

STOC2009 参加報告

伊藤 大雄 吉田 悠一
京都大学大学院情報学研究科

概観

STOC (ACM^{☆1} Symposium on Theory of Computing) とは理論計算機科学における最高峰の会議です。41 回目となる 2009 年の STOC は 5 月 31 日から 6 月 2 日に、アメリカ、メリーランド州のベセズダ (Bethesda) という街にあるホテル Hyatt Regency Bethesda を会場として開催されました。ベセズダという名前は知らない人がほとんどだと思いますが(我々も知りませんでした)、ワシントン D.C. の中心部から地下鉄で 20 分程の場所にある高級住宅街です。ホテル代が高い (1 泊約 2 万円! しかもまわりに安いビジネスホテルなどはありません) 点は問題ですが、夜出歩くにも特に危険を感じることはありませんし、ホワイトハウスやスミソニアン博物館などの見どころもあり^{☆2}、アメリカの会場としては合格点でしょう。

今回の STOC は 321 件の投稿がありそのうち 77 件が採択されました(採択率約 24.0%, 分野別内訳は表-1 参照)。そのうち日本人が著者として入っているのは 2 件です。全体的な傾向としてはやはりアメリカの東海岸、西海岸、イスラエルの大学からの論文が多いように思われます。ビジネスミーティングでの発表によりますと、参加者(登録者)は 225 人で、そのうち約 116 人が学生、日本人の参加者は、我々の見た限り恐らく 5 人でした。

会議の流れは基本的には 2 セッションが同時に進行し、招待講演やベストペーパーのときのみ単独セッションとなりました。講演時間は 20 分ですが、交代の時間をきっちり 5 分とっていたのが印象的でした^{☆3}。朝は 8

アルゴリズムとデータ構造	20/71
計算複雑さ	9/40
アルゴリズム的グラフ理論と組合せ論	9/34
計算生物学	0/5
アルゴリズム的代数とコーディング理論	6/19
計算的ゲーム理論	4/27
計算幾何学	1/6
暗号	7/23
機械学習	1/13
並列分散計算	3/12
量子計算及び異なる計算モデル	4/22
計算におけるランダム性	8/19
情報修復の理論	0/2
ネットワークの理論	1/4
無分野	2/14
その他	2/10
合計	77/321

表-1 分野別採択数(採択数/投稿数)

時 45 分(初日は 8 時半)から夜は 5 時過ぎまでびっしり発表が詰まっていたので聞くだけでもかなり大変です。内容は計算量、データ構造、性質検査、暗号、近似アルゴリズム、グラフ、最適化、プライバシー、量子計算、メカニズムデザイン、幾何など多岐にわたり、とてもすべての内容を理解するのは不可能です。多くの人は興味がない発表のときはロビーに集まって雑談や研究の話をしているようでした。やや余談になりますが、STOC、FOCS^{☆4}ではこのようにロビーで話している人が多いのが特徴です。主にアメリカでやるので適当な観光地が近くにあまりない、というのも原因の 1 つだとは思いますが、それ以外に、STOC、FOCS の常連はこういう機会に間近に締切がある論文の内容の相談をしているので

☆1 Association for Computing Machinery.

☆2 ただ、STOC は重要な発表が目白押しなので、抜け出す隙がないのは困りものです。実際、学生や若手は夕方以降にワシントン D.C. 中心街に繰り出していましたが、中年(つまり伊藤)はホテルでへばっていました。

☆3 その結果、プログラム進行が遅れることはありませんでした。

☆4 Annual IEEE Symposium on Foundations of Computer Science. 理論計算機科学界における STOC と並ぶ最高峰会議。

す。今回で言えば SODA10^{☆5} の論文のいくつかが、このロビーででき上がったと思います。

ベストペーパーとゲーデル賞

招待講演は Shafi Goldwasser の Cryptography without (hardly any) Secrets? です。暗号の話で、残念ながら筆者らは暗号に関してまったくの素人なので中身の紹介はご勘弁ください。

ベストペーパーには以下の2つの論文が選ばれました。

- Chris Peikert : Public-Key Cryptosystems from the Worst-Case Shortest Vector Problem.
- Robin A. Moser : A Constructive Proof of the Lovasz Local Lemma.

前者の論文は、これも暗号の話なので省略します(すみません)。後者ですが、Lovasz Local Lemma とは確率的手法における証明技法の1つです。この補題を用いた応用例の1つとして、「 k -CNF^{☆6}中の各節に対してそれと変数を共有する節が高々 2^{k-2} 個しか存在しなければ、その k -CNF は必ず充足解を持つ」ということが証明できます^{☆7}。ただし元々の Lovasz Local Lemma は存在証明であって、具体的な充足解を与えてはくれません。それに対して Moser は各節に対して高々 2^{k-5} 個しか変数を共有する節が存在しないときには、非常に単純な確率アルゴリズムによって具体的に充足解を得ることができるということを示しました。またそのアルゴリズムが多項式時間で終了することを情報理論を用いた新しい手法で示しています。これは非常に賢い方法で、発表の後の質問の時間では、質問をする代わりに内容を称賛するような人さえいました。さらにこの論文はベストスチュージェントペーパーにも選ばれています。

また今回の STOC ではゲーデル賞の授与も行われました。ゲーデル賞は(解説する必要もないとは思いますが)理論計算機科学における目覚ましい論文に対して EATCS^{☆8} と ACM-SIGACT^{☆9} が与える賞で、1993 年

を第1回として、毎年 STOC と ICALP^{☆10} で交互に授与が行われています^{☆11}。今年は以下の2つの論文に贈られました。

- Omer Reingold : Undirected Connectivity in Log-Space, Journal of ACM, Vol.55, No.4 (2007).
- Omer Reingold, Salil Vadhan and Avi Wigderson : Entropy Waves, the Zig-Zag Graph Product and New Constant Degree Expanders, Annals of Mathematics, Vol.155, pp.157-187 (2002).

前者は Zig-Zag product という手法を用いることで、無向グラフの連結性が対数領域 (LOG-SPACE) の決定性アルゴリズムで判定可能であることを示した論文で、2005 年の STOC のベストペーパーをジャーナル版にしたものです。後者は、この Zig-Zag product を用いて、理論計算機科学のさまざまな分野で応用することができるエキスパンダー^{☆12}を構築する手法を導いた論文です。

印象に残った論文

では印象に残った論文について、いくつか紹介します。

- Emanuele Viola : Bit-Probe Lower Bounds for Succinct Data Structures.
3種類の要素 {0, 1, 2} からなるデータの列 (trits) を2種類の要素 {0, 1} からなるデータの列 (bits) を使って保存したいとします。できるだけ使用する bit 数を抑えつつ、さらに 1trit を取り出す時に見る bit 数も抑えるというのが目標です。保存したい trit の個数を n 個としましょう。情報論的な下限から $n \log_2 3$ bit は必要なことが分かります。実は 1trit を取り出す際に見る bit 数を q としたときに、容量は $n \log_2 3 + O(n/2^q)$ にすることができることが知られているのですが (Patrascu, FOCS'08)、このトレードオフの関係は実は厳密だということを示したのがこの論文の結果です。
- Ryan O'Donnell and Yi Wu : Conditional Hardness for Satisfiable 3-CSPs.
Unique Games Conjecture という PCP^{☆13} に関する

☆5 SODA : ACM-SIAM Symposium on Discrete Algorithms. 離散アルゴリズム分野における最高峰の会議。

☆6 CNF : Conjunctive Normal Form. k -CNF とは、どの節 (clause) もちょうど k 個リテラル (literal) を含んでいるような CNF のこと。

☆7 Alon, N. and Spencer, J. H. : The Probabilistic Method (3rd Edition), Wiley (2008). の5章 The Local Lemma に詳しい解説があります。

☆8 European Association for Theoretical Computer Science.

☆9 Special Interest Group on Algorithms and Computation Theory.

☆10 International Colloquium on Automata, Languages and Programming : EATCS の主催する計算機科学における欧州最高の会議。

☆11 日本人の受賞者は1998年の戸田誠之助先生(日本大学)。

☆12 Expander : グラフの一種。非常におおまかに言うと、任意の頂点部分集合がそのサイズ以上の隣接頂点集合を持つようなグラフ。

☆13 PCP : Probabilistically Checkable Proof ; 確率的検査可能証明。

る有名な予想があるのですが、それと似た予想として d -to-1 Conjecture と呼ばれる予想があります。この論文では 3-CSP^{☆14} のインスタンスが与えられたときに、それが充足可能か、全体の $5/8+\epsilon$ 以下の節しか充足できないかを区別するのは d -to-1 Conjecture を仮定すると NP 困難ということを示しています。逆に充足可能な 3-CSP のインスタンスが与えられると全体の $5/8$ は充足するような変数割り当てを見つけることができることが知られているので (Zwick, SODA'02), この結果は厳密です。

- Erin W. Chambers and Jeff Erickson : Homology Flows, Cohomology Cuts.

平面グラフ上で特別に高速に動くアルゴリズムは、種数 (genus)^{☆15} を一般の定数 g に限定したグラフにも拡張できることが多いのですが、 s - t フロー^{☆16} に関しては上手い拡張が見つかっていませんでした。この論文では、Homology Flow という、フローのある同値類を考え、その上での最大流 = 最小カットの定理に該当する性質を与えることによって $(g \log n)^{O(g)} n$ 時間で、整数容量の場合には $O(g^7 n \log^2 n \log^2 C)$ 時間で動作するアルゴリズムを得ています。

- Tim Roughgarden : Intrinsic Robustness of the Price of Anarchy.

ゲーム理論の均衡解には、pure Nash, mixed Nash, correlated equilibrium, no regret sequence^{☆17} などさまざまありますが、無秩序の代償 (price of anarchy) とそれらを結びつける一般的・基礎的な性質を与えています。コスト関数がある性質を満たすとき (λ, μ) -smooth であると定義し、その場合には、上記の期待値はすべて $\lambda/(1-\mu)$ で抑えられ、さらにこの上界値は厳密であることを証明しています。

日本人著者による 2 件の論文にも触れておきます。

- Ken-ichi Kawarabayashi and Bruce Reed : Hadwiger's Conjecture is Decidable.
- Yuichi Yoshida, Masaki Yamamoto and Hiro Ito : An Improved Constant-Time Approximation

☆14 CSP : Constraint Satisfaction Problem ; 制約充足問題。

☆15 球面上の穴の数。たとえばトーラス(円環)は種数 1。

☆16 2 頂点間の流れ、最大流問題が代表的。

☆17 すべて後者は前者の拡張。

Algorithm for Maximum Matchings.

まず前者ですが、これは今や STOC, FOCS の常連となった日本のエース河原林健一先生 (国立情報学研究所) の論文です。Hadwiger 予想とは K_t マイナーを持たないグラフは $(t-1)$ 彩色可能であるという予想です。 K_t とは t 頂点からなる完全グラフで、 K_t マイナーを持たないとはグラフから枝の削除、頂点の削除、枝の縮約を繰り返しても K_t が得られないことを意味します。Hadwiger の予想は $t \leq 6$ において正しいことがすでに証明されています。この論文では、この予想に対して、もし K_t マイナーを持たない $(t-1)$ 彩色も不可能なグラフが存在するとすれば、その頂点数は $p=10^{(10^{(10^t)})}$ として $f(t)=p^{(p^{(p^t)})}$ で抑えられることを示しています。また、それを利用して入力グラフ G が以下の 3 つのうちどれを満たすか (どれかは必ず満たす) を $O(n^2)$ 時間で判定するアルゴリズムも示しました。(1) G は $(t-1)$ 彩色可能である、(2) G は K_t マイナーを含む、(3) G はあるマイナー H を持ち、 H は K_t マイナーも持たない $(t-1)$ 彩色可能でもなく、さらに H の頂点数は $f(p)$ 以下である。だから Hadwiger 予想は「判定可能 (Decidable)」だということですが、河原林先生によると、この題目は一部の査読者に評判が悪かったそうで、査読報告もはっきり分かれていたそうです (それでも通るあたりが流石ですが)。

我々の結果とその周辺

後者の論文が我々のものです。「定数時間」近似アルゴリズムとは、入力全体の中から入力の大きさ n によらない定数部分だけ見ることによって、最適化問題に対する近似解を出力するようなアルゴリズムのことです。ただし、普通の近似の定義では当然これは不可能ですので 2 つの緩和をしています。1 つ目は出力に加法的誤差 ϵn を許し、さらにアルゴリズムの計算量は $1/\epsilon$ には依存してよいとします。2 つ目はアルゴリズムは確率 $2/3$ 以上で近似解を出せばよいとします^{☆18}。こうすることでさまざまな最適化問題が n によらない定数時間で近似可能になります。この論文では、特に次数上限を d に制限したグラフに注目して、そのようなグラフでは最大マッチング^{☆19} や最小頂点被覆^{☆20} の近似がこれまで知ら

☆18 実用上は、乱数の初期値を変えて何度か計算し、出た結果の中間値を出せばよいことになります。

☆19 頂点を共有しない最大サイズの辺集合のサイズ。

☆20 すべての辺のどちらかの端点を含んでいるような頂点集合で最小のものサイズ。

れている結果よりも d と $1/\epsilon$ に関して指数的に高速なアルゴリズムが作れることを示しました。さらに同じ手法が最小集合被覆^{☆21}の近似にも応用できることを示しています。

定数時間アルゴリズムは、Oded Goldreich, Dana Ron, Noga Alon らの活躍で、ここ 10 年で急激に注目を浴びてきた分野です。始めは判定問題である性質検査 (property testing) がほとんどでしたが、昨年の FOCS2008 で Nguyen と Onak が非凡な発想に基づく、最大マッチングに対する近似アルゴリズム^{☆22}を提案して、こちらの可能性も急に広がりました。今回の我々の論文も、この Nguyen と Onak の結果を改良したものです。定数時間でできるということは、Web グラフやゲノム情報などの超大規模なものを扱うのにうってつけのアプローチで、応用面への期待もさることながら、理論的にも次々と新しい発見があり、たいへん魅力的な分野です。今や STOC, FOCS での重要トピックの 1 つにもなっていますし (今回も性質検査のセッションが組まれました)、歴史が浅いこともあり、多くの脈が眠っていると思われまますので、若い方々はどんどん挑まれてはどうでしょうか。

感想

STOC のような最高峰の会議に参加するのは、自分が発表するしないにかかわらず非常に意味のあることだと思います。もちろん面白い結果が多いので単純に発表を聞いていて楽しいというのがありますが、一体今、理論計算機科学のコミュニティの中でどのようなことが問

☆21 与えられた部分集合族のうちから最小数の部分集合を選んで全要素を被覆する問題。

☆22 こちらは判定問題ではなく、最適化問題の枠組みになります。

題になっていて、どのようなことをすれば評価されるのかというトレンドを知ることができるというのが意味深いことだと思います。そのほかにも、論文の著者としてしか知らなかった人たちに実際に会うことができるので、どんどん質問をぶつけて知り合いを増やすチャンスでもあります。

今回、我々は幸いにも論文が通りましたが、普通は (毎回通している河原林先生のような超人は別にして) めったに通りませんので、「自分の論文がなければ参加しない」というポリシーだと、STOC, FOCS, SODA, ICALP といった最高峰の会議にはほとんど参加できないことになってしまいます。しかし、めったに論文が通らないほどレベルの高い会議にこそ、なるべく顔を出しておく必要があるのではないのでしょうか。

2010 年の STOC はボストンで、2011 年は San Jose で開催されるそうです。皆さんも (論文の在る無しにかかわらず) 参加してみたいかがでしょうか。

(平成 21 年 6 月 8 日受付)

伊藤 大雄 (正会員) itohiro@kuis.kyoto-u.ac.jp

1985 年京大数理工学卒, 1987 年修了. 1995 年京都大学博士. NTT 研究所, 豊橋技科大を経て 2001 年より京大助教授~准教授. 離散アルゴリズムの研究に従事. 著書 (共著) 「ネットワーク設計理論」(岩波書店).

吉田 悠一 (学生会員) yyoshida@lab2.kuis.kyoto-u.ac.jp

2006 年 (株) プリファードインフラストラクチャーを共同設立. 2007 年京大卒 (工学), 2009 年同大学院修了 (情報学). 同年より同大学院博士課程に在籍.