

Computational Complexity of Discrete Problems

Swastik Kopparty^{*1}, Meena Mahajan^{*2}, Rahul Santhanam^{*3},
Till Tantau^{*4}, and Ian Mertz^{†5}

1 University of Toronto, CA. swastik.kopparty@gmail.com

2 The Institute of Mathematical Sciences & HBNI – Chennai, IN.
meena@imsc.res.in

3 University of Oxford, GB. rahul.santhanam@cs.ox.ac.uk

4 Universität zu Lübeck, DE. tantau@tcs.uni-luebeck.de

5 Charles University – Prague, CZ. iwmertz@gmail.com

Abstract

This report documents the program and activities of Dagstuhl Seminar 25111 “Computational Complexity of Discrete Problems,” which was held during March 09–14, 2025. The seminar brought together researchers working in many diverse sub-areas of computational complexity, promoting a vibrant exchange of ideas. Following a description of the seminar’s objectives and its overall organization, this report lists the different major talks given during the seminar in alphabetical order of speakers, followed by the abstracts of the talks, including the main references and relevant sources where applicable.

Seminar March 9–14, 2025 – <http://www.dagstuhl.de/25111>

2012 ACM Subject Classification Theory of computation → Complexity theory and logic; Theory of computation → Complexity classes; Theory of computation → Problems, reductions and completeness; Theory of computation → Circuit complexity; Theory of computation → Proof complexity

Keywords and phrases circuit complexity, communication complexity, computational complexity, lower bounds, randomness

Digital Object Identifier 10.4230/DagRep.15.3.56

1 Executive Summary

Swastik Kopparty

Meena Mahajan

Rahul Santhanam

Till Tantau

License  Creative Commons BY 4.0 International license

© Swastik Kopparty, Meena Mahajan, Rahul Santhanam, and Till Tantau

Overview

Computational complexity studies the amount of resources (such as time, space, randomness, communication, or parallelism) necessary to solve discrete problems – a crucial task both in theoretical and practical applications. Despite a long line of research, for many practical problems it is not known if they can be solved efficiently. Here, “efficiently” can refer to polynomial-time algorithms, whose existence is not known for problems like Satisfiability or Factoring. For the large data sets arising for instance in machine learning, already cubic or

* Editor / Organizer

† Editorial Assistant / Collector



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

Computational Complexity of Discrete Problems, *Dagstuhl Reports*, Vol. 15, Issue 3, pp. 56–76

Editors: Swastik Kopparty, Meena Mahajan, Rahul Santhanam, Till Tantau, and Ian Mertz



Dagstuhl Reports

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

even quadratic time may be too large, but may be unavoidable as research on fine-grained complexity indicates. The ongoing research on such fundamental problems has a recurring theme: the difficulty of proving lower bounds. Indeed, many of the great open problems of theoretical computer science are, in essence, open lower bound problems.

This Dagstuhl Seminar, the 14th in a long-standing series of seminars on this theme, addressed several of these questions in the context of circuit and formula sizes, meta-complexity, proof complexity, fine-grained complexity, communication complexity, and classical computational complexity. In each area, powerful tools for proving lower and upper bounds are known, but particularly interesting and powerful results often arise from establishing connections between the fields. The seminar aimed to bring together a diverse group of leading experts and promising young researchers in these areas, to discuss and to discover new, further connections.

Technical Talks

The Dagstuhl Seminar saw thirty technical lengths, of durations ranging from 10 to 50 minutes, covering and going beyond the themes discussed above. While detailed talk abstracts appear later in this report, here is a brief topic-wise overview.

Hardness of Approximation and Local Testing

When faced with a computational problem for which an efficient solution is hard to find (e.g. if the problem is NP hard), we can hope to efficiently find *approximate* solutions. *Hardness of approximation* is the study of computational limitations to what kinds of approximation can be achieved efficiently, and it has been a flourishing subfield of theoretical computer science. A key ingredient for hardness of approximation theorems are probabilistically checkable proofs and *local testing*: where one wants to check properties of some large object while only querying a small randomly chosen part of it. Yuval Filmus presented a new unified approach to local testing of polymorphisms, generalizing linearity testing and monomial testing, previously proved using quite different techniques. Prahladh Harsha presented an optimal analysis of the classical “lines vs points” low degree test, which can detect when a given function has even just 1%-fraction agreement with a low-degree multivariate polynomial. Such local tests are central ingredients in state-of-the-art probabilistically checkable proofs and hardness of approximation results. Amey Bhangale described a long series of works that are part of a program to classify the hardness of approximating constraint satisfiable problems that are promised to be satisfiable. Shuichi Hirahara presented new results on *average-case* hardness of approximation for matrix multiplication, a topic that has seen much interest in recent years. The key ingredient here is a new proof of the classical Yao XOR lemma, a hardness amplification result with origins in cryptography. Sasha Golovnev gave a talk on barriers to proving exponential time complexity hardness (known as “SETH-hardness”) for many classical problems with unknown complexity like Hamiltonian cycles. Radu Curticapean gave a survey of a recent line of work on hardness of finding subgraphs. This line of work can now determine for every graph H the fine-grained complexity of finding copies of H in a given input graph; remarkably, the hardness results match classical algorithms based on dynamic programming and treewidth.

Meta-Complexity

Meta-complexity studies relationships between lower bounds, learning, pseudorandomness, cryptography and proofs, based on analysing the complexity of compression problems. Valentine Kabanets discussed how a central question in cryptography, namely whether witness encryption exists for NP, is equivalent to a central question in learning theory, namely whether computational learning is hard for NP. Zhenjian Lu defined the Heavy Avoid problem, which asks whether “heavy” elements for a samplable distribution, can be identified efficiently, and showed that this problem is closely related to uniform probabilistic lower bounds. Oliver Korten described connections between the Range Avoidance problem for NC^0 circuits and previously well-studied problems about cell-probe lower bounds and NC^0 pseudo-random generators. In each of these cases, the meta-complexity perspective leads to the identification of new connections and approaches.

Space-bounded Computation

Space-bounded computation was another important theme of the seminar; recent advances in *catalytic* computation have generated much excitement. Ian Mertz discussed the recent breakthrough result of Ryan Williams showing that time can be simulated in nearly square-root space. Michal Koucký described a range of collapses of catalytic classes, including the results that catalytic non-deterministic space and catalytic randomized space are equivalent to catalytic deterministic space. Roei Tell presented work on the long-standing open question of whether randomized logarithmic space can be derandomized, showing that for two standard algorithmic tasks, namely solving connectivity and computing random walk probabilities for graphs, at least one is solvable more efficiently than was hitherto known. Amit Chakrabarti and Sumegha Garg discussed various models of streaming algorithms, which are special kinds of space-bounded algorithms analyzed using various information complexity techniques.

Query and Communication

Kaave Hosseini gave a sweeping overview of various kinds of measures for Boolean matrices – algebraic, analytic, and combinatorial – and their relative strengths in pinpointing the communication complexity of specific Boolean functions. Yogesh Dahiya described recent work focusing on the size of decision trees (a measure of the space required for storing Boolean functions), including a surprising application using size bounds in simple decision trees to derandomize depth (i.e. query complexity) in a generalized decision tree model. Avishay Tal described the connection between query and communication complexities via lifting theorems, and sketched a simpler proof of the lifting theorem of Göös, Pitassi, and Watson for randomized query and communication.

Proof Complexity and Circuits

Several connections between proof complexity and circuit complexity were highlighted in a series of talks. For different complexity measures of the same type of object (proofs, circuits, algorithms), tradeoff results describe the extent to which we can optimize one measure while simultaneously controlling the others. Supercritical tradeoffs describe the phenomenon where a procedure optimizing one complexity measure may make other measures shoot up even beyond the generic worst case bound. Jakob Nordström described recent tightening of supercritical tradeoffs in multiple settings, including cutting-plane proof size vs depth, monotone circuit size vs depth, and more; all hinge upon tradeoff results in propositional

proof complexity. Susanna de Rezende described a generalized query-to-communication lifting theorem and its applications to obtaining lower bounds for monotone circuits and propositional proof sizes. Olaf Beyersdorff sketched a broad framework for translating computational hardness in varied circuit models into QBFs with no short proofs in QBF proof systems naturally corresponding to many real-world solvers.

Pseudorandomness and Combinatorial Constructions

We had several talks on explicit constructions of pseudorandom combinatorial objects – of the kind that are useful for pseudorandom generators and other derandomization tasks. Rachel Zhang presented her new explicit constant-degree expander graphs, breaking a barrier on what is achievable by spectral methods. Gil Cohen presented a new result computing optimal spectral bounds for the zig-zag product, a method for construct expander graphs. Remarkably, their method uses tools from very distant areas of mathematics: free probability and complex analysis. Siqi Liu showed how high dimensional expanders, a hypergraph analogue of expander graphs, could be used to give new locally testable codes with the pointwise multiplication property. Eshan Chattopadhyay presented explicit constructions of extractors from multiple independent sources, that can extract pure randomness when even just three of them are assumed to be weakly random. This result involves several ideas, and in particular develops extractors that fool multiparty communication protocols. Pavel Pudlák showed that nonmalleable affine extractors, due to their strong pseudorandomness, are hard to compute for certain branching programs. Thomas Thierauf gave a survey of several computational problems surrounding graph rigidity. Finally, Makrand Sinha talked about how to generate pseudorandom matrices using random sequences of elementary operations: the study of such problems is motivated by issues in quantum computation.

Open Problems

The seminar also included an open problems session. Interesting research directions and open problems were posed by Sumegha Garg, Mika Göös, Ian Mertz, Jakob Nordström, Hanlin Ren, and Robert Robere.

The seminar included ample time for informal discussions, and interactions in smaller groups. The discussion spaces in the Schloss were put to good and frequent use!

Social Events

The social interactions during the seminar were significantly enhanced by the traditional and well-attended hike on Wednesday afternoon, and the music night on Thursday night (thanks to Antonina Kolokolova for organizing, and to her and Rahul Ilango, Ian Mertz, Noga Ron-Zewi, Avishay Tal, Roei Tell, Rachel Zhang, for actively contributing to this).

Acknowledgments

The organizers, Swastik Kopparty, Meena Mahajan, Rahul Santhanam, and Till Tantau, thank all participants for the many contributions they made. We also especially thank the Dagstuhl staff, who were – as usual – extremely friendly, helpful, and professional regarding all organizational matters surrounding the seminar. Finally, we are deeply grateful to Ian Mertz for his invaluable help assembling and preparing this report.

2 Table of Contents

Executive Summary

<i>Swastik Kopparty, Meena Mahajan, Rahul Santhanam, and Till Tantau</i>	56
--	----

Overview of Talks

Computationally Hard Problems Are Hard for QBF Proof Systems Too <i>Olaf Beyersdorff</i>	62
A New Approximation Algorithm for Satisfiable Constraint Satisfaction Problems <i>Amey Bhangale</i>	62
Leakage-Resilient Extractors Against Number-on-Forehead Protocols <i>Eshan Chattopadhyay</i>	63
Can You Link Up With Treewidth? <i>Radu Curticapean</i>	63
Lifting with Colourful Sunflowers <i>Susanna de Rezende</i>	64
BLR for arbitrary Boolean predicates <i>Yuval Filmus</i>	64
A New Information Complexity Measure for Multi-pass Streaming with Applications <i>Sumegha Garg</i>	65
Polynomial Formulations as a Barrier for Reduction-Based Hardness Proofs <i>Alexander Golovnev</i>	65
An Improved Line-Point Low-Degree Test <i>Prahladh Harsha</i>	66
Error-Correction of Matrix Multiplication Algorithms <i>Shuichi Hirahara</i>	66
Algebraic, Analytic, and Combinatorial complexity measures of boolean matrices <i>Kaave Hosseini</i>	67
Witness Encryption and NP-hardness of Learning <i>Valentine Kabanets</i>	67
Stronger Cell Probe Lower Bounds via Local PRGs <i>Oliver Korten</i>	68
Collapsing Catalytic Classes <i>Michal Koucký</i>	69
High Dimensional Expanders for Error-correcting Codes <i>Siqi Liu</i>	69
On the Complexity of Avoiding Heavy Elements <i>Zhenjian Lu</i>	70
Simulating Time with Square Root Space <i>Ian Mertz</i>	70
Truly Supercritical Trade-offs for Resolution, Cutting Planes, Monotone Circuits, and Weisfeiler–Leman <i>Jakob Nordström</i>	71

Non-malleable affine extractors <i>Pavel Pudlák</i>	71
Recent development in the construction of efficient t-wise independent permutations and unitary designs <i>Makrand Sinha</i>	72
Lifting Barriers: towards query-to-communication lifting with smaller gadgets <i>Avishay Tal</i>	72
When Connectivity is Hard, Random Walks are Easy <i>Roei Tell</i>	73
Graph Rigidity <i>Thomas Thierauf</i>	73
Explicit Vertex Expanders Beyond the Spectral Barrier <i>Rachel Zhang</i>	73
Open problems	
Can Sherali–Adams prove the totality of rwPHP(PLS) in low degree? <i>Hanlin Ren</i>	74
Improving SPACE versus NSPACE via Tree Evaluation <i>Ian Mertz</i>	74
Participants	76

3 Overview of Talks

3.1 Computationally Hard Problems Are Hard for QBF Proof Systems Too

Olaf Beyersdorff (Friedrich-Schiller-Universität Jena, DE)

License © Creative Commons BY 4.0 International license
© Olaf Beyersdorff

Joint work of Agnes Schleitzer, Olaf Beyersdorff

Main reference Agnes Schleitzer, Olaf Beyersdorff: “Computationally Hard Problems Are Hard for QBF Proof Systems Too”, in Proc. of the AAAI-25, Sponsored by the Association for the Advancement of Artificial Intelligence, February 25 – March 4, 2025, Philadelphia, PA, USA, pp. 11336–11344, AAAI Press, 2025.

URL <https://doi.org/10.1609/AAAI.V39I11.33233>

There has been tremendous progress in the past decade in the field of quantified Boolean formulas (QBF), both in practical solving as well as in creating a theory of corresponding proof systems and their proof complexity analysis. Both for solving and for proof complexity, it is important to have interesting formula families on which we can test solvers and gauge the strength of the proof systems. There are currently few such formula families in the literature.

We initiate a general programme on how to transform computationally hard problems (located in the polynomial hierarchy) into QBFs hard for the main QBF resolution systems that relate to core QBF solvers. We illustrate this general approach on three problems from graph theory and logic. This yields QBF families that are provably hard for QBF resolution (without any complexity assumptions).

3.2 A New Approximation Algorithm for Satisfiable Constraint Satisfaction Problems

Amey Bhangale (University of California – Riverside, US)

License © Creative Commons BY 4.0 International license
© Amey Bhangale

Joint work of Amey Bhangale, Subhash Khot, Dor Minzer

Main reference Amey Bhangale, Subhash Khot, Dor Minzer: “On Approximability of Satisfiable k -CSPs: V”, CoRR, Vol. abs/2408.15377, 2024.

URL <https://doi.org/10.48550/ARXIV.2408.15377>

Two algorithms are well-known in the CSP world: Gaussian Elimination and rounding semi-definite program relaxation. In this talk, I will discuss a new ‘hybrid’ approximation algorithm that non-trivially combines these two algorithmic techniques. I will also discuss why we hope that this hybrid algorithm is an optimal approximation algorithm for satisfiable instances of certain CSPs.

References

- 1 Amey Bhangale, Subhash Khot and Dor Minzer. *On Approximability of Satisfiable k -CSPs: V*. In 57th Annual ACM Symposium on Theory of Computing 2025 (to appear), Prague, Czech Republic, 2025

3.3 Leakage-Resilient Extractors Against Number-on-Forehead Protocols

Eshan Chattopadhyay (Cornell University – Ithaca, US)

License © Creative Commons BY 4.0 International license
 © Eshan Chattopadhyay
Joint work of Eshan Chattopadhyay, Jesse Goodman
Main reference Eshan Chattopadhyay, Jesse Goodman: “Leakage-Resilient Extractors against Number-on-Forehead Protocols”, in Proc. of the 57th Annual ACM Symposium on Theory of Computing, STOC 2025, Prague, Czechia, June 23–27, 2025, pp. 604–614, ACM, 2025.
URL <https://doi.org/10.1145/3717823.3718272>

Given a sequence of N independent sources X_1, X_2, \dots, X_N , each on n bits, how many of them must be good (i.e., contain some min-entropy) in order to extract a uniformly random string? This question was first raised by Chattopadhyay, Goodman, Goyal and Li (STOC ’20), motivated by applications in cryptography, distributed computing, and the unreliable nature of real-world sources of randomness. In their paper, they showed how to construct explicit low-error extractors for just $K \geq N/2$ good sources of polylogarithmic min-entropy. In a follow-up, Chattopadhyay and Goodman improved the number of good sources required to just $K \geq N/0.01$ (FOCS ’21). In this paper, we finally achieve $K = 3$. Our key ingredient is a near-optimal explicit construction of a new pseudorandom primitive, called a leakage-resilient extractor (LRE) against number-on-forehead (NOF) protocols. Our LRE can be viewed as a significantly more robust version of Li’s low-error three-source extractor (FOCS ’15), and resolves an open question put forth by Kumar, Meka, and Sahai (FOCS ’19) and Chattopadhyay, Goodman, Goyal, Kumar, Li, Meka, and Zuckerman (FOCS ’20). Our LRE construction is based on a simple new connection we discover between multiparty communication complexity and non-malleable extractors, which shows that such extractors exhibit strong average-case lower bounds against NOF protocols.

3.4 Can You Link Up With Treewidth?

Radu Curticapean (Universität Regensburg, DE)

License © Creative Commons BY 4.0 International license
 © Radu Curticapean
Joint work of Radu Curticapean, Simon Döring, Daniel Neuen, Jiaheng Wang
Main reference Radu Curticapean, Simon Döring, Daniel Neuen, Jiaheng Wang: “Can You Link Up With Treewidth?”, CoRR, Vol. abs/2410.02606, 2024.
URL <https://doi.org/10.48550/ARXIV.2410.02606>

Marx showed that $n^{o(k/\log k)}$ time algorithms for detecting colorful H -subgraphs would refute the exponential-time hypothesis ETH, even when H is a k -vertex expander of constant degree. This shows that colorful H -subgraphs are hard even for sparse H , and this result is widely used to obtain almost-tight conditional lower bounds.

We show a self-contained proof of this result that further simplifies very recent works. For this, we introduce a novel graph parameter, the linkage capacity $\gamma(H)$, and we show that detecting colorful H -subgraphs in time $n^{o(\gamma(H))}$ refutes ETH.

A very simple construction of communication networks credited to Beneš gives k -vertex graphs of maximum degree 3 and linkage capacity $\Omega(k/\log k)$. Additionally, we obtain new tight lower bounds for certain patterns by analyzing their linkage capacity. For example, we prove that almost all k -vertex graphs of polynomial average degree $\Omega(k^\beta)$ for some $\beta > 0$ have linkage capacity $\Theta(k)$, which implies tight lower bounds for such patterns H .

3.5 Lifting with Colourful Sunflowers

Susanna de Rezende (Lund University, SE)

License © Creative Commons BY 4.0 International license
© Susanna de Rezende

Joint work of Susanna de Rezende, Marc Vinyals

Main reference Susanna F. de Rezende, Marc Vinyals: “Lifting with Colorful Sunflowers”. Computational Complexity Conference (CCC), 2025, to appear.

In this talk we will show that a generalization of the DAG-like query-to-communication lifting theorem, when proven using sunflowers over non-binary alphabets, yields lower bounds on the monotone circuit complexity and proof complexity of natural functions and formulas that are better than previously known results obtained using the approximation method. These include an $n^{\Omega(k)}$ lower bound for the clique function up to $k \leq n^{1/2-\epsilon}$, and an $\exp(\Omega(n^{1/3-\epsilon}))$ lower bound for a function in P.

3.6 BLR for arbitrary Boolean predicates

Yuval Filmus (Technion – Haifa, IL)

License © Creative Commons BY 4.0 International license
© Yuval Filmus

Joint work of Yaroslav Alekseev, Yuval Filmus

The celebrated BLR linearity test states that if a Boolean function f satisfies $f(x) \oplus f(y) = f(x \oplus y)$ with probability close to 1, then f is close to a linear function, that is, a function that satisfies this equation for all x, y . Another way to view the BLR test is through the lens of *polymorphisms*, a notion from universal algebra. Linear functions are polymorphisms of the predicate $P_{\oplus} = \{(a, b, c) \in \{0, 1\}^3 \mid a \oplus b = c\}$. The BLR test states that an approximate polymorphism of P_{\oplus} (with respect to the uniform distribution) is close to an exact polymorphism. Other results of a similar sort include Mossel’s approximate Arrow theorem, a result of Friedgut and Regev about Kneser graphs, and a result about AND testing which is a prequel to the present work.

In this work, we show that a BLR-like result holds for all predicates on bits, with respect to any distribution which is fully supported on the predicate (this includes BLR for arbitrary distributions). As in the case of AND testing, the statement needs to be changed to allow “multi-sorted” polymorphisms. The proof resembles the classical proof of the triangle removal lemma using the regularity lemma, with Jones’ regularity lemma replacing Szemerédi’s, and It Ain’t Over Till It’s Over an essential ingredient for the counting lemma.

3.7 A New Information Complexity Measure for Multi-pass Streaming with Applications

Sumegha Garg (Rutgers University – New Brunswick, US)

License © Creative Commons BY 4.0 International license

© Sumegha Garg

Joint work of Mark Braverman, Sumegha Garg, Qian Li, Shuo Wang, David P. Woodruff, Jiapeng Zhang

Main reference Mark Braverman, Sumegha Garg, Qian Li, Shuo Wang, David P. Woodruff, Jiapeng Zhang: “A New Information Complexity Measure for Multi-pass Streaming with Applications”, in Proc. of the 56th Annual ACM Symposium on Theory of Computing, STOC 2024, Vancouver, BC, Canada, June 24–28, 2024, pp. 1781–1792, ACM, 2024.

URL <https://doi.org/10.1145/3618260.3649672>

In this talk, we will introduce a new notion of information complexity for one-pass and multi-pass streaming problems, and use it to prove memory lower bounds for the coin problem. In the coin problem, one sees a stream of n i.i.d. uniform bits and one would like to compute the majority (or sum) with constant advantage. We show that any constant pass algorithm must use $\Omega(\log n)$ bits of memory. This information complexity notion is also useful to prove tight space complexity for the needle problem, which in turn implies tight bounds for the problem of approximating higher frequency moments in a data stream.

3.8 Polynomial Formulations as a Barrier for Reduction-Based Hardness Proofs

Alexander Golovnev (Georgetown University – Washington, DC, US)

License © Creative Commons BY 4.0 International license

© Alexander Golovnev

Joint work of Tatiana Belova, Alexander Golovnev, Alexander S. Kulikov, Ivan Mihajlin, Denil Sharipov,

Main reference Tatiana Belova, Alexander Golovnev, Alexander S. Kulikov, Ivan Mihajlin, Denil Sharipov: “Polynomial Formulations as a Barrier for Reduction-based Hardness Proofs”, ACM Trans. Algorithms, Association for Computing Machinery, 2025.

URL <https://doi.org/10.1145/3721134>

The Strong Exponential Time Hypothesis (SETH) asserts that for every $\varepsilon > 0$ there exists k such that k -SAT requires time $(2 - \varepsilon)^n$. The field of fine-grained complexity has leveraged SETH to prove quite tight conditional lower bounds for dozens of problems in various domains and complexity classes, including Edit Distance, Graph Diameter, Hitting Set, Independent Set, and Orthogonal Vectors. Yet, it has been repeatedly asked in the literature whether SETH-hardness results can be proven for other fundamental problems such as Hamiltonian Path, Independent Set, Chromatic Number, MAX- k -SAT, and Set Cover.

In this paper, we show that fine-grained reductions implying even λ^n -hardness of these problems from SETH for *any* $\lambda > 1$, would imply new circuit lower bounds: super-linear lower bounds for Boolean series-parallel circuits or polynomial lower bounds for arithmetic circuits (each of which is a four-decade open question).

We also extend this barrier result to the class of parameterized problems. Namely, for every $\lambda > 1$ we conditionally rule out fine-grained reductions implying SETH-based lower bounds of λ^k for a number of problems parameterized by the solution size k .

Our main technical tool is a new concept called polynomial formulations. In particular, we show that many problems can be represented by relatively succinct low-degree polynomials, and that any problem with such a representation cannot be proven SETH-hard (without proving new circuit lower bounds).

3.9 An Improved Line-Point Low-Degree Test

Prahladh Harsha (TIFR – Mumbai, IN)

License © Creative Commons BY 4.0 International license
© Prahladh Harsha

Joint work of Prahladh Harsha, Mrinal Kumar, Ramprasad Saptharishi, Madhu Sudan

Main reference Prahladh Harsha, Mrinal Kumar, Ramprasad Saptharishi, Madhu Sudan: “An Improved Line-Point Low-Degree Test”, in Proc. of the 65th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2024, Chicago, IL, USA, October 27-30, 2024, pp. 1883–1892, IEEE, 2024.

URL <https://doi.org/10.1109/FOCS61266.2024.00113>

In this talk, I’ll show that the most natural low-degree test for polynomials over finite fields is “robust” in the high-error regime for linear-sized fields. This settles a long-standing open question in the area of low-degree testing, yielding an $O(d)$ -query robust test in the “high-error” regime. The previous results in this space either worked only in the “low-error” regime (Polishchuk & Spielman, STOC 1994), or required $q = \Omega(d^4)$ (Arora & Sudan, Combinatorica 2003), or needed to measure local distance on 2-dimensional “planes” rather than one-dimensional lines leading to $\Omega(d^2)$ -query complexity (Raz & Safra, STOC 1997).

Our main technical novelty is a new analysis in the bivariate setting that exploits a previously known connection (namely Hensel lifting) between multivariate factorization and finding (or testing) low-degree polynomials, in a non “black-box” manner in the context of root-finding.

3.10 Error-Correction of Matrix Multiplication Algorithms

Shuichi Hirahara (National Institute of Informatics – Tokyo, JP)

License © Creative Commons BY 4.0 International license
© Shuichi Hirahara

Joint work of Shuichi Hirahara, Nobutaka Shimizu

We present an optimal “worst-case exact to average-case approximate” (non-uniform) reduction for Matrix Multiplication: Given an oracle that correctly computes, in expectation, a $(1/p + \epsilon)$ -fraction of pairs (A, B) of uniformly random matrices over a finite field of order p , we design an efficient oracle non-uniform algorithm that computes Matrix Multiplication exactly for all the pairs of matrices. The proof is based on a simple proof for Yao’s XOR lemma, whose complexity overhead is independent of the output length.

3.11 Algebraic, Analytic, and Combinatorial complexity measures of boolean matrices

Kaave Hosseini (University of Rochester, US)

License © Creative Commons BY 4.0 International license

© Kaave Hosseini

Joint work of Hamed Hatami, Ben Cheung, Kaave Hosseini, Morgan Shirley, Toni Pitassi, Alexander Nikolov

Main reference Tsun-Ming Cheung, Hamed Hatami, Kaave Hosseini, Aleksandar Nikolov, Toniann Pitassi, Morgan Shirley: “A Lower Bound on the Trace Norm of Boolean Matrices and Its Applications”, in Proc. of the 16th Innovations in Theoretical Computer Science Conference, ITCS 2025, January 7-10, 2025, Columbia University, New York, NY, USA, LIPIcs, Vol. 325, pp. 37:1–37:15, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2025.

URL <https://doi.org/10.4230/LIPICS.ITCS.2025.37>

I will discuss several fundamental complexity measures for Boolean matrices, such as rank, approximate rank, sign-rank, factorization norm, approximate factorization norm, etc. Then, I will discuss the relationship between these measures by addressing the following question: for two measures, X and Y , is it true that for all Boolean matrices M , if $X(M)$ is small, then $Y(M)$ is small? The quantitative aspects of this question have been an important line of work for several decades, with applications in many areas such as communication complexity, learning theory, dimensionality reduction, etc. However, the question is still poorly understood for several pairs of measures X and Y . I will discuss a few collaborative works to address this question.

3.12 Witness Encryption and NP-hardness of Learning

Valentine Kabanets (Simon Fraser University – Burnaby, CA)

License © Creative Commons BY 4.0 International license

© Valentine Kabanets

Joint work of Halley Goldberg, Valentine Kabanets

We study connections between two fundamental questions from computer science theory. (1) Is *witness encryption* possible for NP [1]? That is, given an instance x of an NP-complete language L , can one encrypt a secret message with security contingent on the ability to provide a witness for $x \in L$? (2) Is *computational learning* (in the sense of [2]) hard for NP? That is, is there a polynomial-time reduction from instances of L to instances of learning?

Our main result is that a certain formulation of NP-hardness of learning (very close to one described in [3]) characterizes the existence of witness encryption for NP. More specifically, we show:

- witness encryption for NP secure against non-uniform polynomial-size adversaries is equivalent to a “half-Levin” reduction from NP to the Computational Gap Learning problem [3];
- witness encryption for NP secure against *uniform* polynomial-time adversaries is equivalent to a BPP-black-box half-Levin reduction from NP to a search version of the same problem;
- witness encryption for NP with ciphertexts having logarithmic length, along with a circuit lower bound for E, are together equivalent to a half-Levin reduction from NP to a “distributional” version of the Minimum Circuit Size Problem.

Next, we prove two unconditional NP-hardness results for agnostic PAC learning. Building on ideas from [5], we prove that agnostic PAC-learning of polynomial-size boolean circuits is NP-hard in the “semi-proper” setting of learning size- $s(n)$ circuits by size- $s(n) \cdot n^{1/(\log \log n)^{O(1)}}$

circuits. We also prove NP-hardness of nearly improper learning in an agnostic “oracle-PAC” model that we define here, in which an algorithm is explicitly given the polynomial-length truth-table of a randomly sampled oracle function \mathcal{O} and is asked to learn with respect to \mathcal{O} -oracle circuits.

Lastly, we give some consequences of our results for the possibility of private- and public-key cryptography. Improving a main result of [3], we show that if improper agnostic PAC learning is NP-hard under a randomized non-adaptive reduction, then $\text{NP} \not\subseteq \text{ioBPP}$ implies the existence of one-way functions. Assuming a half-Levin reduction from an NP-complete language to CGL, we show that $\text{NP} \not\subseteq \text{ioBPP}$ implies the existence of public-key encryption. Along the way, we obtain: if $\text{NP} \not\subseteq \text{ioBPP}$, then witness encryption for NP implies public-key encryption.¹

References

- 1 Sanjam Garg, Craig Gentry, Amit Sahai, Brent Waters. Witness encryption and its applications. Symposium on Theory of Computing Conference (STOC), pp.467–476, 2013. 10.1145/2488608.2488667
- 2 Leslie G. Valiant. A Theory of the Learnable. Comm. ACM, 27(11) pp.1134–1142, 1984. 10.1145/1968.1972
- 3 Benny Applebaum, Boaz Barak, David Xiao. On Basing Lower-Bounds for Learning on Worst-Case Assumptions. Symposium on Foundations of Computer Science (FOCS), pp.211–220, 2008. 10.1109/FOCS.2008.35
- 4 Ilan Komargodski, Tal Moran, Moni Naor, Rafael Pass, Alon Rosen, Eylon Yogev. One-Way Functions and (Im)Perfect Obfuscation. Symposium on Foundations of Computer Science (FOCS), pp.374–383, 2014. 10.1109/FOCS.2014.47
- 5 Shuichi Hirahara. NP-Hardness of Learning Programs and Partial MCSP. Symposium on Foundations of Computer Science (FOCS), pp.968–979, 2022. 10.1109/FOCS54457.2022.00095
- 6 Shuichi Hirahara, Mikito Nanashima. One-Way Functions and Zero Knowledge. Symposium on Theory of Computing (STOC), pp.1731–1738, 2024. 10.1145/3618260.3649701
- 7 Yanyi Liu, Noam Mazon, Rafael Pass. A Note on Zero-Knowledge for NP and One-Way Functions. Electron. Colloquium Comput. Complex. (ECCC), TR24-095, 2024. <https://eccc.weizmann.ac.il/report/2024/095>

3.13 Stronger Cell Probe Lower Bounds via Local PRGs

Oliver Korten (Columbia University – New York, US)

License  Creative Commons BY 4.0 International license
© Oliver Korten

Joint work of Oliver Korten, Toni Pitassi, Russell Impagliazzo

Main reference Oliver Korten, Toniann Pitassi, Russell Impagliazzo: “Stronger Cell Probe Lower Bounds via Local PRGs”, Electron. Colloquium Comput. Complex., Vol. TR25-030, 2025.

URL <https://eccc.weizmann.ac.il/report/2025/030>

In this work, we develop a new method for proving lower bounds for static data structures in the classical cell probe model of Yao. Our methods give the strongest known lower bounds for any explicit problem in this model (quadratically stronger for space as a function of time)

¹ We believe that this last statement follows from a combination of techniques used in prior work ([1, 4, 6]; see [7]), but we have not seen the uniform version stated. In any case, we offer an alternative proof that does not rely on properties of statistical zero knowledge arguments.

and break a barrier which has stood for a few decades. Our lower bounds are based on a connection we establish between the static cell probe model and NC^0 generators, which have been studied extensively in cryptography and more recently in the context of “range avoidance.” With this connection in mind, we analyze the best known cryptographic attacks on NC^0 PRGs, which in turn are based on semirandom CSP refutation, and apply a similar family of arguments to analyze the cell probe model.

3.14 Collapsing Catalytic Classes

Michal Koucký (Charles University – Prague, CZ)

License © Creative Commons BY 4.0 International license
© Michal Koucký

Joint work of Michal Koucký, Ian Mertz, Edward Pyne, Sasha Sami

Main reference Michal Koucký, Ian Mertz, Edward Pyne, Sasha Sami: “Collapsing Catalytic Classes”, Electron. Colloquium Comput. Complex., Vol. TR25-019, 2025.

URL <https://eccc.weizmann.ac.il/report/2025/019>

A catalytic machine is a space-bounded Turing machine with additional access to a second, much larger work tape, with the caveat that this tape is full, and its contents must be preserved by the computation. Catalytic machines were defined by Buhrman et al. (STOC 2014), who, alongside many follow-up works, exhibited the power of catalytic space (CSPACE) and in particular catalytic logspace machines (CL) beyond that of traditional space-bounded machines.

Several variants of CL have been proposed, including non-deterministic and co-non-deterministic catalytic computation by Buhrman et al. (STACS 2016) and randomized catalytic computation by Datta et al. (CSR 2020). These and other works proposed several questions, such as catalytic analogues of the theorems of Savitch and Immerman and Szelepcsényi. Catalytic computation was recently derandomized by Cook et al. (STOC 2025), but only in certain parameter regimes.

We settle almost all questions regarding randomized and non-deterministic catalytic computation, by giving an optimal reduction from catalytic space with additional resources to the corresponding non-catalytic space classes. One main consequence of this is $\text{CL} = \text{CNL}$ i.e. with access to a large filled hard-drive, non-determinism provides no additional power.

Our results build on the compress-or-compute framework of Cook et al. (STOC 2025). Despite proving broader and stronger results, our framework is simpler and more modular.

3.15 High Dimensional Expanders for Error-correcting Codes

Siqi Liu (Institute for Advanced Study – Princeton, US)

License © Creative Commons BY 4.0 International license
© Siqi Liu

Joint work of Siqi Liu, Huy Tuan Pham, Irit Dinur, Rachel Zhang

Main reference Irit Dinur, Siqi Liu, Rachel Yun Zhang: “New Codes on High Dimensional Expanders”, CoRR, Vol. abs/2308.15563, 2023.

URL <https://doi.org/10.48550/ARXIV.2308.15563>

Expanders are well-connected graphs that have been extensively studied and have numerous applications in computer science, including error-correcting codes. High-dimensional expanders (HDXs) generalize expanders to hypergraphs and have the powerful local-to-global

property. Roughly speaking, this property states that the expansion of an HDX can be certified by the expansion of certain local structures. This property has made HDXs crucial in the recent breakthrough on locally testable codes (LTCs) [Dinur et al.'22]. These LTCs simultaneously achieve constant rate, constant relative distance, and constant query complexity. However, despite these desirable properties, these LTCs have yet to find applications in proof systems, as they lack the crucial multiplication property present in widely used polynomial codes. A major open question is: Do there exist LTCs with the multiplication property that achieve the same rate, distance, and query complexity as those constructed by Dinur et al.?

In this talk, I will provide intuition behind the connection between HDXs and LTCs, explain why the LTCs by Dinur et al. lack the multiplication property, and discuss my recent and ongoing work on constructing LTCs with the multiplication property. This talk is based on joint works with Irit Dinur, Rachel Zhang, and Huy Tuan Pham.

3.16 On the Complexity of Avoiding Heavy Elements

Zhenjian Lu (University of Warwick – Coventry, GB)

License  Creative Commons BY 4.0 International license
© Zhenjian Lu

Joint work of Zhenjian Lu, Igor C. Oliveira, Hanlin Ren, Rahul Santhanam

Main reference Zhenjian Lu, Igor C. Oliveira, Hanlin Ren, Rahul Santhanam: “On the Complexity of Avoiding Heavy Elements”, in Proc. of the 65th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2024, Chicago, IL, USA, October 27-30, 2024, pp. 2403–2412, IEEE, 2024.

URL <https://doi.org/10.1109/FOCS61266.2024.00140>

We introduce and study the following natural total search problem, which we call the heavy element avoidance (Heavy Avoid) problem: for a distribution on N bits specified by a Boolean circuit sampling it, and for some parameter $\delta(N) \geq 1/\text{poly}(N)$ fixed in advance, output an N -bit string that has probability less than $\delta(N)$. We show that the complexity of Heavy Avoid is closely tied to frontier open questions in complexity theory about uniform randomized lower bounds and derandomization.

3.17 Simulating Time with Square Root Space

Ian Mertz (Charles University – Prague, CZ)

License  Creative Commons BY 4.0 International license
© Ian Mertz

Joint work of Ian Mertz, Ryan Williams

Main reference R. Ryan Williams: “Simulating Time with Square-Root Space”, in Proc. of the 57th Annual ACM Symposium on Theory of Computing, STOC 2025, Prague, Czechia, June 23-27, 2025, pp. 13–23, ACM, 2025.

URL <https://doi.org/10.1145/3717823.3718225>

We will cover a recent breakthrough result by Williams [3] showing that $\text{TIME}[t]$ is contained in $\text{SPACE}[(t \log t)^{1/2}]$ for all $t \geq n$. We give an overview of the technique, which combines a decomposition of $\text{TIME}[t]$ (given by Hopcroft, Paul, and Valiant [2]) with a recent space-efficient algorithm for solving Tree Evaluation (given by Cook and Mertz [1]). Finally we analyze both ideas and barriers with regards to further progress, as well as potential other directions.

References

- 1 James Cook, Ian Mertz. *Tree Evaluation is in Space $O(\log n \log \log n)$* . Symposium on the Theory of Computing (STOC), 2024.
- 2 John E. Hopcroft, Wolfgang J. Paul, Leslie G. Valiant. *On Time vs Space*. Journal of the ACM (J.ACM), 1977.
- 3 Ryan Williams. *Simulating Time with Square Root Space*. Symposium on the Theory of Computing (STOC) (to appear), 2025.

3.18 Truly Supercritical Trade-offs for Resolution, Cutting Planes, Monotone Circuits, and Weisfeiler–Leman

Jakob Nordström (University of Copenhagen, DK & Lund University, SE)

License © Creative Commons BY 4.0 International license
 © Jakob Nordström
Joint work of Susanna F. de Rezende, Noah Fleming, Duri Andrea Janett, Jakob Nordström, Shuo Pang
Main reference Susanna F. de Rezende, Noah Fleming, Duri Andrea Janett, Jakob Nordström, Shuo Pang: “Truly Supercritical Trade-Offs for Resolution, Cutting Planes, Monotone Circuits, and Weisfeiler–Leman”, in Proc. of the 57th Annual ACM Symposium on Theory of Computing, STOC 2025, Prague, Czechia, June 23–27, 2025, pp. 1371–1382, ACM, 2025.
URL <https://doi.org/10.1145/3717823.3718271>

We exhibit supercritical trade-offs for monotone circuits, showing that there are functions computable by small circuits for which any small circuit must have depth super-linear or even super-polynomial in the number of variables, far exceeding the linear worst-case upper bound. We obtain similar trade-offs in proof complexity, where we establish the first size-depth trade-offs for cutting planes and resolution that are truly supercritical, i.e., in terms of formula size rather than number of variables, and we also show supercritical trade-offs between width and size for treelike resolution.

Our results build on a new supercritical depth-width trade-off for resolution, obtained by refining and strengthening the compression scheme for the cop-robber game in [Grohe, Lichter, Neuen & Schweitzer 2023]. This yields robust supercritical trade-offs for dimension versus iteration number in the Weisfeiler–Leman algorithm. Our other results follow from improved lifting theorems that might be of independent interest.

3.19 Non-malleable affine extractors

Pavel Pudlák (The Czech Academy of Sciences – Prague, CZ)

License © Creative Commons BY 4.0 International license
 © Pavel Pudlák
Joint work of Svyatoslav Gryaznov, Pavel Pudlák, Navid Talebanfar

I will prove an exponential lower bound on bottom regular read-once linear branching programs computing non-malleable affine disperser. This is an improvement of our result [1], where we proved an exponential lower bound on branching programs satisfying a stronger condition.

References

- 1 S. Gryaznov, P. Pudlák, N. Talebanfar: Linear Branching Programs and Directional Affine Extractors. Proc. Computational Complexity Conference 2022, Pages 4:1–4:16.

3.20 Recent development in the construction of efficient t -wise independent permutations and unitary designs

Makrand Sinha (*University of Illinois – Urbana-Champaign, US*)

License © Creative Commons BY 4.0 International license

© Makrand Sinha

Joint work of Tony Metger, Alexander Poremba, Makrand Sinha, Henry Yuen

Main reference Tony Metger, Alexander Poremba, Makrand Sinha, Henry Yuen: “Simple Constructions of Linear-Depth t -Designs and Pseudorandom Unitaries”, in Proc. of the 65th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2024, Chicago, IL, USA, October 27-30, 2024, pp. 485–492, IEEE, 2024.

URL <https://doi.org/10.1109/FOCS61266.2024.00038>

How can we efficiently construct a t -wise independent permutation from local permutation gates that act only on a constant number of bits? This question, originally studied by Gowers in 1996, turns out to be linked to an important object in quantum information theory called t -unitary designs. These designs are pseudorandom unitaries that information-theoretically reproduce the first t moments of the Haar measure on the unitary group. An important recent line of work in quantum computing concerns efficiently constructing such t -unitary designs from local unitary gates that act on a constant number of qubits.

This talk presents a survey of recent developments toward efficient construction of such objects. The talk will mainly be based on my work on the “PFC ensemble” [1], but will also discuss some subsequent followup works by other researchers.

References

- 1 T. Metger, A. Poremba, M. Sinha, and H. Yuen, “Simple Constructions of Linear-Depth t -Designs and Pseudorandom Unitaries,” in *65th IEEE Annual Symposium on Foundations of Computer Science (FOCS)*, Chicago, IL, USA, 2024, pp. 485–492. doi: 10.1109/FOCS61266.2024.00038.

3.21 Lifting Barriers: towards query-to-communication lifting with smaller gadgets

Avishay Tal (*University of California – Berkeley, US*)

License © Creative Commons BY 4.0 International license

© Avishay Tal

Joint work of Avishay Tal, Xinyu Wu

Query-to-communication lifting is a powerful method for transferring lower bounds from the query (or decision-tree) model to the communication model. A landmark result by Göös, Pitassi, and Watson (FOCS 2017, SICOMP 2020) demonstrated how to lift randomized query complexity bounds to randomized communication complexity of a related problem, obtained by replacing each input bit with a small “gadget”. A key lemma in their work is the uniform marginals lemma, whose proof is the most technical component of their paper.

We present a new, simpler proof for this lemma. We also discuss limitations of the lemma and, more broadly, of lifting results with the Index gadget, suggesting a modified gadget to address these limitations.

References

- 1 Göös, M., Pitassi, T. and Watson, T., 2017, October. Query-to-communication lifting for BPP. In *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)* (pp. 132-143). IEEE.

3.22 When Connectivity is Hard, Random Walks are Easy

Roei Tell (*University of Toronto, CA*)

License © Creative Commons BY 4.0 International license
© Roei Tell

Joint work of Dean Doron, Ted Pyne, Roei Tell, Ryan Williams

Classical PRGs are coupled with a reconstruction argument, asserting that if an adversary can break the PRG, then the adversary can also compute the underlying hard function. Classical reconstruction procedures are randomized, but a recent research effort developed reconstruction procedures for various PRGs that are deterministic, when considering limited types of adversaries.

This talk will present a recent result within this research effort. We construct a pair of deterministic low-space algorithms such that on every input graph, at least one of these algorithms solves a classical problem significantly better than the state-of-the-art: either s - t connectivity is solved, or random walk probabilities are estimated. Consequently, we'll see how to connect the $BPL = L$ question to the question of improving on Savitch's theorem.

3.23 Graph Rigidity

Thomas Thierauf (*Hochschule Aalen, DE*)

License © Creative Commons BY 4.0 International license
© Thomas Thierauf

Joint work of Rohit Gurjar, Kilian Rothmund, Thomas Thierauf

We give an introduction to graph rigidity. Similarly as the perfect matching problem it is related to many other algorithmic problems. In particular, minimal graph rigidity reduces to bipartite perfect matching, which puts it in quasi-NC. Our results are that minimal graph rigidity for planar graphs is in NC, as well as for $K_{3,3}$ -free and K_5 -free graphs.

3.24 Explicit Vertex Expanders Beyond the Spectral Barrier

Rachel Zhang (*MIT – Cambridge, US*)

License © Creative Commons BY 4.0 International license
© Rachel Zhang

Joint work of Jun-Ting Hsieh, Ting-Chun Lin, Sidhanth Mohanty, Ryan O'Donnell, Rachel Zhang

Main reference Jun-Ting Hsieh, Ting-Chun Lin, Sidhanth Mohanty, Ryan O'Donnell, Rachel Yun Zhang: "Explicit Two-Sided Vertex Expanders beyond the Spectral Barrier", in Proc. of the 57th Annual ACM Symposium on Theory of Computing, STOC 2025, Prague, Czechia, June 23-27, 2025, pp. 833–842, ACM, 2025.

URL <https://doi.org/10.1145/3717823.3718241>

We give the first explicit constructions of vertex expanders that pass the spectral barrier.

Previously, the strongest known explicit vertex expanders were those given by d -regular Ramanujan graphs, whose spectral properties imply that every small set S of vertices has at least $0.5d|S|$ distinct neighbors. However, it is possible to construct Ramanujan graphs containing a small set S that has no more than $0.5d|S|$ distinct neighbors. In fact, no explicit construction was known to beat the 0.5 barrier.

In this talk, I will discuss how we construct vertex expanders for which every small set expands by a factor of $0.6d$. In fact, our construction satisfies an even stronger property: small sets actually have $0.6d|S|$ *unique neighbors*.

4 Open problems

4.1 Can Sherali–Adams prove the totality of rwPHP(PLS) in low degree?

Hanlin Ren (*University of Oxford, GB*)

License  Creative Commons BY 4.0 International license
© Hanlin Ren

Joint work of Jiawei Li, Yuhao Li, Hanlin Ren

Main reference Jiawei Li, Yuhao Li, Hanlin Ren: “Metamathematics of Resolution Lower Bounds: A TFNP Perspective”, CoRR, Vol. abs/2411.15515, 2024.

URL <https://doi.org/10.48550/arXiv.2411.15515>

It is known that degree-polylog(n) Sherali–Adams can prove the retraction weak pigeonhole principle (rwPHP) as well as the totality of PLS [1]. The class rwPHP(PLS) is a combination of the above two classes, recently introduced in [2] to capture the complexity of proving resolution size lower bounds. Can Sherali–Adams prove the totality of rwPHP(PLS) in degree polylog(n)?


Either a Yes answer or a No answer to the above question would be very interesting. If the answer is Yes, then low-degree Sherali–Adams would be able to prove a large family of resolution size lower bounds (including those for random k -CNFs [3, 2]). On the other hand, a No answer would imply the NP-hardness of automating Sherali–Adams [4].

References

- 1 Mika Göös, Alexandros Hollender, Siddhartha Jain, Gilbert Maystre, William Pires, Robert Robere, Ran Tao. *Separations in Proof Complexity and TFNP*. Journal of the ACM 71(4), 1-45.
- 2 Jiawei Li, Yuhao Li, Hanlin Ren. *Metamathematics of Resolution Lower Bounds: A TFNP Perspective*. arXiv preprint arXiv:2411.15515 (2024).
- 3 Vašek Chvátal, Endre Szemerédi. *Many hard examples for resolution*. Journal of the ACM (JACM), 35(4), 759-768.
- 4 Susanna F. de Rezende, Mika Göös, Jakob Nordström, Toniann Pitassi, Robert Robere, Dmitry Sokolov. *Automating algebraic proof systems is NP-hard*. In STOC’21 (pp. 209-222).

4.2 Improving SPACE versus NSPACE via Tree Evaluation

Ian Mertz (*Charles University – Prague, CZ*)

License  Creative Commons BY 4.0 International license
© Ian Mertz

Savitch’s Theorem [2], which states that $\text{NSPACE}[s]$ is contained in $\text{SPACE}[s^2]$, has stood as a benchmark result in complexity theory for over fifty years. We propose that its tree-like structure can be exploited in conjunction with recent work of Cook and Mertz [1] to show

that $\text{NSPACE}[s] \subseteq \text{SPACE}[o(s^2)]$. This can be achieved by taking the classic NC^2 algorithm implicit in [2] and improving its height by an $\omega(\log \log n)$ factor at the expense of increasing the alphabet size of the wires and functions from $\{0, 1\}$ to $\{0, 1\}^{o(\log^2 n)}$.

References

- 1 James Cook, Ian Mertz. *Tree Evaluation is in Space $O(\log n \log \log n)$* . Symposium on the Theory of Computing (STOC), 2024.
- 2 Walter J. Savitch. *Relationships between nondeterministic and deterministic tape complexities*. Journal of Computer and System Sciences (JCSS), 1970.

Participants

- Olaf Beyersdorff
Friedrich-Schiller-Universität
Jena, DE
- Amey Bhangale
University of California –
Riverside, US
- Igor Carboni Oliveira
University of Warwick –
Coventry, GB
- Amit Chakrabarti
Dartmouth College –
Hanover, US
- Sourav Chakraborty
Indian Statistical Institute –
Kolkata, IN
- Arkadev Chattopadhyay
TIFR – Mumbai, IN
- Eshan Chattopadhyay
Cornell University – Ithaca, US
- Gil Cohen
Tel Aviv University, IL
- Radu Curticapean
Universität Regensburg, DE
- Yogesh Dahiya
The Institute of Mathematical
Sciences – Chennai, IN
- Susanna de Rezende
Lund University, SE
- Yuval Filmus
Technion – Haifa, IL
- Anna Gál
University of Texas – Austin, US
- Sumegha Garg
Rutgers University – New
Brunswick, US
- Mika Göös
EPFL Lausanne, CH
- Alexander Golovnev
Georgetown University –
Washington, DC, US
- Prahladh Harsha
TIFR – Mumbai, IN
- Johan Hastad
KTH Royal Institute of
Technology – Stockholm, SE
- Shuichi Hirahara
National Institute of Informatics –
Tokyo, JP
- Kaave Hosseini
University of Rochester, US
- Rahul Ilango
MIT – Cambridge, US
- Valentine Kabanets
Simon Fraser University –
Burnaby, CA
- Gillat Kol
Princeton University, US
- Antonina Kolokolova
Memorial University of
Newfoundland – St. John's, CA
- Swastik Kopparty
University of Toronto, CA
- Oliver Korten
Columbia University –
New York, US
- Michal Koucký
Charles University – Prague, CZ
- Sophie Laplante
Université Paris Cité, FR
- Nutan Limaye
IT University of
Copenhagen, DK
- Siqi Liu
Institute for Advanced Study –
Princeton, US
- Zhenjian Lu
University of Warwick –
Coventry, GB
- Meena Mahajan
The Institute of Mathematical
Sciences & HBNI – Chennai, IN
- Ian Mertz
Charles University – Prague, CZ
- Jakob Nordström
University of Copenhagen, DK &
Lund University, SE
- Pavel Pudlák
The Czech Academy of Sciences –
Prague, CZ
- Rüdiger Reischuk
Universität zu Lübeck, DE
- Hanlin Ren
University of Oxford, GB
- Robert Robere
McGill University –
Montréal, CA
- Noga Ron-Zewi
University of Haifa, IL
- Michael E. Saks
Rutgers University –
Piscataway, US
- Rahul Santhanam
University of Oxford, GB
- Makrand Sinha
University of Illinois –
Urbana-Champaign, US
- Amnon Ta-Shma
Tel Aviv University, IL
- Avishay Tal
University of California –
Berkeley, US
- Roei Tell
University of Toronto, CA
- Thomas Thierauf
Hochschule Aalen, DE
- Jacobo Torán
Universität Ulm, DE
- Rachel Zhang
MIT – Cambridge, US

