Kyoto Prize Satellite Workshop in Honor of Professor László Lovász

November 16th–18th, 2010
Tokyo Institute of Technology

Preface

Professor László Lovász receives 26th annual Kyoto Prize in Basic Sciences, which for 2010 focuses on the field of Mathematical Sciences. His citation reads "Outstanding Contributions to Mathematical Sciences Based on Discrete Optimization Algorithms".

Professor Lovász has made outstanding contributions to the advancement of both the academic and technological possibilities of the mathematical sciences. He has provided a link among many branches of mathematics. In fact, his methodologies go beyond the framework of discrete mathematics to exert significant influence on a broad spectrum of mathematical sciences, including information theory, analysis, probability and theoretical computer science.

In addition, he has been working very hard to raise visibility of discrete mathematics. As the president of the International Mathematics Union, he has put his enormous effort on the whole mathematics community.

To celebrate Professor Lovász for the Kyoto Prize, which is a great event for our discrete mathematics community, we are going to have a satellite workshop at Tokyo Institute of Technology from November 16 to 18, 2010.

It is great pleasure to announce that twelve outstanding researchers kindly agreed to give an invited talk. They all have provided substantial progress of the area after Professor Lovász' pioneering works.

Finally, we would like to express our special appreciation of the support from National Institute of Informatics and Global COE of the Tokyo Institute of Technology, Compview. We would also extend appreciation to the Inamori Foundation for generous arrangement.

Ken-ichi Kawarabayashi
Satoru Iwata
Osamu Watanabe

Contents

Poster Presentation

On the Topology of Graphons

László Lovász
Eötvös Loránd University
lovasz(at)cs.elte.hu

We define a metric space on the nodes of a graph, by representing each node by the corresponding row vector in the square of the adjacency matrix. Then a (weak) regularity partition (in the sense of Fireze and Kannan) corresponds to partitioning this metric space into sets of small diameter.

If we apply this to graphons (limit objects of growing graph sequences), we see that the Regularity Lemma says that while these spaces may be infinite dimensional, but "just barely". Our main result is that if we exclude a bipartite graph as an induced subgraph (in the bipartite sense), then this space will be finite dimensional. This fact has consequences for the minimum number of classes in a regularity partition.

This is joint work with Balázs Szegedy.

Traveling Salesman Problems

William Cook
Georgia Institute of Technology
bico@isye.gatech.edu

We discuss open research questions surrounding the traveling salesman problem. A focus will be on topics having potential impact on the computational solution of large-scale problem instances.

Optimal Sink-Stable Sets

András Frank
Egerváry Research Group, Mathematical Institute
Eötvös University of Budapest, Hungary

A benzenoid hydrocarbon molecule can be represented by a 2-connected plane graph G whose bounded faces are hexagons. E. Clar introduced a graph-theoretic parameter, called the Clar number of G, as the maximum number of disjoint hexagons for which the rest of the graph has a perfect matching. It was verified experimentally that the larger the Clar number among ismeric benzenoid hydrocarbons, the more stable the corresponding compound.

Recently, Abeledo and Atkinson proved a min-max theorem for the Clar number. In the present talk, we extend their result to arbitrary directed graphs and derive a min-max formula for the maximum cardinality of a sink-stable set, where a subset S of nodes is **sink-stable** if there are disjoint directed cuts so that reorienting their elements makes each node in S a sink-node. We also exhibit an unexpected link to a min-max theorem of Bessy and Thomassé on cyclic stable sets of digraphs, by which they proved a longstanding conjecture of Gallai.

A min-max formula will also be derived for the minimum number of sink-stable sets to cover the node-set. With the help of the same link, we show that this result is equivalent to a (slight sharpening) of Minty's colouring theorem, which in turn is equivalent to another min-max result of Bessy and Thomassé on the minimum number of cyclic stable sets covering the node-set of a strongly connected digraph. Sebő's extensions on optimal families of k cyclic stable sets can also be reformulated in terms of sink-stable sets.

Tree Metrics and Edge-Disjoint S-Paths

Hiroshi Hirai
Department of Mathematical Informatics,
University of Tokyo, Tokyo 113-8656, Japan.
hirai@mist.i.u-tokyo.ac.jp

Abstract

Given an undirected graph $G = (V, E)$ with a terminal set S, a terminal weight $\mu : \binom{S}{2} \to \mathbf{Z}_+$, and an edge-cost $a : E \to \mathbf{Z}_+$, the μ-weighted minimum-cost edge-disjoint S-paths problem (μ-CEDP) is to maximize $\sum_{P \in \mathcal{P}} \mu(s_P, t_P) - a(P)$ over all edge-disjoint sets $\mathcal{P}$ of S-paths, where s_P, t_P denote the ends of P and $a(P)$ is the sum of edge-cost $a(e)$ over edges e in P.

Our main result is a complete characterization of terminal weights μ for which μ-CEDP is tractable and admits a combinatorial min-max theorem for every graph. We prove that if μ is a tree metric, then μ-CEDP is solvable in polynomial time and has a combinatorial min-max theorem, extending Mader's edge-disjoint S-paths theorem and its minimum-cost version by Karzanov. Our min-max formula solves the dual half-integrality conjecture by Karaznov on the minimum-cost edge-disjoint S-paths as a special case. We also prove that the cost-less version (μ-EDP) is NP-hard if μ is not a truncated tree metric, where a truncated tree metric is a weight function represented as pairwise distances among balls in a tree. On the other hand, μ-EDP for a truncated tree metric μ reduces to μ'-CEDP for a tree metric μ'. Thus our result is best possible unless $P = NP$. As an application, we get a good approximation algorithm for μ-EDP with "near" tree metric μ by utilizing results from the theory of low-distortion embedding.

This is a joint work with Gyula Pap (Eötvös Loránd University, Budapest).

Cubic and Higher Forms

Ravi Kannan
Microsoft Research Labs.

Maximizing a quadratic form $\sum_{i,j} A_{ij} x_i x_j$ over unit length vectors x is an eigen-value computation. So it can be done efficiently and this has myriad algorithmic applications. More generally, one could seek the maximum of a cubic form $\sum_{i,j,k} A_{ijk} x_i x_j x_k$ or higher order forms. We survey algorithms that approximately maximize higher order forms. This helps solve (approximately) a class of problems called the maximum constraint satisfaction problems (MAX-CSP) of which maximizing the number of satisfied clauses in a Boolean formula is an example. We also show how maximizing cubic forms would help solve the hidden clique problem in graphs and extensions to higher order forms.

Anatomy of a Young Giant Component in the Random Graph

Jeong Han Kim
National Institute for Mathematical Sciences (NIMS), South Korea
jehkim@yonsei.ac.kr

In this talk, we will completely describe the structures of giant components in random graphs $G(n,p)$ with $n^{-1/3} << pn-1 << n^{-1/4}$. The description can be made by using random 3-regular graphs and Galton–Watson Poisson branching processes. The proof uses the Poisson cloning model and interesting computation arguments. We will also present some results regarding the diameter and the mixing time of the giant component. Joint work with J. Ding, E. Lubetzky and Y. Peres.

The Edge Disjoint Paths Problem in Eulerian Graphs and 4-Edge-Connected Graphs[1]

Yusuke Kobayashi
University of Tokyo
kobayashi@mist.i.u-tokyo.ac.jp

We consider the following well-known problem, which is called the *edge-disjoint paths problem.*

Input: A graph G with n vertices and m edges, k pairs of vertices $(s_1, t_1), (s_2, t_2), \ldots, (s_k, t_k)$ in G.

Find : Edge-disjoint paths $P_1, P_2, \ldots, P_k$ in G such that P_i joins s_i and t_i for $i = 1, 2, \ldots, k$.

Robertson and Seymour's graph minor project gives rise to an $O(m^3)$ algorithm for this problem for any fixed k, but their proof of the correctness needs the whole the graph minor project, spanning 23 papers and at least 500 pages proof.

We give a faster algorithm and a simpler proof of the correctness for the edge-disjoint paths problem for any fixed k. Our results can be summarized as follows:

1. If an input graph G is either 4-edge-connected or Eulerian, then our algorithm only needs to look for the following three simple reductions: (i) Excluding vertices of high degree. (ii) Excluding $\leq$ 3-edge-cuts. (iii) Excluding large clique minors.

2. When an input graph G is either 4-edge-connected or Eulerian, the number of terminals k is allowed to be non-trivially superconstant number, up to $k = O((\log \log \log n)^{\frac{1}{2}-\varepsilon})$ for any $\varepsilon > 0$. Thus our hidden constant in this case is dramatically smaller than Robertson-Seymour's. In addition, if an input graph G is either 4-edge-connected planar or Eulerian planar, k is allowed to be $O((\log n)^{\frac{1}{2}-\varepsilon})$ for any $\varepsilon > 0$. The same thing holds for bounded genus graphs. Moreover, if an input graph is either 4-edge-connected H-minor-free or Eulerian H-minor-free for fixed graph H, k is allowed to be $O((\log \log n)^{\frac{1}{2}-\varepsilon})$ for any $\varepsilon > 0$.

3. We also give our own algorithm for the edge-disjoint paths problem in general graphs. We basically follow Robertson-Seymour's algorithm, but we cut half of the proof of the correctness for their algorithm. In addition, the time complexity of our algorithm is $O(n^2)$, which is faster than Robertson and Seymour's.

This is joint work with Ken-ichi Kawarabayashi.

[1] An extended abstract appears in Proceedings of the 21st Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2010), pp. 345–353.

Average Degree Condition Forcing Complete Graph Immersion

Bojan Mohar
Simon Fraser University
mohar(at)sfu.ca

An immersion of a graph H into a graph G is a one-to-one mapping $f : V(H) \to V(G)$ and a collection of edge-disjoint paths, one for each edge of H, such that the path P_{uv} corresponding to edge uv has endpoints $f(u)$ and $f(v)$. We prove that every simple graph with average degree $\Omega(t)$ immerses the complete graph K_t. Moreover, if G is dense enough, then there is an immersion of K_t in which each path P_{uv} is of length precisely 2. This is joint work with Matt DeVos, Zdenek Dvorak, Jacob Fox, Jessica McDonald, and Diego Scheide.

Left and Right (a journey through jungle of arrows)

Jaroslav Nšetřil
Department of Applied mathematics (KAM) and Institute of Theoretical Computer Science (ITI), Charles University, Prague, Czech Republic
nesetril(at)kam.mff.cuni.cz

We introduce various parameters of finite graphs using homomorphism as the pivotal concept. This relates both to some of the ancient and very recent work of L. Lovász as well as to some more modest contributions of the author. The duality between left and right descriptions will be emphasized. This includes the convergence results of Lovász et al., descriptive results of Lovász and Schrijver and restricted homomorphism dualities of JN and P. Ossona de Mendez.

A New Proof for the Two Disjoint Odd Cycles Theorem

Kenta Ozeki
National Institute of Informatics, Japan
ozeki@nii.ac.jp

1 The two disjoint odd cycles theorem

A characterization of graphs without an odd cycle is easy, of course, it is exactly bipartite. However, graphs without two vertex disjoint odd cycles are not so simple. Lovász (see [Seymour95]) is the first to give a proof of the two disjoint odd cycles theorem which characterizes graphs without two vertex disjoint odd cycles. A graph G is called *internally* 4*-connected* if G is 3-connected, and all 3-cut separates only one vertex from the other.

Theorem 1 (Lovász) *Let G be an internally* 4*-connected graph. Then G has no two vertex disjoint odd cycles if and only if G satisfies one of the following;*

- $G - \{x\}$ *is bipartite for some vertex* $x \in V(G)$,
- $G - \{e_1, e_2, e_3\}$ *is bipartite for some edges* $e_1, e_2, e_3 \in E(G)$ *such that* e_1, e_2, e_3 *form a triangle,*
- $|G| \leq 5$, *and*
- *G can be embedded into the projective plane so that every face has boundary of even length.*

However, his proof heavily depends on the seminal result by Seymour [Seymour80] for decomposing regular matroids. In this talk, we give a new proof to Theorem 1 which only depends on the two paths theorem, which characterizes graphs without two disjoint paths with specified ends (i.e, 2-linked graphs). In addition, our proof is simpler and shorter.

This is a joint work with K. Kawarabayashi (National Institute of Informatics).

References

[Seymour80] P.D. Seymour, Decomposition of regular matroids, *J. Combin. Theory Ser. B*, **28** (1980) 305–359.

[Seymour95] P.D. Seymour, Matroid minors, *Handbook of Combinatorics,* **1** Elsevier, Amsterdam (1995) 527–550.

Hyperbolic Surface Subgroups of One-Ended Doubles of Free Groups

Sang-il Oum
KAIST, Daejeon, Korea
sangil@kaist.edu

A *hyperbolic surface group* is the fundamental group of a closed surface with negative Euler characteristic. Gromov [3, p. 277] raised the following question.

> Does every one-ended word-hyperbolic group contain a hyperbolic surface group?

This question has been answered affirmatively for the following cases.

(i) Coxeter groups [2].

(ii) Graphs of free groups with infinite cyclic edge groups with non-trivial second rational homology [1].

(iii) The fundamental groups of closed hyperbolic 3-manifolds [4].

We have the following graph-theoretic conjecture related to the above question. (We write $\delta(v)$ to denote the set of all edges incident with v.)

Conjecture Let $G = (V, E)$ be a non-acyclic graph with a fixed point free involution $\mu : V \to V$ and a bijection $\sigma_v : \delta(v) \to \delta(\mu(v))$ for every vertex v such that $\sigma_{\mu(v)} = \sigma_v^{-1}$ and G has $\deg(v)$ internally vertex-disjoint paths from v to $\mu(v)$.

Then there exists a nonempty list of cycles of G such that for each pair of edges e and f incident with a vertex v, the number of cycles in the list containing both e and f is equal to the number of cycles in the list containing both $\sigma_v(e)$ and $\sigma_v(f)$.

Moreover, the list can be required to contain at least one cycle of length greater than two if G has a connected component which has at least four vertices.

If this conjecture is true, then it implies the validity of Gromov's question for doubles of a free group.

We proved this conjecture for graphs with at most four vertices or regular graphs. This implies that every one-ended double of a free group contains a hyperbolic surface group if the free group has rank two, or the amalgamating set of words contains each generator the same number of times.

This is a joint work with Sang-hyun Kim.

References

[1] Danny Calegari, *scl*, MSJ Memoirs, vol. 20, Mathematical Society of Japan, Tokyo, 2009. MR 2527432

[2] Cameron McA. Gordon, Darren D. Long, and Alan W. Reid, *Surface subgroups of Coxeter and Artin groups*, J. Pure Appl. Algebra **189** (2004), no. 1–3, 135–148. MR 2038569 (2004k:20077)

[3] Mikhail Gromov, *Asymptotic invariants of infinite groups*, Geometric group theory, Vol. 2 (Sussex, 1991), London Math. Soc. Lecture Note Ser., vol. 182, Cambridge Univ. Press, Cambridge, 1993, pp. 1–295. MR 1253544 (95m:20041)

[4] Jeremy Kahn and Vladimir Markovic, *Immersing almost geodesic surfaces in a closed hyperbolic three manifold*, Preprint, 10 2009.

Extendable Structures in Graphs

Michael D. Plummer
Department of Mathematics Vanderbilt University Nashville, TN 37240, USA
michael.d.plummer@vanderbilt.edu

A general question which has generated considerable interest in various settings in graph theory is:

When can a subgraph having certain properties be *extended* to a *larger* subgraph having the same properties?

We report on progress in three specific areas:

(1) When does a "small" matching extend to a maximal (or perfect) matching?

(2) When does an independent set of vertices extend to a maximum independent set?

(3) When does a cycle extend to a 2-factor?

The Lovász Local Lemma

Bruce Reed
School of Computer Science McGill University
breed@cs.mcgill.ca

The Local Lemma is one of Professor Lovász's many fundamental contributions to mathematics. As with so many of his contributions, he sowed the seeds which allowed other researchers to gather the fruits of his ideas for decades to come. We present the lemma, and then survey some variants and applications.

As befits a talk late in the day, our discussion will avoid technicalities and be easily accessible.

Some Recent Results on the Duality Gap

András Sebö
Laboratoire G-SCOP
Andras.Sebo@g-scop.inpg.fr

Still under the effect of Lovász's Hungarian articles "A kombinatorika minimax te'teleiről" - and another early paper of his on graphs and linear programming (I cannot find the volume right now and not even the title) - I wish to present some recent occurrences of linear programming duality in combinatorial problems. For packing bins (joint work with Shmonin); or multicommodity flows - extending Lovász's half integer T-join packing theorem, or related to the Lovász-Cherkassky theorem on multiflows. For estimating the chromatic gap - which is the difference between the chromatic number and the size of a maximum clique -, a Lemma of Gallai playing a central role in Lovász's courses and his book with Plummer interacts with Ramsey graphs in an efficient way for determining the gap (almost) exactly as a function of the number of vertices (joint work with András Gyárfás and Nicolas Trotignon).

The VPN Problem and Extensions

F. Bruce Shepherd
McGill University
bruce.shepherd(at)mcgill.ca

Given a set W, its fractional matching polytope P_W, consists of all vectors $x : W \times W \rightarrow [0, 1]$ such that $\sum_{j \in W} x_{ij} \leq 1$, for all $i \in W$. We consider the following so-called *robust optimization problem.* For a graph $G = (V, E)$, $W \subseteq V$, and per-unit edge costs, find the minimum cost edge capacity which supports every demand in P_W. We focus on the version where we must fix an oblivious routing ahead of time, i.e., fix apriori a path P_{ij} for each $i, j \in W$ (called the *VPN Problem.* We then discuss a variety of extensions and several open problems.

On the Graph Limit Theory

Balázs Szegedy
University of Toronto, Canada
szegedyb@gmail.com

We give a review on a growing subject developed by Laszlo Lovasz and co-authors. In the frame of the so-called ”graph limit” theory, finite graphs play a similar role as rational numbers in analysis. As we pass from rational numbers to real numbers we can use differential calculus and other tools based on continuity. A similar but more complicated picture arises as we look at dense graphs embedded into the so-called graph limit space. We show for example that problems in extremal combinatorics are connected to finite dimensional topology in an interesting way.

Hard Functions for Low-Degree Polynomials over Prime Fields

Hidetoki Tanaka
Tokyo Institute of Technology
tanaka7(at)is.titech.ac.jp

In this talk, we present a new hardness amplification for low-degree polynomials over *prime fields*, namely, we prove that if some function is mildly hard to approximate by any low-degree polynomials then the sum of independent copies of the function is very hard to approximate by them. This result generalizes the XOR lemma for low-degree polynomials over the binary field given by Viola and Wigderson [VW08]. The main technical contribution is the analysis of the Gowers norm over prime fields. For the analysis, we discuss a generalized low-degree test, which we call the *Gowers test*, for polynomials over prime fields, which is a natural generalization of that over the binary field given by Alon, Kaufman, Krivelevich, Litsyn and Ron [AKK$^+$03]. This Gowers test provides a new technique to analyze the Gowers norm over prime fields. By using our argument, we also prove the hardness of modulo functions for low-degree polynomials over prime fields.
(This is a joint work with Andrej Bogdanov and Akinori Kawachi)

References

[AKK$^+$03] Noga Alon, Tali Kaufman, Michael Krivelevich, Simon Litsyn, and Dana Ron, Testing low-degree polynomials over GF(2), Proceedings of RANDOM-APPROX, pages 188–199, 2003.

[VW08] Emanuele Viola and Avi Wigderson, Norms, XOR Lemmas, and Lower Bounds for Polynomials and Protocols, Theory of Computing, 4(1):137–168, 2008.

A Combinatorial Characterization of a Certain Class of 3-Dimensional Rigidity Matroids

Shin-ichi Tanigawa
Kyoto University
tanigawa@kurims.kyoto-u.ac.jp

One of the main topics in rigidity theory is to find a good characterization of generic rigidity of bar-joint frameworks. After Laman's result on 2-dimensional generic rigidity in 1970, it is still an important unsolved problem to find the 3-dimensional counterpart.

A common strategy to deal with a difficult problem in graph theory is to restrict a graph class, and several partial results are also known for this problem for e.g., triangulations, bipartite graphs, sparse graphs, some minor closed classes, the squares of graphs. In rigidity theory, it is also reasonable to consider a special class of structural models, e.g., the body-bar model by Tay (1984), the body-hinge model by Whiteley (1988), the body-bar-hinge model by Jackson and Jordán (2009), and the rod-bar model by Tay (1991).

In this talk, we will discuss a combinatorial characterization of the 3-dimensional generic rigidity matroid for a structural model including the existing special classes and included in bar-joint frameworks. Inspired by an alternative proof of Laman's theorem by Lovász and Yemini (1982), we will show how to construct the rigidity matroid by applying variants of Dilworth truncation.

Effective Principal Component Analysis

Santosh Vempala
Georgia Tech
vempala@gatech.edu

Principal Component Analysis (PCA) seems to be the most widely used technique on high-dimensional or large data sets. This is despit e the fact that for typical applications (finding nearest neighbors, clustering, learning etc.), it is not hard to build examples on which PCA *fails*. In this talk, we discuss some problems where the performance of PCA is provably near-optimal, and no other method is known to have similar guarantees. The problems include: (a) unraveling a mixture of unknown Gaussians and (b) learning a function of an unknown subpsace. On the way, we will report recent extensions of standard PCA that are noise-resistant, affine-invariant and use higher moments.

The talk is based mostly on work with Charlie Brubaker and Ying Xiao.

(Poster)

Title: Combinatorial Approaches for Estimating Distribution Functions in Stochastic Optimization

Presenter: Ei Ando (ando-ei(at)cis.sojo-u.ac.jp)
Affiliation: Faculty of Computer and Information Sciences, Sojo University

Abstract

The stochastic optimization problems have been researched to deal with the optimization problems that consist of uncertain values in the model. A promising approach to a computation problem in the real world is to model the structure of the problem as a weighted graph and solve the optimization problem in the graph by a known algorithm. However, in some cases, we cannot simply take this approach because the measured values may vary from time to time. Such uncertainty is often observed in measuring the time to go through a road, the throughput of communication links in a computer network, the gate delays in a logical circuit, and so on. At that time, one approach to the uncertain values is to model them as the stochastic variables and solve the optimization problem that consists of these stochastic variables. This is the stochastic optimization problem.

In the stochastic optimization problem, we must be careful about the meaning of “solving the problem.” Since the parameters such as edge weights are random variables, any solution can be optimal depending on the realization of the parameters. There are at least two approaches for the problem: (1) By re-defining the optimality in such a way that optimal solution is determined, one is to choose a solution, or (2) one is to estimate the distribution of the optimal weight, which is a random variable. Here we adopt the second approach.

In this poster session, we see two results. We first consider the stochastic longest path problem in DAGs with random edge weights and consider the time to compute exactly the distribution function of the longest path length and show some previously unknown cases where the problem can be solved in polynomial time. This result has been presented in [1]. After that, we show a generic approximation algorithm; the algorithm approximately computes the distribution function of the optimal weight and it can be applied to any stochastic optimization problem. This result has been presented in [2].

References

[1] E. Ando, H. Ono, K. Sadakane and M. Yamashita, Computing the Exact Distribution Function of the Stochastic Longest Path Length in a DAG, Proc. of the 6th conference on Theory and Application of the Models of Computation, LNCS, 5532, pp. 98-107, Springer, 2009.

[2] E. Ando, H. Ono and M. Yamashita, A Generic Algorithm for Approximately Solving Stochastic Graph Optimization Problems, Proc. of the 5th Symposium on Stochastic Algorithms, Foundations and Applications (SAGA 2009), LNCS, 5792, pp. 89-103, Springer, 2009.

(Poster)

Title: On the Optimality of Lattices for the Coppersmith Technique

Presenter: Yoshinori, AONO (aono5@is.titech.ac.jp)
Affiliation: Department of Computer Science, Tokyo Institute of Technology

Abstract

Coppersmith [1] proposed a polynomial-time algorithm, which we will refer the *Coppersmith technique*, for finding solutions of a modular equation

$$F(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \equiv 0 \pmod{N}, \tag{1}$$

within the range of $|x| < N^{1/d-\varepsilon}$, in polynomial time in $\log N$. The outline of the Coppersmith technique is (i) to convert a given modular equation to a certain algebraic equation keeping the same solutions by using a lattice reduction algorithm and (ii) to solve the algebraic equation by some numerical method. One of the key points of this technique is to construct a good lattice for the lattice reduction algorithm.

Since his work, several improvements of the Coppersmith technique have been proposed together with applications. In particular, several attacks for the RSA cryptography and its variations have designed by considering multivariate versions and unknown modulo versions. Hence, showing some limitation of the technique is important to discuss the security of these cryptographic schemes.

In this presentation, we prove a general type limitation of the direct usage of the Coppersmith technique for solving any univariate equation (1). More precisely, we investigate a *lattice bound* that derives a sufficient condition for the technique to work, and discuss when this bound cannot be satisfied by any lattice construction. We first show that the range $|x| < N^{1/d}$ is necessary for this bound by any "standard" lattice construction in the technique. Thus, for getting a better range, we need to consider some non-standard way to construct a lattice. We then show that any non-standard construction leads a reduction of the original problem (1) to a strictly simpler one. But from this, we can show that such a non-standard construction would be impossible in polynomial-time in general. Hence, for the Coppersmith technique, we may claim that the range $|x| < N^{1/d}$ cannot be achieved by any lattice which is efficiently constructed.

One important future work is to extend our argument to the multivariate situation. In particular, it is interesting if we can prove some bound for the method of Boneh and Durfee [2] by which we can recover the RSA secret key when it is smaller than $N^{0.292}$.

References

[1] D. Coppersmith, Finding a small root of a univariate modular equation, *Proc, of EUROCRYPT 1996*, LNCS, vol. 1070, pp. 155-165, 1996.

[2] D. Boneh and G. Durfee, Cryptanalysis of RSA with private Key d Less Than $N^{0.292}$, in *Proc. of EUROCRYPT 1999*, LNCS, vol. 1592, pp. 389-401, 1999.

(Poster)

Title: Vector Precoding Using Mean Field Approximation

Presenter: Naruhiko Hayashi (hayashi@sp.dis.titech.ac.jp)
Affiliation: Department of Computational Intelligence and Systems Science
Tokyo Institute of Technology

Abstract

We investigate a nonlinear precoding scheme of MIMO communication, which aims to reduce the transmit energy, utilizing methods of statistical mechanics. In the scheme, a message to be transmitted to a receiver is expanded to a space of relaxed alphabets and replaced by a sequence which has the minimum transmit energy in that space. Since this process can be considered as a combinatorial optimization problem, statistical mechanics can be used for estimating a performance. Recently, Mueller et al.[1] investigated the performance of this scheme using the replica method under the replica symmetric ansatz. However, the analysis seems inadequate even in qualitative aspects. Therefore, we handle the same problem in a more advanced framework based on the one-step replica symmetry breaking ansatz. In addition, by using mean field approximation, practical algorithms, which achieve nearly optimal performance with a reasonable amount of time, are developed.

References

[1] R. Muller, Dongning Guo, and A. Moustakas,“ Vector Precoding for Wireless MIMO Systems and its Replica Analysis, ”, 2008.

(Poster)

Title: Reverse Engineering of Data Structures on Strings

Presenter: Tomohiro I (`tomohiro.i@inf.kyushu-u.ac.jp`)
Affiliation: Department of Informatics, Kyushu University

Abstract

A *string* is a sequence of characters. There are useful data structures for string processing such as suffix arrays and border arrays. One of the important problems is to construct them from strings efficiently. In contrast, the *reverse engineering problem* for a string data structure is to compute a string which has a given data structure, whose theoretical interest is to reveal the combinatorial properties of data structures. As far as we know, these types of problems were first introduced in [1], and have been extensively studied since. We consider the reverse problems for *parameterized border arrays* (*p-border arrays*) and palindromic structures on strings.

The parameterized pattern matching problem is to check if there exists a renaming bijection on the alphabet with which a given pattern can be transformed into a substring of a given text. A p-border array is a parameterized version of a standard border array, and we can efficiently solve the parameterized pattern matching problem using the p-border array of the pattern. Here the reverse problem for p-border arrays is to compute a string whose p-border array is a given integer array, if such exists. In the binary case, we presented in [2] a linear time and space algorithm to solve it. For a larger alphabet, we developed an $O(n^{1.5})$-time $O(n)$-space algorithm, where n is the length of the input integer array [3]. The best previously known solution takes time proportional to the n-th Bell number $\frac{1}{e}\sum_{k=0}^{\infty}\frac{k^n}{k!}$, and hence our algorithm is quite efficient.

A palindrome is a symmetric string that reads the same forward and backward. Let $Pals(w)$ denote the set of maximal palindromes of a string w in which each palindrome is represented by a pair (c, r), where c is the center and r is the radius of the palindrome. We remark that $Pals(w)$ represents all palindromic structures of w in space linear in the length of w. In [4] we presented a linear time algorithm which finds a string w such that $Pals(w)$ is identical to a given set of maximal palindromes.

References

[1] F. Franek, S. Gao, W. Lu, P. J. Ryan, W. F. Smyth, Y. Sun, L. Yang, Verifying a border array in linear time, J. Comb. Math. and Comb. Comp. 42 (2002) 223–236.

[2] T. I, S. Inenaga, H. Bannai, M. Takeda, Counting parameterized border arrays for a binary alphabet, in: Proc. LATA'09, Vol. 5457 of LNCS, 2009, pp. 422–433.

[3] T. I, S. Inenaga, H. Bannai, M. Takeda, Verifying a parameterized border array in $O(n^{1.5})$ time, in: Proc. CPM'10, Vol. 6129 of LNCS, 2010, pp. 238–250.

[4] T. I, S. Inenaga, H. Bannai, M. Takeda, Counting and Verifying Maximal Palindromes, in: Proc. SPIRE'10, Vol. 6393 of LNCS, 2010, pp. 135–146.

(Poster)

Title: Testing Classes of First-Order Formulae

Presenter: Charles Jordan (skip@ist.hokudai.ac.jp)
Affiliation: Division of Computer Science, Hokkaido University

Abstract

In property testing, the goal is to distinguish structures that have some desired property from those that are *far* from having the property, based on only a small, random sample of the structure. Here, we introduce our recent work on the classification of first-order sentences according to their testability. This classification was initiated by Alon *et al.* [AFKS00], who showed that graph properties expressible with prefix $\exists^*\forall^*$ are testable but that there is an untestable graph property expressible with quantifier prefix $\forall^{12}\exists^5$. Although they focused only on quantifier *alternations*, it is natural to ask whether one can express an untestable property with fewer quantifiers. Our recent work implies that the minimum number sufficient to express such a property is three or four, including at least two universal and one existential quantifier. It is also natural to consider the vocabulary and pattern of quantifiers, with the goal of attaining a classification similar to that for decidability (see, e.g., Börger *et al.* [BGG97]). The following summarizes what is currently known (for details, see [JZ09], [JZ10a] and [JZ10b]).

Testable : monadic first-order, and all properties expressible with $\exists^*\forall\exists^*$ or $\exists^*\forall^*$ with equality

Untestable : some graph properties expressible with $\forall^3\exists$, $\forall^2\exists\forall$, $\forall\exists\forall^2$ and $\forall\exists\forall\exists$ with equality

This classification is intimately connected with testing non-uniform hypergraphs and extensions of Szemerédi's regularity lemma to hypergraphs. In particular, the extension of the positive result for $\exists^*\forall^*$ from graphs is essentially an application of a result by Austin and Tao [AT10].

References

[AFKS00] N. Alon, E. Fischer, M. Krivelevich, M. Szegedy. Efficient testing of large graphs. *Combinatorica*, 20(4):451–476, 2000.

[AT10] T. Austin and T. Tao. On the testability and repair of hereditary hypergraph properties. *Random Struct. Algorithms*, 36(4):373–463, 2010.

[BGG97] E. Börger, E. Grädel, Y. Gurevich. *The Classical Decision Problem.* Springer, 1997.

[JZ09] C. Jordan and T. Zeugmann. Relational properties expressible with one universal quantifier are testable. In Proc. SAGA 2009, LNCS 5792, pp. 141–155, 2009.

[JZ10a] C. Jordan and T. Zeugmann. Untestable properties expressible with four first-order quantifiers. In Proc. LATA 2010, LNCS 6031, pp. 333–343, 2010.

[JZ10b] C. Jordan and T. Zeugmann. A note on the testability of Ramsey's Class. In Proc. TAMC 2010, LNCS 6108, pp. 296–307, 2010.

(Poster)

Title: A Bound for the Number of Different Basic Solutions Generated by the Simplex Method

Presenter: Tomonari Kitahara (`kitahara.t.ab@m.titech.ac.jp`)
Affiliation: Tokyo Institute of Technology

Abstract

In this presentation, we give an upper bound for the number of different basic feasible solutions generated by the simplex method for linear programming problems having optimal solutions. The bound is polynomial of the number of constraints, the number of variables, and the ratio between the minimum and the maximum values of all the positive elements of primal basic feasible solutions. When the primal problem is nondegenerate, it becomes a bound for the number of iterations. We show some basic results when it is applied to special linear programming problems. The results include strongly polynomiality of the simplex method for Markov Decision Problem by Ye [3].

References

[1] G. B. Dantzig: *Linear Programming and Extensions.* Princeton University Press, Princeton, New Jersey, 1963.

[2] V. Klee and G. J. Minty: How good is the simplex method. In O. Shisha, editor, *Inequalities III*, Academic Press, New York, NY, 1972.

[3] Y. Ye: The Simplex Method is Strongly Polynomial for the Markov Decision Problem with a Fixed Discount Rate. Technical paper, available at http://www.stanford.edu/ yyye/simplexmdp1.pdf, 2010.

(Poster)

Title: Non-Programmable Weakened Random Oracle

Presenter: Mario Larangeira (larangeira.m.aa(at)m.titech.ac.jp)
Affiliation: Department of Computer Science, Tokyo Institute of Technology

Abstract

In the Random Oracle Methodology (ROM) one considers a function h which maps X into Y, for finite sets X and Y, as an ideal hash function. Moreover, it is common to choose arbitrary (but convenient for some security game) values for the outputs of the function h in to prove security of cryptographic schemes. This ability is denoted as the *programmability* of the random oracle and very often proofs in this model use this ability. Variants of this model have appeared in the literature.

The idea of the Weakened Random Oracle Models (WROM)[2] is to provide the adversary with specific oracles which break properties (i.e., *collision*, *second preimage* and *first preimage* resistances) of the random oracle. This defines three new models, respectively CT-ROM (Collision Tractable), SPT-ROM (Second-Preimage Tractable) and FPT-ROM (First-Preimage Tractable) which are closer to real hash functions.

Motivation and Interpretation for Programmability. In general, the main goal of this research, likewise [2], is to investigate the necessary properties of the ROM to prove the security of cryptographic schemes. We define strictly weaker models than the ROM or even WROM, by using the non-programmable random oracle model (NPROM)[1], to remove the programmability from WROM. The non-programmable proofs intuitively mean that the proofs work even when the description of the hash algorithm are publicly available which is natural and desired for cryptographic purposes. This means that any party can run the algorithm by itself but no property of the hash function exists to be exploited other than that the random oracle also has. More formally, it means weaker assumption about the hash functions.

Our Contribution. We extended the results from [2] to non-programmable framework. As far as we know, this work is the first to propose such non-programmable frameworks and consider them to study the security of signature schemes.

References

[1] Jesper Buus Nielsen, "Separating Random Oracle Proofs from Complexity Theoretic Proofs: The Non-commiting Encryption Case," *Crypto 2002 - Advances in Cryptology*, LNCS 2442, Springer, pp. 191-214, 2002.

[2] A. Numayama, T. Isshiki, and K.Tanaka, "Security of digital signature schemes in weakened random oracle models," *PKC 2008*, LNCS 4939, Springer, pp. 268-287, 2008.

(Poster)

Title: Parameterized Complexity of the Spanning Tree Congestion Problem
Presenter: Yota Otachi (otachi@dais.is.tohoku.ac.jp)
Affiliation: Tohoku University

Abstract

Let G be a graph and T a spanning tree of G. The *detour* for an edge $\{u, v\} \in E(G)$ is the unique u–v path in T. We define the *congestion* of $e \in E(T)$, denoted by $\mathrm{cng}_{G,T}(e)$, as the number of detours that contain e. The *congestion of G in T*, denoted by $\mathrm{cng}_G(T)$, is the maximum congestion over all edges in T. The *spanning tree congestion* of G, denoted by $\mathrm{stc}(G)$, is the minimum congestion over all spanning trees of G.

We study the problem of determining the *spanning tree congestion* of a graph. We present some sharp contrasts in the parameterized complexity of this problem. First, we show that on apex-minor-free graphs, a general class of graphs containing planar graphs, graphs of bounded treewidth, and graphs of bounded genus, the problem to determine whether a given graph has spanning tree congestion at most k can be solved in linear time for every fixed k. We also show that for every fixed k and d the problem is solvable in linear time for graphs of degree at most d. In contrast, if we allow only one vertex of unbounded degree, the problem immediately becomes NP-complete for any fixed $k \geq 8$. Moreover, the hardness result holds for graphs excluding the complete graph on 6 vertices as a minor. We also observe that for $k \leq 3$ the problem becomes polynomially time solvable.

This is joint work with Hans L. Bodlaender, Fedor V. Fomin, Petr A. Golovach, and Erik Jan van Leeuwen. Extended abstract of some results in this paper appeared in the proceedings of WG 2010 [OBL2010].

References

[OBL2010] Y. Otachi, H.L. Bodlaender, and E.J. van Leeuwen, Complexity Results for the Spanning Tree Congestion Problem, in Proc. of WG 2010, Lecture Notes in Comput. Sci., vol. 6410.

(Poster)

Title: Average-Case Complexity of Detecting Cliques

Presenter: Benjamin Rossman (brossman@mit.edu)
Affiliation: Tokyo Institute of Technology

Abstract

We investigate the computational complexity of detecting cliques in random graphs. Specifically, we consider the *k-clique problem* (given a graph as input, decide whether it contains a complete subgraph of fixed size k) in Erdős-Rényi random graphs with an appropriate density of edges (such that the probability of containing a k-clique is bounded away from 0 and 1). Our results — both lower and upper bounds — show that the k-clique problem has average-case complexity $n^{k/4+O(1)}$ in two important models of computation: *bounded-depth circuits* ($\{\wedge, \vee, \neg\}$-circuits with unbounded fan-in and depth at most $k^{-2} \log n / \log \log n$) and *monotone circuits* ($\{\wedge, \vee\}$-circuits with no restriction on depth). These results are the first unconditional average-case lower bounds for the k-clique problem and answer longstanding open questions in complexity theory (concerning the complexity class AC^0) and finite model theory (showing that a certain hierarchy of bounded-variable logics is strict).

References

[1] Benjamin Rossman. Average-Case Complexity of Detecting Cliques. Ph.D. Thesis, MIT, 2010.

(Poster)

Title: On Partitioning Colored Points

Presenter: Takahisa Toda (toda.takahisa@hw3.ecs.kyoto-u.ac.jp)
Affiliation: Graduate School of Human and Environmental Studies, Kyoto University

Abstract

Let us imagine that colorful candles, each of which is painted with one of k colors, are placed on the top of a cake. We want to cut this cake with a knife by several times in such a way that all the candles with the same color are on one of the pieces but candles with different colors must not be on the same piece. The question is when we can cut it successfully.

Let us formally describe this problem. Let X be a finite subset of $\mathbf{R}^d$, and suppose that each point is painted with one of k colors. We say that a subset S of X can be *partitioned along the colors by hyperplanes* if there is a family $\mathcal{F}$ of hyperplanes satisfying the following three conditions:

1. every hyperplane in $\mathcal{F}$ avoids the points in S;
2. every two points in S with different colors can be separated by some hyperplane in $\mathcal{F}$;
3. no hyperplane in $\mathcal{F}$ separates points in S with the same color.

We prove the following theorem: if every $(d+1) \cdot \eta_d(k) + k$ or fewer points in X can be partitioned along the colors by hyperplanes, then all the points in X can be partitioned along the colors by hyperplanes, where $\eta_d(k) = \sum_{i=0}^{d} \binom{k-2}{i}$.

Kirchberger [2] proved a theorem answering this problem for 2 colors, which is known as Kirchberger's theorem. Arocha et al. [1] and Pór [3] studied other Kirchberger-type theorems. They introduced the notion of separations for k colors as follows. Let A_i be a finite set of points painted with the i-th color. They say that $\bigcup_{i=1}^{k} A_i$ is *separated* if $\bigcap_{i=1}^{k} \operatorname{conv} A_i = \emptyset$, where $\operatorname{conv} A_i$ denotes the convex hull of A_i. Their theorems are based on this notion.

References

[1] J.L. Arocha, I. Bárány, J. Bracho, R. Fabila, and L. Montejano, "Very colorful theorems," Discrete Comput. Geom., vol.42, no.2, pp.142–154, 2009.

[2] P. Kirchberger, "Über tschebyscheffsche annäherungsmethoden," Math. Ann., vol.57, pp.509–540, 1903.

[3] A. Pór, Diploma Thesis, Eötvös University, Budapest, 1998.

(Poster)

Title: Geometric Realization of Triangulations on Nonorientable Surfaces
Presenter: Shoichi Tsuchiya (s-s-t-b@mail.goo.ne.jp)
Affiliation: Yokohama National University

Abstract

A *map* is a fixed embedding of a graph on a surface F^2. A *triangulation* on a surface F^2 is a map on F^2 such that each face is bounded by a 3-cycle, where a k*-cycle* means a cycle of length k. We suppose that the graph of a map is always *simple*, i.e., with no multiple edges and no loops. Let M be a map on a surface F^2. A *geometric realization* of M is an embedding of F^2 into a Euclidean 3-space with no self-intersection such that each face of M is a flat polygon.

It has been proved that every spherical or toroidal triangulation has a geometric realization [4, 1]. Bokowski et al. have shown that a triangulation by the complete graph K_{12} with twelve vertices on the orientable closed surface of genus 6 has no geometric realization [2].

We would like to consider the case when a surface is a nonorientable one in particular the Möbius band. Brehm has shown a *Möbius triangulation* (i.e., a triangulation on the Möbius band) with no geometric realization [3].

Theorem 1 (Brehm [3]) *If a Möbius triangulation M has a boundary 3-cycle C and a 3-cycle C' disjoint from C which forms an annular region with C, then M has no geometric realization.*

Recently we characterize geometrically realizable Möbius triangulations as follows.

Theorem 2 *A Möbius triangulation M has a geometric realization if and only if M does not have two disjoint 3-cycles homotopic to the boundary of M.*

Theorem 2 claims that the structure shown by Brehm is the only obstruction breaking a geometric realizability of Möbius triangulations.

References

[1] D. Archdeacon, C.P. Bonnington and J.A. Ellis-Monanghan, How to exhibit toroidal maps in space, *Discrete Comp. Geom.* **38** (2007), 573–594.

[2] J. Bokowski and A. Guedes de Oliveira, On the generation of oriented matroids, *Discrete Comput. Geom.* **24** (2004), 197–208.

[3] U. Brehm, A nonpolyhedral triangulated Möbius strip, *Proc. Amer. Math. Soc.* **89** (1983), 519–522.

[4] E. Steinitz, Polyeder und Raumeinteilungen, *Enzykl. Math. Wiss.* Vol. 3, Teil 3A612 (1922), 1–139.

(Poster)

Title: Optimal Constant-Time Approximation Algorithms and (Unconditional) Inapproximability Results for Every Bounded-Degree CSP

Presenter: Yuichi Yoshida (`yyoshida@lab2.kuis.kyoto-u.ac.jp`)

Affiliation: Kyoto University and Preferred Infrastructure

Abstract

Raghavendra [1] gave an elegant and surprising result: if Khot's Unique Games Conjecture [2] is true, then for every constraint satisfaction problem (CSP), the best approximation ratio is attained by a certain simple semidefinite programming and a rounding scheme for it.

In this paper, we show that similar results hold for constant-time approximation algorithms in the bounded-degree model. Specifically, we present the followings: (i) For every CSP, we construct an oracle that serves an access, in constant time, to a nearly optimal solution to a basic LP relaxation of the CSP. (ii) Using the oracle, we give a constant-time rounding scheme that achieves an approximation ratio coincident with the integrality gap of the basic LP. (iii) Finally, we give a generic conversion from integrality gaps of basic LPs to hardness results. All of those results are *unconditional.* Therefore, for every bounded-degree CSP, we give the best constant-time approximation algorithm among all.

A CSP instance is called ϵ-far from satisfiability if we must remove at least an ϵ-fraction of constraints to make it satisfiable. A CSP is called testable if there is a constant-time algorithm that distinguishes satisfiable instances from ϵ-far instances with probability at least 2/3. Using the results above, we also derive, under a technical assumption, an equivalent condition under which a CSP is testable in the bounded-degree model.

References

[1] Prasad Raghavendra. Optimal algorithms and inapproximability results for every CSP? In *Proc. of STOC 08*, pages 245–254, 2008.

[2] Subhash Khot. On the power of unique 2-prover 1-round games. In *Proc. of STOC 2002*, pages 767–775, 2002.