Report from Dagstuhl Seminar 21121

# Computational Complexity of Discrete Problems

**Edited by**

**Anna Gál[1], Meena Mahajan[2], Rahul Santhanam[3], and Till Tantau[4]**

1 **University of Texas, Austin, United States,** panni@cs.utexas.edu
2 **The Institute of Mathematical Sciences, HBNI, Chennai, India** meena@imsc.res.in
3 **University of Oxford, Great Britain,** rahul.santhanam@cs.ox.ac.uk
4 **Universität zu Lübeck, Germany,** tantau@tcs.uni-luebeck.de

## Abstract

This report documents the program and activities of Dagstuhl Seminar 21121 "Computational Complexity of Discrete Problems," which was held online in March 2021. Starting with a description of the organization of the online meeting and the topics covered, we then list the different 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. Despite the fact that only a compressed daily time slot was available for the seminar with participants from time zones spanning the whole globe and despite the fact that informal discussions were harder to hold than in a typical on-site seminar, the rate of participation throughout the seminar was very high and many lively scientific debates were held.

**Seminar** March 21–26, 2021 – http://www.dagstuhl.de/21121

**2012 ACM Subject Classification** Theory of computation → Computational complexity and cryptography; Theory of computation → Design and analysis of algorithms

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

**Digital Object Identifier** 10.4230/DagRep.11.2.1

**Edited in cooperation with** Max Bannach[1]

## 1 Executive Summary

*Anna Gál (University of Texas, Austin, Unites States)*
*Meena Mahajan (The Institute of Mathematical Sciences, HBNI, Chennai, India)*
*Rahul Santhanam (University of Oxford, Great Britain)*
*Till Tantau (Universität zu Lübeck, Germany)*

Computational complexity studies the amount of resources (such as time, space, randomness, or communication) that are necessary to solve computational problems in various models of computation. Finding efficient algorithms for solving computational tasks is crucial for practical applications. Despite a long line of research, for many problems that arise in practice it is not known if they can be solved efficiently – in particular, in polynomial time. Beside questions about the existence of polynomial time algorithms for problems like Satisfiability or Factoring, where the best known algorithms run in exponential time, there is a huge

[1] Universität zu Lübeck, Germany, bannach@tcs.uni-luebeck.de

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

class of practical problems where algorithms with polynomial running time (such as cubic or even quadratic time) are known, but it would be important to establish whether these running times are best possible, to what extent they can be improved, and whether parallel algorithms allow improvements of the runtime.

These fundamental questions motivate developments in various areas from algorithm design to circuit complexity, communication complexity and proof complexity. During this Dagstuhl Seminar 21121, some of the most exciting recent developments in those areas related to computational complexity were presented in a series of talks. The seminar was the most recent one in the series of Dagstuhl Seminars entitled “Computational Complexity of Discrete Problems” – seminars 19121, 17121, 14121, 11121.

Owing to the pandemic and associated travel restrictions, the seminar was held in a purely online format. With 52 researchers from across the world participating in the event, resident in time zones ranging from Japan to California, the window for common acceptable time slots was small. We decided to have a two-hour time slot each day for technical sessions, followed by an additional hour or more each day for social interactions. The Webex platform was used for technical sessions, and gather.town additionally for some of the social interactions. Despite the challenges of making the online event interesting given the ubiquitous screen-time fatigue, the meetings saw high participation level (between at least 80% and typically over 90% participation on all days) and were highly interactive – primarily due to the excellent nature of the given talks.

The seminar started with the creation of a “graph of interests” (using a Miro whiteboard), enabling participants to discover shared research interests with other participants. Following this, during the week, there were 20 research talks, coming from a range of topics including lower bounds on formula size and circuit size, complexity measures of Boolean functions, the algorithmic method for proving lower bounds, fixed parameter tractability and hardness magnification, communication complexity and lifting techniques, as well as proof complexity. Some specific results presented include:

- An improved lower bound, after many years, on the number of hyperplanes needed to slice all edges of the Boolean hypercube.
- A lower bound for monotone arithmetic circuit size using techniques from communication complexity.
- A new potential technique for de Morgan formula lower bounds.
- More refined notions of unambiguous certificate complexity and block sensitivity, with a separation that lifts to communication complexity.

The titles and abstracts of all the talks appear later in this report.

In addition, there was a rump session with short talks by Amit Chakrabarti, Amit Sinhababu, and Prahladh Harsha.

On the social interactions front, in the designated coffee slots there were some meet-random-people-in-a-break-out sessions. The traditional Wednesday hike was replaced by a “virtual hike” using Google Earth imagery, that went over one of the shorter hike trails near Schloss Dagstuhl and then virtually visited some participants’ institutes. The “wine-cheese-music party” became an online party on gather.town following the Schloss Dagstuhl map, and included music, games, and a commentary on the hardness of travelling.

The organizers, Anna Gál, Meena Mahajan, Rahul Santhanam, and Till Tantau, thank all participants for the many contributions they made. We would also like to especially thank the Dagstuhl staff for their cooperation in the current challenging circumstances, their encouragement for going ahead with an online event, and their unstinted help with organizational matters. We would also like to thank Max Bannach for his invaluable help assembling and preparing this report.

## 2 Table of Contents

**Executive Summary**

**Overview of Talks**

# 3 Overview of Talks

## 3.1 Cryptographic Hardness under Projections for Time-Bounded Kolmogorov Complexity

*Eric Allender (Rutgers University – Piscataway, US)*

**Joint work of** Eric Allender, John Gouwar, Shuichi Hirahara, Caleb Robelle
**Main reference** Eric Allender, John Gouwar, Shuichi Hirahara, Caleb Robelle: "Cryptographic Hardness under Projections for Time-Bounded Kolmogorov Complexity", Electron. Colloquium Comput. Complex., Vol. 28, p. 10, 2021.
**URL** https://eccc.weizmann.ac.il/report/2021/010

A version of time-bounded Kolmogorov complexity, denoted KT, has received attention in the past several years, due to its close connection to circuit complexity and to the Minimum Circuit Size Problem MCSP. Essentially all results about the complexity of MCSP hold also for MKTP (the problem of computing the KT complexity of a string). Both MKTP and MCSP are hard for SZK (Statistical Zero Knowledge) under BPP-Turing reductions; neither is known to be NP-complete. Recently, some hardness results for MKTP were proved that are not (yet) known to hold for MCSP. In particular, MKTP is hard for DET (a subclass of P) under nonuniform $\mathrm{NC}^0$ m-reductions.

We improve this, to show that MKTP is hard for the (apparently larger) class $\mathrm{NISZK}_L$ under not only $\mathrm{NC}^0$ m-reductions but even under projections. Also MKTP is hard for NISZK under P/poly m-reductions. Here, NISZK is the class of problems with non-interactive zero-knowledge proofs, and $\mathrm{NISZK}_L$ is the non-interactive version of the class $\mathrm{SZK}_L$ that was studied by Dvir et al.

As an application, we provide several improved worst-case to average-case reductions to problems in NP.

This is joint work with John Gouwar, Shuichi Hirahara, and Caleb Robelle.

## 3.2 Dynamic Kernels for Hitting Sets and Set Packing

*Max Bannach (Universität zu Lübeck, DE)*

**Joint work of** Max Bannach, Zacharias Heinrich, Rüdiger Reischuk, Till Tantau
**Main reference** Max Bannach, Zacharias Heinrich, Rüdiger Reischuk, Till Tantau: "Dynamic Kernels for Hitting Sets and Set Packing", Electron. Colloquium Comput. Complex., Vol. 26, p. 146, 2019.
**URL** https://eccc.weizmann.ac.il/report/2019/146

Computing kernels for the hitting set problem (the problem of finding a size-$k$ set that intersects each hyperedge of a hypergraph) is a well-studied computational problem. For hypergraphs with $m$ hyperedges, each of size at most $d$, the best algorithms can compute kernels of size $O(k^d)$ in time $O(2^d m)$. We generalize this task to the dynamic setting where hyperedges may be continuously added and deleted and we always have to keep track of a hitting set kernel (including moments when no size-$k$ hitting set exists). We present a deterministic solution, based on a novel data structure, that needs worst-case time $O^*(3^d)$ for updating the kernel upon hyperedge inserts and time $O^*(5^d)$ for updates upon deletions – thus nearly matching the time $O^*(2^d)$ needed by the best static algorithm per hyperedge.

## 3.3 Quantified Boolean formulas: proofs, solving, and circuits

*Olaf Beyersdorff (Universität Jena, DE)*

**Joint work of** Beyersdorff, Olaf, Benjamin Böhm, Meena Mahajan, Joshua Blinkhorn
**Main reference** Olaf Beyersdorff, Benjamin Böhm: "Understanding the Relative Strength of QBF CDCL Solvers and QBF Resolution", in Proc. of the 12th Innovations in Theoretical Computer Science Conference, ITCS 2021, January 6-8, 2021, Virtual Conference, LIPIcs, Vol. 185, pp. 12:1–12:20, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021.
**URL** https://doi.org/10.4230/LIPIcs.ITCS.2021.12
**Main reference** Olaf Beyersdorff, Joshua Blinkhorn, Meena Mahajan: "Hardness Characterisations and Size-Width Lower Bounds for QBF Resolution", in Proc. of the LICS '20: 35th Annual ACM/IEEE Symposium on Logic in Computer Science, Saarbrücken, Germany, July 8-11, 2020, pp. 209–223, ACM, 2020.
**URL** https://doi.org/10.1145/3373718.3394793

This talk will start with an overview of the relatively young field of QBF proof complexity, explaining QBF proof systems (including QBF resolution) and an assessment of which lower bound techniques are available for QBF proof systems. In the main part of the talk, I will explain hardness characterisations for QBF proof systems in terms of circuit complexity, yielding very direct connections between circuit lower bounds and QBF proof system lower bounds. The talk will also cover the relations between QBF resolution and QCDCL solving algorithms. Modelling QCDCL as proof systems we show that QCDCL and Q-Resolution are incomparable.

This talk is based on two recent papers, joint with Joshua Blinkhorn and Meena Mahajan (LICS'20) and with Benjamin Böhm (ITCS'21).

## 3.4 Majority versus Approximate Linear Sum and Average-Case Complexity Below NC$^1$

*Igor Carboni Oliveira (University of Warwick – Coventry, GB)*

**Joint work of** Igor Carboni Oliviera, Lijie Chen, Zhenjian Lu, Xin Lyu
**Main reference** Lijie Chen, Zhenjian Lu, Xin Lyu, Igor Carboni Oliveira: "Majority vs. Approximate Linear Sum and Average-Case Complexity Below NC1", Electron. Colloquium Comput. Complex., Vol. 28, p. 40, 2021.
**URL** https://eccc.weizmann.ac.il/report/2021/040

We develop a general framework that characterizes strong average-case lower bounds against circuit classes C contained in NC$^1$, such as AC$^0$[mod 2] and ACC$^0$. We apply this framework to show:

- Generic seed reduction: Pseudorandom generators (PRGs) against C of seed length $< n$ and error $\epsilon = n^{-\omega(1)}$ can be converted into PRGs of sub-polynomial seed length.
- Hardness under natural distributions: If E (deterministic exponential time) is average-case hard against C under some distribution, then E is average-case hard against C under the uniform distribution.
- Equivalence between worst-case and average-case hardness: Worst-case lower bounds against MAJ-C for problems in E are equivalent to strong average-case lower bounds against C. This can be seen as a certain converse to the Discriminator Lemma [Hajnal et al., JCSS'93].

These results were not known to hold for circuit classes that do not compute majority. Additionally, we prove that classical and recent approaches to worst-case lower bounds against ACC$^0$ via communication lower bounds for NOF multi-party protocols [Hastad and

Goldmann, CC'91; Razborov and Wigderson, IPL'93] and Torus polynomials degree lower bounds [Bhrushundi et al., ITCS'19] also imply strong average-case hardness against $\mathrm{ACC}^0$ under the uniform distribution.

Crucial to these results is the use of non-black-box hardness amplification techniques and the interplay between Majority (MAJ) and Approximate Linear Sum (apxSUM) gates. Roughly speaking, while a MAJ gate outputs 1 when the sum of the m input bits is at least $m/2$, a apxSUM gate computes a real-valued bounded weighted sum of the input bits and outputs 1 (resp. 0) if the sum is close to 1 (resp. close to 0), with the promise that one of the two cases always holds. As part of our framework, we explore ideas introduced in [Chen and Ren, STOC'20] to show that, for the purpose of proving lower bounds, a top layer MAJ gate is equivalent to a (weaker) apxSUM gate. Motivated by this result, we extend the algorithmic method and establish stronger lower bounds against bounded-depth circuits with layers of MAJ and apxSUM gates. Among them, we prove that:

- Lower bound: NQP does not admit fixed quasi-polynomial size MAJ-apxSUM-$\mathrm{ACC}^0$-THR circuits.

This is the first explicit lower bound against circuits with distinct layers of MAJ, apxSUM, and THR gates. Consequently, if the aforementioned equivalence between MAJ and apxSUM as a top gate can be extended to intermediate layers, long sought-after lower bounds against the class THR-THR of depth-2 polynomial-size threshold circuits would follow.

## 3.5 Estimating Size of Union of Sets in Streaming Model

*Sourav Chakraborty (Indian Statistical Institute – Kolkata, IN)*

**Joint work of** Sourav Chakraborty, Kuldeep Meel, N.V. Vinodchandran

We present a very simple and efficient sampling-based algorithm for estimating the union of sets in the streaming setting. Suppose we have a collection of sets $S_1, \ldots, S_M$ subsets of $T$, arriving one by one in a stream; the sets are not given explicitly to us but rather defined implicitly via the following oracles: for each set, we can know the size of the set, get a uniform sample from the set, and given a point check whether it belongs to the set. The goal is to estimate the size of union of the sets $S_1, \ldots, S_M$.

We present a simple algorithm that estimates the size of the union, upto a $(1 + \epsilon)$ factor, in space complexity and update time complexity $O(\log(M) \log(T)/\epsilon^2)$.

Our algorithm gives the best streaming solutions for various problems like the Klee Measure, Test Coverage Estimation, and DNF Model Counting. Our algorithm provides the first algorithm with linear dependence on the dimension for Klee's measure problem in streaming setting, thereby settling the open problem of Woodruff and Tirthpura (PODS-12).

This work is from a recent paper, with Kuldeep Meel and Vinodchandran, that was accepted to PODS recently.

## 3.6 Lower Bounds for Monotone Arithmetic Circuits Via Communication Complexity

*Arkadev Chattopadhyay (TIFR – Mumbai, IN)*

**Joint work of** Arkadev Chattopadhyay, Rajit Datta, 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** https://doi.org/10.1145/3406325.3451069

Valiant (1980) showed that general arithmetic circuits with negation can be exponentially more powerful than monotone ones. We give the first improvement to this classical result: we construct a family of polynomials $P_n$ in $n$ variables, each of its monomials has non-negative coefficient, such that $P_n$ can be computed by a polynomial-size *depth-three formula* but every monotone circuit computing it has size $2^{\Omega(n^{1/4}/\log(n))}$. Moreover, our result shows an exponential separation of the powers of multilinear and monotone arithmetic circuits for computing a monotone polynomial. As far as we know, no super-polynomial separation was known before our work.

The polynomial $P_n$ embeds the SINK $\circ$ XOR function devised recently by Chattopadhyay, Mande and Sherif (2020) to refute the Log-Approximate-Rank Conjecture in communication complexity. To prove our lower bound for $P_n$, we develop a general connection between corruption of combinatorial rectangles by any function $f \circ$ XOR and corruption of product polynomials by a certain polynomial $P^f$ that is an arithmetic embedding of $f$. This connection should be of independent interest.

Using further ideas from communication complexity, we construct another family of set-multilinear polynomials $f_{n,m}$ such that both $F_{n,m} - -\epsilon \cdot f_{n,m}$ and $F_{n,m} + \epsilon \cdot f_{n,m}$ have monotone circuit complexity $2^{\Omega(n/\log(n))}$ if $\epsilon \geq 2^{-\Omega(m)}$ and $F_{n,m} := \prod_{i=1}^{n} \left(x_{i,1} + \cdots + x_{i,m}\right)$, with $m = O(n/\log n)$. The polynomials $f_{n,m}$ have 0/1 coefficients and are in VNP. Proving such lower bounds for monotone circuits has been advocated recently by Hrubeš (2020) as a first step towards proving lower bounds against *general circuits* via his new approach.

## 3.7 Convex influences and a quantitative Gaussian correlation inequality

*Anindya De (University of Pennsylvania – Philadelphia, US)*

**Joint work of** Anindya De, Shivam Nadimpalli, Rocco Servedio
**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** https://doi.org/10.4230/LIPIcs.ITCS.2021.69

The Gaussian correlation inequality (GCI), proven by Royen in 2014, states that any two centrally symmetric convex sets (say $K$ and $L$) in the Gaussian space are positively correlated. We will prove 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 functions. To obtain this inequality, we propose a new approach, based on analysis of Littlewood type polynomials, which gives a recipe to transfer qualitative correlation inequalities into quantitative correlation inequalities. En route, we also give a new notion of influences for convex symmetric sets over the Gaussian space which has many of the properties of influences from Boolean functions over the discrete cube. Much remains to be explored, in particular, about this new notion of influences for convex sets.

## 3.8 Bounded indistinguishability for simple sources

*Yuval Filmus (Technion – Haifa, IL)*

**Joint work of** Yuval Filmus, Akshayaram Srinivasan, Andrej Bogdanov, Avi Kaplan, Krishnamoorthy Dinesh, Yuval Ishai

Bogdanov, Ishai, Viola, and Williamson constructed a pair of $\sqrt{n}$-indistinguishable sources $X, Y$ which OR tells apart.

In contrast, Braverman showed that if $X, Y$ are polylog$(n)$-indistinguishable and $Y$ is the uniform distribution, then $X, Y$ fool all of $\mathrm{AC}^0$.

For which sources $Y$ beside the uniform distribution does a Braverman-style theorem hold?

## 3.9 Circuit Depth Reductions

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

**Joint work of** Alexander Golovnev, Alexander S. Kulikov, Ryan Williams
**Main reference** Alexander Golovnev, Alexander S. Kulikov: "Circuit Depth Reductions", CoRR, Vol. abs/1811.04828, 2018.
**URL** https://arxiv.org/abs/1811.04828

The best known size lower bounds against unrestricted circuits have remained around $3n$ for several decades. Moreover, the only known technique for proving lower bounds in this model, gate elimination, is inherently limited to proving lower bounds of less than $5n$. In this work, we propose a non-gate-elimination approach for obtaining circuit lower bounds, via certain depth-three lower bounds. We prove that every (unbounded-depth) circuit of size s can be expressed as an OR of $2^{s/3.9}$ 16-CNFs. For DeMorgan formulas, the best known size lower bounds have been stuck at around $n^{3-o(1)}$ for decades. Under a plausible hypothesis about probabilistic polynomials, we show that $n^{4-\epsilon}$-size DeMorgan formulas have $2^{n^{1-\Omega(\epsilon)}}$-size depth-3 circuits which are approximate sums of $n^{1-\Omega(\epsilon)}$-degree polynomials over $\mathrm{F}_2$. While these structural results do not immediately lead to new lower bounds, they do suggest new avenues of attack on these longstanding lower bound problems.

Our results complement the classical depth-3 reduction results of Valiant, which show that logarithmic-depth circuits of linear size can be computed by an OR of $2^{\epsilon n} n^{\delta}$-CNFs, and slightly stronger results for series-parallel circuits. It is known that no purely graph-theoretic reduction could yield interesting depth-3 circuits from circuits of super-logarithmic depth. We overcome this limitation (for small-size circuits) by taking into account both the graph-theoretic and functional properties of circuits and formulas.

We show that improvements of the following pseudorandom constructions imply superlinear circuit lower bounds for log-depth circuits via Valiant's reduction: dispersers for varieties, correlation with constant degree polynomials, matrix rigidity, and hardness for depth-3 circuits with constant bottom fan-in. On the other hand, our depth reductions show that even modest improvements of the known constructions give elementary proofs of improved (but still linear) circuit lower bounds.

## 3.10 Unambiguous DNFs from Hex

*Mika Göös (EPFL Lausanne, CH)*

**Joint work of** Mika Göös, Kaspars Balodis, Shalev Ben-David, Siddhartha Jain, Robin Kothari
**Main reference** Shalev Ben-David, Mika Göös, Siddhartha Jain, Robin Kothari: "Unambiguous DNFs from Hex", Electron. Colloquium Comput. Complex., Vol. 28, p. 16, 2021.
**URL** https://eccc.weizmann.ac.il/report/2021/016

We exhibit an unambiguous $k$-DNF formula that requires CNF width $\Omega(k^2)$. As a corollary, we get a near-optimal solution for the Alon-Saks-Seymour problem in graph theory, which asks: How large a gap can there be between the chromatic number of a graph and its bipartite packing number?

## 3.11 Ideal-theoretic Explanation of Capacity-achieving codes

*Prahladh Harsha (TIFR – Mumbai, IN)*

**Joint work of** Siddharth Bhandari, Prahladh Harsha, Mrinal Kumar, Madhu Sudan
**Main reference** Siddharth Bhandari, Prahladh Harsha, Mrinal Kumar, Madhu Sudan: "Ideal-theoretic Explanation of Capacity-achieving Decoding", CoRR, Vol. abs/2103.07930, 2021.
**URL** https://arxiv.org/abs/2103.07930

In this work, we present an abstract framework for some algebraic error-correcting codes with the aim of capturing codes that are list-decodable to capacity, along with their decoding algorithm. In the polynomial ideal framework, a code is specified by some ideals in a polynomial ring, messages are polynomials and their encoding is the residue modulo the ideals. We present an alternate way of viewing this class of codes in terms of linear operators, and show that this alternate view makes their algorithmic list-decodability amenable to analysis. Our framework leads to a new class of codes that we call affine Folded Reed-Solomon codes (which are themselves a special case of the broader class we explore). These codes are common generalizations of the well-studied Folded Reed-Solomon codes and Multiplicity codes, while also capturing the less-studied Additive Folded Reed-Solomon codes as well as a large family of codes that were not previously known/studied.

More significantly our framework also captures the algorithmic list-decodability of the constituent codes. Specifically, we present a unified view of the decoding algorithm for ideal theoretic codes and show that the decodability reduces to the analysis of the distance of some related codes. We show that good bounds on this distance lead to capacity-achieving performance of the underlying code, providing a unifying explanation of known capacity-achieving results. In the specific case of affine Folded Reed-Solomon codes, our framework shows that they are list-decodable up to capacity (for appropriate setting of the parameters), thereby unifying the previous results for Folded Reed-Solomon, Multiplicity and Additive Folded Reed-Solomon codes.

## 3.12 Average-Case Hardness of NP from Exponential Worst-Case Hardness Assumptions

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

**Main reference** Shuichi Hirahara: "Average-Case Hardness of NP from Exponential Worst-Case Hardness Assumptions", Electron. Colloquium Comput. Complex., Vol. 28, p. 58, 2021.
**URL** https://eccc.weizmann.ac.il/report/2021/058

Basing the average-case hardness of NP on the worst-case hardness of NP is a long-standing and central open question in complexity theory, which is known as the question of excluding Heuristica from Impagliazzo's five possible worlds. It has been a long-standing open question to base the average-case hardness of PH on the exponential worst-case hardness of UP, and a large body of research has been devoted to explaining why standard proof techniques fail to resolve the open question.

In this work, we develop new proof techniques and resolve the open question. We prove that if UP is not in DTIME($2^{O(n/\log n)}$), then NP is hard on average. Our proofs are based on the meta-complexity of time-bounded Kolmogorov complexity: We analyze average-case complexity through the lens of worst-case meta-complexity by using several new notions such as universal heuristic scheme and P-computable average-case polynomial-time.

## 3.13 Interactive Error Correcting Codes and the Magical Power of Adaptivity

*Gillat Kol (Princeton University, US)*

Error correcting codes (ECCs) allow for reliable data transfer over noisy channels. They had a profound impact on both the practical and theoretical communities, and over the last decades were one of the main enablers of the digital revolution. However, modern communication systems often go beyond one-way data transfer and instead operate over many rounds of interactive communication between different parties. Interactive ECCs are a generalization of classical ECCs, and they allow the conversion of any interactive communication protocol to a noise resilient one. In this talk we will focus on a modeling decision that is unique to interactive ECCs, namely, the order of communication, and see its impact on the existence of good interactive ECCs.

## 3.14 Network Coding Conjecture and Data Structure Lower Bounds

*Michal Koucký (Charles University – Prague, CZ)*

**Joint work of** Pavel Dvorák, Michal Koucký, Karel Král, Veronika Slívová
**Main reference** Pavel Dvorák, Michal Koucký, Karel Král, Veronika Slívová: "Data Structures Lower Bounds and Popular Conjectures", CoRR, Vol. abs/2102.09294, 2021.
**URL** https://arxiv.org/abs/2102.09294

In this talk I will present our new results on the relative power of several conjectures that attracted recently a lot of interest. We establish a connection between the Network Coding Conjecture of Li and Li (2010) and several data structure like problems such as non-adaptive function inversion of Hellman (1980) and the well studied problem of polynomial evaluation and interpolation. In turn these data structure problems imply super-linear circuit lower bounds for explicit functions such as integer sorting and multi-point polynomial evaluation.

## 3.15 Complexity of Linear Operators

*Alexander S. Kulikov (Steklov Institute – St. Petersburg, RU)*

**Joint work of** Alexander S. Kulikov, Ivan Mikhailin, Andrey Mokhov, Vladimir V. Podolskii
**Main reference** Alexander S. Kulikov, Ivan Mikhailin, Andrey Mokhov, Vladimir V. Podolskii: "Complexity of Linear Operators", in Proc. of the 30th International Symposium on Algorithms and Computation, ISAAC 2019, December 8-11, 2019, Shanghai University of Finance and Economics, Shanghai, China, LIPIcs, Vol. 149, pp. 17:1–17:12, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2019.
**URL** https://doi.org/10.4230/LIPIcs.ISAAC.2019.17

Let $A$ be an $n \times n$ 0/1-matrix with $z$ zeroes and $u$ ones and $x$ be an $n$-dimensional vector of formal variables over a semigroup $(S, \circ)$. How many semigroup operations are required to compute the linear operator $Ax$? As we observe in this paper, this problem contains as a special case the well-known range queries problem and has a rich variety of applications in such areas as graph algorithms, functional programming, circuit complexity, and others. It is easy to compute $Ax$ using $O(u)$ semigroup operations. The main question studied in this paper is: can $Ax$ be computed using $O(z)$ semigroup operations? We prove that in general this is not possible: there exists a matrix $A$ with exactly two zeroes in every row (hence $z = 2n$) whose complexity is $\Theta(n\alpha(n))$ where $\alpha(n)$ is the inverse Ackermann function. However, for the case when the semigroup is commutative, we give a constructive proof of an $O(z)$ upper bound. This implies that in commutative settings, complements of sparse matrices can be processed as efficiently as sparse matrices (though the corresponding algorithms are more involved). Note that this covers the cases of Boolean and tropical semirings that have numerous applications, e. g., in graph theory. As a simple application of the presented linear-size construction, we show how to multiply two $n \times n$ matrices over an arbitrary semiring in $O(n^2)$ time if one of these matrices is a 0/1-matrix with $O(n)$ zeroes (i. e., a complement of a sparse matrix).

## 3.16 Amortized Circuit Complexity, Formal Complexity Measures, and Catalytic Algorithms

*Robert Robere (McGill University – Montreal, CA)*

**Joint work of** Robert Robere, Jeroen Zuiddam
**Main reference** Robert Robere, Jeroen Zuiddam: "Amortized Circuit Complexity, Formal Complexity Measures, and Catalytic Algorithms", Electron. Colloquium Comput. Complex., Vol. 28, p. 35, 2021.
**URL** https://eccc.weizmann.ac.il/report/2021/035

Some of the central questions in complexity theory address the amortized complexity of computation (also sometimes known as direct sum problems). While these questions appear in many contexts, they are all variants of the following:

Is the best way of computing $T$ many times in parallel simply to compute $T$ independently each time, or, can we achieve an economy of scale and compute all copies of $T$ more efficiently on average?

In this talk, we discuss some recent results studying the amortized circuit complexity of computing boolean functions in various circuit models. The amortized circuit complexity of a Boolean function $f$ is defined to be the limit, as $m$ tends to infinity, of the circuit complexity of computing $f$ on the same input $m$ times, divided by $m$. We prove a new duality theorem for amortized circuit complexity in any circuit model, showing that the amortized circuit complexity of computing $f$ is equal to the best lower bound achieved by any "formal complexity measure" applied to $f$. This new duality theorem is inspired by, and closely related to, Strassen's duality theorem for semirings, which has been fruitfully used to characterize the matrix multiplication exponent, the Shannon Capacity of graphs, as well as other important parameters in combinatorics and complexity. We discuss how our new duality theorem can be used to give alternative proofs of upper bounds on amortized circuit complexity, and also the close relationship between amortized circuit complexity and catalytic algorithms, in which an algorithm is provided with an extra input of advice bits that it is free to use, as long as it outputs a new copy of the extra advice on termination.

## 3.17 Reconstruction Algorithms for Low-Rank Tensors

*Shubhangi Saraf (Rutgers University – Piscataway, US)*

**Joint work of** Vishwas Bhargava, Shubhangi Saraf, Ilya Volkovich
**Main reference** Vishwas Bhargava, Shubhangi Saraf, Ilya Volkovich: "Reconstruction Algorithms for Low-Rank Tensors and Depth-3 Multilinear Circuits", Electron. Colloquium Comput. Complex., Vol. 28, p. 45, 2021.
**URL** https://eccc.weizmann.ac.il/report/2021/045

In this talk we will discuss new and efficient black-box reconstruction algorithms for some classes of depth-3 arithmetic circuits. As a consequence, we will show how to obtain the first randomized polynomial-time algorithm for computing the tensor rank and for finding the optimal tensor decomposition as a sum of rank-one tensors when then input is a constant-rank tensor.

## 3.18 A Lower Bound on Determinantal Complexity

*Ben Lee Volk (University of Texas – Austin, US)*

**Joint work of** Mrinal Kumar, Ben Lee Volk
**Main reference** Mrinal Kumar, Ben Lee Volk: "A Lower Bound on Determinantal Complexity", Electron. Colloquium Comput. Complex., Vol. 27, p. 129, 2020.
**URL** https://eccc.weizmann.ac.il/report/2020/129

The determinantal complexity of a polynomial $f$ is the minimal integer $m$ such that there exists an $m \times m$ matrix $M$ of linear functions such that $f(x) = \det(M(x))$. This is an important measure in algebraic complexity which is related to circuit and formula complexity. I will show a proof of a lower bound of $1.5n$ on the determinantal complexity of an explicit $n$-variate polynomial. This is the strongest lower bound known as a function of the number of variables. I will also talk about possible ways of extending this result to a super-linear lower bound.

## 3.19 Toward Solving LPs in Matrix-Multiplication Time

*Omri Weinstein (Columbia University – New York, US)*

**Joint work of** Shunhua Jiang, Zhao Song, Omri Weinstein, Hengjie Zhang
**Main reference** Shunhua Jiang, Zhao Song, Omri Weinstein, Hengjie Zhang: "Faster Dynamic Matrix Inverse for Faster LPs", CoRR, Vol. abs/2004.07470, 2020.
**URL** https://arxiv.org/abs/2004.07470

Interior-point methods (IPMs) make a clever use of second-order local search (Newton steps) to reduce a convex optimization problem to a dynamic sequence of *slowly-changing linear systems*. The past three or so years have witnessed the dramatic potential of dynamic data structures in reducing the cost-per-iteration of IPMs, leading to many breakthroughs on decade-old problems in TCS (e. g., solving LPs and Empirical Risk Minimization in *close* to matrix-multiplication time ($\sim n^{w+1/18}$), and near-linear time bipartite matching). I will give a (short) high-level overview of this framework.

## 3.20 Slicing the Hypercube is Not Easy

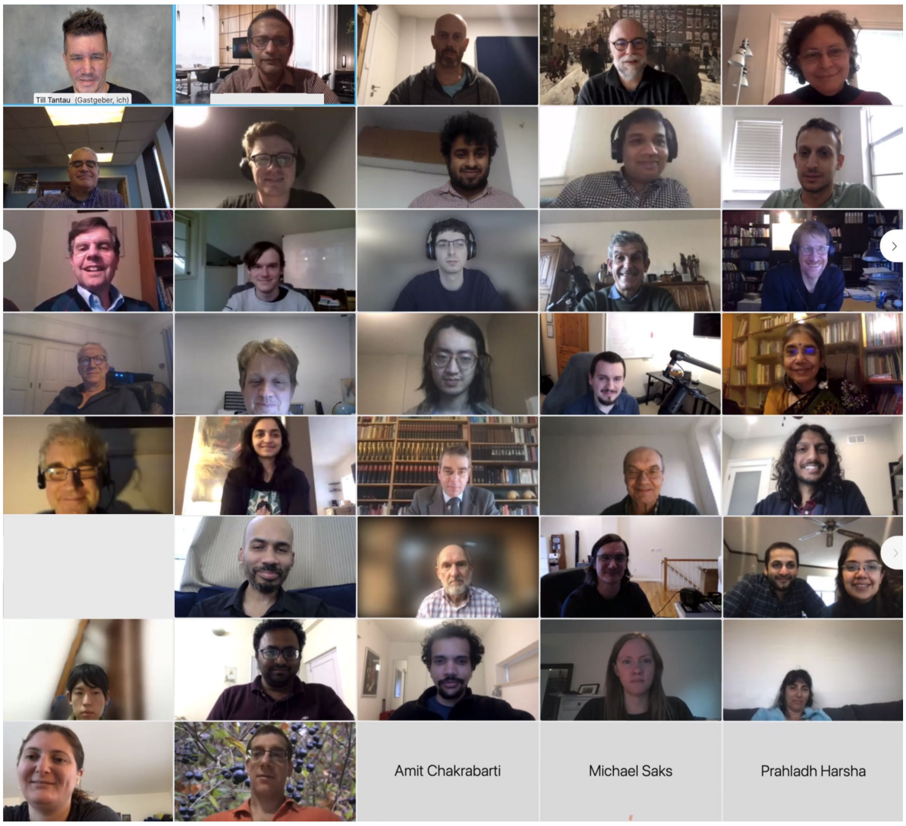
*Amir Yehudayoff (Technion – Haifa, IL)*

**Joint work of** Gal Yehuda, Amir Yehudayoff
**Main reference** Gal Yehuda, Amir Yehudayoff: "Slicing the hypercube is not easy", CoRR, Vol. abs/2102.05536, 2021.
**URL** https://arxiv.org/abs/2102.05536

We prove that at least order $n^{0.57}$ hyperplanes are needed to slice all edges of the n-dimensional hypercube. We provide a couple of applications: lower bounds on the computational complexity of parity, and a lower bound on the cover number of the hypercube by skew hyperplanes.

## Remote Participants

- Eric Allender
Rutgers University – Piscataway, US
- Max Bannach
Universität zu Lübeck, DE
- Olaf Beyersdorff
Universität Jena, DE
- Harry Buhrman
CWI – Amsterdam, NL
- 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
- Lijie Chen
MIT – Cambridge, US
- Anindya De
University of Pennsylvania – Philadelphia, US
- Yuval Filmus
Technion – Haifa, IL
- Lance Fortnow
Illinois Institute of Technology, US
- Anna Gál
University of Texas – Austin, US
- Mika Göös
EPFL Lausanne, CH
- Alexander Golovnev
Georgetown University – Washington, DC, US
- Rohit Gurjar
Indian Institute of Technology – Mumbai, IN
- Kristoffer Arnsfelt Hansen
Aarhus University, DK
- Prahladh Harsha
TIFR – Mumbai, IN
- Johan Hastad
KTH Royal Institute of Technology – Stockholm, SE
- Shuichi Hirahara
National Institute of Informatics – Tokyo, JP
- Rahul Ilango
MIT – Cambridge, US
- Stacey Jeffery
CWI – Amsterdam, NL
- Gillat Kol
Princeton University, US
- Swastik Kopparty
Rutgers University – Piscataway, US
- Michal Koucký
Charles University – Prague, CZ
- Alexander S. Kulikov
Steklov Institute – St. Petersburg, RU
- Sophie Laplante
University Paris Diderot, FR
- Nutan Limaye
Indian Institute of Technology – Mumbai, IN
- Meena Mahajan
The Institute of Mathematical Sciences, HBNI – Chennai, IN
- Ian Mertz
University of Toronto, CA
- Jakob Nordström
University of Copenhagen, DK & Lund University, SE
- Ramamohan Paturi
University of California – San Diego, US
- Toniann Pitassi
University of Toronto, CA
- Pavel Pudlák
The Czech Academy of Sciences – Prague, CZ
- Oded Regev
New York University, US
- Rüdiger Reischuk
Universität zu Lübeck, DE
- Robert Robere
McGill University – Montreal, CA
- Michael E. Saks
Rutgers University – Piscataway, US
- Rahul Santhanam
University of Oxford, GB
- Shubhangi Saraf
Rutgers University – Piscataway, US
- Amit Sinhababu
Hochschule Aalen, DE
- Srikanth Srinivasan
Aarhus University, DK
- Amnon Ta-Shma
Tel Aviv University, IL
- Li-Yang Tan
Stanford University, US
- Till Tantau
Universität zu Lübeck, DE
- Thomas Thierauf
Hochschule Aalen, DE
- Jacobo Torán
Universität Ulm, DE
- Virginia Vassilevska Williams
MIT – Cambridge, US
- Ben Lee Volk
University of Texas – Austin, US
- Omri Weinstein
Columbia University – New York, US
- Ryan Williams
MIT – Cambridge, US
- Amir Yehudayoff
Technion – Haifa, IL


Till Tantau (Gastgeber, ich)
Amit Chakrabarti
Michael Saks
Prahladh Harsha