Report from Dagstuhl Seminar 18391

Algebraic Methods in Computational Complexity

Edited by

Markus Bläser[1], Valentine Kabanets[2], Jacobo Torán[3], and Christopher Umans[4]

1 **Universität des Saarlandes, DE,** mblaeser@cs.uni-saarland.de
2 **Simon Fraser University – Burnaby, CA,** kabanets@cs.sfu.ca
3 **Universität Ulm, DE,** jacobo.toran@uni-ulm.de
4 **Caltech – Pasadena, US,** umans@cs.caltech.edu

Abstract

Computational Complexity is concerned with the resources that are required for algorithms to detect properties of combinatorial objects and structures. It has often proven true that the best way to argue about these combinatorial objects is by establishing a connection (perhaps approximate) to a more well-behaved algebraic setting. Indeed, many of the deepest and most powerful results in Computational Complexity rely on algebraic proof techniques. The Razborov-Smolensky polynomial-approximation method for proving constant-depth circuit lower bounds, the PCP characterization of NP, and the Agrawal-Kayal-Saxena polynomial-time primality test are some of the most prominent examples.

In some of the most exciting recent progress in Computational Complexity the algebraic theme still plays a central role. There have been significant recent advances in algebraic circuit lower bounds, and the so-called chasm at depth 4 suggests that the restricted models now being considered are not so far from ones that would lead to a general result. There have been similar successes concerning the related problems of polynomial identity testing and circuit reconstruction in the algebraic model (and these are tied to central questions regarding the power of randomness in computation). Also the areas of derandomization and coding theory have experimented important advances.

The seminar aimed to capitalize on recent progress and bring together researchers who are using a diverse array of algebraic methods in a variety of settings. Researchers in these areas are relying on ever more sophisticated and specialized mathematics and the goal of the seminar was to play an important role in educating a diverse community about the latest new techniques.

Seminar September 23–28, 2018 – http://www.dagstuhl.de/18391

1998 ACM Subject Classification Theory of computation → Algebraic complexity theory, Theory of computation → Problems, reductions and completeness, Theory of computation → Circuit complexity

Keywords and phrases computational complexity, algebra, (de-) randomization, circuits, coding, lower bounds

Digital Object Identifier 10.4230/DagRep.8.9.133

Algebraic Methods in Computational Complexity, *Dagstuhl Reports*, Vol. 8, Issue 09, pp. 133–153
Editors: Markus Bläser, Valentine Kabanets, Jacobo Torán, and Christopher Umans

Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Executive Summary

Markus Bläser
Valentine Kabanets
Jacobo Torán
Christopher Umans

The seminar brought together more than 40 researchers covering a wide spectrum of complexity theory. The focus on algebraic methods showed the great importance of such techniques for theoretical computer science. We had 24 talks, most of them lasting about 45 minutes, leaving ample room for discussions. We also had a much appreciated rump session on Tuesday evening in which Antonina Kolokolova, Bill Gasarch, Lance Fortnow, Chandran Saha, William Hoza, Neeraj Kajal and Arpita Korwar presented some open questions. In the following we describe the major topics of discussion in more detail.

Circuit Complexity

This is an area of fundamental importance to Complexity. Circuits studied from many different perspectives were one of the main topics in the seminar. *Eric Allender* gave an overview of the Minimum Circuit Size Problem (MCSP): given the truth-table for a Boolean function, what is the size of the minimum circuit computing it? In his talk he mentioned some interesting results proving that some low complexity classes cannot be reduced to the problem of computing superlinear approximations to circuit size.

Arithmetic circuits and formulas are a special computation model that uses $+$ and $\times$ as operators for computing polynomials instead of Boolean operations. *Nutan Limaye* presented a depth hierarchy theorem for this model showing that there is a polynomial computed by a depth $D+1$ polynomial sized multilinear formula such that any depth D multilinear formula computing the polynomial must have exponential size.

Chandan Saha considered a further restriction to depth three circuits C computing a polynomial $f = T_1 + T_2 + \cdots + T_s$, where each T_i is a product of d linear forms in n variables. He presented a randomized algorithm to reconstruct non-degenerate homogeneous depth three circuits, for the case $n > (3d)^2$, given black-box access to f. The algorithm works in polynomial time in n, s and d.

Depth-2 circuits with polynomial size and linear threshold functions were presented by *Meena Mahajan*. She surveyed the landscape below these circuits and present one new result concerning decision lists.

Algebraic Complexity

There were also several presentations discussing the complexity of several problems over algebraic structures.

Nitin Saxena considered in his talk the problem of testing whether a set F of polynomials given as algebraic circuits has an algebraic dependence. He showed that this problem can be computed in AM $\cap$ coAM thus solving an open question from 2007.

Problems related to the minimum code-word problem and the existence of non-trivial automorphism moving few vertices in graphs or hypergraphs, were presented by *V. Arvind* in his talk. He discuss the parameterized complexity of this and related algebraic problems.

Josh Alman gave an interesting talk on Matrix Multiplication (MM). He surveyed the two main approaches for MM algorithms: the Laser method of Strassen, and the Group theoretic approach of Cohn and Umans and defined a generalization which subsumes these two approaches. He then explained ways to obtain lower bounds for algorithms for MM when using these algorithmic methods.

Rohit Gurjar studied the class of matrices A for which the lattice $L(A)$ formed by all integral vectors v in the null-space of A, has only polynomially many near-shortest vectors. He proved that this is the case when the matrix A is totally unimodular (all sub-determinants are 0, +1, or −1). As a consequence he could show a deterministic algorithm for PIT for any polynomial of the form $\det(\sum x_i A_i)$ for rank-1 matrices A_i.

Pseudo-Randomness and Derandomization

Derandomization is an area where there are tight connections between lower bounds and algorithms. Strong enough circuit lower bounds can be used to construct pseudo-random generators that can then be used to deterministically simulate randomized algorithms. A central question in derandomization is whether randomized logspace RL equals deterministic logspace L. To show that RL = L, it suffices to construct explicit pseudorandom generators that fool polynomial-size read-once (oblivious) branching programs (roBPs). There were two talks related to this question. *Michael Forbes* presented a method to obtain an explicit PRG with seed-length $O(\log^3 n)$ for polynomial-size roBPs reading their bits in an unknown order. *William Hoza* gave an explicit hitting set generator for read-once branching programs with known variable order. As a corollary of this construction, it follows that every RL algorithm that uses r random bits can be simulated by an NL algorithm that uses only $O(r/\log^c n)$ nondeterministic bits, where c is an arbitrarily large constant. Another consequence of the result is that any RL algorithm with small success probability ϵ can be simulated deterministically in space $O(\log^{3/2} n + \log n \log\log(1/\epsilon))$.

A hitting set is a set of instances such that every non-zero polynomial in the model has a non-root in the set. This would solve the Polynomial Identity Testing problem (PIT) in that model. *Ramprasad Saptharishi* showed that by barely improving the trivial $(s+1)^n$ size hitting set even for n-variate degree s, size s algebraic circuits, we could get an almost complete derandomization of PIT.

In a second talk, *William Hoza* talked about the possibility of derandomizing an algorithm by using randomness from the input itself. For a language L with a bounded-error randomized algorithm in space S and time $n \cdot poly(S)$ he gave a randomized algorithm for L with the same time and space resources but using only $O(S)$ random bits; the algorithm has a low failure probability on all but a negligible fraction of inputs of each length.

Andrej Bogdanov considered the problem of extracting true randomness from a set biased dice (Santha-Vazirani sources). He presented a recent result in which he completely classified all non-trivial randomness sources of this type into: non-extractable ones, extractable from polynomially many samples, and extractable from an logarithmically many samples (in the inverse of the error).

Coding Theory

Error-correcting codes and other kinds of codes, particularly those constructed from polynomials, i.e. Reed-Solomon codes or Reed-Muller codes, lie at the heart of many significant results in Computational Complexity. This is an area in which the relation between different areas of complexity, like the analysis of algebraic structures or derandomization becomes especially fruitful.

Greatly improving previously known constructions for an odd size alphabet, *Michal Koucký* presented a construction of quasi-Gray codes of dimension n and length 3^n over the ternary alphabet $\{0, 1, 2\}$ with worst-case read complexity $O(\log n)$ and write complexity 2. This generalizes to arbitrary odd-size alphabets. These results were obtained via a novel application of algebraic tools together with the principles of catalytic computation.

Noga Ron-Zewi presented a very recent result showing that Folded Reed-Solomon codes achieve list decoding capacity with constant list sizes, independent of the block length. She explained that multiplicity codes exhibit similar behavior, and used this to obtain capacity achieving locally list decodable codes with query complexity significantly lower than previous constructions.

Binary error correcting code with relative distance $(1-\epsilon)/2$ and relative rate $\epsilon^{2+o(1)}$ were explained in one of the talks given by *Amnon Ta-Shma*. Previous explicit constructions had rate about ϵ^3. The main tool used for this construction are *Parity Samplers*. He explained how to get better explicit parity samplers using a variant of the zig-zag product.

In his second talk, Amnon talked about $(1-\tau, L)$ erasure list-decodable codes. He presented a recent work where he constructed for the first time an explicit binary $(1-\tau, L)$ erasure list-decodable code having rate $\tau^{1+\gamma}$ (for any constant $\gamma > 0$ and τ small enough) and list-size $\text{poly}(\log 1/\tau)$, exhibiting an explicit non-linear code that provably beats the best possible linear one. The main ingredient in his construction is a new (and almost-optimal) *unbalanced* two-source extractor.

Quantum Complexity

Complexity issues arising in the context of quantum computation are an important area in Complexity Theory since several decades. In this workshop we had one talk on this topic. *Sevag Gharibian* talked about quantum versions of the classical k-SAT problem. He talked about the problem of computing satisfying assignments to k-QSAT instances which have a "matching" or "dimer covering"; this is an NP problem whose decision variant is trivial, but whose search complexity remains open. He presented a parameterized algorithm for k-QSAT instances from a non-trivial class, which allows to obtain exponential speedups over brute force methods.

Conclusion

As is evident from the list above, the talks ranged over a broad assortment of subjects with the underlying theme of using algebraic and combinatorial techniques. It was a very fruitful meeting and has hopefully initiated new directions in research. Several participants specifically mentioned that they appreciated the particular focus on a common class of *techniques* (rather than end results) as a unifying theme of the workshop. We look forward to our next meeting!

2 Table of Contents

3 Overview of Talks

3.1 The Non-Hardness of Approximating Circuit Size

Eric Allender (Rutgers University – Piscataway, US)

The Minimum Circuit Size Problem (MCSP) has been the focus of intense study recently; MCSP is hard for SZK under rather powerful reductions, and is provably not hard under "local" reductions computable in TIME($n^{0.49}$). The question of whether MCSP is NP hard (or indeed, hard even for small subclasses of P) under some of the more familiar notions of reducibility (such as many-one or Turing reductions computable in polynomial time or in AC^0) is closely related to many of the longstanding open questions in complexity theory.

All known hardness results for MCSP hold also for computing somewhat weak approximations to the circuit complexity of a function. Some of these results were proved by exploiting a connection to a notion of time-bounded Kolmogorov complexity (KT) and the corresponding decision problem (MKTP). More recently, a new approach for proving improved hardness results for MKTP was developed, but this approach establishes only hardness of extremely good approximations of the form $1 + o(1)$, and these improved hardness results are not yet known to hold for MCSP. In particular, it is known that MKTP is hard for the complexity class DET under nonuniform AC^0-many-one reductions, implying that MKTP is not in $AC^0[p]$ for any prime p. It is still open if similar circuit lower bounds hold for MCSP. One possible avenue for proving a similar hardness result for MCSP would be to improve the hardness of approximation for MKTP beyond $1 + o(1)$ to $\omega(1)$. In this paper, we show that this is impossible.

More specifically, we prove that PARITY does not reduce to the problem of computing superlinear approximations to KT-complexity or circuit size via AC^0-Turing reductions that make $O(1)$ queries. This is significant, since it is known that just ONE query to a much worse approximation of circuit size or KT-complexity suffices, for an AC^0 reduction to compute an approximation to any set in P/poly. For weaker approximations, we also prove non-hardness results for more powerful reductions. Our non-hardness results are unconditional, in contrast to conditional results presented in earlier work of [Allender, Hirahara] (for more powerful reductions, but for much worse approximations). This also highlights obstacles that would have to be overcome by any proof that MKTP or MCSP is hard for NP under AC^0 reductions. It may also be a step toward confirming a conjecture of Murray and Williams, that MCSP is not NP-complete under logtime-uniform AC^0-many-one reductions.

3.2 Limits on All Known (and Some Unknown) Approaches to Matrix Multiplication

Josh Alman (MIT – Cambridge, US)

Joint work of Josh Alman, Virginia Vassilevska Williams
Main reference Josh Alman, Virginia Vassilevska Williams: "Further Limitations of the Known Approaches for Matrix Multiplication", in Proc. of the 9th Innovations in Theoretical Computer Science Conference, ITCS 2018, January 11-14, 2018, Cambridge, MA, USA, LIPIcs, Vol. 94, pp. 25:1–25:15, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2018.
URL https://doi.org/10.4230/LIPIcs.ITCS.2018.25

We study the known techniques for designing Matrix Multiplication (MM) algorithms. The two main approaches are the Laser method of Strassen, and the Group theoretic approach of Cohn and Umans. We define a generalization based on zeroing outs which subsumes these two approaches, which we call the Solar method, and an even more general method based on monomial degenerations, which we call the Galactic method.

We then design a suite of techniques for proving lower bounds on the value of omega, the exponent of MM, which can be achieved by algorithms using many tensors T and the Galactic method. Some of our techniques exploit "local" properties of T, like finding a sub-tensor of T which is so "weak" that T itself couldn't be used to achieve a good bound on ω, while others exploit "global" properties, like T being a monomial degeneration of the structural tensor of a group algebra. Our main result is that there is a universal constant $c > 2$ such that a large class of tensors generalizing the Coppersmith-Winograd tensor CW_q cannot be used within the Galactic method to show a bound on ω better than c, for any q.

3.3 The Complexity of Computing Small Weight Graph Automorphisms

V. Arvind (Institute of Mathematical Sciences – Chennai, IN)

Joint work of V. Arvind, Johannes Köbler, Sebastian Kuhnert, Jacobo Torán
Main reference Vikraman Arvind, Johannes Köbler, Sebastian Kuhnert, Jacobo Torán: "Parameterized Complexity of Small Weight Automorphisms", in Proc. of the 34th Symposium on Theoretical Aspects of Computer Science, STACS 2017, March 8-11, 2017, Hannover, Germany, LIPIcs, Vol. 66, pp. 7:1–7:13, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2017.
URL https://doi.org/10.4230/LIPIcs.STACS.2017.7

Given a graph (or hypergraph) G as input and a parameter k, does G have an automorphism of weight exactly k? We discuss the parameterized complexity of this and related problems, and also connections to the minimum weight codeword problem showing some cases in which the problems are fixed parameter tractable. As a building block for our algorithms, we generalize Schweitzer's FPT algorithm [ESA 2011] that, given two graphs on the same vertex set and a parameter k, decides whether there is an isomorphism between the two graphs that moves at most k vertices. We extend this result to hypergraphs, using the maximum hyperedge size as a second parameter. Another key component of our algorithm is an orbit-shrinking technique that preserves permutations that move few points and that may be of independent interest. Applying it to a suitable subgroup of the automorphism group allows us to switch from bounded hyperedge size to bounded color classes in the exactly-k case.

3.4 Optimal Extractors for Generalized Santha-Vazirani Sources

Andrej Bogdanov (The Chinese University of Hong Kong, HK)

Joint work of Salman Beigi, Andrej Bogdanov, Omid Etesami, Siyao Guo
Main reference Salman Beigi, Andrej Bogdanov, Omid Etesami, Siyao Guo: "Optimal Deterministic Extractors for Generalized Santha-Vazirani Sources", in Proc. of the Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2018, August 20-22, 2018 – Princeton, NJ, USA, LIPIcs, Vol. 116, pp. 30:1–30:15, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2018.
URL https://doi.org/10.4230/LIPIcs.APPROX-RANDOM.2018.30

Take a finite set of biased dice that share some common faces. An adversary repeatedly tosses them, with each choice of die possibly depending on the previous outcomes. Can you extract true randomness? In 1986 Santha and Vazirani gave a negative answer when the dice are (two-sided) coins. In 2015 Beigi, Etesami, and Gohari showed how to obtain an almost-unbiased bit for other sets of dice. The sample complexity of their extractor is polynomial in the inverse of the error. We completely classify all non-trivial randomness sources of this type into: (1) non-extractable ones; (2) extractable from polynomially many samples; and (3) extractable from an logarithmically many samples (in the inverse of the error). The extraction algorithms are efficient and easy to describe. I will discuss the relevance to distributed and cryptographic computation from imperfect randomness and point out some open questions in this context.

3.5 Degree vs Sparsity of Flat Polynomials that Approximate Boolean Functions

Sourav Chakraborty (Indian Statistical Institute – Kolkata, IN)

Various conjectures and theorems about the Fourier spectrum of Boolean functions impose various constraints of what type of polynomials can approximate a Boolean function. One such conjecture is the Fourier Entropy Influence Conjecture (FEI). As an implication of the conjecture we can observe a relation between the degree and sparsity of any polynomial that approximates a Boolean function. Can we prove these implications directly without using the conjecture? This question is related to the B-H conjecture in mathematics, which can be thought of as a generalised balancing lights problem.

3.6 A PSPACE Construction of a Hitting Set for the Closure of Small Algebraic Circuits

Michael A. Forbes (University of Illinois – Urbana-Champaign, US)

Joint work of Michael A. Forbes, Amir Shpilka
Main reference Michael A. Forbes, Amir Shpilka: "A PSPACE Construction of a Hitting Set for the Closure of Small Algebraic Circuits", CoRR, Vol. abs/1712.09967, 2017.
URL https://arxiv.org/abs/1712.09967

In this paper we study the complexity of constructing a hitting set for the closure of VP, the class of polynomials that can be infinitesimally approximated by polynomials that are computed by polynomial sized algebraic circuits, over the real or complex numbers. Specifically, we show that there is a PSPACE algorithm that given n, s, r in unary outputs a set of n-tuples over the rationals of size $\text{poly}(n, s, r)$, with $\text{poly}(n, s, r)$ bit complexity, that hits all n-variate polynomials of degree-r that are the limit of size-s algebraic circuits. Previously it was known that a random set of this size is a hitting set, but a construction that is certified to work was only known in EXPSPACE (or EXPH assuming the generalized Riemann hypothesis). As a corollary we get that a host of other algebraic problems such as Noether Normalization Lemma, can also be solved in PSPACE deterministically, where earlier only randomized algorithms and EXPSPACE algorithms (or EXPH assuming the generalized Riemann hypothesis) were known. The proof relies on the new notion of a robust hitting set which is a set of inputs such that any nonzero polynomial that can be computed by a polynomial size algebraic circuit, evaluates to a not too small value on at least one element of the set. Proving the existence of such a robust hitting set is the main technical difficulty in the proof. Our proof uses anti-concentration results for polynomials, basic tools from algebraic geometry and the existential theory of the reals.

3.7 Pseudorandom Generators for Read-Once Branching Programs, in any Order

Michael A. Forbes (University of Illinois – Urbana-Champaign, US)

Joint work of Michael A. Forbes, Zander Kelley
Main reference Michael A. Forbes, Zander Kelley: "Pseudorandom Generators for Read-Once Branching Programs, in any Order", CoRR, Vol. abs/1808.06265, 2018.
URL https://arxiv.org/abs/1808.06265

A central question in derandomization is whether randomized logspace (RL) equals deterministic logspace (L). To show that RL = L, it suffices to construct explicit pseudorandom generators (PRGs) that fool polynomial-size read-once (oblivious) branching programs (roBPs). Starting with the work of Nisan, pseudorandom generators with seed-length $O(\log^2 n)$ were constructed. Unfortunately, improving on this seed-length in general has proven challenging and seems to require new ideas. A recent line of inquiry has suggested focusing on a particular limitation of the existing PRGs, which is that they only fool roBPs when the variables are read in a particular known order, such as $x_1 < \cdots < x_n$. In comparison, existentially one can obtain logarithmic seed-length for fooling the set of polynomial-size roBPs that read the variables under any fixed unknown permutation $x_{\pi(1)} < \cdots < x_{\pi(n)}$. While recent works have established novel PRGs in this setting for subclasses of roBPs, there were no known $n^{o(1)}$

seed-length explicit PRGs for general polynomial-size roBPs in this setting. In this work, we follow the "bounded independence plus noise" paradigm of Haramaty, Lee and Viola, and give an improved analysis in the general roBP unknown-order setting. With this analysis we obtain an explicit PRG with seed-length $O(\log^3 n)$ for polynomial-size roBPs reading their bits in an unknown order. Plugging in a recent Fourier tail bound of Chattopadhyay, Hatami, Reingold, and Tal, we can obtain a $\widetilde{O}(\log^2 n)$ seed-length when the roBP is of constant width.

3.8 The Muffin Problem: Complexity Questions

William Gasarch (University of Maryland – College Park, US)

Joint work of Guangqi Cui, John Dickerson, Naveen Durvasula, William Gasarch, Erik Metz, Jacob Prinz, Naveen Raman, Daniel Smolyak, Sung Hyun Yoo
Main reference Guangqi Cui, John P. Dickerson, Naveen Durvasula, William Gasarch, Erik Metz, Jacob Prinz, Naveen Raman, Daniel Smolyak, Sung Hyun Yoo: "A Muffin-Theorem Generator", in Proc. of the 9th International Conference on Fun with Algorithms, FUN 2018, June 13-15, 2018, La Maddalena, Italy, LIPIcs, Vol. 100, pp. 15:1–15:19, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2018.
URL https://doi.org/10.4230/LIPIcs.FUN.2018.15

Consider the following problem: You have m muffins and s students. You want to divide the muffins and give out pieces so that everyone gets m/s muffins. You can clearly divide each muffin in s pieces and give each person m s-sized pieces. Since students do not like crumbs we want to maximize the smallest piece. Let $f(m, s)$ be the size of the smallest piece in the procedure which maximizes the smallest piece.

We have proven many theorems and have many procedures to find $f(m, s)$. We have used these to obtain $f(m, s)$ for all $s \leq 60$ and $m \leq 70$. However, these procedures are somewhat ad-hoc.

- If s is fixed then, for $m \geq s^3$, $f(m, s)$ has an easy formula. So $f(m, s)$ is FPT.
- There is a Mixed Integer Program for $f(m, s)$ in $O(ms)$ variables. Note that the input is of size $\log m + \log s$.
- Is computing $f(m, s)$ in P? We do not know.
- Is computing $f(m, s)$ in NP (phrased as a set). We do not know.

3.9 On Efficiently Solvable Cases of Quantum k-SAT

Sevag Gharibian (Universität Paderborn, DE)

Joint work of Sevag Gharibian, Marco Aldi, Niel de Beaudrap, Seyran Saeedi
Main reference Marco Aldi, Niel de Beaudrap, Sevag Gharibian, Seyran Saeedi: "On Efficiently Solvable Cases of Quantum k-SAT", in Proc. of the 43rd International Symposium on Mathematical Foundations of Computer Science, MFCS 2018, August 27-31, 2018, Liverpool, UK, LIPIcs, Vol. 117, pp. 38:1–38:16, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2018.
URL https://doi.org/10.4230/LIPIcs.MFCS.2018.38

The constraint satisfaction problems k-SAT and Quantum k-SAT (k-QSAT) are canonical NP-complete and QMA_1-complete problems (for $k \geq 3$), respectively, where QMA_1 is a quantum generalization of NP with one-sided error. Whereas k-SAT has been well-studied for special tractable cases, as well as from a parameterized complexity perspective, much

less is known in similar settings for k-QSAT. Here, we study the open problem of computing satisfying assignments to k-QSAT instances which have a "matching" or "dimer covering"; this is an NP problem whose decision variant is trivial, but whose search complexity remains open.

Among other results, our main contribution is a parameterized algorithm for k-QSAT instances from a certain non-trivial class, which allows us to obtain exponential speedups over brute force methods in some cases. This is, to our knowledge, the first known such parameterized algorithm. The techniques behind our work stem from algebraic geometry, although no background in the topic is required for this presentation.

3.10 Number of near-shortest vectors in Lattices and Polynomial Identity Testing

Rohit Gurjar (Indian Institute of Technology – Mumbai, IN)

For a matrix A, consider the lattice $L(A)$ formed by all integral vectors v in the null-space of A. We ask for which matrices A, the lattice $L(A)$ has only polynomially many near-shortest vectors i.e., vectors whose length is close to the shortest length in $L(A)$. The motivation for this question comes from the fact that we can get a deterministic black-box polynomial identity testing algorithm for any polynomial whose newton polytope has faces described by matrices with the aforementioned property.

We show that when the matrix A is totally unimodular (all sub-determinants are 0, +1, or −1) then the lattice $L(A)$ has only polynomially many near-shortest vectors. The proof of this statement goes via a remarkable theorem of Seymour on a decomposition for totally unimodular matrices. The statement generalizes two earlier known results – the number of near-shortest cycles and the number of near-shorest cuts in a graph are poly-bounded. As a special case, we get PIT for any polynomial of the form $\det(\sum x_i A_i)$ for rank-1 matrices A_i.

3.11 Simple Optimal Hitting Sets for Small-Success RL

William Hoza (University of Texas – Austin, US)

Joint work of William Hoza, David Zuckerman

We give a simple explicit hitting set generator for read-once branching programs of width w and length r with known variable order. When $r = w$, our generator has seed length $O(\log^2 r + \log(1/\epsilon))$. When $r = \text{polylog } w$, our generator has optimal seed length $O(\log w + \log(1/\epsilon))$. For intermediate values of r, our generator's seed length smoothly interpolates between these two extremes.

Our generator's seed length improves on recent work by Braverman, Cohen, and Garg (STOC '18). In addition, our generator and its analysis are dramatically simpler than the work by Braverman et al. Our generator's seed length improves on all the classic generators for space-bounded computation (Nisan Combinatorica '92; Impagliazzo, Nisan, and Wigderson STOC '94; Nisan and Zuckerman JCSS '96) when ϵ is small.

As a corollary of our construction, we show that every RL algorithm that uses r random bits can be simulated by an NL algorithm that uses only $O(r/\log^c n)$ nondeterministic bits, where c is an arbitrarily large constant. Finally, we show that any RL algorithm with small success probability ϵ can be simulated deterministically in space $O(\log^{3/2} n + \log n \log\log(1/\epsilon))$. This improves on work by Saks and Zhou (JCSS '99), who gave an algorithm that runs in space $O(\log^{3/2} n + \sqrt{(\log n)\log(1/\epsilon)})$.

3.12 Typically-Correct Derandomization for Small Time and Space

William Hoza (University of Texas – Austin, US)

Main reference William M. Hoza: "Typically-Correct Derandomization for Small Time and Space", CoRR, Vol. abs/1711.00565, 2017.
URL http://arxiv.org/abs/1711.00565

Suppose a language L can be decided by a bounded-error randomized algorithm that runs in space S and time $n \cdot poly(S)$. We give a randomized algorithm for L that still runs in space $O(S)$ and time $n \cdot poly(S)$ that uses only $O(S)$ random bits; our algorithm has a low failure probability on all but a negligible fraction of inputs of each length. An immediate corollary is a deterministic algorithm for L that runs in space $O(S)$ and succeeds on all but a negligible fraction of inputs of each length. We also give several other complexity-theoretic applications of our technique.

3.13 Orbits of Monomials and Factorization into Products of Linear Forms

Pascal Koiran (ENS – Lyon, FR)

Joint work of Pascal Koiran, Nicolas Ressayre
Main reference Pascal Koiran, Nicolas Ressayre: "Orbits of monomials and factorization into products of linear forms", CoRR, Vol. abs/1807.03663, 2018.
URL http://arxiv.org/abs/1807.03663

This talk is devoted to the factorization of multivariate polynomials into products of linear forms, a problem which has applications to differential algebra, to the resolution of systems of polynomial equations and to Waring decomposition (i.e., decomposition in sums of d-th powers of linear forms; this problem is also known as symmetric tensor decomposition). We provide three black box algorithms for this problem. Our main contribution is an algorithm motivated by the application to Waring decomposition. This algorithm reduces the corresponding factorization problem to simultaenous matrix diagonalization, a standard task in linear algebra. The algorithm relies on ideas from invariant theory, and more specifically on Lie algebras. Our second algorithm reconstructs a factorization from several bi-variate projections. Our third algorithm reconstructs it from the determination of the zero set of the input polynomial, which is a union of hyperplanes.

3.14 Optimal Quasi-Gray Codes: The Alphabet Matters

Michal Koucký (Charles University – Prague, CZ)

Joint work of Diptarka Chakraborty, Debarati Das, Michal Koucký, Nitin Saurabh
Main reference Diptarka Chakraborty, Debarati Das, Michal Koucký, Nitin Saurabh: "Space-Optimal Quasi-Gray Codes with Logarithmic Read Complexity", in Proc. of the 26th Annual European Symposium on Algorithms, ESA 2018, August 20-22, 2018, Helsinki, Finland, LIPIcs, Vol. 112, pp. 12:1–12:15, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2018.
URL http://dx.doi.org/10.4230/LIPIcs.ESA.2018.12

A quasi-Gray code of dimension n and length ℓ over an alphabet A is a sequence of distinct words $w_1, w_2, \ldots, w_e$ from A^n such that any two consecutive words differ in at most c coordinates, for some fixed constant $c > 0$. In this talk we are interested in the read and write complexity of quasi-Gray codes in the bit-probe model, where we measure the number of symbols read and written in order to transform any word w_i into its successor w_{i+1}.

We present construction of quasi-Gray codes of dimension n and length 3^n over the ternary alphabet $\{0, 1, 2\}$ with worst-case read complexity $O(\log n)$ and write complexity 2. This generalizes to arbitrary odd-size alphabets. For the binary alphabet, we present quasi-Gray codes of dimension n and length at least $2^n - -20n$ with worst-case read complexity $6 + \log n$ and write complexity 2. This complements a recent result by Raskin (2017) who shows that any quasi-Gray code over binary alphabet of length 2^n has read complexity $\Omega(n)$.

Our results significantly improve on previously known constructions and for the odd-size alphabets we break the $\Omega(n)$ worst-case barrier for space-optimal (non-redundant) quasi-Gray codes with constant number of writes. We obtain our results via a novel application of algebraic tools together with the principles of catalytic computation [Buhrman et al. '14, Ben-Or and Cleve '92, Barrington '89, Coppersmith and Grossman '75].

3.15 A Near-Optimal Depth-Hierarchy Theorem for Small-Depth Multilinear Circuits

Nutan Limaye (Indian Institute of Technology – Mumbai, IN)

Joint work of Suryajith Chillara, Christian Engels, Nutan Limaye, Srikanth Srinivasan
Main reference Suryajith Chillara, Christian Engels, Nutan Limaye, Srikanth Srinivasan: "A Near-Optimal Depth-Hierarchy Theorem for Small-Depth Multilinear Circuits", CoRR, Vol. abs/1804.02520, 2018.
URL http://arxiv.org/abs/1804.02520

The field of Computational Complexity deals with the study of resources necessary and sufficient for computations. One classical theme well-studied in the literature deals with quantifying the additional power gained by a model of computation with extra resources. For instance one could ask: does a Turing machine that runs for T steps necessarily compute more functions than the machines that only run for $o(T)$ steps? In general, does more resources mean more power? A hierarchy theorem is exactly such a statement for a model of computation and a resource.

The Time Hierarchy Theorem, Space Hierarchy theorem and many more such theorems for the Turing machines are classical results in Computational Complexity theory. In this work the model of computation we focus on is arithmetic formulas. An arithmetic formula is a natural model of computation for polynomials. It uses $+$ and $\times$ as operators for computing

polynomials. The size of the formula is the number of such operators it uses. The depth of the formula is the longest input to output path in the formula. Here we provide a depth hierarchy theorem for multilinear arithmetic formulas, where a formula is said to be multilinear if each gate in it computes a multilinear polynomial.

Here we show that there is a polynomial computed by depth $D+1$ polynomial sized multilinear formula such that any depth D multilinear formula computing the polynomial must have exponential size. In particular, we show that for every $D \leq o(\log n/\log\log n)$, there is a polynomial P_D on n variables that can be computed by a multilinear formula of depth $D+1$ and size $O(n)$ but cannot be computed by any multilinear formula of depth D and size $\exp(n^{1/D})$. This strengthens the result of Raz and Yehudayoff (Computational Complexity 2009) who showed a quasipolynomial separation, and the result of Kayal, Nair and Saha (STACS 2016) who gave an exponential separation when $D = 3$. Our separating examples may be viewed as algebraic analogues of variants of the Graph Reachability problem studied by Chen, Oliveira, Servedio and Tan (STOC 2016), who used them to prove lower bounds for constant-depth Boolean circuits.

3.16 Locating linear decision lists within TC^0

Meena Mahajan (Institute of Mathematical Sciences – Chennai, IN)

Joint work of Arkadev Chattopadhyay, Meena Mahajan, Nikhil Mande, Nitin Saurabh

Polynomial-size depth-2 circuits with linear threshold functions at each gate lie at the frontier of known circuit lower bounds. In this talk I will briefly survey the landscape below these circuits – the very-low-depth threshold hierarchy – and present one new result concerning decision lists, obtained jointly with Arkadev Chattopadhyay, Nikhil Mande and Nitin Saurabh. I will also describe a (somewhat related) question from proof complexity.

3.17 Improved List Decoding of Algebraic Codes

Noga Ron-Zewi (University of Haifa, IL)

Joint work of Swastik Kopparty, Noga Ron-Zewi, Shubhangi Saraf, Mary Wootters
Main reference To appear in FOCS 2018

We show that Folded Reed-Solomon codes achieve list decoding capacity with constant list sizes, independent of the block length. Prior work yielded list sizes that are polynomial in the block length, and relied on elaborate subspace evasive machinery to reduce the list sizes to constant.

We further show that multiplicity codes exhibit similar behavior, and use this to obtain capacity achieving locally list decodable codes with query complexity significantly lower than was known before.

3.18 Proper Learning of Non-degenerate Homogeneous Depth Three Arithmetic Circuits

Chandan Saha (Indian Institute of Science – Bangalore, IN)

Joint work of Neeraj Kayal, Chandan Saha

A homogeneous depth three circuit C computes a polynomial $f = T_1 + T_2 + \cdots + T_s$, where each T_i is a product of d linear forms in n variables. Given black-box access to f, can we efficiently reconstruct (i.e. proper learn) a homogeneous depth three circuit computing f? Learning homogeneous depth three circuits is stated as an open problem in a work by Klivans and Shpilka (COLT 2003).

We give a randomized poly(n, d, s) time algorithm to reconstruct non-degenerate homogeneous depth three circuits, if $n > (3d)^2$. The algorithm works over any field F, provided $\mathrm{char}(F) = 0$ or greater than poly(nds). Loosely speaking, a circuit C is non-degenerate if the dimension of the partial derivative (similarly, shifted partial derivative) space of f equals the sum of the dimensions of the partial derivative (resp., shifted partial derivative) spaces of the terms $T_1, \ldots, T_s$; in this sense, the terms are "independent" of each other. A random homogeneous depth three circuit (chosen according to any reasonable distribution) is almost surely non-degenerate. Previous learning algorithms for homogeneous depth three circuits are either improper (with an exponential dependence on d), or they work for constant s (with a doubly exponential dependence on s).

Our algorithm hinges on simultaneous block-diagonalization of a basis of the shifted differential operator space that acts on the partials of f. The block-diagonalization yields a decomposition of the partial derivative space of f into subspaces which, in turn, leads to the terms of C via another application of shifts. To our knowledge, this is the first time shifted partial derivative has been used to make progress on reconstruction algorithms.

3.19 Near Optimal Bootstrapping for Algebraic Models

Ramprasad Saptharishi (TIFR Mumbai, IN)

Joint work of Mrinal Kumar, Ramprasad Saptharishi, Anamay Tengse
Main reference Mrinal Kumar, Ramprasad Saptharishi, Anamay Tengse: "Near-optimal Bootstrapping of Hitting Sets for Algebraic Circuits", Electronic Colloquium on Computational Complexity (ECCC), Vol. 25, p. 132, 2018.
URL https://eccc.weizmann.ac.il/report/2018/132

The classical lemma of Ore-DeMillo-Lipton-Schwartz-Zippel states that any nonzero polynomial $f(x_1, \ldots, x_n)$ of degree at most s will evaluate to a nonzero value at some point on a grid S^n in F^n with $|S| > s$. Thus, there is an explicit hitting set for all n-variate degree s, size s algebraic circuits of size $(s + 1)^n$.

In this paper, we prove the following results:

- Let $\epsilon > 0$ be a constant. For a sufficiently large constant n and all $s \geq n$, if we have an explicit hitting set of size $(s + 1)^{n-\epsilon}$ for the class of n-variate degree s polynomials that are computable by algebraic circuits of size s, then for all s, we have an explicit hitting set of size $s^{\exp\exp(O(\log^* s))}$ for s-variate circuits of degree s and size s. That is, if we can

- obtain a barely non-trivial exponent compared to the trivial $(s+1)^n$ sized hitting set even for constant variate circuits, we can get an almost complete derandomization of PIT.
- The above result holds when "circuits" are replaced by "formulas" or "algebraic branching programs".

This extends a recent surprising result of Agrawal, Ghosh and Saxena (STOC 2018) who proved the same conclusion for the class of algebraic circuits, if the hypothesis provided a hitting set of size at most $(s^{n^{0.5--\epsilon}})$ (where $\epsilon > 0$ is any constant). Hence, our work significantly weakens the hypothesis of Agrawal, Ghosh and Saxena to only require a slightly non-trivial saving over the trivial hitting set, and also presents the first such result for algebraic branching programs and formulas.

3.20 Algebraic Dependence is Not Hard

Nitin Saxena (Indian Institute of Technology Kanpur, IN)

Joint work of Zeyu Guo, Nitin Saxena, Amit Sinhababu
Main reference Zeyu Guo, Nitin Saxena, Amit Sinhababu: "Algebraic Dependencies and PSPACE Algorithms in Approximative Complexity", in Proc. of the 33rd Computational Complexity Conference, CCC 2018, June 22-24, 2018, San Diego, CA, USA, LIPIcs, Vol. 102, pp. 10:1–10:21, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2018.
URL https://doi.org/10.4230/LIPIcs.CCC.2018.10

Testing whether a set F of polynomials has an algebraic dependence is a basic problem with several applications. The polynomials are given as algebraic circuits. Algebraic independence testing question is wide open over finite fields (Dvir, Gabizon, Wigderson, FOCS'07). In this work we put the problem in AM ∩ coAM. In particular, dependence testing is unlikely to be NP-hard. Our proof method is algebro-geometric, estimating the size of the image/preimage of the polynomial map F over the finite field. A gap in this size is utilized in the AM protocols.

Next, we introduce a new problem called *approximate* polynomials satisfiability (APS). We show that APS is NP-hard and, using projective algebraic-geometry ideas, we put APS in PSPACE (prior best was EXPSPACE via Gröbner bases). This has many unexpected applications to approximative complexity theory. This solves an open problem posed in (Mulmuley, FOCS'12, J. AMS 2017); greatly mitigating the GCT Chasm (exponentially in terms of space complexity).

3.21 Indistinguishability by Adaptive Procedures with Advice, and Lower Bounds on Hardness Amplification Proofs

Ronen Shaltiel (University of Haifa, IL)

Joint work of Aryeh Grinberg, Ronen Shaltiel, Emanuele Viola
Main reference Aryeh Grinberg, Ronen Shaltiel, Emanuele Viola: "Indistinguishability by adaptive procedures with advice, and lower bounds on hardness amplification proofs", Electronic Colloquium on Computational Complexity (ECCC) Vol. 25 p. 61, 2018.
URL https://eccc.weizmann.ac.il/report/2018/061

We study how well can q-query decision trees distinguish between the following two distributions: (i) $R = (R_1, \ldots, R_N)$ that are i.i.d. indicator random variables, (ii) $X = (R|R \in A)$ where A is an event s.t. $\Pr[R \in A] \geq 2^{-a}$. We prove two lemmas:

Forbidden-set lemma: There exists $B \subseteq [N]$ of size $\text{poly}(a, q, \frac{1}{\eta})$ such that q-query trees that do not query variables in B cannot distinguish X from R with advantage η.

Fixed-set lemma: There exists $B \subseteq [N]$ of size $\text{poly}(a, q, \frac{1}{\eta})$ and $v \in B^B$ such that q-query trees do not distinguish $(X|X_B = v)$ from $(R|R_B = v)$ with advantage η.

The first can be seen as an extension of past work by Edmonds, Impagliazzo, Rudich and Sgall (Computational Complexity 2001), Raz (SICOMP 1998), and Shaltiel and Viola (SICOMP 2010) to *adaptive* decision trees. It is independent of recent work by Meir and Wigderson (ECCC 2017) bounding the number of $i \in [N]$ for which there exists a q-query tree that predicts X_i from the other bits.

We use the second, fixed-set lemma to prove lower bounds on black-box proofs for hardness amplification that amplify hardness from δ to $\frac{1}{2} - \epsilon$. Specifically:

- Reductions must make $q = \Omega(\log(1/\delta)/\epsilon^2)$ queries, implying a "size loss factor" of q. We also prove the lower bound $q = \Omega(\log(1/\delta)/\epsilon)$ for "error-less" hardness amplification proofs, and for direct-product lemmas. These bounds are tight.
- Reductions can be used to compute Majority on $\Omega(1/\epsilon)$ bits, implying that black box proofs cannot amplify hardness of functions that are hard against constant depth circuits (unless they are allowed to use Majority gates).

Both items extend to pseudorandom-generator constructions.

These results prove 15-year-old conjectures by Viola, and improve on three incomparable previous works (Shaltiel and Viola, SICOMP 2010; Gutfreund and Rothblum, RANDOM 2008; Artemenko and Shaltiel, Computational Complexity 2014).

3.22 Memory Augmented Markovian Walks and Explicit Parity Samplers Giving Almost Optimal Binary Codes

Amnon Ta-Shma (Tel Aviv University, IL)

I will show an explicit construction of a binary error correcting code with relative distance $(1 - \epsilon)/2$ and relative rate $\epsilon^{2+o(1)}$. This comes close to the Gilbert-Varshamov bound that shows such codes with rate ϵ^2 exist, and the LP lower bound that shows rate $\epsilon^2/\log(1/\epsilon)$ is necessary. Previous explicit constructions had rate about ϵ^3, and this is the first explicit construction to get that close to the Gilbert-Varshamov bound.

The main tool we use are "Parity Samplers". A parity sampler is a collection of sets $S_i \subset \Lambda$ with the property that for every "test" $A \subset \Lambda$ of a given constant density ϵ_0, the probability a set S_i from the collection falls into the test set A an *even* number of times is about half. A *sparse* parity sampler immediately implies a good code with distance close to 1/2. The complete t-complex of all sequences of cardinality t is a good parity sampler, but with too many sets in the collection. Rozenman and Wigderson, and independently Alon, used random walks over expanders to explicitly construct sparse parity samplers, and their construction implies explicit codes with relative rate ϵ^4.

In the last part of the talk I will explain how one can get better explicit parity samplers (and therefore also better explicit codes) using a variant of the zig-zag product. In the random walk sampler, there exist many sets with substantial overlap. One way to look at the zig-zag product is that it takes a sub-collection of the random walk sampler, and this sub-collection has a smaller overlap between sets in the collection. The zig-zag product achieves that by keeping a small internal state. I will show that by enlarging the internal state one can further reduce the overlap, and as a result improve the quality of the parity sampler. One may view this process as a memory augmented Markovian process.

3.23 Near-Optimal Strong Dispersers and Erasure List-Decodable Codes

Amnon Ta-Shma (Tel Aviv University, IL)

Joint work of Avraham Ben-Aroya, Dean Doron, Amnon Ta-Shma
Main reference Avraham Ben-Aroya, Dean Doron, Amnon Ta-Shma: "Near-Optimal Strong Dispersers, Erasure List-Decodable Codes and Friends", Electronic Colloquium on Computational Complexity (ECCC), Vol. 25, p. 65, 2018.
URL https://eccc.weizmann.ac.il/report/2018/065

A code C is $(1-\tau, L)$ erasure list-decodable if for every word w, after erasing any $1-\tau$ fraction of the symbols of w, the remaining tau-fraction of its symbols have at most L possible completions into codewords of C. Non-explicitly, there exist binary $(1-\tau, L)$ erasure list-decodable codes having rate $O(\tau)$ and tiny list-size $L = O(\log 1/\tau)$. Achieving either of these parameters explicitly is a natural open problem and was brought up in several prior works. While partial progress on the problem has been achieved, no explicit construction up to this work achieved rate better than $\Omega(\tau^2)$ or list-size smaller than $\Omega(1/\tau)$ (for τ small enough). Furthermore, Guruswami showed that no *linear* code can have list-size smaller than $\Omega(1/\tau)$. In this work we construct an explicit binary $(1-\tau, L)$ erasure list-decodable code having rate $\tau^{1+\gamma}$ (for any constant $\gamma > 0$ and τ small enough) and list-size $\mathrm{poly}(\log 1/\tau)$, answering simultaneously both questions, and exhibiting an explicit non-linear code that provably beats the best possible linear one.

The binary erasure list-decoding problem is equivalent to the construction of explicit, low-error, strong dispersers outputting one bit with minimal entropy-loss and seed-length. Specifically, such dispersers with error ϵ have an unavoidable entropy-loss of $\log\log 1/\epsilon$ and seed-length at least $\log 1/\epsilon$. Similarly to the situation with erasure list-decodable codes, no explicit construction achieved seed-length better than $2\log 1/\epsilon$ or entropy-loss smaller than $2\log 1/\epsilon$, which are the best possible parameters for extractors. For every constant $\gamma > 0$ and every small ϵ, we explicitly construct an ϵ-error one-bit strong disperser with near-optimal seed-length $(1+\gamma)\log 1/\epsilon$ and near-optimal entropy-loss $O(\log\log 1/\epsilon)$.

The main ingredient in our construction is a new (and almost-optimal) *unbalanced* two-source extractor. The extractor extracts one bit with constant error from two independent sources, where one source has length n and tiny min-entropy $O(\log \log n)$ and the other source has length $O(\log n)$ and arbitrarily small constant min-entropy rate. The construction incorporates recent components and ideas from extractor theory with a delicate and novel analysis needed in order to solve dependency and error issues.

3.24 A Conditional Information Inequality and its Combinatorial Applications

Nikolay K. Vereshchagin (NRU Higher School of Economics – Moscow, RU)

Joint work of Tarik Kaced, Nikolay Vereshchagin
Main reference Tarik Kaced, Andrei E. Romashchenko, Nikolai K. Vereshchagin: "A Conditional Information Inequality and Its Combinatorial Applications", IEEE Trans. Information Theory, Vol. 64(5), pp. 3610–3615, 2018.
URL https://doi.org/10.1109/TIT.2018.2806486

We show that the inequality $H(A \mid B, X) + H(A \mid B, Y) \leq H(A \mid B)$ for jointly distributed random variables A, B, X, Y, which does not hold in general case, holds under some natural condition on the support of the probability distribution of A, B, X, Y. This result generalizes a version of the conditional Ingleton inequality: if for some distribution $I(X : Y \mid A) = H(A \mid X, Y) = 0$, then $I(A : B) \leq I(A : B \mid X) + I(A : B \mid Y) + I(X : Y)$.

We present the following applications of our result. The first one is the following easy-to-formulate theorem on edge colorings of bipartite graphs: assume that the edges of a bipartite graph are colored in K colors so that each two edges sharing a vertex have different colors and for each pair (left vertex x, right vertex y) there is at most one color a such both x and y are incident to edges with color a; assume further that the degree of each left vertex is at least L and the degree of each right vertex is at least R. Then $K \geq LR$.

Participants

- Farid Ablayev
Kazan State University, RU
- Eric Allender
Rutgers University – Piscataway, US
- Josh Alman
MIT – Cambridge, US
- Vikraman Arvind
Institute of Mathematical Sciences – Chennai, IN
- Nikhil Balaji
Universität Ulm, DE
- Markus Bläser
Universität des Saarlandes, DE
- Andrej Bogdanov
The Chinese University of Hong Kong, HK
- Sourav Chakraborty
Indian Statistical Institute – Kolkata, IN
- Stephen A. Fenner
University of South Carolina – Columbia, US
- Michael A. Forbes
University of Illinois – Urbana-Champaign, US
- Lance Fortnow
Georgia Institute of Technology – Atlanta, US
- Anna Gál
University of Texas – Austin, US
- William Gasarch
University of Maryland – College Park, US
- Sevag Gharibian
Universität Paderborn, DE
- Frederic Green
Clark University – Worcester, US
- Rohit Gurjar
Indian Institute of Technology – Mumbai, IN
- William Hoza
University of Texas – Austin, US
- Christian Ikenmeyer
MPI für Informatik – Saarbrücken, DE
- Valentine Kabanets
Simon Fraser University – Burnaby, CA
- Neeraj Kayal
Microsoft Research India – Bangalore, IN
- Pascal Koiran
ENS – Lyon, FR
- Antonina Kolokolova
Memorial University of Newfoundland – St. John's, CA
- Arpita Korwar
University Paris-Diderot, FR
- Michal Koucký
Charles University – Prague, CZ
- Nutan Limaye
Indian Institute of Technology – Mumbai, IN
- Zhenjian Lu
Simon Fraser University – Burnaby, CA
- Vladimir Lysikov
Universität des Saarlandes, DE
- Meena Mahajan
Institute of Mathematical Sciences – Chennai, IN
- David A. Mix Barrington
University of Massachusetts – Amherst, US
- Anurag Pandey
Universität des Saarlandes, DE
- Natacha Portier
ENS – Lyon, FR
- Noga Ron-Zewi
University of Haifa, IL
- Chandan Saha
Indian Institute of Science – Bangalore, IN
- Ramprasad Saptharishi
TIFR Mumbai, IN
- Nitin Saxena
Indian Institute of Technology Kanpur, IN
- Uwe Schöning
Universität Ulm, DE
- Ronen Shaltiel
University of Haifa, IL
- Amnon Ta-Shma
Tel Aviv University, IL
- Thomas Thierauf
Hochschule Aalen, DE
- Jacobo Torán
Universität Ulm, DE
- Christopher Umans
Caltech – Pasadena, US
- Nikolay K. Vereshchagin
NRU Higher School of Economics – Moscow, RU