

Algebraic and Analytic Methods in Computational Complexity

Markus Bläser^{*1}, Valentine Kabanets^{*2}, Ronen Shaltiel^{*3}, and Jacobo Torán^{*4}

1 Universität des Saarlandes – Saarbrücken, DE. mblaeser@cs.uni-saarland.de

2 Simon Fraser University – Burnaby, CA. kabanets@cs.sfu.ca

3 University of Haifa, IL. ronen@cs.haifa.ac.il

4 Universität Ulm, DE. jacobo.toran@uni-ulm.de

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 2237 “Algebraic and Analytic Methods in Computational Complexity”.

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.

Beside algebraic methods, analytic methods have been used for quite some time in theoretical computer science. These methods can also be used to solve algebraic problems as show by many recent examples in the areas of derandomization, coding theory or circuit lower bounds. These new directions were in the focus of the Dagstuhl Seminar and reflect the developments in the field since the previous Dagstuhl Seminar 18391.

This Dagstuhl Seminar brought together researchers who are using a diverse array of algebraic and analytic methods in a variety of settings. Researchers in these areas are relying on ever more sophisticated and specialized mathematics and this seminar played a role in educating a diverse community about the latest new techniques, spurring further progress.

Seminar September 11–16, 2022 – <http://www.dagstuhl.de/22371>

2012 ACM Subject Classification Theory of computation → Algebraic complexity theory; Theory of computation → Circuit complexity; Theory of computation → Problems, reductions and completeness; Theory of computation

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

Digital Object Identifier 10.4230/DagRep.12.9.41

1 Executive Summary

Markus Bläser (Universität des Saarlandes – Saarbrücken, DE)

Valentine Kabanets (Simon Fraser University – Burnaby, CA)

Ronen Shaltiel (University of Haifa, IL)

Jacobo Torán (Universität Ulm, DE)

License © Creative Commons BY 4.0 International license

© Markus Bläser, Valentine Kabanets, Ronen Shaltiel, and Jacobo Torán

Introduction

The seminar on algebraic methods in computational complexity has traditionally taken place every two years in Dagstuhl for many years. In these meetings, we try to bring together leading researchers in a very active and broad area of theoretical computer science, having

* Editor / Organizer



Except where otherwise noted, content of this report is licensed under a Creative Commons BY 4.0 International license

Algebraic and Analytic Methods in Computational Complexity, *Dagstuhl Reports*, Vol. 12, Issue 9, pp. 41–59

Editors: Markus Bläser, Valentine Kabanets, Ronen Shaltiel, and Jacobo Torán



Dagstuhl Reports

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

the algebraic methods as a unifying thread. Researchers in these areas are relying on ever more sophisticated and specialized mathematics and this seminar can play an important role in educating a diverse community about the latest new techniques, spurring further progress. For the year 2022, we added a new direction that focused besides the algebraic aspect also on methods from analysis. The seminar brought together more than 40 researchers covering a wide spectrum of complexity theory. We had 24 talks, most of them lasting about 45 minutes, leaving ample room for discussions. In the following we describe the major topics of discussion in more detail.

Some areas of focus

Computational complexity is a fundamental and active subarea of theoretical computer science that has produced some of the most well known results in theoretical computer science in recent years. Here we discuss a few broad themes which highlight the importance of algebra as well as analytic methods in computational complexity, and which represent some focus areas of our present seminar.

Circuit complexity

Boolean circuits are one of the most fundamental model of computation. Due to its combinatorial nature, they seem more amenable to formal analysis than the uniform models such as Turing machines. The classical lower bound techniques of Razborov and Smolensky are algebraic: they work by first approximating $AC^0[p]$ circuits (constant-depth circuits with AND, OR, NOT, and counting modulo prime p gates) by low-degree polynomials, and then proving that certain functions (like Majority) are not well correlated with such polynomials. The Fourier expansion of a Boolean function and its representation as a real multilinear polynomial as well as other analytic tools have been added in the last years to the bag of tools used for the analysis of Boolean circuits. In the seminar, we talked about recent results in circuit complexity.

Andrej Bogdanov talked about property testing. He constructed a natural tester that tells if a function from $\{0, 1\}^n$ to some Abelian group is linear (or far from linear).

Frederic Green proved a new correlation bound for certain exponential sums over characteristic 5.

William Hoza presented the construction of a Boolean function F on n bits such that F can be computed by a uniform depth- $(d + 1)$ AC^0 circuit with $O(n)$ wires, but F cannot be computed by any depth- d TC^0 circuit with $n^{1+\gamma}$ wires, where $\gamma = 2^{-\Theta(d)}$ and $d = o(\log \log n)$.

Michal Koucký dealt with a classical problem, the simulation of Turing machines by circuits. He gave a new simple proof for the classical result that Turing machines running in time $t(n)$ and space $s(n)$ can be simulated by Boolean circuits of size $O(t(n) \log s(n))$ and of depth $O(t(n))$.

Meena Mahajan presented relations between the minimum rank of a decision tree computing a Boolean function and other complexity measures of the function, as well as a new composition theorem in terms of rank and decision tree depth.

In his talk, *Rocco Servedio* establish a new quantitative version of the Gaussian correlation inequality. It gives a lower bound on the correlation of two centrally symmetric convex sets based on their “common influential directions”.

A new family of sampling tasks was presented by *Rahul Santhanam*. He showed that any non-trivial algorithmic solutions to tasks from this family imply new uniform lower bounds such as “NP not in uniform ACC^0 ” or “NP does not have uniform depth-2 threshold circuits”.

Algebraic complexity

A class of circuits especially suited for the use of algebraic techniques is that of *arithmetic circuits*. These are circuit models that compute polynomial functions by using gates performing arithmetic operations (additions, subtractions, multiplications, divisions, etc.) Two fundamental complexity measures for arithmetic circuits are the *size* and the *depth* or *product depth*.

Prerona Chatterjee considered the question of proving lower bounds against non-commutative circuits better than $\Omega(n \log n)$. She showed a quadratic lower bound against the n -variate central symmetric polynomial.

Arkadev Chattopadhyay talked about connections between communication complexity measures and monotone arithmetic circuit lower bounds. He constructed a (set-multilinear) monotone polynomial that can be computed by depth-3 multilinear formulas in sub-cubic size but requires exponential size to be computed by monotone arithmetic circuits. Second, he proved the existence of a polynomial over n variables in VNP, for which $2^{\Omega(n)}$ size ϵ -sensitive lower bounds hold if $\epsilon = 2^{-O(n)}$.

Barrier results in the group-theoretic approach to bounding the exponent of matrix multiplication was the topic of the talk by *Chris Umans*. He showed that finite groups of Lie type cannot prove $\omega = 2$ and presented a further barrier result. Then he gave constructions in the continuous setting, which can potentially evade these two barriers.

Pascal Koiran studied the decomposition of multivariate polynomials as sums of powers of linear forms. He presented a randomized algorithm for the following problem: Given a homogeneous polynomial of degree d as a blackbox, decide whether it can be written as a linear combination of d th powers of linearly independent complex linear forms.

Nutan Limaye proved in her talk that there exist monomial symmetric polynomials that are hard for the class VNP.

Pseudorandomness and derandomization

The theory of pseudorandomness studies explicit constructions and applications of “random-like” objects of combinatorial or algebraic type. The common feature of such objects is that it is easy to construct one by random sampling, but a very important problem is to get efficient *deterministic* constructions.

Eric Allender proved that Kolmogorov complexity characterizes statistical zero knowledge. Every decidable promise problem has a non-interactive statistical zero-knowledge proof system if and only if it is randomly reducible to a promise problem for Kolmogorov-random strings.

Random walks on expanders are a useful tool in complexity theory. *Gil Cohen* explained how the inherent cost can be reduced from exponential to linear by applying a permutation after each random step.

Sylvester-Gallai type problems have found applications in polynomial identity testing and coding theory. *Rafael Oliveira* discussed such problems and their relation to algebraic computation, and presented a theorem that radical Sylvester-Gallai configurations for cubic polynomials must have small dimension.

Ryan O’Donnell explained how to construct high-dimensional expanders from Chevalley groups.

Motivated by applications from cryptography, *Noga Ron-Zewi* studied a new interactive variant of PCPs, so-called interactive oracle proofs. She showed that for this model the overhead in the encoding can be made arbitrarily small and the prover complexity overhead can be made constant.

In his talk, *Amon Ta-Shma* gave an alternative construction of the lossless condenser by Guruswami, Umans and Vadhan. Instead of Parvaresh-Vardy codes, the new construction is based on multiplicity codes.

A Chor-Goldreich source is a sequence of random variables where each has min-entropy, even conditioned on the previous ones. *David Zuckerman* showed how to extend this notion in several ways, most notably allowing each random variable to have Shannon entropy conditioned on previous ones. He then proved new pseudorandomness results for Shannon-CG sources.

Border complexity and invariant theory

Many problems in algebraic complexity theory can be written as an orbit closure problem. We are given a vector space V and a group G acting on it. The orbit Gv of an element $v \in V$ is the set $\{gv \mid g \in G\}$ and its closure is the usual closure in the Zariski topology. For instance, we can formulate the tensor border rank problem in this language: Alder and Strassen proved that the question whether a tensor t has border rank $\leq r$ is equivalent to deciding whether t is in the orbit closure (under the standard action $\mathrm{GL}_n \times \mathrm{GL}_n \times \mathrm{GL}_n$) of the so-called unit tensor of size r . As second example is provided by Mulmuley and Sohoni who formulated a variant of the permanent versus determinant question as an orbit closure problem.

Peter Bürgisser gave an introduction to new algorithmic and analysis techniques that extend convex optimization from the classical Euclidean setting to a general geodesic setting. He pointed out the relevance of invariant and representation theory for complexity theory and highlighted connections to different areas of mathematics, statistics, computer science, and physics.

Rohit Gurjar considered determinants of the matrices of the form $(\sum_i A_i x_i)$ where each A_i is rank one. He showed that this class of polynomials is closed under approximation.

Approximate complexity was also the topic of *Nitin Saxena's* talk. He proved that the border of bounded-top-fanin depth-3 circuits is relatively easy, since it can be computed by a polynomial-size algebraic branching program.

Counting and quantum complexity

In order to study the $\#P$ (non-)membership of some concrete problems, *Christian Ikenmeyer* started the development of a classification of the $\#P$ closure properties on affine varieties. He obtained oracle separations between counting classes, where the existence of the oracle is based on properties of the vanishing ideal of an affine variety.

Steve Fenner considered a problem in quantum computing, the construction of a “realistic” Hamiltonian for quantum fanout.

Conclusion

The talks of the seminar ranged over a broad assortment of subjects with the underlying theme of using algebraic and analytic techniques. It was a very fruitful meeting and it 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 seminar.

2 Table of Contents

Executive Summary

Markus Bläser, Valentine Kabanets, Ronen Shaltiel, and Jacobo Torán 41

Overview of Talks

Kolmogorov Complexity Characterizes Statistical Zero Knowledge <i>Eric Allender</i>	47
Direct sum testing over Abelian groups <i>Andrej Bogdanov</i>	47
Optimization, Complexity and Invariant Theory <i>Peter Bürgisser</i>	47
A Quadratic Lower Bound Against Homogeneous Non-Commutative Circuits <i>Prerona Chatterjee</i>	48
Monotone Arithmetic Lower Bounds Via Communication Complexity <i>Arkadev Chattopadhyay</i>	48
Random walks on rotating expanders <i>Gil Cohen</i>	49
A “Realistic” Hamiltonian for Quantum Fanout <i>Stephen A. Fenner</i>	49
New Correlation Bounds for Quadratic Polynomials <i>Frederic Green</i>	50
Set of rank-1 determinant polynomials is closed under approximations <i>Rohit Gurjar</i>	50
Depth-d Threshold Circuits vs. Depth-(d + 1) AND-OR Trees <i>William Hoza</i>	51
The algebraic geometry of the closure properties of #P <i>Christian Ikenmeyer</i>	51
Black Box Absolute Reconstruction for Sums of Powers of Linear Forms <i>Pascal Koïran</i>	52
Turning Turing Machines into Boolean Circuits <i>Michal Koucký</i>	52
The complexity of monomial symmetric polynomials <i>Nutan Limaye</i>	53
Decision tree rank for Boolean functions <i>Meena Mahajan</i>	53
Radical Sylvester-Gallai theorem for cubics – and beyond <i>Rafael Mendes de Oliveira</i>	53
High-dimensional expanders from Chevalley groups <i>Ryan O’Donnell</i>	54
Highly-efficient local proofs <i>Noga Ron-Zewi</i>	54

An Algorithmic Approach to Uniform Lower Bounds <i>Rahul Santhanam</i>	55
Demystifying the border of depth-3 algebraic circuits <i>Nitin Saxena</i>	55
Convex influences and a quantitative Gaussian correlation inequality <i>Rocco Servedio</i>	56
Lossless Condensers from Multiplicity Codes <i>Amnon Ta-Shma</i>	56
Matrix multiplication via matrix groups <i>Christopher Umans</i>	57
Almost Chor-Goldreich Sources and Adversarial Random Walks <i>David Zuckerman</i>	58
Participants	59

3 Overview of Talks

3.1 Kolmogorov Complexity Characterizes Statistical Zero Knowledge

Eric Allender (Rutgers University – Piscataway, US)

License © Creative Commons BY 4.0 International license
© Eric Allender

Joint work of Eric Allender, Harsha Tirumala, and Shuichi Hirahara

Main reference Eric Allender, Shuichi Hirahara, Harsha Tirumala: “Kolmogorov Complexity Characterizes Statistical Zero Knowledge”, ECCCC TR22-127, 2022

URL <https://ecccc.weizmann.ac.il/report/2022/127/>

We show that a decidable promise problem has a non-interactive statistical zero-knowledge proof system if and only if it is randomly reducible to a promise problem for Kolmogorov-random strings, with a superlogarithmic additive approximation term. This extends recent work by Saks and Santhanam (CCC 2022). We build on this to give new characterizations of Statistical Zero Knowledge (SZK), as well as the related classes NISZK_L and SZK_L .

3.2 Direct sum testing over Abelian groups

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

License © Creative Commons BY 4.0 International license
© Andrej Bogdanov

Joint work of Andrej Bogdanov, Gautam Prakriya

Main reference Andrej Bogdanov, Gautam Prakriya: “Direct Sum and Partitionability Testing over General Groups”, in Proc. of the 48th International Colloquium on Automata, Languages, and Programming, ICALP 2021, July 12-16, 2021, Glasgow, Scotland (Virtual Conference), LIPIcs, Vol. 198, pp. 33:1–33:19, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021.

URL <http://dx.doi.org/10.4230/LIPIcs.ICALP.2021.33>

I spoke about a natural tester that tells if a function from $\{0, 1\}^n$ to some Abelian group like Z_3 is linear (or far from linear). More generally, the tester can be used to tell if a multivariate function $g(x_1, \dots, x_n)$ admits a direct sum decomposition $f(x_1) + \dots + f(x_n)$ for some f .

3.3 Optimization, Complexity and Invariant Theory

Peter Bürgisser (TU Berlin, DE)

License © Creative Commons BY 4.0 International license
© Peter Bürgisser

Joint work of Peter Bürgisser, Cole Franks, Ankit Garg, Rafael Oliveira, Michael Walter, Avi Wigderson

Main reference Peter Bürgisser, Cole Franks, Ankit Garg, Rafael Oliveira, Michael Walter, Avi Wigderson: “Towards a Theory of Non-Commutative Optimization: Geodesic 1st and 2nd Order Methods for Moment Maps and Polytopes”, in Proc. of the 2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS), IEEE, 2019.

URL <http://dx.doi.org/10.1109/focs.2019.00055>

Invariant and representation theory studies symmetries by means of group actions and is a well established source of unifying principles in mathematics and physics. Recent research suggests its relevance for complexity and optimization through quantitative and algorithmic questions. The goal of the talk is to give an introduction to new algorithmic and analysis techniques that extend convex optimization from the classical Euclidean setting to a general geodesic setting. We also point out surprising connections to a diverse set of problems in different areas of mathematics, statistics, computer science, and physics.

3.4 A Quadratic Lower Bound Against Homogeneous Non-Commutative Circuits

Prerona Chatterjee (*The Czech Academy of Sciences – Prague, CZ*)


License  Creative Commons BY 4.0 International license
© Prerona Chatterjee

Joint work of Prerona Chatterjee, Pavel Hrubeš

In spite of the various strong lower bounds against constant depth circuits and the depth reduction results in algebraic circuit complexity, the best lower bound known against general algebraic circuits remains $\Omega(n \log n)$ [Strassen, 1973; Baur-Strassen 1983]. Nothing better is known even in the more restrictive non-commutative setting where the product gates are considered to denote non-commutative multiplication. This is surprising since exponential lower bounds are known against algebraic formulas [Nisan 1991] and super polynomial lower bounds are known against homogenous formulas for polynomials computable even by ABPs [Tavenas, Limaye, Srinivasan, 2022]. A natural question is therefore to prove better lower bounds against non-commutative circuits. In this talk, we make progress in this question by showing a quadratic lower bound against the n -variate central symmetric polynomial. Further, the simplicity of the proof motivates us to ask whether a similar lower bound can be shown against general non-commutative circuits. This is ongoing work with Pavel Hrubeš.

3.5 Monotone Arithmetic Lower Bounds Via Communication Complexity

Arkadev Chattopadhyay (*TIFR – Mumbai, IN*)

License  Creative Commons BY 4.0 International license
© Arkadev Chattopadhyay

Joint work of Arkadev Chattopadhyay, Rajit Datta, Utsab Ghosal, Partha Mukhopadhyay

Main reference Arkadev Chattopadhyay, Rajit Datta, Partha Mukhopadhyay: “Lower bounds for monotone arithmetic circuits via communication complexity”, in Proc. of the STOC ’21: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, June 21-25, 2021, pp. 786–799, ACM, 2021.

URL <http://dx.doi.org/10.1145/3406325.3451069>

We make two novel connections between communication complexity measures and monotone arithmetic circuit lower bounds. The first connection exploits the corruption measure. We formulate a general method that constructs a set-multilinear polynomial P_f from a Boolean function f and uses the corruption bound of $f \circ \text{XOR}$ to imply a size lower bound on monotone arithmetic circuits computing P_f . Using this method, we construct [1] a (set-multilinear) monotone polynomial that can be computed by depth-3 multilinear formulas in sub-cubic size but require exponential size to be computed by monotone arithmetic circuits. It was not even known, before our work, if general formulas of arbitrary depth could provide exponential savings in size over monotone circuits.

The second connection uses the discrepancy measure from communication complexity to lower bound the size of monotone circuits computing a polynomial even in an ϵ -sensitive way. Very recently, Hrubeš [3] showed that ϵ -sensitive monotone lower bounds, for arbitrary small positive ϵ , implies general circuit lower bounds. We formulate [2] a general recipe between discrepancy under a *universal* distribution and ϵ -sensitive bounds. Using this connection, we show the following:

- there exists a polynomial over n variables, crafted out of the Boolean inner-product function defined using expander graphs, that is in VNP and for which $2^{\Omega(n)}$ size ϵ -sensitive lower bounds hold if $\epsilon = 2^{-O(n)}$.
- the spanning tree polynomial, defined over the edge variables of a complete graph on n vertices, needs $2^{\Omega(n)}$ size to be computed by monotone circuits in an ϵ -sensitive way as long as $\epsilon = 2^{-O(n)}$. Recall that the number of variables of this spanning tree polynomial is $\Theta(n^2)$ and it is in VP.


This is based on two papers referenced below.

References

- 1 Arkadev Chattopadhyay, Rajit Datta, and Partha Mukhopadhyay, *Lower bounds for monotone arithmetic circuits via communication complexity*, STOC, 2021.
- 2 Arkadev Chattopadhyay, Rajit Datta, Utsab Ghosal, and Partha Mukhopadhyay, *Monotone complexity of spanning tree polynomial revisited*, ITCS, 2022.
- 3 Pavel Hrubes, *On ϵ -sensitive monotone computations*, Computational Complexity, 2020.

3.6 Random walks on rotating expanders

Gil Cohen (Tel Aviv University, IL)

License  Creative Commons BY 4.0 International license
© Gil Cohen

Joint work of Gil Cohen, Gal Maor

Random walks on expanders are extremely useful in TOC. Unfortunately though, they have an inherent cost. E.g., the spectral expansion of a Ramanujan graph deteriorates exponentially with the length of the walk (when compared to a Ramanujan graph of the same degree). In this talk, we will see how this exponential cost can be reduced to linear by applying a permutation after each random step. These permutations are tailor-made to the graph at hand, requiring no randomness. Our proof is established using the powerful framework of finite free probability and interlacing families that was introduced, around ten years ago, by Marcus, Spielman and Srivastava in their seminal works on the existence of bipartite Ramanujan graphs of every size and every degree, and in their solution to the Kadison-Singer problem.

3.7 A “Realistic” Hamiltonian for Quantum Fanout

Stephen A. Fenner (University of South Carolina – Columbia, US)

License  Creative Commons BY 4.0 International license
© Stephen A. Fenner

Joint work of Stephen A Fenner, Rabins Wosti

Main reference Stephen Fenner, Rabins Wosti: “Implementing the fanout operation with simple pairwise interactions”, arXiv, 2022.

URL <http://dx.doi.org/10.48550/ARXIV.2203.01141>


We give a swap-invariant diagonal gate U_n equivalent in constant depth to the n -qubit fanout gate. For $t = \pi/4$ and real coupling constants $\{\alpha_{i,j} : 1 \leq i, j \leq n\}$ with $\alpha_{i,j} = \alpha_{j,i}$, $\alpha_{ii} = 0$, the Hamiltonian $H_{\vec{\alpha}} := \sum_{i < j} \alpha_{i,j} Z_i Z_j$ implements U_n (i.e., $U_n = \exp(-iH_{\vec{\alpha}}t)$ up to a global phase factor) if and only if: (1) all the $\alpha_{i,j}$ are odd integers; and (2) for all i ,

$\prod_{j \neq i} \alpha_{i,j} \equiv 1 \pmod{4}$. We give tight constraints on $\{\alpha_{i,j}\}$ as above for spatial arrangements of identical qubits satisfying an inverse square law. These constraints are obtained using modular arithmetic on rational numbers.

Joint work with Rabins Wosti.

3.8 New Correlation Bounds for Quadratic Polynomials

Frederic Green (Clark University – Worcester, US)

License  Creative Commons BY 4.0 International license
© Frederic Green

Let p be an odd prime, $\zeta = e^{2\pi i/p}$ a complex primitive p^{th} root of unity, and $\chi : \mathbb{Z}_p \rightarrow \mathbb{C}$ the quadratic character over \mathbb{Z}_p . Let $t \in \mathbb{Z}_p[x_1, \dots, x_n]$ be an n -variable quadratic polynomial $\sum_{i,j} c_{ij}x_i x_j + \sum_i \ell_i x_i$. Consider the exponential sum,

$$S = \frac{1}{(p-1)^n} \sum_{\mathbf{x} \in \mathbb{Z}_p^n} \chi\left(\prod_{i=1}^n x_i\right) \zeta^{t(\mathbf{x})},$$

which can be interpreted as the correlation between the parity of the number of x_i 's which are quadratic residues and whether $t(\mathbf{x}) \equiv 0 \pmod{p}$. In 2001, Green (JCSS **69**, 2004, pp. 28–44) showed that for $p = 3$, $|S| \leq (|\zeta - \bar{\zeta}|/2)^{\lceil n/2 \rceil}$, and that this bound can be met by $x_1 x_2 + x_3 x_4 + \dots$. In this talk, we prove a tight bound for $|S|$ when $p = 5$: $|S| \leq (|\zeta - \bar{\zeta}|/2)^n$, which can be met by the polynomial $x_1^2 + x_2^2 + \dots + x_n^2$. The technique relies on some of the simpler methods of those recently developed by Ivanov, Pavlovic, and Viola (ECCC TR22-092, July 2022). The latter paper consider sums of the form,

$$\frac{1}{2^n} \sum_{\mathbf{x} \in \{0,1\}^n} \zeta^{\sum_{i=1}^n x_i} (-1)^{t(\mathbf{x})},$$

again with t quadratic, and, remarkably, prove tight upper bounds met by symmetric polynomials for *any* complex unit ζ . It is not yet clear how to extend the simpler method for $p = 5$ to other odd moduli.

3.9 Set of rank-1 determinant polynomials is closed under approximations

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

License  Creative Commons BY 4.0 International license
© Rohit Gurjar

Joint work of Rohit Gurjar, Abhranil Chatterjee, Sumanta Ghosh, Roshan Raj

Consider the class of polynomials computed by rank-one determinants – determinants of the matrices of the form $(\sum_i A_i x_i)$ where each A_i is rank one. These polynomials appear naturally in the study of bipartite matching and related combinatorial problems. We show that this class of polynomials is closed under approximation. Interestingly, the proof of closure uses ideas from combinatorial optimization, specifically Rado's theorem on matroid transversals.

3.10 Depth- d Threshold Circuits vs. Depth- $(d + 1)$ AND-OR Trees

William Hoza (University of California – Berkeley, US)

License © Creative Commons BY 4.0 International license
© William Hoza

Joint work of William Hoza, Avishay Tal, Pooya Hatami, Roei Tell

Main reference Pooya Hatami, William Hoza, Avishay Tal, Roei Tell: “Depth- d Threshold Circuits vs. Depth- $(d + 1)$ AND-OR Trees”, Electron. Colloquium Comput. Complex., Vol. TR22-087, 2022.

URL <https://eccc.weizmann.ac.il/report/2022/087>

For $n \in \mathbb{N}$ and $d = o(\log \log n)$, we prove that there is a Boolean function F on n bits and a value $\gamma = 2^{-\Theta(d)}$ such that F can be computed by a uniform depth- $(d + 1)$ AC^0 circuit with $O(n)$ wires, but F cannot be computed by any depth- d TC^0 circuit with $n^{1+\gamma}$ wires. This bound matches the current state-of-the-art lower bounds for computing explicit functions by threshold circuits of depth $d > 2$, which were previously known only for functions outside AC^0 such as the parity function. Furthermore, in our result, the AC^0 circuit computing F is a monotone *read-once formula* (i.e., an AND-OR tree), and the lower bound holds even in the average-case setting with respect to advantage $n^{-\gamma}$.

Our proof builds on the *random projection* procedure of Håstad, Rossman, Servedio, and Tan, which they used to prove the celebrated average-case depth hierarchy theorem for AC^0 (J. ACM, 2017). We show that under a modified version of their projection procedure, any depth- d threshold circuit with $n^{1+\gamma}$ wires simplifies to a near-trivial function, whereas an appropriately parameterized AND-OR tree of depth $d + 1$ maintains structure.

3.11 The algebraic geometry of the closure properties of #P

Christian Ikenmeyer (University of Liverpool, GB)

License © Creative Commons BY 4.0 International license
© Christian Ikenmeyer

Joint work of Christian Ikenmeyer, Igor Pak

Main reference Christian Ikenmeyer, Igor Pak: “What is in #P and what is not?”, in Proc. of the 63rd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2022, Denver, CO, USA, October 31 – November 3, 2022, pp. 860–871, IEEE, 2022.

URL <http://dx.doi.org/10.1109/FOCS54457.2022.00087>



Since 1995 the functional closure properties of #P are beautifully classified via the coefficients in the expansion over the binomial basis. In order to study the #P (non-)membership of concrete problems related to counting versions of TFNP problems, we start the development of a classification of the #P closure properties on affine varieties. We obtain oracle separations between counting classes, where the existence of the oracle is based on properties of the vanishing ideal of an affine variety, which then translates to a specific polyhedron having no integer point. This is a part of the recent FOCS 2022 paper “What is in #P and what is not”, which is joint work with Igor Pak.

References

- 1 Christian Ikenmeyer and Igor Pak. *What is in #P and what is not*. Proceedings FOCS 2022, full version on arXiv:2204.13149

3.12 Black Box Absolute Reconstruction for Sums of Powers of Linear Forms

Pascal Koiran (ENS – Lyon, FR)

License  Creative Commons BY 4.0 International license
 Pascal Koiran

Joint work of Pascal Koiran and Subhayan Saha

Main reference Pascal Koiran, Subhayan Saha: “Black Box Absolute Reconstruction for Sums of Powers of Linear Forms”, in Proc. of the 42nd IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science, FSTTCS 2022, December 18-20, 2022, IIT Madras, Chennai, India, LIPIcs, Vol. 250, pp. 24:1–24:17, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022.

URL <http://dx.doi.org/10.4230/LIPIcs.FSTTCS.2022.24>

We study the decomposition of multivariate polynomials as sums of powers of linear forms. We give a randomized algorithm for the following problem: If a homogeneous polynomial $f \in K[x_1, \dots, x_n]$ (where $K \subseteq \mathbb{C}$) of degree d is given as a blackbox, decide whether it can be written as a linear combination of d -th powers of linearly independent complex linear forms. The main novel features of the algorithm are:

- For $d = 3$, we improve by a factor of n on the running time from the algorithm in (Koiran and Skomra, 2020). The price to be paid for this improvement is that the algorithm now has two-sided error.
- For $d > 3$, we provide the first randomized blackbox algorithm for this problem that runs in time $\text{poly}(n, d)$ (in an algebraic model where only arithmetic operations and equality tests are allowed). Previous algorithms for this problem (Kayal, 2011) as well as most of the existing reconstruction algorithms for other classes appeal to a polynomial factorization subroutine. This requires extraction of complex polynomial roots at unit cost and in standard models such as the unit-cost RAM or the Turing machine this approach does not yield polynomial time algorithms.
- For $d > 3$, when f has rational coefficients (i.e. $K = \mathbb{Q}$), the running time of the blackbox algorithm is polynomial in n, d and the maximal bit size of any coefficient of f . This yields the first algorithm for this problem over \mathbb{C} with polynomial running time in the bit model of computation.

These results are true even when we replace \mathbb{C} by \mathbb{R} . We view the problem as a tensor decomposition problem and use linear algebraic methods such as checking the simultaneous diagonalisability of the slices of a tensor. The number of such slices is exponential in d . But surprisingly, we show that after a random change of variables, computing just 3 special slices is enough. We also show that our approach can be extended to the computation of the actual decomposition. This step relies on matrix diagonalisation which is not an algebraic step over \mathbb{C} . In forthcoming work we plan to extend these results to overcomplete decompositions, i.e., decompositions in more than n powers of linear forms.

3.13 Turning Turing Machines into Boolean Circuits

Michal Koucký (Charles University – Prague, CZ)

License  Creative Commons BY 4.0 International license
 Michal Koucký

We give a new simple proof for the classical result that Turing machines running in time $t(n)$ and space $s(n)$ can be simulated by boolean circuits of size $O(t(n)\log s(n))$ and of depth $O(t(n))$. When we allow unbounded fan-in gates we can get circuits of the same size and depth $O(t(n)/\log \log s(n))$.

3.14 The complexity of monomial symmetric polynomials

Nutan Limaye (IT University of Copenhagen, DK)

License © Creative Commons BY 4.0 International license
© Nutan Limaye

Joint work of Nutan Limaye, Radu Curticapean, Srikanth Srinivasan

Main reference Radu Curticapean, Nutan Limaye, Srikanth Srinivasan: “On the VNP-Hardness of Some Monomial Symmetric Polynomials”, in Proc. of the 42nd IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science, FSTTCS 2022, December 18-20, 2022, IIT Madras, Chennai, India, LIPIcs, Vol. 250, pp. 16:1–16:14, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022.

URL <http://dx.doi.org/10.4230/LIPIcs.FSTTCS.2022.16>

The determinant of the Vandermonde matrix has a very simple algebraic formula. However, the complexity of its permanent, denoted in this talk as $\text{Perm}(V)$, is not known. The permanent of the Vandermonde matrix is a “monomial symmetric polynomial”. In this talk we show that there exist monomial symmetric polynomials that are hard for VNP.

3.15 Decision tree rank for Boolean functions

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

License © Creative Commons BY 4.0 International license
© Meena Mahajan

Joint work of Yogesh Dahiya, Meena Mahajan

Main reference Yogesh Dahiya, Meena Mahajan: “On (Simple) Decision Tree Rank”, in Proc. of the 41st IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science, FSTTCS 2021, December 15-17, 2021, Virtual Conference, LIPIcs, Vol. 213, pp. 15:1–15:16, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021.

URL <http://dx.doi.org/10.4230/LIPIcs.FSTTCS.2021.15>

In this talk, I describe some relations between the minimum rank of a decision tree computing a Boolean function and other complexity measures of the function. I also describe a composition theorem in terms of rank and decision tree depth, and show how it simplifies some known lower bounds on decision tree size and rank.

Joint work with Yogesh Dahiya.

3.16 Radical Sylvester-Gallai theorem for cubics – and beyond

Rafael Mendes de Oliveira (University of Waterloo, CA)

License © Creative Commons BY 4.0 International license
© Rafael Mendes de Oliveira

Joint work of Rafael Oliveira, Akash Kumar Sengupta

Main reference Rafael Mendes de Oliveira, Akash Sengupta: “Radical Sylvester-Gallai for Cubics”, Electron. Colloquium Comput. Complex., Vol. TR22-131, 2022.

URL <https://eccc.weizmann.ac.il/report/2022/131>

In 1893, Sylvester asked a basic question in combinatorial geometry: given a finite set of distinct points $v_1, \dots, v_m \in \mathbb{R}^N$ such that the line defined by any pair of distinct points v_i, v_j contains a third point v_k in the set, must all points in the set be collinear?

Generalizations of Sylvester’s problem, which are known as Sylvester-Gallai type problems, have found applications in algebraic complexity theory (in Polynomial Identity Testing – PIT) and coding theory (Locally Correctable Codes). The underlying theme in all these types of questions is the following:

Are Sylvester-Gallai type configurations always low-dimensional?

In 2014, Gupta, motivated by such applications in algebraic complexity theory, proposed wide-ranging non-linear generalizations of Sylvester’s question, with applications on the PIT problem.

In this talk, we will discuss these non-linear generalizations of Sylvester’s conjecture, their intrinsic relation to algebraic computation, and a recent theorem proving that radical Sylvester-Gallai configurations for cubic polynomials must have small dimension.

Joint work with Akash Kumar Sengupta.

3.17 High-dimensional expanders from Chevalley groups

Ryan O’Donnell (Carnegie Mellon University – Pittsburgh, US)

License © Creative Commons BY 4.0 International license
© Ryan O’Donnell

Joint work of Ryan O’Donnell, Kevin Pratt

Main reference Ryan O’Donnell, Kevin Pratt: “High-Dimensional Expanders from Chevalley Groups”, in Proc. of the 37th Computational Complexity Conference, CCC 2022, July 20-23, 2022, Philadelphia, PA, USA, LIPIcs, Vol. 234, pp. 18:1–18:26, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022.

URL <http://dx.doi.org/10.4230/LIPIcs.CCC.2022.18>

In this talk I discussed recent joint work with Kevin Pratt on constructing high-dimensional expanders.

Let Φ be an irreducible root system (other than G_2) of rank at least 2, let \mathbb{F} be a finite field with $p = \text{char } \mathbb{F} > 3$, and let $G_\Phi \mathbb{F}$ be the corresponding Chevalley group. We describe a strongly explicit high-dimensional expander (HDX) family of dimension $\text{rank}(\Phi)$, where $G_\Phi \mathbb{F}$ acts simply transitively on the top-dimensional faces; these are λ -spectral HDXs with $\lambda \rightarrow 0$ as $p \rightarrow \infty$. This generalizes a construction of Kaufman and Oppenheim (STOC 2018), which corresponds to the case $\Phi = A_d$. Our work gives three new families of spectral HDXs of any dimension ≥ 2 , and four exceptional constructions of dimension 4, 6, 7, and 8.

3.18 Highly-efficient local proofs

Noga Ron-Zewi (University of Haifa, IL)

License © Creative Commons BY 4.0 International license
© Noga Ron-Zewi

Joint work of Noga Ron-Zewi, Ron Rothblum

The celebrated PCP theorem from the 90’s shows that any mathematical proof can be encoded in such a way that its correctness can be verified locally by reading only a tiny number of bits from the encoding. A fundamental question that has drawn a great amount of interest is what is the minimal overhead in encoding that is needed to allow for such highly efficient local verification. While the original PCP theorem only guarantees a polynomial overhead, a beautiful line of work has culminated in remarkably short encodings with only a poly-logarithmic overhead. Motivated by cryptographic applications, we study a relatively new interactive variant of PCPs, called Interactive Oracle Proofs, and show that for this model the overhead in the encoding can be made arbitrarily small (approaching 1), and moreover, the prover complexity overhead can be made constant.


The improved efficiency was obtained by replacing polynomial-based codes, commonly used in such proof systems, with more efficient (tensor-based) codes. In particular, these constructions bypassed a barrier imposed by the need to encode the computation using a multiplication code.

References

- 1 Noga Ron-Zewi and Ron D. Rothblum, Proving as fast as computing: succinct arguments with constant prover overhead, STOC '22: 54th Annual ACM SIGACT Symposium on Theory of Computing, Rome, Italy, June 20 – 24, 2022, 1353–1363, ACM, 2022,
- 2 Noga Ron-Zewi and Ron D. Rothblum, Local Proofs Approaching the Witness Length [Extended Abstract], 61st IEEE Annual Symposium on Foundations of Computer Science, FOCS 2020, Durham, NC, USA, November 16-19, 2020, 846–857, IEEE, 2020

3.19 An Algorithmic Approach to Uniform Lower Bounds

Rahul Santhanam (*University of Oxford, GB*)


License  Creative Commons BY 4.0 International license
© Rahul Santhanam

We propose a new family of sampling tasks such that non-trivial algorithmic solutions to certain tasks from this family imply frontier uniform lower bounds such as “NP not in uniform ACC⁰” and “NP does not have uniform depth-2 threshold circuits”. Indeed, the most general versions of these sampling tasks have implications even for central open problems such as PSPACE vs P and NP vs P.

We observe that these sampling tasks do have non-trivial solutions under standard cryptographic assumptions. Moreover, we can use our framework to capture uniform versions of known non-uniform lower bounds, as well as classical results such as the space hierarchy theorem and Allender’s uniform lower bound for the Permanent. Our framework can also be used to show that NP does not have uniform AC⁰ circuits with a bottom layer of Mod 6 gates – the non-uniform version of this lower bound appears to be an open question.

3.20 Demystifying the border of depth-3 algebraic circuits

Nitin Saxena (*Indian Institute of Technology Kanpur, IN*)

License  Creative Commons BY 4.0 International license
© Nitin Saxena

Joint work of Pranjal Dutta, Prateek Dwivedi, Nitin Saxena

Main reference Pranjal Dutta, Prateek Dwivedi, Nitin Saxena: “Demystifying the border of depth-3 algebraic circuits”, in Proc. of the 62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021, Denver, CO, USA, February 7-10, 2022, pp. 92–103, IEEE, 2021.

URL <http://dx.doi.org/10.1109/FOCS52979.2021.00018>

Main reference Pranjal Dutta, Prateek Dwivedi, Nitin Saxena: “Deterministic Identity Testing Paradigms for Bounded Top-Fanin Depth-4 Circuits”, in Proc. of the 36th Computational Complexity Conference, CCC 2021, July 20-23, 2021, Toronto, Ontario, Canada (Virtual Conference), LIPIcs, Vol. 200, pp. 11:1–11:27, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021.

URL <http://dx.doi.org/10.4230/LIPIcs.CCC.2021.11>

Border (or approximative) complexity of polynomials plays an integral role in GCT approach to P≠NP. This raises an important open question: can a border circuit be *efficiently* debordered (i.e. convert from approximative to exact)? Or, could the approximation involve exponential-precision which may not be efficiently simulable? Circuits of depth 3 or 4, are a good testing ground for this question.

Recently, (Kumar ToCT’20) proved the universal power of the border of top-fanin-2 depth-3 circuits. We recently solved some of the related open questions. In this talk we outline our result: border of bounded-top-fanin depth-3 circuits is relatively easy– it can be computed by a polynomial-size algebraic branching program (ABP). Our de-bordering paradigm has many applications, especially in identity testing and lower bounds.

Based on the works with Prateek Dwivedi & Pranjal Dutta (CCC 2021) (FOCS 2021, invited to SICOMP).

3.21 Convex influences and a quantitative Gaussian correlation inequality

Rocco Servedio (Columbia University – New York, US)

License © Creative Commons BY 4.0 International license
© Rocco Servedio

Joint work of Anindya De, Shivam Nadimpalli, Rocco Servedio

Main reference Anindya De, Shivam Nadimpalli, Rocco A. Servedio: “Convex Influences”, in Proc. of the 13th Innovations in Theoretical Computer Science Conference, ITCS 2022, January 31 – February 3, 2022, Berkeley, CA, USA, LIPIcs, Vol. 215, pp. 53:1–53:21, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022.

URL <http://dx.doi.org/10.4230/LIPIcs.ITCS.2022.53>

Main reference Anindya De, Shivam Nadimpalli, Rocco A. Servedio: “Quantitative Correlation Inequalities via Semigroup Interpolation”, in Proc. of the 12th Innovations in Theoretical Computer Science Conference, ITCS 2021, January 6-8, 2021, Virtual Conference, LIPIcs, Vol. 185, pp. 69:1–69:20, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021.

URL <http://dx.doi.org/10.4230/LIPIcs.ITCS.2021.69>

The Gaussian correlation inequality (GCI), proved by Royen in 2014, states that any two centrally symmetric convex sets (say K and L) in Gaussian space are positively correlated. We establish a new quantitative version of the GCI which gives a lower bound on this correlation based on the “common influential directions” of K and L . This can be seen as a Gaussian space analogue of Talagrand’s well known correlation inequality for monotone Boolean functions.

To obtain this inequality, we propose a new approach, based on analysis of Littlewood type polynomials, which gives a recipe for transferring qualitative correlation inequalities into quantitative correlation inequalities. En route, we also give a new notion of influences for symmetric convex symmetric sets over Gaussian space which has many of the properties of influences of Boolean functions over the discrete cube. Much remains to be explored about this new notion of influences for convex sets.

Based on joint work with Anindya De and Shivam Nadimpalli.

3.22 Lossless Condensers from Multiplicity Codes

Amnon Ta-Shma (Tel Aviv University, IL)

License © Creative Commons BY 4.0 International license
© Amnon Ta-Shma

Joint work of Itay Kalev, Amnon Ta-Shma

Main reference Itay Kalev, Amnon Ta-Shma: “Unbalanced Expanders from Multiplicity Codes”, in Proc. of the Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2022, September 19-21, 2022, University of Illinois, Urbana-Champaign, USA (Virtual Conference), LIPIcs, Vol. 245, pp. 12:1–12:14, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022.

URL <http://dx.doi.org/10.4230/LIPIcs.APPROX/RANDOM.2022.12>

In 2007 Guruswami, Umans and Vadhan gave an explicit construction of a lossless condenser based on Parvaresh-Vardy codes. This lossless condenser is a fundamental building block in many constructions, and, in particular, is behind state-of-the-art extractor constructions.

We give an alternative construction that is based on Multiplicity codes. While the bottom-line result is similar to the GUV result, the analysis is very different. In GUV (and Parvaresh-Vardy codes) the polynomial ring is closed to a finite field, and every polynomial is associated with related elements in the finite field. In our construction a polynomial from the polynomial ring is associated with its iterated derivatives. Our analysis boils down to solving a differential equation over a finite field, and uses previous techniques, introduced by Kopparty for the list-decoding setting. We also observe that these (and more general) questions were studied in differential algebra, and we use the terminology and result developed there.

We believe these techniques have the potential to get better constructions and solve the current bottlenecks in the area.

3.23 Matrix multiplication via matrix groups

Christopher Umans (California Institute of Technology – Pasadena, US)

License © Creative Commons BY 4.0 International license
© Christopher Umans

Joint work of Christopher Umans, Henry Cohn, Jonah Blasiak, Josh Grochow, Kevin Pratt

Main reference Jonah Blasiak, Henry Cohn, Joshua A. Grochow, Kevin Pratt, Chris Umans: “Matrix multiplication via matrix groups”, CoRR, Vol. abs/2204.03826, 2022.

URL <http://dx.doi.org/10.48550/arXiv.2204.03826>

Cohn and Umans proposed a group-theoretic approach to bounding the exponent of matrix multiplication. Previous work within this approach ruled out certain families of groups as a route to obtaining $\omega = 2$, while other families of groups remain potentially viable. In this work we turn our attention to matrix groups, whose usefulness within this framework was relatively unexplored.

We first show that finite groups of Lie type cannot prove $\omega = 2$ within the group-theoretic approach. This is based on a representation-theoretic argument that identifies the second-smallest dimension of an irreducible representation of a group as a key parameter that determines its viability in this framework. Our proof builds on Gowers’ result concerning product-free sets in quasirandom groups. We then give another barrier that rules out certain natural matrix group constructions that make use of subgroups that are far from being self-normalizing.

Our barrier results leave open several natural paths to obtain exponent 2 via matrix groups. To explore these routes we propose working in the continuous setting of Lie groups, in which we develop an analogous theory. Obtaining the analogue of exponent 2 in this potentially easier setting is a key challenge that represents an intermediate goal short of actually proving $\omega = 2$. We give constructions in the continuous setting, which evade our two barriers, and indeed are “best-possible” in a precise sense. We then describe a new ingredient – “separating polynomials” – which allow us to recover a full-fledged framework yielding actual algorithms in the Lie setting (rather than constructions whose interest is only by analogy).

3.24 Almost Chor-Goldreich Sources and Adversarial Random Walks

David Zuckerman (*University of Texas – Austin, US*)

License © Creative Commons BY 4.0 International license
© David Zuckerman

Joint work of Dean Doron, Dana Moshkovitz, Justin Oh, David Zuckerman

Main reference Dean Doron, Dana Moshkovitz, Justin Oh, David Zuckerman: “Almost Chor-Goldreich Sources and Adversarial Random Walks”, *Electron. Colloquium Comput. Complex.*, Vol. TR22-103, 2022.

URL <https://eccc.weizmann.ac.il/report/2022/103>

A Chor-Goldreich (CG) source is a sequence of random variables where each has min-entropy, even conditioned on the previous ones. We extend this notion in several ways, most notably allowing each random variable to have Shannon entropy conditioned on previous ones. We achieve pseudorandomness results for Shannon-CG sources that were not known to hold even for standard CG sources, and even for the weaker model of Santha-Vazirani sources.

Specifically, we construct a deterministic condenser that on input a Shannon-CG source, outputs a distribution that is close to having constant entropy gap, namely its min-entropy is only an additive constant less than its length. Therefore, we can simulate any randomized algorithm with small failure probability using almost CG sources with no multiplicative slowdown. This result extends to randomized protocols as well, and any setting in which we cannot simply cycle over all seeds, and a “one-shot” simulation is needed. Moreover, our construction works in an online manner, since it is based on random walks on expanders.

Our main technical contribution is a novel analysis of random walks, which should be of independent interest. We analyze walks with adversarially correlated steps, each step being entropy-deficient, on good enough lossless expanders. We prove that such walks (or certain interleaved walks on two expanders) accumulate entropy.

Participants

- Eric Allender
Rutgers University –
Piscataway, US
- Markus Bläser
Universität des Saarlandes –
Saarbrücken, DE
- Andrej Bogdanov
The Chinese University of
Hong Kong, HK
- Peter Bürgisser
TU Berlin, DE
- Prerona Chatterjee
The Czech Academy of Sciences –
Prague, CZ
- Arkadev Chattopadhyay
TIFR – Mumbai, IN
- Gil Cohen
Tel Aviv University, IL
- Julian Dörfler
Universität des Saarlandes –
Saarbrücken, DE
- Stephen A. Fenner
University of South Carolina –
Columbia, US
- Michael A. Forbes
University of Illinois –
Urbana-Champaign, US
- Lance Fortnow
Illinois Institute of Technology –
Chicago, US
- Anna Gál
University of Texas – Austin, US
- Frederic Green
Clark University – Worcester, US
- Rohit Gurjar
Indian Institute of Technology –
Mumbai, IN
- William Hoza
University of California –
Berkeley, US
- Christian Ikenmeyer
University of Liverpool, GB
- Valentine Kabanets
Simon Fraser University –
Burnaby, CA
- Pascal Koiran
ENS – Lyon, FR
- Antonina Kolokolova
University of Newfoundland –
St. John's, CA
- Michal Koucký
Charles University – Prague, CZ
- Sophie Laplante
University Paris Diderot, FR
- Nutan Limaye
IT University of
Copenhagen, DK
- Meena Mahajan
The Institute of Mathematical
Sciences – Chennai, IN
- Rafael Mendes de Oliveira
University of Waterloo, CA
- Ryan O'Donnell
Carnegie Mellon University –
Pittsburgh, US
- Natacha Portier
ENS – Lyon, FR
- Noga Ron-Zewi
University of Haifa, IL
- Rahul Santhanam
University of Oxford, GB
- Nitin Saxena
Indian Institute of Technology
Kanpur, IN
- Rocco Servedio
Columbia University –
New York, US
- Ronen Shaltiel
University of Haifa, IL
- Amir Shpilka
Tel Aviv University, IL
- Srikanth Srinivasan
Aarhus University, DK
- Amnon Ta-Shma
Tel Aviv University, IL
- Jacobo Torán
Universität Ulm, DE
- Christopher Umans
California Institute of Technology
– Pasadena, US
- Mary Wootters
Stanford University, US
- David Zuckerman
University of Texas – Austin, US
- Jeroen Zuiddam
University of Amsterdam, NL

