づく計算複雑さの指標 (牧野との共著).

アウトリーチ活動

1. 牧野和久:
楽して計算するには—計算を科学する, 高校生のための数理工学見学会 (東京大学), 2012 年 8 月 10 日.

2. 小林佑輔:
ネットワークにおける最適化, 東京大学 父母のためのオープンキャンパス (東京大学), 2012 年 7 月 14 日.

学術論文

1. Akitoshi Kawamura and Yusuke Kobayashi: Fence Patrolling by Mobile Agents with Distinct Speeds, *Proc. 23rd International Symposium on Algorithms and Computation (ISAAC 2012),* Lecture Notes in Computer Science, 7676, 598–608. December 2012

2. Naonori Kakimura, Kazuhisa Makino, and Kento Seimi:
Computing Knapsack Solutions with Cardinality Robustness, *Japan Journal of Industrial and Applied Mathematics,* 29, 469–483, October 2012.

3. Naonori Kakimura and Ken-ichi Kawarabayashi:
Half-Integral Packing of Odd Cycles through Prescribed Vertices, *Combinatorica,* (掲載予定).

4. Xin Han, Yasushi Kawase, and Kazuhisa Makino:
Online Knapsack Problem with Removal Cost, *Proc. 18th Annual International Conference, COCOON 2012,* Lecture Notes in Computer Science 7434, 61–73, August 2012.

5. Kazuhisa Makino and Hirotaka Ono:
Deductive Inference for the Interiors and Exteriors of Horn Theories, *ACM Transactions on Computational Logic,* 13, 23, August 2012.

6. Marek Chrobak, Gerhard J. Woeginger, Kazuhisa Makino, Haifeng Xu:
Caching Is Hard - Even in the Fault Model, *Algorithmica,* 63, 781-794, August 2012.

7. Hanna Sumita, Naonori Kakimura, and Kazuhisa Makino:
Sparse Linear Complementarity Problems, *Proc. 8th International Conference on Algorithms and Complexity,* (掲載予定).

研究会等

1. 河村彰星:
再帰的解析学における計算量, 数理解析研究所研究集会「証明論と複雑性」, 2012 年 9 月.

2. Akitoshi Kawamura, Yusuke Kobayashi:
Fence Patrolling by Mobile Agents with Distinct Speeds, *22nd Annual Fall Workshop on Computational Geometry,* November 2012.

3. 河村彰星，マルティン・ツィーグラー，ノルベルト・ミュラー，カルステン・レースニク:
解析函数の表現と計算量について, 平成 *24* 年

度冬のエルエーシンポジウム, 19, 2013 年 1 月.

4. 太田浩行，河村彰星:
対数空間階層の相対化, 平成 *24* 年度冬のエルエーシンポジウム, 20, 2013 年 1 月.

5. Akitoshi Kawamura, Norbert Th. Müller, Carsten Rösnick, Martin Ziegler:
Parameterized uniform complexity in numerics: from smooth to analytic, from NP-hard to polytime, *Computability Theory and Foundations of Mathematics,* February 2013.

6. 岡本拓馬，辰雄一，大和雅英，河村彰星，宇野裕之:
Morpion Solitaire：最大手数の新しい上界, 第八回組合せゲーム・パズル研究集会, 2013 年 3 月.

7. V. Suppakitpaisarn, M. Edahiro, H. Imai:
Optimal Elliptic Curve Cryptography Using Fibonacci Sequence, *5th Thailand-Japan International Academic Conference (TJIA2012),* 2012 年 10 月 20 日.

8. V. Suppakitpaisarn:
Generalized Analysis Methods for Efficiency of Representations for Elliptic Curve Scalar Multiplication, *ELC* ミニワークショップ *(*暗号理論*),* 2012 年 12 月.

9. V. Suppakitpaisarn, H. Imai:
Yet Another Proof for Optimal Joint Average Hamming Weight of Width-3 Joint Sparse Form, *6th Annual Meeting of Asian Association for Algorithms and Computation (AAAC 2013),* (発表予定).

10. Han Xin, 河瀬康志，牧野和久:
キャンセルコスト付きオンラインナップサック問題, 日本オペレーションズ・リサーチ学会「最適化の理論と応用」研究部会 *SOTA,* 2012 年 6–7 月.

11. 澄田範奈，垣村尚徳，牧野和久:
疎な線形相補性問題の計算複雑度, 日本オペレーションズ・リサーチ学会「最適化の理論と応用」研究部会 *SOTA,* 2012 年 6–7 月.

学会大会等

1. 河村彰星，マルティン・ツィーグラー，ノルベルト・ミュラー，カルステン・レースニク:
解析函数の表現と演算子の計算量について, 日本数学会年会, 2013 年 3 月.

2. Naonori Kakimura, Kazuhisa Makino, and Kento Seimi:
Computing Knapsack Solutions with Cardinality Robustness, *The 21th International Symposium on Mathematical Programming (ISMP),* 2012 年 8 月.

3. Naonori Kakimura and Mizuyo Takamatsu:
Matching Problems with Delta-Matroid Constraints, *The 21th International Symposium on Mathematical Programming (ISMP),* 2012 年 8 月.

4. 木村 慧，牧野 和久:
整数線形不等式系の実行可能性問題に対する符号情報に基づく計算複雑さの指標, *2013* 年電子情報通信学会 総合大会, S11-S12, 2013 年 3 月 19 日.

5. Han Xin, 河瀬 康志, 牧野 和久:
キャンセルコスト付きオンラインナップサック問題, 日本オペレーションズ・リサーチ学会秋季研究発表会, 50–51, 2012 年 9 月.

6. Han Xin, 河瀬 康志, 牧野 和久:
キャンセルコスト付きオンライン重みなしナップサック問題, *2013* 年電子情報通信学会総合大会, S13–S14, 2013 年 3 月.

7. 澄田範奈，垣村尚徳，牧野和久:
疎な線形相補性問題に対する組合せ的アルゴリズム, 日本オペレーションズ・リサーチ学会 秋季研究発表会, 54–55, 2012 年 9 月.

8. 澄田範奈，垣村尚徳，牧野和久:
疎な線形相補性問題に対する組合せ的アルゴリズム, *2013* 年電子情報通信学会 総合大会, S15-S16, 2013 年 3 月.

文部科学省科学研究費補助金 新学術領域研究 (課題番号 24106003)

A02: 情報理論・符号理論からの計算限界研究

研究代表者：	河原林 健一	国立情報学研究所 情報学プリンシプル研究系 ERATO 河原林巨大グラフプロジェクト
研究分担者：	伊藤 大雄	電気通信大学 大学院 情報理工学研究科
	玉置 卓	京都大学 大学院 情報学研究科
	吉田 悠一	国立情報学研究所 情報学プリンシプル研究系 ERATO 河原林巨大グラフプロジェクト プリファードインフラストラクチャー
	脊戸 和寿	電気通信大学 大学院 情報理工学研究科
連携研究者：	Skip Jordan	北海道大学 大学院 情報科学研究科 ERATO 湊離散構造処理系プロジェクト

開催した研究集会

1. ELC Mini-Workshop (A02)
   期間: 2012 年 12 月 17 日
   場所: CELC
   講演者: Skip Jordan（JST ERATO Minato Project and 北海道大学）, 吉田 悠一（国立情報学研究所 and Preferred Infrastructure, Inc.）, 脊戸 和寿（電気通信大学）, 玉置 卓（京都大学）

2. ELC Seminar (Kazuhisa Seto)
   期間: 2012 年 11 月 9 日
   場所: 東工大大岡山キャンパス
   講演者: Kazuhisa Seto (The University of Electro-Communications)

3. ELC Seminar (Laszlo Egri, Yuichi Yoshida)
   期間: 2012 年 11 月 2 日
   場所: 東工大大岡山キャンパス
   講演者: Laszlo Egri (McGill Univ.), Yuichi Yoshida (NII and Preferred Infrastructure, Inc.)

受賞

1. 吉田 悠一:
   船井情報科学振興財団　船井研究奨励賞, .

2. Martin Grohe, Ken-ichi Kawarabayashi and Bruce Reed:
   Best Paper Awards, ACM-SIAM Symposium on Discrete Algorithms 2013, Jan, 2013.
   A Simple Algorithm for the Graph Minor Decomposition - Logic meets Structural Graph Theory.

3. 河原林 健一:
   日本学士院学術奨励賞, 2013 年 1 月.
   先端的グラフ理論を利用した離散数学，計算機学にわたる横断的研究.

4. 河原林 健一:
   日本学術振興会賞, 2012 年 12 月.
   先端的グラフ理論を利用した離散数学，計算機学にわたる横断的研究.

アウトリーチ活動

1. 吉田悠一:
   ACM-ICPC 東京大会実行委員会 審判, 2012 年 11 月 17 日–19 日.

著書

1. 河原林 健一，田井中 麻都佳:
   これも数学だった!?: カーナビ，路線図，SNS (丸善ライブラリー), 丸善出版, 2013.

学術論文

1. Karl Wimmer and Yuichi Yoshida:
   Testing Linear-Invariant Function Isomorphism, *Proc. 40th International Colloquium on Automata, Languages and Programming (ICALP),* (掲載予定).

2. Arnab Bhattacharyya and Yuichi Yoshida:
   An Algebraic Characterization of Testable CSPs, *Proc. 40th International Colloquium on Automata, Languages and Programming (ICALP),* (掲載予定).

3. Takuya Akiba, Yoichi Iwata, and Yuichi Yoshida:
   Fast Exact Shortest-Path Distance Queries on Large Networks by Pruned Landmark Labeling, *Proc. ACM Special Interest Group on Management of Data (SIGMOD),* (掲載予定).

4. Danushka Bollegala, Mitsuru Kusumoto, Yuichi Yoshida, and Ken-ichi Kawarabayashi:
   Mining for Analogous Tuples from an Entity-Relation Graph, *Proc. International Joint Conferences on Artificial Intelligence,* (掲載予定).

5. UMESATO Takuya, SAITOH Toshiki, UEHARA Ryuhei, ITO Hiro, and OKAMOTO Yoshio:
   Complexity of the stamp folding problem, *Theoretical Computer Science,* (掲載予定).

6. Szilard Zsolt Fazekas, Hiro Ito, Yasushi Okuno, Shinnosuke Seki, and Kei Taneishi:
   On computational complexity of graph inference from counting, *Natural Computing,* (掲載予定).

7. Kazuhisa Makino, Suguru Tamaki and Masaki Yamamoto:
   Derandomizing HSSW algorithm for 3-SAT, *Algorithmica,* (掲載予定).

8. Ken-ichi Kawarabayashi and Yuichi Yoshida:
   Testing Subdivision-Freeness: — Property Testing Meets Structural Graph Theory —, *Proc. 45th ACM Symposium on the Theory of Computing (STOC),* 2013 (掲載予定).

9. Ken-ichi Kawarabayashi and Yusuke Kobayashi:
   An O(log n)-Approximation Algorithm for the Edge-Disjoint Paths Problem in Eulerian Planar Graphs, *ACM Transactions on Algorithms,* 9(2), 16, 2013.

10. Kazuhisa Seto and Suguru Tamaki:
    A Satisfiability Algorithm and Average-Case Hardness for Formulas over the Full Binary Basis, *Computational Complexity,* 22(2), 245–274, 2013.

11. Yoichi Iwata and Yuichi Yoshida:
    Exact and Approximation Algorithms for the Constraint Satisfaction Problem over the Point Algebra, *Proc. 30th Symposium on Theoretical Aspects of Computer Science (STACS),* 127–138, 2013.

12. Ken-ichi Kawarabayashi, Christian Sommer and Mikkel Thorup:
    More Compact Oracles for Approximate Distances in Undirected Planar Graphs, *Proc. ACM-SIAM Symposium on Discrete Algorithms (SODA),* 550–563, 2013.

13. Zdenek Dvorak and Ken-ichi Kawarabayashi:
    List-coloring embedded graphs, *Proc. ACM-SIAM Symposium on Discrete Algorithms (SODA),* 1004–1012, 2013.

14. Martin Grohe, Ken-ichi Kawarabayashi and Bruce Reed:

A Simple Algorithm for the Graph Minor Decomposition - Logic meets Structural Graph Theory, *Proc. ACM-SIAM Symposium on Discrete Algorithms (SODA),* 414–431, 2013.

15. Ken-ichi Kawarabayashi and Kenta Ozeki:
4-connected projective-planar graphs are hamiltonian-connected, *Proc. ACM-SIAM Symposium on Discrete Algorithms (SODA),* 378–395, 2013.

16. Ken-ichi Kawarabayashi:
Totally odd subdivisions and parity subdivisions: Structures and Coloring, *Proc. ACM-SIAM Symposium on Discrete Algorithms (SODA),* 1013–1029, 2013.

17. Ken-ichi Kawarabayashi, Marek Krcal, Daniel Kral and Stephan Kreutzer:
Packing directed cycles through a specified vertex set, *Proc. ACM-SIAM Symposium on Discrete Algorithms (SODA),* 365–377, 2013.

18. Ken-ichi Kawarabayashi:
5-coloring $K_{3,k}$-minor-free graphs: Beyond Thomassen, *Proc. ACM-SIAM Symposium on Discrete Algorithms (SODA),* 985–1003, 2013.

19. Mitsuru Kusumoto and Yuichi Yoshida and Hiro Ito:
Constant-Time Approximation Algorithms for the Optimum Branching Problem on Sparse Graphs, *Proc. 3rd International Conference on Networking and Computing (ICNC),* 69, 1–6, 2012.

20. Reinhard Diestel, Ken-ichi Kawarabayashi, Theodor Müller and Paul Wollan:
On the excluded minor structure theorem for graphs of large tree-width, *Journal of Combinatorial Theory, Series B,* 102(6), 1189–1210, 2012.

21. Ken-ichi Kawarabayashi and Mikkel Thorup:
Combinatorial Coloring of 3-Colorable Graphs, *Proc. 53rd Annual IEEE Symposium on Foundations of Computer Science (FOCS),* 68–75, 2012.

22. Eric Blais and Amit Weinstein and Yuichi Yoshida:
Partially Symmetric Functions are Efficiently Isomorphism-Testable, *Proc. 53rd Annual IEEE Symposium on Foundations of Computer Science (FOCS),* 556–560, 2012.

23. Ken-ichi Kawarabayashi and John Maharry:
Minors in large almost-5-connected nonplanar graphs, *Journal of Graph Theory,* 71(2), 128–141, 2012.

24. Richard Hoshino and Ken-ichi Kawarabayashi:
Generating Approximate Solutions to the TTP using a Linear Distance Relaxation, *Journal of Artificial Intelligence Research,* 45, 257–286, 2012.

25. Suguru Tamaki and Yuichi Yoshida:
Approximation Guarantees for the Minimum Linear Arrangement Problem by Higher Eigenvalues, *Proc. 15th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems (APPROX),* LNCS 6842, 313–324, 2012.

26. Yuichi Yoshida, Masaki Yamamoto, and Hiro Ito:
Constant-Time Algorithms for Sparsity Matroids, *SIAM Journal on Computing,* 41(4), 1074–1093, 2012.

27. Hiro Ito, Shin-ichi Tanigawa and Yuichi Yoshida:
Improved Constant-Time Approximation Algorithms for Maximum Matchings and Other Optimization Problems., *Proc. 40th International Colloquium on Automata,*

Languages and Programming (ICALP), 498–509, 2012.

研究会等

1. Yuichi Yoshida:
   Robust approximation of CSPs: Universal algebra meets optimization, *ELC Tokyo Complexity Workshop,* 2013 年 3 月.

2. Takuya Akiba, Yoichi Iwata, and Yuichi Yoshida:
   Fast Exact Distance Queries on Large Networks by Pruned Shortest-Path Trees, *Proc. 3rd Workshop on Algorithms for Large-Scale Information Processing (ALSIP),* 2012 年 11 月.

3. Eric Blais, Amit Weinstein, and Yuichi Yoshida:
   Partially Symmetric Functions are Efficiently Isomorphism-Testable, コンピューテーション研究会 *(COMP)* , 112(199), 35–40, 2012 年 9 月.

学会大会等

1. Yuichi Yoshida:
   制約充足問題に対する頑健な近似アルゴリズム, 電子情報通信学会 総合大会 *DS-1. COMP* 学生シンポジウム, 2013 年 3 月 (掲載予定).

文部科学省科学研究費補助金 新学術領域研究 (課題番号 24106004)

A03：記憶領域制限シナリオにおける計算限界の解明

研究代表者：	浅野 哲夫	北陸先端科学技術大学院大学 情報科学研究科
研究分担者：	垂井 淳	電気通信大学大学院 情報理工学研究科
	上原 隆平	北陸先端科学技術大学院大学 情報科学研究科
	小野 廣隆	九州大学 大学院 経済学研究院
	清見 礼	横浜市立大学 国際総合科学部
研究協力者：	Guenter Rote	ベルリン自由大学
	Wolfgang Mulzer	ベルリン自由大学
	Ovidiu Daescu	テキサス大学ダラス校
	小長谷 松雄	北陸先端科学技術大学院大学 情報科学研究科

開催した研究集会

1. JAIST 群馬大学 共同ワークショップ
   期間: 2012 年 8 月 31 日–9 月 1 日
   場所: 群馬大学伊香保研修所
   講演者: 浅野哲夫 (JAIST), 大舘陽太 (JAIST), 中野眞一 (群馬大), 天野一幸 (群馬大）, 山崎浩一 (群馬大)

招聘研究者

1. Pascal Schweitzer ()
   期間: 2012年7月 11日 ～ 2013年1月 31日
   受入: 北陸先端科学技術大学院大学

アウトリーチ活動

1. 上原 隆平:
   JAIST ギャラリー立ち上げ (研究紹介展示), 2012 年 9 月.
2. 上原 隆平:
   ３通りの箱が折れる展開図 (研究解説記事), 『数学セミナー』, 日本評論社, 2012 年 11 月.
3. 上原 隆平:
   バルセロナ UPC での講演, The Graph Isomorphism Problem on Geometric graph classes, 2013 年 1 月 16 日.
4. 上原 隆平:
   ブリュッセル ULB での講演, Common developments of two or more polyhedra, 2013 年 1 月 30 日.
5. 小野 廣隆:
   九州大学経済学部オープンキャンパス・模擬講義 (研究紹介), 2012 年 8 月 5 日.

学術論文

1. Tetsuo Asano:
   In-place Algorithm for Erasing a Connected Component in a Binary Image, *Theory of Computing Systems,* 50(1), 111–123, 2012.
2. Tetsuo Asano, Erik D. Demaine, Martin L. Demaine, and Ryuhei Uehara:
   NP-completeness of generalized Kaboozle, *Journal of Information Processing,* Vol. 20, No. 3, 713-718, 2012.
3. Tetsuo Asano, Jesper Jansson, Kunihiko Sadakane, Ryuhei Uehara, and Gabriel Valiente:
   Faster Computation of the Robinson-Foulds Distance between Phylogenetic Networks, *Information Sciences,* Vol. 197, 77-90, 2012.

4. Brad Ballinger, Nadia Benbernou, Prosenjit Bose, Mirela Damian, Erik D. Demaine, Vida Dujmovic, Robin Flatland, Ferran Hurtado, John Iacono, Anna Lubiw, Pat Morin, Vera Sacristan, Diane Souvaine, and Ryuhei Uehara:
Coverage with k-Transmitters in the Presence of Obstacles, *Journal of Combinatorial Optimization,* Vol. 25(2), 208-233, 2013.

5. David Charlton, Erik D. Demaine, Martin L. Demaine, Vida Dujmovic, Pat Morin, and Ryuhei Uehara:
Ghost Chimneys, *International Journal of Computational Geometry and Applications,* Vol. 22, No. 3, 207–214, 2012.

6. Takehiro Ito, Yuichiro Miyamoto, Hirotaka Ono, Hisao Tamaki, and Ryuhei Uehara:
Route-Enabling Graph Orientation Problems, *Algorithmica,* Vol. 65, 317-338, 2013.

7. Masashi Kiyomi, Toshiki Saitoh, and Ryuhei Uehara:
Bipartite Permutation Graphs are Reconstructible, *Discrete Mathematics, Algorithms and Applications,* Vol. 4, No. 3, 1250039:1–14, 2012.

8. Ryu Mizoguchi, Hirotaka Ono, Shuji Kijima, and Masafumi Yamashita:
On space complexity of self-stabilizing leader election in mediated population protocol, *Distributed Computing,* 25(6), 451–460, 2012.

9. Yoshio Okamoto, Yota Otachi, and Ryuhei Uehara:
On bipartite powers of bigraphs, *Discrete Mathematics and Theoretical Computer Science,* Vol. 14, No.2, 11–20, 2012.

10. Yosuke Okayama, Masashi Kiyomi, and Ryuhei Uehara:
On Covering of Any Point Configuration by Disjoint Unit Disks, *Geombinatorics,* vol. XXI(1), 14-23, 2012.

11. Tetsuo Asano and Revant Kumar:
A Small-Space Algorithm for Removing Small Connected Components from a Binary Image, *IEICE Trans. EA, Special Section on Discrete Mathematics and Its Applications,* (掲載予定).

12. Masashi Kiyomi, Toshiki Saitoh, and Ryuhei Uehara:
Reconstruction Algorithms for Permutation Graphs and Distance-Hereditary Graphs, *IEICE Trans. Inf. & Syst.,* E96-D (3), (掲載予定).

13. Matsuo Konagaya and Tetsuo Asano:
Algorithm for Reporting All Segment Intersections Using Work Space of Arbitrary Size, *IEICE Trans. EA, Special Section on Discrete Mathematics and Its Applications,* (掲載予定).

14. Shin-ichi Nakano, Ryuhei Uehara, and Takeaki Uno:
Efficient algorithms for a simple network design problem, *Networks,* (掲載予定).

15. Ryuhei Uehara:
Tractabilities and Intractabilities on Geometric Intersection Graphs, *Algorithms,* (掲載予定).

16. Takuya Umesato, Toshiki Saitoh, Ryuhei Uehara, Hiro Ito, and Yoshio Okamoto:
Complexity of the stamp folding problem, *Theoretical Computer Science,* (掲載予定).

17. Zachary Abel, Erik D. Demaine, Martin L. Demaine, Takashi Horiyama and Ryuhei Uehara:
Computational Complexity of Piano-Hinged Dissections, *Proc. The European Workshop on Computational Geometry (EuroCG 2013),* 2013.

18. Greg Aloupis, Robert Hearn, Hirokazu Iwasawa and Ryuhei Uehara:
Covering points with disjoint unit disks,

Proc. The 24th Canadian Conference on Computational Geometry (CCCG 2012), 49–54, 2012.

19. Tetsuo Asano and Sergey Bereg:
A New Framework for Connected Components Labeling of Binary Images, *Proc. the 15th International Workshop on Combinatorial Image Analysis,* 90–102, 2012.

20. Tetsuo Asano, Sergey Bereg, and Lilian Buzer:
Small Work Space Algorithms for Some Basic Problems on Binary Images, *Proc. the 15th International Workshop on Combinatorial Image Analysis,* 103–114, 2012.

21. Tetsuo Asano, Kevin Buchin, Maike Buchin, Matias Korman, Wolfgang Mulzer, Gunter Rote, and Andre Schulz:
Memory-Constrained Algorithms for Simple Polygons, *Proc. European Workshop on Computational Geometry,* 2012.

22. Jinhee Chun, Takashi Horiyama, Takehiro Ito, Natsuda Kaothanthong, Hirotaka Ono, Yota Otachi, Takeshi Tokuyama, Ryuhei Uehara and Takeaki Uno:
Base location problems for base-monotone regions, *Proc. 7th International Workshop on Algorithms and Computation (WALCOM 2013), Lecture Notes in Computer Science,* 7748, 53–64, 2013.

23. Hiroyuki Fukui, Ryuhei Uehara, Takeaki Uno and Yushi Uno:
On Complexity of Flooding Games on Graphs with Interval Representations, *Proc. Thailand-Japan Joint Conference on Computational Geometry and Graphs (TJJCCGG 2012),* 2012.

24. Takashi Horiyama, Takehiro Ito, Natsuda Kaothanthong, Hirotaka Ono, Yota Otachi, Takeshi Tokuyama, Ryuhei Uehara, and Takeaki Uno:
Algorithms for Computing Optimal Image Segmentation using Quadtree Decomposition, *Proc. Thailand-Japan Joint Conference on Computational Geometry and Graphs (TJJCCGG 2012),* 2012.

25. Takashi Horiyama, Takehiro Ito, Keita Nakatsuka, Akira Suzuki and Ryuhei Uehara:
Packing Trominoes is NP-Complete, #P-hard and ASP-Complete, *Proc. The 24th Canadian Conference on Computational Geometry (CCCG 2012),* 219–224, 2012.

26. Takehiro Ito, Shin-Ichi Nakano, Yoshio Okamoto, Yota Otachi, Ryuhei Uehara, Takeaki Uno and Yushi Uno:
A Polynomial-Time Approximation Scheme for the Geometric Unique Coverage Problem on Unit Squares, *Proc. 13th Scandinavian Symposium and Workshops on Algorithm Theory (SWAT 2012), Lecture Notes in Computer Science,* 7357, 24–35, 2012.

27. Takehiro Ito, Shin-Ichi Nakano, Yoshio Okamoto, Yota Otachi, Ryuhei Uehara, Takeaki Uno, and Yushi Uno:
A 4.31-Approximation for the Geometric Unique Coverage Problem on Unit Disks, *Proc. 23rd Annual International Symposium on Algorithms and Computation (ISAAC 2012), Lecture Notes in Computer Science,* 7676, 372–381, 2012.

28. Masashi Kiyomi, Yoshio Okamoto and Toshiki Saitoh:
Efficient Enumeration of the Directed Binary Perfect Phylogenies bibliographical record in from Incomplete Data, *Proc. SEA,* 248–259, 2012.

29. Toshihiro Shirakawa and Ryuhei Uehara:
Common Developments of Three Different Orthogonal Boxes, *Proc. The 24th Canadian Conference on Computational Geometry (CCCG 2012),* 19–23, 2012.

研究会等

1. 垂井淳:
   計算の複雑さと証明の複雑さ（招待講演）, 京大数理研研究集会「証明論と複雑性」, 京大数理研講究録, 2012 年 9 月.

2. Jun Tarui:
   Complexity of Finding a Duplicate in a Stream（招待講演）, *NII Shonan Meeting "Large-Scale Distributed Computation"*, 2012 年 1 月.

文部科学省科学研究費補助金 新学術領域研究 (課題番号 24106005)

B01: 最適化技法との融合による計算限界解析法の深化

研究代表者： 加藤 直樹　京都大学 工学研究科
研究分担者： 岩田 覚　東京大学 情報理工学系研究科
岡本 吉央　電気通信大学 情報理工学研究科
来嶋 秀治　九州大学 システム情報科学研究科
神山 直之　九州大学 マス・フォア・インダストリ研究所

開催した研究集会

1. ELC Mini-Workshop (B01)
   期間: 2012 年 9 月 5 日 ～ 9 月 7 日
   場所: 京都大学 桂キャンパス
   講演者: 上野 賢哉 (京都大学), 内澤 啓 (東北大学), 岡本 吉央 (電気通信大学)

2. 国際研究集会「Discrete Convexity and Optimization (離散凸性と最適化)」
   期間: 2013 年 10 月 15 日 ～ 10 月 18 日
   場所: 京都大学数理解析研究所
   Kristof Berczi, 福永拓郎, 平井広志, Tibor Jordan, Viktoria Kaszanitzky, Tamas Kiraly, Gleb Koshevoy, S. Thomas McCormick, 室田一雄, Sang-il Oum, 高澤兼二郎, 谷川眞一, Prasad Tetali, Louis Theran, Standa Zivny

招聘研究者

1. Kristóf Bérczi (Eötvös Loránd University)
   期間: 2012 年 10 月 13 日 ～ 10 月 20 日
   受入: 京都大学

2. Viktória Kaszanitzky (Eötvös Loránd University)
   期間: 2012 年 10 月 13 日 ～ 10 月 25 日
   受入: 京都大学

3. Tamás Király (Eötvös Loránd University)
   期間: 2012 年 10 月 12 日 ～ 10 月 19 日
   受入: 京都大学

4. 今道貴司 (日本アイ・ビー・エム株式会社 東京基礎研究所)
   期間: 2012 年 11 月 28 日 ～ 11 月 30 日
   受入: 九州大学

アウトリーチ活動

1. 横尾真, 岩崎敦, 櫻井祐子, 岡本吉央: 『計算機科学者のためのゲーム理論入門』シリーズについて, コンピュータ ソフトウェア, 29, 2_65–2_68, 2012.

2. 横尾真, 岩崎敦, 櫻井祐子, 岡本吉央: 『計算機科学者のためのゲーム理論入門』シリーズ第 1 回 非協力ゲーム（基礎編）, コンピュータ ソフトウェア, 29, 2_69–2_84, 2012.

3. 横尾真, 岩崎敦, 櫻井祐子, 岡本吉央: 『計算機科学者のためのゲーム理論入門』シリーズ第 2 回 非協力ゲーム（発展編）, コンピュータ ソフトウェア, 29, 3_39–3_53, 2012.

4. 横尾真, 岩崎敦, 櫻井祐子, 岡本吉央: 『計算機科学者のためのゲーム理論入門』シリーズ第 3 回 メカニズムデザイン（基礎編）, コンピュータ ソフトウェア, 29, 4_15–4_31, 2012.

5. 横尾真, 岩崎敦, 櫻井祐子, 岡本吉央: 『計算機科学者のためのゲーム理論入門』シリーズ第 4 回 メカニズムデザイン（応用編）, コンピュータ ソフトウェア, 30, 1_34–1_52, 2013.

6. 岡本吉央:
グラフを通したパズル・ゲームの一般化, オペレーションズ・リサーチ, 58(3), 161–166, 2013.

7. 岡本吉央:
列挙の基本と基礎的なアルゴリズム, 電子情報通信学会誌, 95(6), 477–483, 2012.

8. 岡本吉央:
エレガントな解答を求む (出題), 数学セミナー, 2013 年 2 月号, 2013.

9. 岡本吉央:
エレガントな解答を求む (解答), 数学セミナー, 2013 年 5 月号, 2013.

10. 神山直之:
離散最適化入門, 平成 24 年度九州大学オープンキャンパス理学部学科企画, 2012 年 8 月 4 日.

受賞

1. 岡本吉央:
日本 OR 学会第 2 回研究奨励賞, 2012 年 9 月.

著書

1. N. Katoh and A. Takizawa:
Emerging Pattern Based Analysis of Crime Spots and Rental Price (in Contrast Data Mining: Concepts, Algorithms and Applications), Chapman & Hall/CRC, 2012.

2. N. Katoh, A. Shioura and T. Ibaraki:
Resource Allocation Problems (in Handbook of Combinatorial Optimization, 2nd ed.), Kluwer Academic Publishers, 2013.

学術論文

1. N. Katoh, S. Tanigawa:
Rooted-tree Decompositions with Matroid Constraints and the Infinitesimal Rigidity of Frameworks with Boundaries, *SIAM J. Discrete Mathematics,* to appear.

2. Y. Higashikawa, N. Katoh:
Online Vertex Exploration Problems in a Simple Polygon, *IEICE Transaction on Fundamentals,* to appear.

3. Y. Higashikawa, N. Katoh, S. Langerman, S. Tanigawa:
Online Graph Exploration Algorithms for Cycles and Trees by Multiple Searchers, *J. Combinatorial Optimization,* to appear.

4. A. Frank, S. Fujishige, N. Kamiyama, N. Katoh:
Independent Arborescences in Directed Graphs, *Discrete Mathematics,* 313(4), 453-459, 2013.

5. M. X. Goemans, S. Iwata, R. Zenklusen:
A Flow Model Based on Polylinking Systems, *Mathematical Programming,* 135(1-2), 1-23, 2012.

6. T. Itoko, S. Iwata:
Computational Geometric Approach to Submodular Function Minimization for Multiclass Queueing Systems, *Japan J. Industrial and Applied Mathematics,* 29, 453-468, 2012.

7. S. Boyd, S. Iwata, K. Takazawa:
Finding 2-Factors Closer to TSP Tours in Cubic Graphs, *SIAM J. Discrete Mathematics,* 27, 918-939, 2013.

8. M. F. Balcan, F. Constantin, S. Iwata, L. Wang:
Learning Valuation Functions, *Proceedings of COLT,* 4-24, 2012.

9. S. Iwata, P. Tetali, and P. Tripathi:
Approximating Minimum Linear Ordering Problems, *Proceedings of APPROX,* LNCS 7408, 206-217, 2012.

10. S. Iwata, R. Ravi:
Approximating Max-Min Weighted T-joins, *Operations Research Letters,* 41, 321-324, 2013.

11. S. Iwata, M. Takamatsu:
Computing the Maximum Degree of Minors in Mixed Polynomial Matrices via Combinatorial Relaxation, *Algorithmica,* 66, 346–368, 2013.

12. S. W. Bae, Y. Okamoto:
Querying Two Boundary Points for Shortest Paths in a Polygonal Domain, *Computational Geometry: Theory and Applications,* 45, 284-293, 2012.

13. W. Didimo, M. Kaufmann, G. Liotta, Y. Okamoto, A. Spillner:
Vertex Angle and Crossing Angle Resolution of Leveled Tree Drawings, *Information Processing Letters,* 112, 630-635, 2012.

14. M. Hoffmann, J. Matousek, Y. Okamoto, P. Zumstein:
Minimum and Maximum against k Lies, *Chicago Journal of Theoretical Computer Science,* Article 2, 1-10, 2012.

15. H. Toyoizumi, S. Tani, N. Miyoshi, Y. Okamoto:
Reverse Preferential Spread in Complex Networks, *Physical Review E,* 86(2), 021103, 2012.

16. Y. Okamoto, Y. Otachi, R. Uehara:
On Bipartite Powers of Bigraphs, *Discrete Mathematics & Theoretical Computer Science,* 14(2), 11-20, 2012.

17. M. Kiyomi, Y. Okamoto, T. Saitoh:
Efficient Enumeration of the Directed Binary Perfect Phylogenies from Incomplete Data, *Proceedings of SEA,* LNCS 7276, 248-259, 2012.

18. T. Ito, S. Nakano, Y. Okamoto, Y. Otachi, R. Uehara, T. Uno, Y. Uno:
A Polynomial-Time Approximation Scheme for the Geometric Unique Coverage Problem on Unit Squares, *Proceedings of SWAT,* LNCS 7357, 24-35, 2012.

19. M. Cygan, H. Dell, D. Lokshtanov, D. Marx, J. Nederlof, Y. Okamoto, R. Paturi, S. Saurabh, M. Wahlström:
On problems as hard as CNF-SAT, *Proceedings of CCC,* 74-84, 2012.

20. T. Ito, S. Nakano, Y. Okamoto, Y. Otachi, R. Uehara, T. Uno, Y. Uno:
A 4.31-Approximation for the Geometric Unique Coverage Problem on Unit Disks, *Proceedings of ISAAC,* LNCS 7676, 372-381, 2012.

21. P. Angelini, C. Binucci, W. Evans, F. Hurtado, G. Liott, T. Mchedlidze, H. Meijer, Y. Okamoto:
Universal Point Subsets for Planar Graphs, *Proceedings of ISAAC,* LNCS 7676, 423-432, 2012.

22. S. W. Bae, Y. Okamoto, C. Shin:
Area Bounds of Rectilinear Polygons Realized by Angle Sequences, *Proceedings of ISAAC,* LNCS 7676, 629-638, 2012.

23. R. Mizoguchi, H. Ono, S. Kijima, M. Yamashita:
On space complexity of self-stabilizing leader election in mediated population protocol, *Distributed Computing,* 25(6), 451–460, 2012.

24. S. Kijima, Y. Otachi, T. Saitoh, T. Uno:
Subgraph isomorphism in graph classes, *Discrete Mathematics,* 312(21), 3164–3173, 2012.

25. S. Kijima, S. Tanigawa:
Sparsity and connectivity of medial graphs: concerning two edge-disjoint Hamiltonian paths in planar rigidity circuits, *Discrete Mathematics,* 312(16), 2466–2472, 2012.

26. N. Fujinaga, Y. Yamauchi, S. Kijima, M. Yamashita:
Asynchronous pattern formation by anonymous oblivious mobile robots, *Proceedings of DISC,* LNCS 7611, 312–325, 2012.

27. Y. Yamauchi, S. Tixeuil, S. Kijima, M. Yamashita:
Brief Announcement: Probabilistic Stabilization under Probabilistic Schedulers, *Proceedings of DISC,* LNCS 7611, 413–414, 2012.

28. D. Suehiro, K. Hatano, S. Kijima, E. Takimoto, K. Nagano:
Online prediction under submodular constraints, *Proceedings of ALT,* LNCS 7568, 260–274, 2012.

29. Y. Hosaka, Y. Yamauchi, S. Kijima, H. Ono, M. Yamashita:
An extension of Matthews' bound to multiplex random walks, *Proceedings of IPDPS,* 872–877, 2012.

30. N. Kamiyama:
A Note on the Quasi-additive Bound for Boolean Functions, *Journal of Math-for-Industry,* 4-B, 119–122, 2012.

31. N. Kamiyama:
On Counting Output Patterns of Logic Circuits, *MI Preprint Series (Kyushu University),* 2013-4, 2013.

32. N. Kamiyama:
Matroid Intersection with Priority Constraints, *Journal of the Operations Research Society of Japan,* 56(1), 15–25, 2013.
Naoyuki Kamiyama Robustness of Minimum Cost Arborescences Japan Journal of Industrial and Applied Mathematics 29(3)3 485–497 2012

33. S. Fujishige, N. Kamiyama:
The Root Location Problem for Arc-disjoint Arborescences, *Discrete Applied Mathematics,* 160(13-14), 1964–1970, 2012.

研究会等

1. 清見礼，岡本吉央，斎藤寿樹:
不完全データと矛盾しない有向二値完全系統樹を列挙する効率的手法, COMP 研 6 月研究会, 2012 年 6 月.

2. 並河雄紀，岡本吉央，大舘陽太:
施設配置ゲームにおける仁・シャープレイ値の計算について, COMP 研 10 月研究会, 2012 年 10 月.

3. 並河雄紀，岡本吉央，大舘陽太:
費用 2 種類の施設配置ゲームの仁とシャープレイ値の計算について, AL 研 3 月研究会, 2013 年 3 月.

4. 園田尚人，山内由紀子, 来嶋秀治, 山下雅史:
ストリームに対する $O(\log \log n)$ 領域を用いた Reservoir sampling, COMP 研 3 月研究会, 2013 年 3 月.

5. 園田尚人，山内由紀子, 来嶋秀治, 山下雅史:
複数ストリーム間の特徴比較に対する乱択アルゴリズム, 2012 年度冬の LA シンポジウム, 2013 年 1 月.

6. 木場孝輔，山内由紀子, 来嶋秀治, 山下雅史:
動的グラフ上のランダムウォークの到達時間と全訪問時間, 2012 年度冬の LA シンポジウム, 2013 年 1 月.

7. タウフィックラチマン，山内由紀子, 来嶋秀治, 山下雅史:
分散システムでの剛性グラフに対する局所交換可能性, 2012 年度冬の LA シンポジウム, 2013 年 1 月.

8. 三原勇治，山内由紀子, 来嶋秀治, 山下雅史:
森および連結全域部分グラフの乱択近似数え上げ, 2012 年度冬の LA シンポジウム, 2013 年 1 月.

9. 佐々木徹，山内由紀子, 来嶋秀治, 山下雅史:
完全 k 部グラフにおける移動ビザンチン合意アルゴリズムの提案, 日本 OR 学会九州支部第 3 回若手 OR 研究交流会, 2012 年 10 月.

10. 平川瑞樹，山内由紀子, 来嶋秀治, 山下雅史:
ポピュラーマッチングの解構造に対する一考察, 日本 OR 学会九州支部第 3 回若手 OR 研究交流会, 2012 年 10 月.

11. 西山宏，山内由紀子, 来嶋秀治, 山下雅史:
パリティ最長路の存在性, 日本OR学会九州支部第3回若手OR研究交流会, 2012年10月.

12. 山内由紀子，神山直之, 来嶋秀治, 大舘陽太:
Transitivity in Distributed Systems using Exchange Property of Matroid Bases, 2012年度夏のLAシンポジウム, 2012年7月.

13. 三原勇治，山内由紀子, 来嶋秀治, 山下雅史:
森および連結全域部分グラフに対するブロックマトロイドのbases-cobasesグラフについて, 2012年度夏のLAシンポジウム, 2012年7月.

14. 末廣大貴，畑埜晃平, 来嶋秀治, 瀧本英二, 永野清仁:
基多面体上のオンライン予測, 2012年度夏のLAシンポジウム, 2012年7月.

15. D. Suehiro, K. Hatano, S. Kijima, E. Takimoto, K. Nagano:
Online Prediction under Submodular Constraints, 第*9*回情報論的学習理論と機械学習研究会, 2012年6月.

16. 神山直之:
離散最適化〜ネットワークフローを中心に〜, IMIチュートリアル「数学モデリングの基礎と展開」, 2013年2月.

17. 神山直之:
最速輸送問題, 京都大学数理解析研究所研究集会共同研究「組合せ最適化セミナー」, 2012年7月.

学会大会等

1. 三原勇治，山内由紀子, 来嶋秀治, 山下雅史:
森および連結全域部分グラフの乱択近似数え上げ, 電子情報通信学会2013年総合大会, 2013年3月.

2. 穂坂祐輔，山内由紀子, 来嶋秀治, 山下雅史:
ランダムウォークの定常分布と到達時間および全訪問時間の関係, 電子情報通信学会2013年総合大会, 2013年3月.

3. 木場孝輔，山内由紀子, 来嶋秀治, 山下雅史:
動的グラフ上のランダムウォークの到達時間と全訪問時間, 電子情報通信学会2013年総合大会, 2013年3月.

4. 西山宏，山内由紀子, 来嶋秀治, 山下雅史:
パリティ最長路問題, 日本OR学会2013年春季研究発表会, 2013年3月.

5. タウフィックラチマン，山内由紀子, 来嶋秀治, 山下雅史:
ラーマングラフの局所遷移可能性, 日本OR学会2013年春季研究発表会, 2013年3月.

6. K. Koba, Y. Yamauchi, S. Kijima, M. Yamashita:
Hitting Time and Cover Time on Dynamic Graphs, In ACCMCC, 2012年12月.

7. Y. Hosaka, Y. Yamauchi, S. Kijima, M. Yamashita:
Fast Random Walk and its Stationary Distribution, In ACCMCC, 2012年12月.

8. 西山宏，山内由紀子, 来嶋秀治, 山下雅史:
パリティ最長路問題, 平成24年度電気関係学会九州支部連合大会, 2012年9月.

9. 平川瑞樹，山内由紀子, 来嶋秀治, 山下雅史:
安定結婚問題におけるポピュラーマッチングの解構造に対する一考察, 平成24年度電気関係学会九州支部連合大会, 2012年9月.

10. 佐々木徹，山内由紀子, 来嶋秀治, 山下雅史:
完全k部グラフにおける移動ビザンチン合意問題アルゴリズムの提案, 平成24年度電気関係学会九州支部連合大会, 2012年9月.

11. T. Rachman，山内由紀子, 来嶋秀治, 山下雅史:
剛性グラフに対する局所交換可能性, 平成24年度電気関係学会九州支部連合大会, 2012年9月.

12. 神山直之:
パレート安定マッチング問題に対する新算法, 日本オペレーションズ・リサーチ学会春季研究発表会, 2013年3月.

文部科学省科学研究費補助金 新学術領域研究 (課題番号 24106007)

B02: 大規模数理計画による計算限界解析法の展開

研究代表者：	David Avis	京都大学　大学院　情報学研究科　&　McGill University
研究分担者：	天野 一幸	群馬大学 大学院 工学研究科
	上野 賢哉	京都大学 白眉センター
研究協力者：	福田 公明	ETH Zurich
	Antoine Deza	McMaster University
	Oliver Friedmann	University of Munich
	Samuel Fiorini	Universite Libre de Bruxelles
	Hans Raj Tiwary	Universite Libre de Bruxelles

開催した研究集会

1. ELC Mini-Workshop (B02, B03)
   期間: 2012 年 10 月 28 日 ～ 10 月 29 日
   場所: 宮城県 仙台市 秋保温泉
   講演者: 徳山 豪 (東北大学), David Avis (京都大学), Peter Eades (University of Sydney), Hans Raj Tiwary (ULB), 堀山 貴史 (埼玉大学), 宇野 毅明 (NII), 渋谷 哲朗 (東京大学), 上野 賢哉 (京都大学)

招聘研究者

1. Hans Raj Tiwary (Universite Libre de Bruxelles)
   期間: 2012 年 10 月 3 日 ～ 11 月 30 日
   受入: 京都大学

2. Stefan Langerman (McGill University)
   期間: 2013 年 1 月 7 日 ～ 1 月 13 日
   受入: 京都大学

アウトリーチ活動

1. 天野 一幸:
   出張講義「計算の科学」, 埼玉県立与野高等学校, 2012 年 12 月 17 日.

2. 上野 賢哉:
   異分野融合ワークショップ「科学の限界に舞う小さな青い鳥 – 人文・社会・自然科学を含む全ての学術領域のために」 (講演・討論), 2013 年 3 月 11 日.

学術論文

1. Yoshikazu Aoshima, David Avis, Theresa Deering, Yoshitake Matsumoto, Sonoko Moriyama:
   On the existence of Hamiltonian paths for history based pivot rules on acyclic unique sink orientations of hypercubes, *Discrete Applied Mathematics,* 160 (15), 2104-2115, 2012.

2. David Avis, Hiroyuki Miyata, Sonoko Moriyama:
   Families of polytopal digraphs that do not satisfy the shelling property, *Computational Geometry,* 46(3), 382-393, 2013.

3. David Avis, Hans Raj Tiwary:
   On the extension complexity of combinatorial polytopes, *Proc. 40th International Colloquium on Automata, Languages and Programming (ICALP 2013),* (掲載予定).

4. Kazuyuki Amano:
   On Extremal k-CNF Formulas, *European Journal of Combinatorics,* (掲載予定).

5. Kenya Ueno:
Formula Complexity of Ternary Majorities, *Proc. 18th Annual International Computing and Combinatorics Conference (COCOON 2012),* LNCS 7434, 433-444, 2012.

6. Komei Fukuda, Hiroyuki Miyata, Sonoko Moriyama:
Complete Enumeration of Small Realizable Oriented Matroids, *Discrete & Computational Geometry,* 49(2), 359-381, 2013.

7. Andrew Baker, Antoine Deza, Frantisek Franek:
On the structure of run-maximal strings, *Journal of Discrete Algorithms,* 10, 10-14, 2012.

8. Antoine Deza, Frantisek Franek, Min Jing Liu:
On a conjecture of Erdos for multiplicities of cliques, *Journal of Discrete Algorithms,* 17, 9-14, 2012.

9. Antoine Deza, Tamon Stephen, Feng Xie:
A Note on Lower Bounds for Colourful Simplicial Depth, *Symmetry,* 5(1), 47-53, 2013.

10. Antoine Deza, Frantisek Franek, Mei Jiang:
A Computational Framework for Determining Square-maximal Strings, *Stringology 2012,* 111-119, 2012.

11. Oliver Friedmann, Martin Lange:
Two Local Strategy Iteration Schemes for Parity Game Solving, *International Journal of Foundations of Computer Science,* 23(3), 669-685, 2012.

12. Oliver Friedmann, Martin Lange:
Ramsey-Based Analysis of Parity Automata, *Proc. 18th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2012),* LNCS 7214, 64-78, 2012.

13. Samuel Fiorini, Thomas Rothvos, Hans Raj Tiwary:
Extended Formulations for Polygons, *Discrete & Computational Geometry,* 48(3), 658-668, 2012.

14. Samuel Fiorini, Gwenael Joret, Dirk Oliver Theis, David R. Wood:
Small minors in dense graphs, *European Journal of Combinatorics,* 33(6), 1226-1245, 2012.

15. Jean Cardinal, Samuel Fiorini, Gwenael Joret:
Minimum Entropy Combinatorial Optimization Problems, *Theory of Computing Systems,* 51(1), 4-21, 2012.

16. Gabor Braun, Samuel Fiorini, Sebastian Pokutta, David Steurer:
Approximation Limits of Linear Programs (Beyond Hierarchies), *Proc. IEEE 53rd Annual Symposium on Foundations of Computer Science (FOCS 2012),* 480-489, 2012.

17. Therese C. Biedl, Stephane Durocher, Celine Engelbeen, Samuel Fiorini, Maxwell Young:
Faster optimal algorithms for segment minimization with small maximal value, *Discrete Applied Mathematics,* 161(3), 317-329, 2013.

18. Samuel Fiorini, Volker Kaibel, Kanstantsin Pashkovich, Dirk Oliver Theis:
Combinatorial bounds on nonnegative rank and extended formulations, *Discrete Mathematics,* 313(1), 67-83, 2013.

19. Jean Cardinal, Erik D. Demaine, Samuel Fiorini, Gwenael Joret, Ilan Newman, Oren Weimann:
The Stackelberg minimum spanning tree game on planar and bounded-treewidth graphs, *Journal of Combinatorial Optimization,* 25(1), 19-46, 2013.

20. Barry Balof, Jean-Paul Doignon, Samuel Fiorini:

The Representation Polyhedron of a Semiorder, *Order,* 30(1), 103-135, 2013.

文部科学省科学研究費補助金 新学術領域研究 (課題番号 24106007)

B03: 計算限界解析法から革新的データ構造化技術への展開

研究代表者： 徳山 豪　東北大学 大学院 情報科学研究科
研究分担者： 宇野 毅明　国立情報学研究所 情報学プリンシプル研究系
渋谷 哲朗　東京大学 医科学研究所
堀山 貴史　埼玉大学 情報メディア基盤センター
連携研究者： 定兼 邦彦　国立情報学研究所 情報学プリンシプル研究系

開催した研究集会

1. ELC Mini-Workshop (B02, B03)
   期間: 2012 年 10 月 28 日 ～ 10 月 29 日
   場所: 開催場所: 秋保温泉　ホテル瑞鳳
   講演者: 徳山豪 (東北大学), 上野賢哉 (京都大学), Hans Tiwary (ULB), 堀山貴史 (埼玉大学), Problem session 話題提供：宇野毅明 (NII), 渋谷哲朗 (東京大学), David Avis (京都大学), Peter Eades (シドニー大学)

招聘研究者

1. Peter Eades (University of Sydney)
   期間: 2012 年 10 月 23 日 ～ 11 月 1 日
   受入: 東北大学

2. Matias Korman (カタロニア工科大学)
   期間: 2013 年 2 月 27 日 ～ 3 月 9 日
   受入: 東北大学

3. Sang Won Bae (Kyongi University)
   期間: 2012 年 9 月 19 日 ～ 9 月 23 日
   受入: 東北大学

受賞

1. 徳山 豪:
   電子情報通信学会 フェロー,
   2012 年 9 月 12 日.
   幾何学構造を利用したアルゴリズム理論の開拓とその応用.

アウトリーチ活動

1. 徳山豪:
   理論計算機科学への招待, 科学者の卵プロジェクト (スクール講演), 2012 年 9 月 8 日.

2. Takeaki Uno:
   Deep of Enumeration Algorithms: Theory and Practice, Enumeration Algorithms & Exact Methods For Exponential Problems in Computational Biology, (招待チュートリアル講演), 2012 年 9 月 25 日, 26 日.

3. Takashi Horiyama:
   Edge unfoldings of Platonic solids never overlap, Polyhedral Computation: Theory, Practice and Applications in Engineering and Science, International Courses in Communications and Computer Engineering, Kyoto University, 2012 年 12 月.

著書

1. Tetsuo Shibuya, Hisashi Kashima, Jun Sese, and Shandar Ahmad (Eds):
   Pattern Recognition in Bioinformatics — 7th IAPR International Conference, (PRIB 2012). LNCS 7632, Springer, 2012.

学術論文

1. Akitoshi Kawamura, Jiri Matousek, Takeshi Tokuyama:
   Zone Diagrams in Euclidean Spaces and

in Other Normed Spaces, *Mathematish Anallen,* 354-4, 1201–1221, 2012.

2. Jinhee Chun, Natsuda Kaothanthong, Ryosei Kasai, Matias Korman, Martin Nollenburg, Takeshi Tokuyama:
   Algorithms for computig the maximum weight region decomposable into elementary shapes, *Computer Vision and Image Understanding,* 116 (7), 803–814, 2012.

3. Hee-Kap Ahn, Sang Won Bae, Otfried Cheong, Joachim Gudmundsson, Takeshi Tokuyama, Antoine Vigneron:
   A Generalization of the Convex Kakeya Problem, *In Proc. of Latin American Symposium on Theoretical Informatics (LATIN 2012),* LNCS 7256, 1–12, 2012.

4. Jinhee Chun, Akiyoshi Shioura, Truong Minh Tien and Takeshi Tokuyama:
   A Unified View to Greedy Geometric Routing Algorithms in Ad Hoc Networks, *In Proc. of the 8th International Symposium on Algorithms for Sensor Systems, Wireless Ad Hoc Networks and Autonomous Mobile Entities (ALGOSENSORS 2012),* LNCS 7718, 54–65, 2012.

5. Kunihiro Wasa, Yusaku Kaneta, Takeaki Uno, Hiroki Arimura:
   Constant Time Enumeration of Bounded-Size Subtrees in Trees and Its Application, *In Proc. of the 18th Annual International Computing and Combinatorics Conference (COCOON 2012),* 347–359, 2012.

6. Takashi Horiyama, Takehiro Ito, Keita Nakatsuka, Akira Suzuki, Ryuhei Uehara:
   Packing Trominoes is NP-Complete, #P-hard and ASP-Complete, *In Proc. of the 24th Canadian Conference on Computational Geometry (CCCG 2012),* 219–224, 2012 年 8 月.

7. Genki Terashi, Tetsuo Shibuya, and Mayuko Takeda-Shitaka:
   LB3D: a protein 3D substructure search program based on the lower bound of a RMSD value, *Journal of Computational Biology,* 19 (5), 493–503, 2012.

8. Tetsuo Asano, Jesper Jansson, Kunihiko Sadakane, Ryuhei Uehara, Gabriel Valiente:
   Faster Computation of the Robinson-Foulds Distance between Phylogenetic Networks, *Information Sciences,* 197, 77–90, 2012 年 8 月.

9. Xin Man, Takashi Horiyama, Shinji Kimura:
   Automatic Multi-Stage Clock Gating Optimization Using ILP Formulation, *IEICE Transactions on Fundamentals,* E95-A (8), 1347–1358, 2012 年 8 月.

10. Takeaki Uno:
    Deep of Enumeration Algorithm —Theory and Practice— (Invited talk), *Enumeration Algorithms & Exact Methods,* 2012 年 9 月.

11. Gonzalo Navarro, Kunihiko Sadakane:
    Fully-Functional Static and Dynamic Succinct Trees, *ACM Transactions on Algorithms,* 2012 年 9 月.

12. Shuji Kijima, Yota Otachi, Toshiki Saitoh, Takeaki Uno:
    Subgraph isomorphism in graph classes, *Discrete Mathematics,* 312 (21), 3164–3173, 2012.

13. Takehiro Ito, Shin-Ichi Nakano, Yoshio Okamoto, Yota Otachi, Ryuhei Uehara, Takeaki Uno, Yushi Uno:
    A 4.31-Approximation for the Geometric Unique Coverage Problem on Unit Disks, *In Proc. of the 23rd Annual International Symposium on Algorithms and Computation (ISAAC 2012),* LNCS 7676, 372–381, 2012 年 12 月.

14. Takeaki Uno:
    Efficient Computation of Power Indices for

Weighted Majority Games, *In Proc. of the 23rd Annual International Symposium on Algorithms and Computation (ISAAC 2012),* LNCS 7676, 679–689, 2012 年 12 月.

15. Takehiro Ito, Shin-Ichi Nakano, Yoshio Okamoto, Yota Otachi, Ryuhei Uehara, Takeaki Uno, Yushi Uno:
A Polynomial-Time Approximation Scheme for the Geometric Unique Coverage Problem on Unit Squares, *In Proc. of the 13th Scandinavian Symposium and Workshops on Algorithm Theory (SWAT 2012),* 24–35, 2012 年.

16. Jinhee Chun, Takashi Horiyama, Takehiro Ito, Natsuda Kaothanthong, Hirotaka Ono, Yota Otachi, Takeshi Tokuyama, Ryuhei Uehara, Takeaki Uno:
Base Location Problems for Base-Monotone Regions, *In Proc. of the 7th International Workshop on Algorithms and Computation (WALCOM 2013),* LNCS 7748, 53–64, 2013 年 2 月.

17. Luis Barba, Matias Korman, Stefan Langerman, Rodrigo I. Silveira, Kunihiko Sadakane:
Space-Time Trade-offs for Stack-Based Algorithms, *In Proc. of the 30th Symposium on Theoretical Aspects of Computer Science (STACS 2013),* LIPIcs20, 281–292, 2013 年 2 月.

18. Takashi Horiyama, Wataru Shoji:
The Number of Different Unfoldings of Polyhedra, *In Proc. of the 29th European Workshop on Computational Geometry (EuroCG 2013),* 143–146, 2013 年 3 月.

19. 徳山豪:
計算限界の解明 : その意義とシナリオ (前編), 情報処理, 2013 年 4 月号 (掲載決定), 374–384, 2013.

20. Taku Onodera, Tetsuo Shibuya:
The Gapped Spectrum Kernel for Support Vector Machines, *In Proc. of Machine Learning and Data Mining (MLDM 2013),* (to appear).

研究会等

1. Alexander Bowe, Taku Onodera, Kunihiko Sadakane, Tetsuo Shibuya:
Compressing de Bruijn Graphs, 電子情報通信学会技術報告, COMP2012-29, 25–32, 2012 年 9 月.

2. 小池敦, 定兼邦彦:
GPU のための並列計算モデル, 電子情報通信学会技術報告, COMP2012-42, 53–60, 2012 年 10 月.

3. Jinhee Chun, Akiyoshi Shioura, Truong Minh Tien and Takeshi Tokuyama:
A Uniied View to Greedy Geometric Routing Algorithms in Ad Hoc Networks , 電子情報通信学会技術報告, COMP2012-34, 1–8, 2012 年 10 月.

4. 小野寺拓, 渋谷哲朗:
不連続な部分構造に基づく文字列カーネルとそのタンパク質の分類への応用, 情報処理学会バイオ情報学研究会, 2012-BIO-31(4), 2012 年 10 月.

5. Takashi Horiyama, Takehiro Ito, Keita Nakatsuka, Akira Suzuki, Ryuhei Uehara:
On the Complexity of Packing Trominoes, 電子情報通信学会技術研究報告, vol. 112, no. 272, COMP2012-40, 37–43, 2012 年 10 月.

6. 徳山豪:
計算理論の意義と影響力:情報社会における役割, 電子情報通信学会技術報告, COMP2012-36, (発表予定).

学会大会等

1. Jinhee Chun, Akiyoshi Shioura, Truong Minh Tien and Takeshi Tokuyama:
A Unified View to Greedy Routing Algorithms in Ad Hoc Networks, *In Proc. of the*

15th Korea-Japan Joint Workshop on Algorithms and Computation (WAAC 2012), 33–40, 2012 年 7 月.

2. 堀山貴史:
   多面体の展開図の列挙と索引化について, 学習理論における組合せ論ワークショップ, 2012 年 9 月.

3. Jinhee Chun, Takasi Horiyama, Takehiro Ito, Natsuda Kaothanthong, Hirotaka Ono, Yota Otachi, Takeshi Tokuyama, Ryuhei Uehara and Takeaki Uno:
   Algorithms for Computing Optimal Image Segmentation using Quadtree Decomposition, *Thailand-Japan Joint Conference on Computational Geometry and Graphs (TJJCCGG 2012),* 23–24, 2012 年 12 月.

4. 渋谷哲朗:
   タンパク質構造比較アルゴリズム, 第 *35* 回日本分子生物学会, 2012 年 12 月.

5. 寺師玄記, 渋谷哲朗, 竹田–志鷹真由子:
   タンパク質立体構造データベースに対する高速類似部分構造検索法の開発, 日本薬学会構造活性相関部会第 *40* 回構造活性相関シンポジウム, 2012 年 (共著学生の発表に対し優秀発表賞受賞).

文部科学省科学研究費補助金 新学術領域研究 (課題番号 24106007)

C01: 統計力学からの計算限界解明へのアプローチ

研究代表者： 渡辺 治　東京工業大学 情報理工学研究科
研究分担者： 伊東 利哉　東京工業大学 像情報工学研究所
小柴 健史　埼玉大学 理工学研究科
山本 真基　成蹊大学 情報科学科
連携研究者： 樺島 祥介　東京工業大学 総合理工研究科
福島 孝治　東京大学 総合文化研究科

開催した研究集会

1. ELC Mini Workshop on Randomness and Computation
期間: 2013 年 1 月 17 日
場所: CELC
講演者: Lenka Zdeborova (CNRS, Institute of Theoret. Physics at CEA), Haijun Zhou (Chinese Academy of Science), 樺島祥介 (東工大), 福島孝治 (東大)

招聘研究者

1. Lenka Zdeborova (CNRS, Institute of Theoret. Physics at CEA)
期間: 2013 年 1 月 15 日 ～ 1 月 18 日
受入: CELC

2. Haijun Zhou (Chinese Academy of Science)
期間: 2013 年 1 月 14 日 ～ 1 月 18 日
受入: CELC

アウトリーチ活動

1. 渡辺治:
講演 : 情報科学入門「計算の神秘を探る」, 松戸市教育委員会, 2012 年 7 月 30 日.

2. 渡辺治:
講演 : 情報科学とは, 藤嶺学園藤沢中・高等学校, 2012 年 9 月 15 日.

3. 渡辺治:
課題作成 : スーパーコンピューティングコンテスト２０１２（高校生・高専生対象）, 東京工業大学, 大阪大学, 2012 年 8 月 20 日～24 日.

学術論文

1. A. Coja-Oghlan, M. Onsjo, O. Watanabe: Propagation connectivity of random hypergraphs, *The Electronic Journal of Combinatorics,* 19(P17), 1–25, 2012.

2. A. Kawachi, H. Tanaka, O. Watanabe: Estimating the Gowers norm of modulo functions over prime fields, *IEICE Transactions on Information and Systems,* E95-D(3), 755–762, 2012.

3. K. Nakagawa and H. Yamaguchi: The first eigenvalue of (c, d)-regular graph, *IEICE Transactions on Information and Systems,* E96-D(3), 433–442, 2012.

4. Y. Aono, M. Agrawal, T. Satoh, O. Watanabe: On the optimality of lattices for the Coppersmith technique, *Proc. 17th Australasian Conference on Information Security and Privacy (ACISP 2012),* LNCS 7372, 376–389, 2012.

5. H. Dell, V. Kabanets, D. van Melkebeek, O. Watanabe:

Is Valiant-Vazirani's isolation probability improvable?, *Proc. 27th Conference on Computational Complexity (CCC 2012),* IEEE, 10–20, 2012.

6. J. Köbler, S. Kuhnert, O. Watanabe:
Interval graphg representation with given interval and intersection lengths, *Proc. 23rd International Symposium on Algorithms and Computation (ISAAC 2012),* LNCS 7676, 517–526, 2012.

7. Y. Yoshida, M. Yamamoto, H. Ito:
Improved constant-time approximation algorithms for maximum matchings and other optimization problems, *SIAM Journal on Computing,* 41(4), 1074–1093, 2012.

8. M. Yamamoto:
A combinatorial analysis for the critical clause tree, *Theory of Computing Systems,* 52(2), 271–284, 2013.

9. A. Sakata, K. Hukushima, K. Kaneko:
Replica symmetry breaking in an adiabatic spin-glass model of adaptative evolution, *Europhysics Letters,* 99, 68004 1–6, 2012.

10. T. Goto, Y.Kabashima, H. Takamura:
Mechanical analysis of semantic orientations on lexical network, *Proc. 24th International Conference on Computational Linguistics (COLING 2012),* 977–994, 2012.

学会大会等

1. T. Koshiba:
Quantum cryptography, *Handbook of Natural Computing,* Section V: Quantum Computing, Springer, 1521–1543, 2012.

2. T. Sueki, T. Koshiba, T. Morimae:
Ancilla-driven blind quantum computation, *2nd Conference on Quantum Cryptography (QCRYPT 2012), CQT, Singapore,* 2012 年 9 月 10〜14 日.

3. T. Koshiba:
Quantum oblivious transfer and quantum one-way functions (招待講演), *Japan-Singapore Workshop on Multi-User Quantum Network, CQT, Singapore,* 2012 年 9 月 17〜20 日.

4. O. Watanabe:
On most-likely solution problems and their average-case complexity (招待講演), *Workshop on Logic and Complexity, IIT Kanpur, India,* 2012 年 8 月 17〜19 日.

研究会等

1. 末木貴洋, 小柴健史, 森前智行:
補助キュービット駆動型万能ブラインド量子計算, 第 *26* 回量子情報技術研究会 *(QIT 26),* 福井大学, 155–157, 2012 年 5 月 21 日.

文部科学省科学研究費補助金 新学術領域研究 (課題番号 24106009)

C02: 量子力学からの計算限界解明へのアプローチ

研究代表者：	山下 茂	立命館大学 情報理工学部
研究分担者：	河内 亮周	東京工業大学 大学院 情報理工学研究科
	中西 正樹	山形大学 地域教育文化学部
	西村 治道	名古屋大学 大学院 情報科学研究科
	Le Gall Francois	東京大学 大学院 情報理工学系研究科
連携研究者：	小林 弘忠	国立情報学研究所 情報学プリンシプル研究系
	谷 誠一郎	日本電信電話株式会社 ＮＴＴコミュニケーション科学基礎研究所
	根本 香絵	国立情報学研究所 情報学プリンシプル研究系
	村尾 美緒	東京大学 大学院 理学系研究科

開催した研究集会

1. ELC Mini-Workshop (C02)
   期間: 2012 年 11 月 12 日 ～ 11 月 13 日
   場所: 名古屋大学情報科学研究科棟
   講演者: 山下茂（立命館大），河内亮周（東京工業大），中西正樹（山形大），フランソワルガル（東京大），西村治道（名古屋大），小林弘忠（NII），谷誠一郎（NTT），小柴健史（埼玉大），伊藤剛志（NEC ラボラトリーズアメリカ）

学術論文

1. Yasuhiro Takahashi and Seiichiro Tani:
   Collapse of the Hierarchy of Constant-Depth Exact Quantum Circuits, *to appear in the proceedings of IEEE Conference on Computational Complexity,* 2013.

2. Hirotada Kobayashi, Francois Le Gall, and Harumichi Nishimura:
   Stronger methods of making quantum interactive proofs perfectly complete, *In Proc. of the 2013 ACM Conference on Innovations in Theoretical Computer Science,* pp 329–352, 2013.

3. K. Fujii, Y. Nakata, M. Ohzeki, M. Murao:
   Measurement-Based Quantum Computation on Symmetry Breaking Thermal States, *Phys. Rev. Lett.,* Vol. 110, Issue 12, 120502, March 2013.

4. M. Villagra, M. Nakanishi, S. Yamashita, and Y. Nakashima:
   Tensor rank and strong quantum nondeterminism in multiparty communication, *IEICE Trans. on Inf. & Syst.,* vol.E96-D, no. 1, pp. 1–8, January 2013.

5. S. J. Devitt, Kae Nemoto:
   Programming a Topological Quantum Computer, *Proc. of IEEE ATS2012,* pp. 55–60, Nov. 2012.

6. S. Yamashita:
   An Optimization Problem for Topological Quantum Computation, *Proc. of IEEE ATS2012,* pp. 61–66, Nov. 2012.

7. S. Yamashita, S. Hiratsuka, S. Devitt and K. Nemoto:
   Circuit Optimization by Clique Finding for Topological Quantum Computation, *Proc. of AQIS'12,* pp. 161–162, Aug. 2012.

8. A. Paler, S. J. Devitt, K. Nemoto, I. Polian: Synthesis of Topological Quantum Circuits, *Proc. of 2012 IEEE/ACM International Symposium on Nanoscale Architectures,* pp. 181–187, Jul. 2012.

9. M. Villagra, M. Nakanishi, S. Yamashita, and Y. Nakashima: Tensor rank and strong quantum nondeterminism in multiparty communication, *Proc. of the 9th Annual Conference on Theory and Applications of Models of Computation (TAMC2012),* pp. 400–411, May 2012.

10. Francois Le Gall: Time-Efficient Output-Sensitive Quantum Algorithms for Boolean Matrix Multiplication, *Proc. of the 23rd International Symposium on Algorithms and Computation (ISAAC 2012), LNCS 7676,* pp. 639–648, 2012.

11. Takahiko Satoh, Francois Le Gall and Hiroshi Imai: Quantum network coding for quantum repeaters, *Physical Review A,* Vol. 83, 032331, 2012.

12. Francois Le Gall: Faster Algorithms for Rectangular Matrix Multiplication, *Proc. of the 53rd Annual IEEE Symposium on Foundations of Computer Science (FOCS 2012),* pp. 514–523, 2012.

13. Francois Le Gall: Quantum Private Information Retrieval with Sublinear Communication Complexity, *Theory of Computing,* Vol. 8, pp. 369–374, 2012.

14. Richard Cleve, Kazuo Iwama, Francois Le Gall, Harumichi Nishimura, Seiichiro Tani, Junichi Teruyama and Shigeru Yamashita: Reconstructing Strings from Substrings with Quantum Queries, *Proc. of the 13th Scandinavian Symposium and Workshops on Algorithm Theory (SWAT 2012),* pp. 388–397, 2012.

15. Francois Le Gall, Shota Nakagawa and Harumichi Nishimura: On QMA Protocols with Two Short Quantum Proofs, *Quantum Information and Computation,* Vol. 12 No.7&8, pp. 589–600, 2012.

16. Gabor Ivanyos, Francois Le Gall and Yuichi Yoshida: On the distance between non-isomorphic groups, *European Journal of Combinatorics,* Vol. 33 No. 4, pp. 474–476, 2012.

17. Andrej Bogdanov, Akinori Kawachi and Hidetoki Tanaka: Hard Functions for Low-Degree Polynomials over Prime Fields, *ACM Transactions on Computation Theory,* to appear.

18. Akinori Kawachi, Hirotoshi Takebe, and Keisuke Tanaka: Symmetric-Key Encryption Scheme with Multi-Ciphertext Non-Malleability, *Proceedings of the 7th International Workshop on Security (IWSEC 2012),* pp. 123–137, 2012.

研究会等

1. 上田圭祐，西村治道: 時間ドロボー問題の物質的ゼロ知識証明, 数理解析研究所研究集会「理論計算機科学の新展開」（冬の *LA* シンポジウム *2012*）, 2013 年 1 月 28 － 30 日.

2. 大和雅英，西村治道: 衝突の列挙に関する量子質問計算量, 第 *27* 回量子情報技術研究会研究会資料, pp. 154–157, 2012 年 12 月 27 日－ 28 日.

3. Francois Le Gall: Faster Algorithms for Rectangular Matrix Multiplication, 信学技報 *COMP2012-32,* vol. 112, no. 199, pp. 41–48, 2012 年 9 月.

学会大会等

1. Stephen Jordan, Hirotada Kobayashi, Francois Le Gall, Daniel Nagaj, and Harumichi Nishimura:
   Towards Perfect Completeness in QMA, *Contributed talk at the 16th Workshop on Quantum Information Processing,* 2013年1月.

2. S. Yamashita, S. Devitt and K. Nemoto:
   Qubit Order Optimization Problem for Topological Quantum Computation, *TQC2012,* May. 2012.

3. 河内 亮周:
   計算複雑さへの招待 (2): アルゴリズムから攻める計算複雑さの下界証明, 電子情報通信学会コンピュテーション研究会，招待チュートリアル講演, 2013年3月.

文部科学省科学研究費補助金 新学術領域研究 (課題番号 24106010)

C03: 学習理論からの計算限界解明へのアプローチ

研究代表者：	瀧本 英二	九州大学 大学院システム情報科学研究院
研究分担者：	正代 隆義	九州大学 大学院システム情報科学研究院
	畑埜 晃平	九州大学 大学院システム情報科学研究院
	篠原 歩	東北大学 大学院情報科学研究科
	内沢 啓	山形大学 大学院理工学研究科
連携研究者：	吉仲 亮	京都大学 大学院情報学研究科
研究協力者：	津田 宏治	産業技術総合研究所 生命情報工学研究センター
	Cuturi Marco	京都大学 大学院情報学研究科

開催した研究集会

1. ELC Mini-Workshop (C03)
   期間: 2012 年 12 月 17 日 ～ 12 月 18 日
   場所: 開催場所: JR 博多シティ
   講演者: C03 班のメンバー全員

アウトリーチ活動

1. 畑埜 晃平:
   “基多面体の上のオンライン予測”, 文科省 数学・数理科学と諸科学・産業との連携研究ワークショップ「離散構造と最適化：展開と連携」, 2012 年 11 月 29 日 ～ 11 月 30 日.

2. 瀧本 英二:
   “オンラインアルゴリズムとストリームアルゴリズム”, 計測自動制御学会ニューラルネットワークフォーラム 2013, 2013 年 3 月 29 日.

学術論文

1. Daiki Suehiro, Kohei Hatano, Shuji Kijima, Kiyohito Nagano, and Eiji Takimoto:
   Online Prediction under Submodular Constraints, *Proc. 23th Conference on Algorithmic Learning Theory (ALT 2012),* LNAI 7568, 260–274, 2012.

2. Shota Yasutake, Kohei Hatano, Eiji Takimoto, and Masayuki Takeda:
   Online Rank Aggregation, *Proc. 4th Conference on Asian Conference on Machine Learning,* JMLR Workshop and Conference Proceedings, Vol. 25, 539–553, 2012.

3. Yuta Yoshimura and Takayoshi Shoudai:
   Learning Unordered Tree Contraction Patterns in Polynomial Time, *Proc. 22nd International Conference on Inductive Logic Programming (ILP 2012),* LNAI 7842, 257–272, 2013.

4. Atsushi Okamoto and Takayoshi Shoudai:
   Mining First-Come-First-Served Frequent Time Sequence Patterns in Streaming Data, *Proc. IADIS International Conference e-Society 2013,* 283–290, 2013.

5. Kazuhiko Kusano, Kazuyuki Narisawa, and Ayumi Shinohara:
   Computing Maximum Number of Runs in Strings, *Proc. 19th International Symposium on String Processing and Information Retrieval (SPIRE 2012),* LNCS 7608, 318–329, 2012.

6. Takashi Katsura, Kazuyuki Narisawa, Ayumi Shinohara, Hideo Bannai, and Shunsuke Inenaga:
   Permuted Pattern Matching on Multi-track Strings, *Proc. 39th International Confer-*

ence on Current Trends in Theory and Practice of Computer Science (SOFSEM 2013), LNCS 7741, 280–291, 2013.

7. Akira Suzuki, Kei Uchizawa, and Xiao Zhou:
   Energy and Fan-in of Logic Circuits Computing Symmetric Boolean Functions, *Theoretical Computer Science,* (掲載予定).

8. Akira Suzuki, Kei Uchizawa, and Xiao Zhou:
   Energy-Efficient Threshold Circuits Computing Mod Functions, *International Journal of Foundations of Computer Science,* 24: 1, 15–29, 2013.

9. Kei Uchizawa, Zhenghong Wang, Hiroki Morizumi, and Xiao Zhou:
   Complexity of Counting Output Patterns of Logic Circuits, *Proc. 19th edition of Computing: the Australasian Theory Symposium (CATS 2013),* CRIPT 141, 37–42, 2013.

10. Kei Uchizawa, Takanori Aoki, Takehiro Ito, and Xiao Zhou:
    Generalized Rainbow Connectivity of Graphs, *Proc. 7th International Workshop on Algorithms and Computation (WALCOM 2013),* 7748, 233–244, 2013.

11. Ryo Yoshinaka, Jun Kawahara, Shuhei Denzumi, Hiroki Arimura, and Shin-ichi Minato:
    Counterexamples to the Long-Standing Conjecture on the Complexity of BDD Binary Operations, *Information Processing Letters,* 112:16, 636–640, 2012.

12. Alexander Clark and Ryo Yoshinaka:
    Beyond Semilinearity: Distributional Learning of Parallel Multiple Context-free Grammars, *Proc. 11th International Conference on Grammatical Inference (ICGI 2012),* JMLR Workshop and Conference Proceedings, Vol. 21, 84–96, 2012.

13. Chihiro Shibata and Ryo Yoshinaka:
    Marginalizing Out Transition Probabilities for Several Subclasses of PFAs, *Proc. 11th International Conference on Grammatical Inference (ICGI 2012),* JMLR Workshop and Conference Proceedings, Vol. 21, 259–263, 2012.

14. Ryo Yoshinaka:
    An Attempt Towards Learning Semantics: Distributional Learning of IO Context-Free Tree Grammars, *Proc. 11th International Workshop on Tree Adjoining Grammars and Related Formalisms (TAG+11),* 90–98, 2012.

15. Ichigaku Takigawa, Koji Tsuda, and Hiroshi Mamitsuka:
    An In Silico Model for Interpreting Polypharmacological Relationships in Drug-Target Networks, *Methods in Molecular Biology,* 993, 67–80, 2013.

16. Koji Tsuda and Elisabeth Georgii:
    Dense Module Enumeration in Biological Networks, *Methods in Molecular Biology,* 939, 1–8, 2013.

17. Chuan Xiao, Jianbin Qin, Wei Wang, Yoshiharu Ishikawa, Koji Tsuda, and Kuhiniko Sadakane:
    Efficient Error-tolerant Query Autocompletion, *Proc. 39th International Conference on Very Large Data Bases (VLDB 2013),* 掲載予定.

18. Marco Cuturi, Alexandre d'Aspremont:
    Mean Reversion with a Variance Threshold, *Proc. 30th International Conference on Machine Learning (ICML 2013),* JMLR Workshop and Conference Proceedings, Vol. 28, No. 3, 271–279, 2013.

研究会等

1. Takahiro Fujita, Kohei Hatano, Eiji Takimoto:

Combinatorial Online Prediction Using Oine Approximation Algorithms, *The 6th Annual Meeting of the Asian Association for Algorithms and Computation (AAAC 2013),* 2013 年 4 月.

2. 立石 大悟, 畑埜 晃平, 瀧本 英二:
バイアス付き Passive Agressive アルゴリズム, 電子情報通信学会 *IBISML* 研究会, 1–8, 2013 年 3 月.

3. 藤田 隆寛, 畑埜 晃平, 瀧本 英二:
オフラインアルゴリズムを用いた離散構造のオンライン予測, 冬の *LA* シンポジウム, 2013 年 1 月.

4. Daiki Suehiro, Kohei Hatano, Shuji Kijima, Kiyohito Nagano, and Eiji Takimoto:
Online Prediction over Base Polyhedra, *NIPS Workshop on Discrete Optimization in Machine Learning (DISCML 2012),* 2012 年 12 月.

5. Daiki Suehiro, Kohei Hatano, and Eiji Takimoto:
Efficient AUC Maximization by Approximate Reduction of Ranking SVMs, 第 *15* 回情報論的学習理論ワークショップ（*IBIS2012*）, 243–249, 2012 年 11 月.

6. 松本 一成, 畑埜 晃平, 瀧本 英二:
Bradley-Terry モデルのオンライン予測, 夏の *LA* シンポジウム, 2012 年 7 月.

7. 末廣 大貴, 畑埜 晃平, 来嶋 秀治, 瀧本 英二, 永野 清仁:
基多面体上のオンライン予測, 夏の *LA* シンポジウム, 2012 年 7 月.

8. 末廣 大貴, 畑埜 晃平, 来嶋 秀治, 瀧本 英二, 永野 清仁:
劣モジュラ制約下におけるオンライン予測, 電子情報通信学会 *IBISML* 研究会, 15–22, 2012 年 6 月.

9. 相原 高雄, 篠原 歩, 成澤 和志:
圧縮文字列に対する省メモリなパターンマッチアルゴリズム, 電子情報通信学会コンピュテーション研究会, COMP2012-37, 17–24, 2012 年 10 月.

10. 大友 雄平, 成澤 和志, 篠原 歩:
種々のパターン照合問題に対するポジションヒープの構築, 電子情報通信学会コンピュテーション研究会, COMP2012-44, 7–14, 2012 年 12 月.

11. 大田 裕之, 桂 敬史, 成澤 和志, 篠原 歩:
マルチトラックデータ上の近似順列パターン照合と索引構造, 電子情報通信学会コンピュテーション研究会, COMP2013-2, 9–16, 2013 年 4 月.

12. 草野 一彦, 奥田 遼介, 成澤 和志, 篠原 歩:
文字列に含まれる連の最大指数和の解析〜n=57 までの厳密値と新たな下界 2.03696 の発見, 電子情報通信学会コンピュテーション研究会, COMP2013-2, 17–24, 2013 年 4 月.

13. 縫田 光司, 清水 佳奈, 荒井 ひろみ, 浜田 道昭, 津田 宏治, 広川 貴次, 花岡 悟一郎, 佐久間 淳, 浅井 潔:
加法準同型暗号を用いた化合物データベースの秘匿検索プロトコル, コンピュータセキュリティシンポジウム *2012,* 2012: 3, 382–389, 2012 年 10 月.

14. 井上 武, 高野 圭司, 渡辺 喬之, 川原 純, 吉仲 亮, 岸本章宏, 津田 宏治, 湊 真一, 林 泰弘:
フロンティア法を用いた電力網解析手法, 電子情報通信学会情報ネットワーク研究会, IN2012-39, 37–42, 2012 年 7 月.

学会大会等

1. 岡本 康宏, 吉村 友太, 正代 隆義:
辺縮約に基づく木構造パターンの多項式時間学習アルゴリズム, 平成 *24* 年度 *(*第 *65* 回*)* 電気関係学会九州支部連合大会, 2012 年 9 月.

2. 岡本 敦, 正代 隆義:
ストリーム上の頻出時系列とその近似発見アルゴリズムについて, 情報処理学会第 *75* 回全国大会, 2013 年 3 月.

3. 村井 光, 吉村 友太, 岡本 康宏, 正代 隆義, 宮原 哲浩:
辺縮約に基づく木構造パターンの列挙とそのデータマイニングへの応用, 火の国情報シンポジウム *2013,* 情報処理学会九州支部, 2013年3月.

4. Kei Uchizawa, Zhenghong Wang, Hiroki Morizumi, Xiao Zhou:
Computational complexity of counting output patterns of logic circuits, 電子情報通信学会コンピュテーション研究会, 2013年5月.

5. Kei Uchizawa:
Computational complexity of counting output patterns of logic circuits, コンピュータサイエンス研究会, 2013年1月.

6. Kei Uchizawa:
論理回路の出力パターン数解析とその応用, 応用数学連携フォーラム第 *31* 回ワークショップ, 2012年12月.