Report from Dagstuhl Seminar 17121

Computational Complexity of Discrete Problems

Edited by

Anna Gál[1], Michal Koucký[2], Oded Regev[3], and Till Tantau[4]

1 **University of Texas – Austin, US,** panni@cs.utexas.edu
2 **Charles University – Prague, CZ,** koucky@iuuk.mff.cuni.cz
3 **New York University, US**
4 **Universität zu Lübeck, DE,** tantau@tcs.uni-luebeck.de

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 17121 "Computational Complexity of Discrete Problems". The first section gives an overview of the topics covered and the organization of the meeting. Section 2 lists the talks given in alphabetical order. The last section contains the abstracts of the talks.

Seminar March 19–24, 2017 – http://www.dagstuhl.de/17121
1998 ACM Subject Classification Theory of Computing
Keywords and phrases Computational Complexity
Digital Object Identifier 10.4230/DagRep.7.3.45
Edited in cooperation with Bruno Loff

1 Executive Summary

Anna Gál (University of Texas – Austin, US)
Michal Koucký (Charles University – Prague, CZ)
Oded Regev (Courant Institute – New York, US)
Till Tantau (Universität Lübeck – DE)

Introduction and goals

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 and becomes even more important with the use of computers becoming part of everyday life. 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 class of practical problems where algorithms with polynomial running time (e.g. cubic or even quadratic time) are known, but it would be important to establish whether these running times are best possible, or to what extent they can be improved.

These fundamental questions motivate developments in various areas from algorithm design to circuit complexity, communication complexity and coding theory. During this Dagstuhl Seminar, we discussed some of the most exciting recent developments in those areas related to computational complexity.

Computational Complexity of Discrete Problems, *Dagstuhl Reports*, Vol. 7, Issue 3, pp. 45–69
Editors: Anna Gál, Michal Koucký, Oded Regev, and Till Tantau

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

The seminar "Computational Complexity of Discrete Problems" has evolved out of the series of seminars entitled "Complexity of Boolean Functions," a topic that has been covered at Dagstuhl on a regular basis since the foundation of this research center. An important feature of the current research in computational complexity is the integration of ideas from different subareas of computational complexity and from other fields in computer science and mathematics. We have aimed to attract researchers from various subareas connected to core questions in boolean function complexity and foster further fruitful interactions.

2 Table of Contents

3 Organization of the seminar

40 researches from around the world participated in the seminar including a substantial number of young researchers. Each day we had two to three *regular* talks in the morning and in the afternoon. In addition to that we dispersed in the schedule a set of short talks that we called *talks to talk about*. The regular talks allowed participants to explain in depth various problems and results. The short talks were meant for posing open problems and for brief announcements. They were usually scheduled before the meal time so that participants could discuss the problems over the meal. This schedule proved quite successful as it allowed for plenty of time for discussions in impromptu groups in the afternoon as well as it gave essentially everyone interested the opportunity to speak.

3.1 Topics covered by the seminar

The talks of the workshop fit into several subareas of computational complexity. We summarize the talks next. Detailed abstracts of the talks can be found at the end of this report.

3.1.1 Circuit complexity

Proving lower bounds on the size of circuits and formulas computing specific functions is one of the main goals of computational complexity. However, proving such lower bounds seems exceedingly hard. Avishay Tal presented a new method of amplifying formula size lower bounds from non-approximability lower bounds. As an application he showed the currently best formula size lower bound.

The difficulties of proving lower bounds can be sometimes formally analyzed. In past several *barriers* for proving strong lower bounds have been identified. The most intriguing one is the Natural Proof framework of Razborov and Rudich for Boolean circuit lower bounds. Ben Lee Volk presented a Natural Proof framework for proving *algebraic* circuit lower bounds. He explained its connection to succinct hitting sets for algebraic circuits.

Many circuit lower bounds we currently have fit into the Natural Proof framework, e.g., lower bounds for $\mathrm{AC}^0[p]$ circuits. In a surprising twist, Valentine Kabanets used Natural Proof Properties from these proofs to construct new learning algorithms for $\mathrm{AC}^0[p]$.

One of the tools to reason about circuits is provided by the logical framework of descriptive complexity. Heribert Vollmer developed a model-theoretic characterization of the counting class $\#\mathrm{AC}^0$ based on counting winning strategies in certain games.

Sasha Golovnev asked about devising new circuit lower bound techniques other than gate-elimination as the gate-elimination technique implies better algorithms for circuit-SAT.

The Minimum Circuit Size Problem is a particular computational problem with inputs being truth-tables of functions and the goal being to determine the size of the smallest circuit computing the function. This problem is not know to be in P nor NP-hard, it is a candidate NP-intermediate problem. Rahul Santhanam discussed the unusual complexity properties of the Minimum Circuit Size Problem and its relevance to circuit lower bounds.

Eric Allender presented further new hardness results for the Kolmogorov-complexity variant of the Minimum Circuit Size Problem and its relationship to the circuit variant.

3.1.2 Proof complexity

Proof complexity aims at separating complexity classes by proving lower bounds on various proof systems. It also helps in understanding the running time of various satisfiability algorithms and heuristics. Meena Mahajan defined a new cutting plane based proof system for refuting Quantified Boolean Formulas (QBF) and exhibited exponential lower bounds for this proof system.

Johan Håstad used new random restrictions for Tseitin contradictions to obtain exponential lower bounds for bounded-depth Frege systems.

Jakob Nordström presented a technique to prove exponential lower bounds for polynomial calculus for the functional pigeonhole principle with consequences for running time of a certain class of SAT-solvers.

Related to the barriers for proving lower bounds one may naturally ask what kind of mathematics is necessary to prove lower bounds or *upper* bounds. Igor Carboni Oliveira exhibited existence of languages in P for which one cannot prove within Cook's theory PV that they have running time $O(n^k)$.

Pavel Hrubeš posed a communication complexity open problem with consequences for cutting plane lower bounds.

3.1.3 Pseudorandomness and derandomization

Pseudorandom generators are useful for replacing truly random strings by pseudorandomly chosen ones in running randomized algorithms. Pseudorandom generators should have small support, be easy to compute and algorithms should behave on them in approximately the same way as on random strings chosen truly at random.

Rohit Gurjar used geometric view to construct pseudorandom generators for weight assignments for graphs and matroids that isolate a perfect matching in bi-partite graphs and a common bases of two matroids. This puts the two problems in uniform quasi-NC.

Dieter van Melkebeek presented a new simple pseudorandom generator with seed length $O(\log^{3/2} n)$ to isolate a shortest path in a directed graph with consequences for non-deterministic and unambiguous log-space.

Randomness extraction is a process of purifying random strings from biased sources of random strings. Gil Cohen surveyed recent developments in multi-source extractors and presented the key ideas for a simplified construction of such extractors.

3.1.4 Codes and communication complexity

Error correcting codes have multitude of applications in computational complexity and beyond. Obtaining good codes of various properties with efficient encoding and decoding is of primal interest for theory and applications. Swastik Kopparty described list-decoding algorithm for lifted Reed-Solomon codes.

Motivated by codes for distributed storage, Shachar Lovett presented results on the Birkhoff polytope graph with applications to the alphabet size of codes for the distributed storage.

A special class of errors for which one can use particular codes are erasures. If the data are not protected by the code but we have several noisy copies of the data we may still attempt to reconstruct the data. Anindya De discussed the number of samples one needs to reconstruct a string x from its noisy version where the noise erases coordinates of x.

A super-efficient decoding algorithm does not need to read the whole encoded string of data to reliably recover a single bit of the original data. This is called local decoding, and related to it is the local correction. It is a major open question to construct good locally-decodable and locally-correctable codes with constant number of queries. Or Meir exhibit

new unexpected constructions of locally-correctable codes in the regime of non-constant number of queries.

In the realm of communication complexity where we want to optimize the number of bits transmitted between parties jointly computing some function, Harry Buhrman presented an intriguing concept of clean communication complexity and posed open problems related to that.

Motivated by proving computational lower bounds, Or Meir presented open questions for direct sum of relationships, and Bruno Loff discussed asymmetric direct-sum theorems.

3.1.5 Fine-grained complexity

Recently a new area emerged in computational complexity so called *fine-grained complexity*. It aims to understand the complexity of various problems at very fine-tuned level with direct consequences for practice. Mohan Paturi presented the Least-Weight Subsequence Problem and its relationship to the fine-grained complexity of various other problems.

Motivated by practical applications, Matthias Krause introduced a new stream cipher with provable time-memory trade-off's and better internal state complexity than known ciphers.

Pavel Dvořák summarized results and open problems on the fixed-parameter tractability of Steiner tree problem.

3.1.6 Other models

Several participants addressed fundamental properties of boolean functions. Shachar Lovett asked questions about sparsity of polynomial representation of boolean functions, and Sourav Chakraborty posed a question regarding lower bounding the Fourier min-entropy of a boolean function in terms of its degree.

Prahladh Harsha presented problems regarding the decay of the value in multi-player parallel repetition games, a direct generalization of the celebrated *Parallel Repetition Theorem*.

Lance Fortnow introduced a new notion of *compression complexity* which addresses a question dual to Kolmogorov complexity namely, how complex has to be a string compression algorithm.

Rüdiger Reischuk disproved a conjecture about a particular learning algorithm for alternating finite automata and presented an alternative algorithm with required properties for the same problem.

Nikhil Bansal presented an elegant algorithm to solve the Subset Sum Problem in polynomial *space*.

Shay Moran talked about the classical problem of 20-questions when we limit the complexity of the allowed questions.

Mike Saks presented open questions regarding the randomized complexity of the on-line labeling problem.

3.2 Conclusion

Understanding the computational complexity of various problems is the primary goal of theory of computing. Over the years we are witnessing a continuous stream of new ideas and techniques in various areas of complexity for example, in communication complexity, arithmetic circuit complexity and derandomization. This seminar gave us the opportunity

to discuss some of these exciting developments and there was a general consensus among the participant that the meeting was helpful in facilitating new ideas and collaborations for further research.

We like to thank the staff at Dagstuhl who – as usual – provided a marvelous surrounding to make this a successful meeting with ample space for undisturbed interactions between the participants.

4 Overview of Talks

4.1 New Insights on the (Non)-Hardness of Circuit Minimization and Related Problems

Eric Allender (Rutgers University, US)

Joint work of Eric Allender, Shuichi Hirahara
Main reference E. Allender, S. Hirahara, "New Insights on the (Non)-Hardness of Circuit Minimization and Related Problems", ECCC Technical Report TR17-073, 2017.
URL https://eccc.weizmann.ac.il/report/2017/073/

The Minimum Circuit Size Problem (MCSP) and a related problem (MKTP) that deals with time-bounded Kolmogorov complexity are prominent candidates for NP-intermediate status. We show that, under very modest cryptographic assumptions (such as the existence of one-way functions), the problem of approximating the minimum circuit size (or time-bounded Kolmogorov complexity) within a factor of $n^{1-o(1)}$ is indeed NP-intermediate. To the best of our knowledge, these problems are the first natural NP-intermediate problems under the existence of an arbitrary one-way function.

We also prove that MKTP is hard for the complexity class DET under non-uniform NC^0 reductions. This is surprising, since prior work on MCSP and MKTP had highlighted weaknesses of "local" reductions (such as NC^0 reductions). We exploit this local reduction to obtain several new consequences:

- MKTP is not in $AC^0[p]$.
- Circuit size lower bounds are equivalent to hardness of a relativized version $MKTP^A$ of MKTP under a class of uniform AC^0 reductions, for a large class of sets A.
- Hardness of $MCSP^A$ implies hardness of $MKTP^A$ for a wide class of sets A. This is the first result directly relating the complexity of $MCSP^A$ and $MKTP^A$, for any A.

4.2 Clean quantum and classical communication protocols

Harry Buhrman (CWI – Amsterdam, NL)

Joint work of Harry Buhrman, Matthias Christandl, Christopher Perry, Jeroen Zuiddam
Main reference H. Buhrman, M. Christandl, C. Perry, J. Zuiddam, "Clean quantum and classical communication protocols", arXiv:1605.07948v3 [quant-ph], 2016.
URL https://arxiv.org/abs/1605.07948

By how much must the communication complexity of a function increase if we demand that the parties not only correctly compute the function but also return all registers (other

than the one containing the answer) to their initial states at the end of the communication protocol? Protocols that achieve this are referred to as *clean* and the associated cost as the *clean communication complexity*. Here we present clean protocols for calculating the Inner Product of two n-bit strings, showing that (in the absence of pre-shared entanglement) at most $n + 3$ qubits or $n + O(\sqrt{n})$ bits of communication are required. The quantum protocol provides inspiration for obtaining the optimal method to implement distributed $CNOT$ gates in parallel whilst minimizing the amount of quantum communication. For more general functions, we show that nearly all Boolean functions require close to $2n$ bits of classical communication to compute and close to n qubits if the parties have access to pre-shared entanglement. Both of these values are maximal for their respective paradigms.

4.3 Unprovability of circuit upper bounds in Cook's theory PV

Igor Carboni Oliveira (Charles University – Prague, CZ)

Joint work of Igor Carboni Oliveira, Jan Krajíček
Main reference J. Krajicek, I. C. Oliveira, "Unprovability of circuit upper bounds in Cook's theory PV", arXiv:1605.00263v3 [math.LO], 2016.
URL https://arxiv.org/abs/1605.00263

We establish unconditionally that for every integer $k > 1$ there is a language L in P such that it is consistent with Cook's theory PV that L is not in SIZE(n^k). Our argument is non-constructive and does not provide an explicit description of this language.

4.4 Towards the FEI conjecture

Sourav Chakraborty (CWI – Amsterdam, NL)

FEI conjecture is a well-known conjecture. The conjecture states that the Fourier entropy is less than a constant multiple of the average sensitivity. A weakening of the conjecture states that the min-entropy is less than approximate degree of the function. A even more weakening is that if g is a 1/3- approximating polynomial of a Boolean function f, then at least on the the coefficients of g has to be bigger than $1/2^d$, where d is the degree of g.

4.5 Recent advances in randomness extractors and their applications

Gil Cohen (Princeton University, US)

A randomness extractor is a function that "extracts" or "purifies" the randomness of a defective source of randomness. Randomness extractors have applications in abundance and unexpected connections to error-correcting codes, expander graphs and pseudorandom generators. In this talk we survey recent developments in randomness extractors theory

and give a simplified, weaker, construction of multi-source extractors so as to present the underlying ideas.

4.6 New results in trace reconstruction

Anindya De (Northwestern University – Evanston, US)

Joint work of Anindya De, Ryan O'Donnell, Rocco Servedio
Main reference A. De, R. O'Donnell, R. Servedio, "Optimal mean-based algorithms for trace reconstruction", arXiv:1612.03148v1 [cs.CC], 2016.
URL https://arxiv.org/abs/1612.03148

There is an unknown n-bit string x. A "trace" is a random substring of x formed by deleting each bit with probability (say) 1/2. Suppose an algorithm has access to independent traces of x. How many does it need to reconstruct x? The previous best method needed about $\exp(n^{1/2})$ traces. We give a simple "mean-based" algorithm that uses about $\exp(n^{1/3})$ traces (and time). We also show that any algorithm working in the restricted "mean-based" framework requires $\exp(n^{1/3})$ traces. The main tool in our work is elementary complex analysis.

4.7 Compression Complexity

Lance Fortnow (Georgia Institute of Technology – Atlanta, US)

Joint work of Lance Fortnow, Stephen Fenner
Main reference A. Fenner, L. Fortnow, "Compression Complexity", arXiv:1702.04779v1 [cs.CC], 2017.
URL https://arxiv.org/abs/1702.04779

The Kolmogorov complexity of x, denoted $C(x)$, is the length of the shortest program that generates x. For such a simple definition, Kolmogorov complexity has a rich and deep theory, as well as applications to a wide variety of topics including learning theory, complexity lower bounds and SAT algorithms.

Kolmogorov complexity typically focuses on decompression, going from the compressed program to the original string. This paper develops a dual notion of compression, the mapping from a string to its compressed version. Typical lossless compression algorithms such as Lempel-Ziv or Huffman Encoding always produce a string that will decompress to the original. We define a general compression concept based on this observation.

For every m, we exhibit a single compression algorithm q of length about m which for n and strings x of length $n \geq m$, the output of q will have length within $n - m + O(1)$ bits of $C(x)$. We also show this bound is tight in a strong way, for every $n \geq m$ there is an x of length n with $C(x)$ about m such that no compression program of size slightly less than m can compress x at all. We also consider a polynomial time-bounded version of compression complexity and show that similar results for this version would rule out cryptographic one-way functions.

4.8 Non-gate-elimination circuit lower bounds

Alexander Golovnev (New York University, US)

Joint work of Alexander Golovnev, Edward A. Hirsch, Alexander Knop, Alexander S. Kulikov
Main reference A. Golovnev, E. A. Hirsch, A. Knop, A. S. Kulikov, "On the Limits of Gate Elimination", in Proc. of the 41st Int'l Symp. on Mathematical Foundations of Computer Science (MFCS 2016), LIPIcs, Vol. 58, pp. 46:1–46:13, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2016.
URL http://dx.doi.org/10.4230/LIPIcs.MFCS.2016.46

We study lower bounds in the following computational model: Boolean circuits where each gate has fan-in two, and there are no restrictions on the fan-out or depth of the circuit. The circuit size of a Boolean function f is defined as the minimal number of internal gates (i.e., non-input gates) in a circuit computing f. It is easy to show by counting that almost all Boolean functions have exponential circuit size, however no functions of high circuit complexity are known to lie in **NP**.

Essentially, the only known method of proving lower bounds in this model is gate elimination. The best known lower bound is slightly greater than $3n$. It is shown that the currently known gate elimination techniques cannot prove a lower bound of cn for a small explicit constant c. (c here depends on the exact definition of gate elimination, and for most applications can be thought of as small as 5 or 10.)

One of the few examples of lower bounds in this model which does not use gate elimination is the work of Chashkin [2]. He proves a lower bound of $2n - o(n)$ on the complexity of the parity-check matrix of Hamming codes. A classical example of a lower bound which does not use gate elimination is a lower bound of Blum and Seysen [1] who show that an optimal circuit computing AND and OR must have two separate trees computing outputs (which also gives a lower bound of $2n - 2$). Melanich [3] proved a similar property and a lower bound of $2n - o(n)$ for a function whose outputs compute products of specific subsets of inputs.

Question Is it possible to extend the ideas used in non-gate-elimination proofs to get stronger lower bounds?

References

1 Norbert Blum and Martin Seysen. Characterization of all optimal networks for a simultaneous computation of AND and NOR. *Acta informatica*, 21(2):171–181, 1984.
2 Aleksandr V. Chashkin. On the complexity of Boolean matrices, graphs and their corresponding Boolean functions. *Diskretnaya matematika*, 6(2):43–73, 1994.
3 Olga Melanich. Personal communication, 2012.

4.9 Derandomizing Isolation Lemma: A geometric approach

Rohit Gurjar (Tel Aviv University, IL)

Joint work of Rohit Gurjar, Stephen Fenner, Thomas Thierauf
Main reference S. Fenner, R. Gurjar, T. Thierauf, "Bipartite perfect matching is in quasi-NC", in Proc. of the 48th Annual ACM SIGACT Symp. on Theory of Computing (STOC 2016), pp. 754–763, ACM, 2016.
URL http://doi.acm.org/10.1145/2897518.2897564

We present a geometric approach towards derandomizing the Isolation lemma for a given family, i.e., deterministically constructing a weight assingnment which ensures a unique

minimum weight set in the family. The idea is to work with a polytope corresponding to the family of sets. In this talk, we present the approach in terms of general polytopes and describe a sufficient condition on the polytope for this approach to work. The approach gives a quasi-polynomially bounded weight assignment. Finally, we show that two specific families – perfect matchings in bipartite graphs and common base sets of two matroids – satisfy the required condition and thus, we get an isolating weight assignment for these cases. This also puts the two problems in quasi-NC.

4.10 Multiplayer parallel repetition for expander games

Prahladh Harsha (TIFR – Mumbai, IN)

Joint work of Irit Dinur, Prahladh Harsha, Rakesh Venkat, Henry Yuen
Main reference I. Dinur, P. Harsha, R. Venkat, H. Yuen, "Multiplayer parallel repetition for expander games", arXiv:1610.08349v2 [cs.CC], 2016.
URL https://arxiv.org/abs/1610.08349

We investigate the value of parallel repetition of one-round games with any number of players $k \geq 2$. It has been an open question whether an analogue of Raz's Parallel Repetition Theorem holds for games with more than two players, i.e., whether the value of the repeated game decays exponentially with the number of repetitions. Verbitsky has shown, via a reduction to the density Hales-Jewett theorem, that the value of the repeated game must approach zero, as the number of repetitions increases. However, the rate of decay obtained in this way is extremely slow, and it is an open question whether the true rate is exponential as is the case for all two-player games.

Exponential decay bounds are known for several special cases of multi-player games, e.g., free games and anchored games. In this work, we identify a certain expansion property of the base game and show all games with this property satisfy an exponential decay parallel repetition bound. Free games and anchored games satisfy this expansion property, and thus our parallel repetition theorem reproduces all earlier exponential-decay bounds for multiplayer games. More generally, our parallel repetition bound applies to all multiplayer games that are connected in a certain sense.

We also describe a very simple game, called the GHZ game, that does not satisfy this connectivity property, and for which we do not know an exponential decay bound. We suspect that progress on bounding the value of this the parallel repetition of the GHZ game will lead to further progress on the general question.

4.11 A Generalized Method for Resolution and Polynomial Calculus Lower Bounds

Jakob Nordström (KTH Royal Institute of Technology – Stockholm, SE)

Joint work of Massimo Lauria, Mladen Miksa and Jakob Nordström

We study the problem of certifying unsatisfiability of formulas in propositional logic. For proof systems such as resolution and polynomial calculus it is known that if the clause-

variable incidence graph of a CNF formula is an expander, then proving that this formula is unsatisfiable is hard. We further develop techniques in [Alekhnovich and Razborov '03] to show that if one can "cluster" clauses and variables in a way that "respects the structure" of the formula in a certain sense, then it is sufficient that the incidence graph of this clustered version is an expander. We also give a unified view of resolution and polynomial calculus lower bounds in terms of a 2-player game played on this graph, where the difference between resolution and polynomial calculus is just in which player has to move first.

As a corollary, we prove that the functional pigeonhole principle (FPHP) formulas are hard for polynomial calculus, answering an open question in [Razborov '02]. This result can in turn be used to construct k-colouring instances where the standard encoding requires linear degree, and hence exponential size, for polynomial calculus. This implies a linear degree lower bound for any algorithms based on Gröbner bases, as well as for the algorithm studied in a sequence of papers [De Loera et al. '08, '09, '11, '15] based on Hilbert's Nullstellensatz proofs for a slightly different encoding, thus resolving an open problem mentioned, e.g., in [De Loera et al. '09] and [Li et al. '16].

4.12 On small-depth Frege proofs for Tseitin for grids

Johan Håstad (KTH Royal Institute of Technology – Stockholm, SE)

We prove that a depth-d Frege refutation of the Tseitin contradiction on the grid requires size $\exp(\Omega(n^{1/60(d+1)}))$. We conclude that polynomial size Frege refutations of the Tseitin contradiction must use formulas of depth $\Omega(\frac{\log n}{\log\log n})$.

4.13 The Uncanny Usefulness of Constructive Proofs of Pseudorandomness

Valentine Kabanets (Simon Fraser University – Burnaby, CA)

Joint work of Marco L. Carmosino, Russell Impagliazzo, Valentine Kabanets, Antonina Kolokolova
Main reference M. L. Carmosino, R. Impagliazzo, V. Kabanets, A. Kolokolova, "Learning Algorithms from Natural Proofs", in Proc. of the 31st Conference on Computational Complexity (CCC 2016), LIPIcs, Vol. 50, pp. 10:1–10:24, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2016.
URL http://dx.doi.org/10.4230/LIPIcs.CCC.2016.10

Explicit constructions of pseudorandom objects (e.g., pseudorandom generators, expander graphs, or boolean functions of large circuit complexity) often come with very constructive proofs of existence. For example,

(1) the Nisan-Wigderson (NW) generator based on an assumed "hard" function f (of large circuit complexity) has the constructive analysis: There is an efficient uniform reduction (with oracle access to f) taking an algorithm "breaking" the generator into a small circuit for f;

(2) the Natural Proofs framework of Razborov and Rudich argues that most circuit lower bound proofs come with an efficiently testable property that distinguishes "easy" functions (with small circuit complexity) from random functions;

I'll talk about some recent applications of such constructive proofs. In particular, I'll show that properties (1) + (2) yield an efficient (agnostic) learning query algorithm for every sufficiently strong circuit class that has a natural proof of circuit lower bounds. As an application, the class $AC^0[p]$, for any prime p, is (agnostically) learnable in quasi-polynomial time. (Previously, only the case of AC^0 was known by the results of Linial, Mansour, and Nisan.) [joint with Carmosino, Impagliazzo, and Kolokolova.]

4.14 List-decoding lifted codes

Swastik Kopparty (Rutgers University – Piscataway, US)

Joint work of Alan Guo and Swastik Kopparty
Main reference A. Guo, S. Kopparty, "List-Decoding Algorithms for Lifted Codes", IEEE Trans. Information Theory 62(5):2719–2725, 2016.
URL http://dx.doi.org/10.1109/TIT.2016.2538766

Lifted Reed-Solomon codes are a natural generalization of multivariate polynomial codes. In this talk, I will describe list-decoding algorithms for these codes. They are based on a technical theorem that says that m-variate functions over F_q which are codewords of the lifted Reed-Solomon code, despite being high-degree as m-variate functions, are low degree when viewed as univariate functions over the big field F_{q^m}

4.15 On Stream Ciphers with provable Beyond-the-Birthday-Bound Resistance against Time-memory-Data Tradeoff Attacks

Matthias Krause (Universität Mannheim, DE)

Joint work of Matthias Hamann, Matthias Krause, Willi Meier
Main reference M. Hamann, M. Krause, W. Meier, "LIZARD – A Lightweight Stream Cipher for Power-constrained Devices", IACR Transactions on Symmetric Cryptology, 2017(1):45–79, 2017.
URL http://dx.doi.org/10.13154/tosc.v2017.i1.45-79

A common way to prove the security of a cryptographic construction is to give a formal security proof in a so-called ideal component model. Here it is supposed that a generic adversary, Eve, has chosen-plaintext access to the construction and black-box access to the components of the construction, which are supposed to be ideal.The security of the construction is measured by the minimal number of component- and construction queries which have to be performed by Eve for distinguishing the construction from a random construction, or for recovering the secret key.

In this talk, we consider an ideal component model for stream ciphers, a well-established kind of lightweight symmetric encryption algorithm which produce pseudorandom bitstreams in dependence of of a secret symmetric session key and so-called (public) initial values, and which are widely used in mobile phones, WLAN etc. for an online encryption of secret messages.

Most stream cipher constructions suffer from a vulnerability against generic Time-Memory-Data Tradeoff attacks, which reduce the effective key length to $n/2$, where n denotes the

inner state length of the cipher. This is the reason why modern stream ciphers like TRIVIUM or GRAIN have a comparatively large inner state length of at least 160.

We introcuce and analyze here a new stream cipher construction, the LIZARD-construction, and give a formal proof that the security of this construction against generic Time-Memory-Data Tradeoff attacks is $(2/3)n$.

Based in this we proposed in (Hamann, Krause and Meier 2017) the ultralightweight stream cipher LIZARD, which has an inner state length of only 121.

4.16 Asymmetric direct-sum theorems

Bruno Loff (Charles University – Prague, CZ)

Joint work of Arkadev Chattopadhyay, Michal Koucký, Sagnik Mukhopadhyay

We mention some results about the following communication problem: Alice is given k instances $x_1, \ldots, x_k$ and Bob is given a single instance y, and Bob must learn the vector $(f(x_1, y), \ldots, f(x_k, y))$. This is a so-called *asymmetric direct-sum problem*, and naturally appears in the setting of data-structure lower-bounds.

We show that if the distributional communication-complexity of f under product distributions is at least C, then any randomized protocol to solve the above problem needs to have Alice send $\tilde{\Omega}(kC)$ bits and Bob send $\tilde{\Omega}(C)$ bits of communication.

We also show that this result is tight when f is disjointness, by exhibiting a protocol for $k = n$ where Alice communicates $n\sqrt{n}$ and Bob communicates $\sqrt{n}$ bits.

4.17 The Birkhoff polytope and coding for distributed storage

Shachar Lovett (University of California – San Diego, US)

Joint work of Daniel Kane, Shachar Lovett, Sankeerth Rao
Main reference D. Kane, S. Lovett, S. Rao, "The independence number of the Birkhoff polytope graph, and applications to maximally recoverable codes", arXiv:1702.05773v2 [math.CO], 2017.
URL https://arxiv.org/abs/1702.05773

I will describe a journey that starts at error correcting codes for distributed storage, and leads to graph labeling, the study of the Birkhoff polytope graph, the representation theory of the symmetric group and a structure-vs-randomness extension to the Hoffman bound.

On the technical side, we prove tight bounds for the chromatic number of the Birkhoff polytope graph, and use it to characterize the alphabet size needed for maximally recoverable codes in grid topologies.

4.18 Learning Residual Alternating Automata

Rüdiger Reischuk (Universität zu Lübeck, DE)

Joint work of Maciej Liśkiewicz, Matthias Lutter, Sebastian Berndt

Residuality plays an essential role for learning finite automata. While residual deterministic and nondeterministic automata have been understood quite well, fundamental questions concerning alternating automata (AFA) remain open.

Recently, Angluin, Eisenstat, and Fisman have initiated a systematic study of residual AFAs and proposed an algorithm called AL* an extension of the popular L* algorithm to learn AFAs. Based on computer experiments they conjectured that AL* produces residual AFAs, but have not been able to give a proof.

We disprove this conjecture by constructing a counterexample. As our main positive result we design an efficient learning algorithm, named AL**, and give a proof that it outputs residual AFAs only. In addition, we investigate the succinctness of these different FA types in more detail.

4.19 Understanding Cutting Planes for QBFs

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

Joint work of Olaf Beyersdorff, Leroy Chew, Meena Mahajan, Anil Shukla
Main reference O. Beyersdorff, L. Chew, M. Mahajan, A. Shukla, "Understanding Cutting Planes for QBFs", in Proc. of the 36th IARCS Ann. Conf. on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2016), LIPIcs, Vol. 65, pp. 40:1–40:15, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2017.
URL http://dx.doi.org/10.4230/LIPIcs.FSTTCS.2016.40

We define a new system for refuting false QBFs, by augmenting the propositional cutting planes system with a universal variable reduction rule. We show that lower bounds for the new system can be obtained via two independent techniques. One is the feasible interpolation method, extended to handle the reduction rule. Along with the known lower bounds for real monotone circuits for the Clique function, it yields an exponential lower bound for very simple false QBFs based on Clique. The other is the strategy extraction method: from a cutting planes proof of size s, we extract a decision list of threshold functions, of length s, computing a winning strategy for the universal player. Along with known lower bounds for such decision lists, it yields an exponential lower bound for a very simple false QBF based on the Inner product mod 2 function. These lower bounds also hold for the semantic cutting planes based system.

4.20 Recent developments in high-rate locally-testable and locally-correctable codes

Or Meir (University of Haifa, IL)

Joint work of Swastik Kopparty, Or Meir, Noga Ron-Zewi, Shubhangi Saraf
Main reference S. Kopparty, O. Meir, N. Ron-Zewi, S. Saraf, "High-rate locally-correctable and locally-testable codes with sub-polynomial query complexity", in Proc. of the 48th Annual ACM Symposium on Theory of Computing (STOC 2016), pp. 202–215, ACM, 2016.
URL http://doi.acm.org/10.1145/2897518.2897523

Locally-testable codes (LTCs) and locally-correctable codes (LCCs) are error-correcting codes for which there are extremely efficient algorithms. Specifically, there are algorithms for verifying and decoding that only need to read very few bits of the corrupted codeword. The number of bits that are read is called the "query complexity".

Historically, most work on LTCs and LCCs focused on the parameter regime of constant query complexity. In the recent years, however, a few works considered the parameter regime in which the query complexity is much larger, but still sublinear. It turns out that in such a regime, it is possible to obtain very interesting and unexpected constructions.

In this talk, I will present this new line of research, and focus on a recent paper that obtained the state-of-the-art results.

4.21 Twenty (simple) questions

Shay Moran (University of California – San Diego, US)

Joint work of Yuval Dagan, Yuval Filmus, Ariel Gabizon, Shay Moran
Main reference Y. Dagan, Y. Filmus, A. Gabizon, S. Moran, "Twenty (simple) questions", in Proc. of the 49th Ann. ACM SIGACT Symp. on Theory of Computing (STOC 2017), pp. 9–21, ACM, 2017.
URL http://doi.acm.org/10.1145/3055399.3055422

A basic combinatorial interpretation of Shannon's entropy function is via the "20 questions" game. This cooperative game is played by two players, Alice and Bob: Alice picks a distribution π over the numbers $\{1, \ldots, n\}$, and announces it to Bob. She then chooses a number x according to π, and Bob attempts to identify x using as few Yes/No queries as possible, on average.

An optimal strategy for the "20 questions" game is given by a Huffman code for π: Bob's questions reveal the codeword for x bit by bit. This strategy finds x using fewer than $H(\pi)+1$ questions on average. However, the questions asked by Bob could be arbitrary. In this paper, we investigate the following question: *Are there restricted sets of questions that match the performance of Huffman codes, either exactly or approximately?*

Our first main result shows that for every distribution π, Bob has a strategy that uses only questions of the form "$x < c$?" and "$x = c$?", and uncovers x using at most $H(\pi) + 1$ questions on average, matching the performance of Huffman codes in this sense. We also give a natural set of $O(rn^{1/r})$ questions that achieve a performance of at most $H(\pi) + r$, and show that $\Omega(rn^{1/r})$ questions are required to achieve such a guarantee.

Our second main result gives a set $\mathcal{Q}$ of $1.25^{n+o(n)}$ questions such that for every distribution π, Bob can implement an *optimal* strategy for π using only questions from $\mathcal{Q}$. We also show

that $1.25^{n-o(n)}$ questions are needed, for infinitely many n. If we allow a small slack of r over the optimal strategy, then roughly $(rn)^{\Theta(1/r)}$ questions are necessary and sufficient.

4.22 Fast Space-efficient subset sum

Nikhil Bansal (TU Eindhoven, NL)

Joint work of Nikhil Bansal, Shashwat Garg, Jesper Nederlof, Nikhil Vyas
Main reference N. Bansal, S. Garg, J. Nederlof, N, Vyas, "Faster Space-Efficient Algorithms for Subset Sum and k-Sum", in Proc. of the 49th Ann. ACM SIGACT Symp. on Theory of Computing (STOC 2017), pp. 198–209, ACM, 2017.
URL http://doi.acm.org/10.1145/3055399.3055467

I will describe a randomized algorithm for the subset sum problem that runs in $2^{0.86n}$ time and uses polynomial space, provided the algorithm has read only random access to exponentially many random bits. Previously, all algorithms with running time less than 2^n used exponential space, and obtaining such a guarantee was open. Our algorithm is based on two main ingredients. First, Floyd's space efficient technique for cycle finding, which is also referred to as the Pollard Rho method, and second some additive combinatorics of subset sums. Time permitting, I will also talk about extensions to problems such as k-sum, knapsack, binary integer linear programming.

4.23 Random formulas in Cutting Planes

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

Joint work of Pavel Pudlák, Pavel Hrubeš
Main reference P. Hrubeš, P. Pudlák, "Random formulas, monotone circuits, and interpolation", ECCC, 2017.
URL https://eccc.weizmann.ac.il/report/2017/042/download/

I discuss results and open problems related to random CNFs in the Cutting Planes proof system.

4.24 On the Fine-grained Complexity of One-Dimensional Dynamic Programming

Ramamohan Paturi (University of California – San Diego, US)

Joint work of Marvin Künnemann, Ramamohan Paturi, Stefan Schneider
Main reference M. Kunnemann, R. Paturi, S. Schneider, "On the Fine-grained Complexity of One-Dimensional Dynamic Programming", in Proc. of the 44th Int'l Colloquium on Automata, Languages, and Programming (ICALP 2017), LIPIcs, Vol. 80, pp. 21:1–21:15, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2017.
URL http://dx.doi.org/10.4230/LIPIcs.ICALP.2017.21

In this paper, we investigate the complexity of one-dimensional dynamic programming, or more specifically, of the Least-Weight Subsequence (LWS) problem: Given a sequence of

n data items together with weights for every pair of the items, the task is to determine a subsequence S minimizing the total weight of the pairs adjacent in S. A large number of natural problems can be formulated as LWS problems, yielding obvious $O(n^2)$-time solutions.

In many interesting instances, the $O(n^2)$-many weights can be succinctly represented. Yet except for near-linear time algorithms for some specific special cases, little is known about when an LWS instantiation admits a subquadratic-time algorithm and when it does not. In particular, no lower bounds for LWS instantiations have been known before. In an attempt to remedy this situation, we provide a general approach to study the fine-grained complexity of succinct instantiations of the LWS problem. In particular, given an LWS instantiation we identify a highly parallel core problem that is subquadratically equivalent. This provides either an explanation for the apparent hardness of the problem or an avenue to find improved algorithms as the case may be.

More specifically, we prove subquadratic equivalences between the following pairs (an LWS instantiation and the corresponding core problem) of problems: a low-rank version of LWS and minimum inner product, finding the longest chain of nested boxes and vector domination, and a coin change problem which is closely related to the knapsack problem and (min,+)-convolution. Using these equivalences and known SETH-hardness results for some of the core problems, we deduce tight conditional lower bounds for the corresponding LWS instantiations. We also establish the (min,+)-convolution-hardness of the knapsack problem. Furthermore, we revisit some of the LWS instantiations which are known to be solvable in near-linear time

4.25 The Minimum Circuit Size Problem and its Complexities

Rahul Santhanam (University of Oxford, GB)

Joint work of Shuichi Hirahara, Igor Carboni Oliveira, Rahul Santhanam

Recent work in complexity theory has emphasized the links between complexity lower bounds and algorithmic problems such as circuit satisfiability, derandomization and learning. An important computational problem in this connection is the Minimum Circuit Size Problem (MCSP), where the input is the truth table of a Boolean function and the question is whether the function has small circuits.

MCSP belongs to NP, but it and its variants have several unusual and interesting features, which distinguish it from other natural problems in NP. I will discuss these features, survey previous work on the problem, and explain the relevance of MCSP to circuit lower bounds, learning and natural proofs.

This talk is partly based on 2 recent works of the speaker, one with Igor Carboni Oliveira on "Conspiracies between Circuit Lower Bounds, Learning Algorithms and Pseudorandomness" and the other with Shuichi Hirahara "On the Average-Case Complexity of MCSP and its Variants".

4.26 Computing Requires Larger Formulas than Approximating

Avishay Tal (Institute for Advanced Study – Princeton, US)

Main reference A. Tal, "Computing Requires Larger Formulas than Approximating", ECCC, 2016.
URL https://eccc.weizmann.ac.il/report/2016/179/

A de Morgan formula over Boolean variables $x_1, \ldots, x_n$ is a binary tree whose internal nodes are marked with AND or OR gates and whose leaves are marked with variables or their negation. We define the size of the formula as the number of leaves in it. Proving that some explicit function (in P or NP) requires large formula is a central open question in computational complexity.

In this work, we introduce a size-amplification hardness reduction for de-Morgan formulas. We show that average-case hardness implies worst-case hardness for a larger size. More precisely, if a function f cannot be computed correctly on more than $1/2 + 2^{-k}$ of the inputs by any formula of size s, then computing f correctly on all inputs requires size ks. The tradeoff is essentially tight. Quite surprisingly, the proof relies on a result from quantum query complexity by Reichardt.

As an application, we improve the best known formula size lower bounds for explicit functions by logarithmic factors to $n^3/\log(n)$. In addition, we propose candidates for explicit functions that we believe have formula size n^4, and prove non-trivial super-quadratic formula size lower bounds for them using our reduction.

4.27 Derandomizing Isolation in Space-Bounded Settings

Dieter van Melkebeek (University of Wisconsin – Madison, US)

Joint work of Dieter van Melkebeek, Gautam Prakriya
Main reference D. van Melkebeek, G. Prakriya, "Derandomizing Isolation in Space-Bounded Settings", in Proc. of the 32nd Computational Complexity Conf. (CCC 2017), LIPIcs, Vol. 79, pp. 5:1–5:32, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2017.
URL http://dx.doi.org//10.4230/LIPIcs.CCC.2017.5

Isolation is the process of singling out a solution to a problem that may have many solutions. It plays an important role in the design of efficient parallel algorithms as it ensures that the various parallel processes all work towards a single global solution rather than towards individual solutions that may not be compatible with one another. For example, the best parallel algorithms for finding perfect matchings in graphs hinge on isolation for this reason. Isolation is also an ingredient in some efficient sequential algorithms. For example, the best running times for certain NP-hard problems like finding hamiltonian paths in graphs are achieved via isolation.

All of these algorithms are randomized, and the only reason is the use of the Isolation Lemma – that for any set system over a finite universe, a random assignment of small integer weights to the elements of the universe has a high probability of yielding a unique set of minimum weight in the system. For each of the underlying problems it is open whether deterministic algorithms of similar efficiency exist.

I will talk about the possibility of deterministic isolation in the space-bounded setting. The question is: Can one always make the accepting computation paths of nondeterministic space-bounded machines unique without changing the underlying language and without

blowing up the space by more than a constant factor? Or equivalently, does there exist a deterministic logarithmic space mapping reduction from directed st-connectivity to itself that transforms positive instances into ones where there is a unique path from s to t?

I will present some recent results towards a resolution of this question, obtained jointly with Gautam Prakriya. Our approach towards a positive resolution can be viewed as derandomizing the Isolation Lemma in the context of space-bounded computation.

4.28 Succinct Hitting Sets and Barriers to Proving Algebraic Circuits Lower Bounds

Ben Lee Volk (Tel Aviv University, IL)

Joint work of Micahel Forbes, Amir Shpilka, Ben Lee Volk
Main reference M. A. Forbes, A. Shpilka, B. L. Volk, "Succinct Hitting Sets and Barriers to Proving Algebraic Circuits Lower Bounds", in Proc. of the 49th Ann. ACM SIGACT Symp. on Theory of Computing (STOC 2017), pp. 653–664, ACM, 2017.
URL http://doi.acm.org/10.1145/3055399.3055496

This talk presents a framework of "algebraically natural lower bounds" for algebraic circuits, which is similar to the natural proofs notion of Razborov and Rudich for boolean circuit lower bounds, and captures nearly all lower bound techniques known. However, unlike the boolean setting, there has been little concrete evidence demonstrating that this is a barrier to obtaining super-polynomial lower bounds for general algebraic circuits.

We show that the existence of an algebraic natural proofs barrier is equivalent to the existence of succinct derandomization of the polynomial identity testing problem. That is, whether the coefficient vectors of polylog(N)-degree polylog(N)-size circuits is a hitting set for the class of poly(N)-degree poly(N)-size circuits. Further, we give an explicit universal construction showing that if such a succinct hitting set exists, then our universal construction suffices.

We assess the existing literature constructing hitting sets for restricted classes of algebraic circuits and modify some of these constructions to obtain succinct hitting sets, thus suggesting evidence supporting the existence of an algebraic natural proofs barrier.

Our framework is similar to the Geometric Complexity Theory (GCT) program of Mulmuley and Sohoni, except that here we emphasize constructiveness of the proofs while the GCT program emphasizes symmetry. Nevertheless, our succinct hitting sets have relevance to the GCT program as they imply lower bounds for the complexity of the defining equations of polynomials computed by small circuits.

4.29 Descriptive Complexity of Arithmetic Complexity Classes

Heribert Vollmer (Leibniz Universität Hannover, DE)

Joint work of Juha Kontinen, Anselm Haak, Juha Kontinen, Heribert Vollmer
Main reference A. Durand, A. Haak, J. Kontinen, H. Vollmer, "Descriptive Complexity of #AC0 Functions, in Proc. of the 25th EACSL Annual Conference on Computer Science Logic (CSL 2016), LIPIcs,

Vol. 62, pp. 20:1-20:16, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2017.
URL http://dx.doi.org/10.4230/LIPIcs.CSL.2016.20

We study the class $\#AC^0$ of functions computed by constant-depth polynomial-size arithmetic circuits of unbounded fan-in addition and multiplication gates. Inspired by Immerman's characterization of the Boolean class AC^0, we develop a model-theoretic characterization of $\#AC^0$, which can be interpreted as follows: Functions in $\#AC^0$ are exactly those functions counting winning strategies in first-order model checking games.

Extending this, we introduce a new framework for a descriptive complexity approach to arithmetic computations. We define a hierarchy of classes based on the idea of counting assignments to free function variables in first-order formulas. We completely determine the inclusion structure and show that #P and $\#AC^0$ appear as classes of this hierarchy. In this way, we unconditionally place #AC0 properly in a strict hierarchy of arithmetic classes within #P.

5 Open problems

5.1 The direct sum of the fork relation

Or Meir (University of Haifa, IL)

An old open problem in complexity theory is proving a direct-sum theorem for deterministic communication complexity. While partial results are known for total Boolean functions [1], nothing is known for relations. As a first step toward attacking this problem, I suggest proving a direct-sum theorem for the fork relation of Grigni and Sipser [MS].

References

1 Tomás Feder, Eyal Kushilevitz, Moni Naor and Noam Nisan. *Amortized Communication Complexity*. SIAM Journal of Computing 28(4), pages 736–750, 1995.
2 Michelangelo Grigni and Michael Sipser. *Monotone Separation of Logarithmic Space from Logarithmic Depth*. J. Comput. Syst. Sci. 50(3), pages 433–437, 1995.

5.2 Parameterized approximation scheme for Steiner tree

Pavel Dvořák (Charles University – Prague, CZ)

Joint work of Pavel Dvořák, Andreas Feldmann, Dušan Knop, Tomáš Masařík, Tomáš Toufar, Pavel Veselý

We study the Steiner tree problem. In this problem a graph $G = (V, E)$ is given where the set of vertices is split into two disjoint sets of terminals and Steiner vertices. The task is to find a minimum connected subgraph of G which contains all terminals. We consider a parameter p, which is the number of Steiner vertices in the optimal solution. This problem is W[2]-hard and APX-hard. Thus, we try to find an algorithm for the problem which runs in time $f(p, e)$ poly(n), where n is the size of G and f is some computable function, and returns e-approximation of the solution. We succeeded in directed and undirected cases. And we

know that there is no such algorithm for the weighted directed case (with some standard complexity assumptions). We still try to solve the case when the input graph G is weighted and undirected.

5.3 The randomized complexity of online labeling

Michael E. Saks (Rutgers University – Piscataway, US)

Joint work of Jan Bulánek, Michal Koucký

In the online labeling problem with parameters n and m we are presented with a sequence of n *items* from a totally ordered universe U and must assign each arriving item a label from the label set $\{1, 2, \ldots, m\}$ so that the order of labels (strictly) respects the ordering on U. As new items arrive it may be necessary to change the labels of some items; such changes may be done at any time at unit cost for each change. The goal is to minimize the total cost. An alternative formulation of this problem is the *file maintenance problem*, in which the items, instead of being labeled, are maintained in sorted order in an array of length m, and we pay unit cost for moving an item.

The parameter m, the size of the *label space* must be at least the number of items n for a labeling to be possible. There are two natural ranges of parameters which have received the most attention. In the case of *linearly many labels* we have $m = cn$ for some $c > 1$, and in the case of *polynomially many labels* we have $m = \theta(n^C)$ for some constant $C > 1$. The size r of the universe U is also a parameter which is not discussed explicitly in most of the literature on the problem. If $r \leq m$, the problem can be solved with cost n, since then we can simply fix an order preserving bijection from U to $\{1, \ldots, m\}$ in advance. In this paper we assume $U = \{1, \ldots, 2^n\}$.

The problem was introduced by Itai, Konheim and Rodeh [6] who also gave an algorithm for the case of linearly many labels having worst case total cost $O(n \log(n)^2)$. In the special case that $m = n$, algorithms with cost $O(\log(n)^3)$ per item are known [7, 2]. It is also well known that the algorithm of Itai et al. can be adapted to give total cost $O(n \log(n))$ in the case of polynomially many labels. All of these algorithms are deterministic.

Tight lower bounds are known for most ranges of m. In the case that $m = n^{O(1)}$, Dietz, Seiferas and Zhang [5] proved an $\Omega(n \log(n))$ lower bound. Bulánek, Koucký and Saks proved [4], proved an $\Omega(n \log(n)^2)$ lower bound in the case of linearly many labels, and $\Omega(n \log(n)^3)$ lower bound for the case $m = n$. The same authors with Babka and Čunát [1] proved a $\Omega(n \log(n)/(\log\log(m) - \log\log(n)))$ lower bound, that holds for all $n \leq m \leq 2^n$. When $m = O(1)$ this matches the above-mentioned bound proved by [5].

All of these lower bounds apply only to *deterministic* algorithms, leaving open the possibility of better randomized algorithms. As usual we measure the cost of a randomized algorithm as the worst case over all input sequences of a given length n of the expected number of moves made by the algorithm. This corresponds to running the algorithm against an *oblivious adversary* who selects the input sequence having full knowledge of the algorithm, but not of the random bits flipped in the execution of the algorithm.

Bulánek, Koucký and Saks[3] showed that the $\Omega(n \log n)$ bound (proved in [5]) for deterministic algorithms in the case of polynomially many labels $m = n^{O(1)}$, extends to randomized algorithms.

The randomized complexity in the case of a linear number of labels, $m = O(n)$ remains open.

References

1 Babka, M., Bulánek, J., Čunát, V., Koucký, M., Saks, M.: On Online Labeling with Polynomially Many Labels. In *ESA*, 121–132 (2012)

2 Bird, R., Sadnicki, S.: Minimal on-line labelling. *Inf. Process. Lett.*, 101(1), 41–45 (2007)

3 Bulánek, J., Koucký, M., Saks, M., On Randomized Online Labeling with Polynomially Many Labels. ICALP (1) 2013:291–302

4 Bulánek, J., Koucký, M., Saks, M., Tight lower bounds for online labeling problem, *SIAM J. Computing* 44(6), 1765–1797 (2015)

5 Dietz, P., Seiferas, J., Zhang, J.: A tight lower bound for online monotonic list labeling. *SIAM J. Discrete Math.*, 18(3), 626–637 (2004)

6 Itai, A., Konheim, A., Rodeh, M.: A sparse table implementation of priority queues. In *ICALP*, 417–431 (1981)

7 Zhang, J.: Density Control and On-Line Labeling Problems. *PhD thesis*, University of Rochester (1993).

Participants

- Eric Allender
Rutgers University, US
- Nikhil Bansal
TU Eindhoven, NL
- Harry Buhrman
CWI – Amsterdam, NL
- Igor Carboni Oliveira
Charles University – Prague, CZ
- Sourav Chakraborty
CWI – Amsterdam, NL
- Gil Cohen
Princeton University, US
- Anindya De
Northwestern University – Evanston, US
- Pavel Dvorak
Charles University – Prague, CZ
- Lance Fortnow
Georgia Institute of Technology – Atlanta, US
- Anna Gál
University of Texas – Austin, US
- Alexander Golovnev
New York University, US
- Rohit Gurjar
Tel Aviv University, IL
- Kristoffer Arnsfelt Hansen
Aarhus University, DK
- Prahladh Harsha
TIFR – Mumbai, IN
- Johan Hastad
KTH Royal Institute of Technology – Stockholm, SE
- Pavel Hrubes
The Czech Academy of Sciences – Prague, CZ
- Valentine Kabanets
Simon Fraser University – Burnaby, CA
- Swastik Kopparty
Rutgers University – Piscataway, US
- Michal Koucký
Charles University – Prague, CZ
- Matthias Krause
Universität Mannheim, DE
- Bruno Loff
Charles University – Prague, CZ
- Shachar Lovett
University of California – San Diego, US
- Meena Mahajan
Institute of Mathematical Sciences – Chennai, IN
- Or Meir
University of Haifa, IL
- Shay Moran
University of California – San Diego, US
- Jakob Nordström
KTH Royal Institute of Technology – Stockholm, SE
- Ramamohan Paturi
University of California – San Diego, US
- Pavel Pudlák
The Czech Academy of Sciences – Prague, CZ
- Oded Regev
New York University, US
- Rüdiger Reischuk
Universität zu Lübeck, DE
- Michael E. Saks
Rutgers University – Piscataway, US
- Rahul Santhanam
University of Oxford, GB
- Ronen Shaltiel
University of Haifa, IL
- Avishay Tal
Institute for Advanced Study – Princeton, US
- Till Tantau
Universität zu Lübeck, DE
- Thomas Thierauf
Hochschule Aalen, DE
- Jacobo Torán
Universität Ulm, DE
- Dieter van Melkebeek
University of Wisconsin – Madison, US
- Ben Lee Volk
Tel Aviv University, IL
- Heribert Vollmer
Leibniz Universität Hannover, DE