Computational Complexity of Discrete Problems

Edited by
Anna Gál¹, Rahul Santhanam², and Till Tantau³

¹ University of Texas – Austin, US, panni@cs.utexas.edu
² University of Oxford, GB, rahul.santhanam@cs.ox.ac.uk
³ Universität zu Lübeck, DE, tantau@tcs.uni-luebeck.de

Abstract
The following report archives the presentations and activities of the March 2019 Dagstuhl Seminar 19121 “Computational Complexity of Discrete Problems”. Section 1 summarizes the topics and some specific results offered in selected talks during the course of the week. Section 2 provides a table of contents, listing each of the talks given in alphabetical order. Section 3 contains the abstracts, indicating both the main reference and other relevant sources (where applicable) to allow the reader to investigate the topics further.

Seminar March 17-22, 2019 – http://www.dagstuhl.de/19121
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, parametrisation, randomness
Digital Object Identifier 10.4230/DagRep.9.3.64
Edited in cooperation with Matthew J. Katzman

1 Executive Summary

Anna Gál (University of Texas – Austin, US)
Rahul Santhanam (University of Oxford, GB)
Till Tantau (Universität zu Lübeck, DE)

Computational complexity theory is the study of computation under bounded resources, and the tradeoffs thereof offered by specific problems and classes of problems in various computational models. Such resources include time and space for classical computation, randomness, non-determinism, and oracles for more advanced uniform machines, size/advice for circuits/non-uniform computation, interaction for communication protocols, length and depth for proof complexity, and much more. The goals of work in this field are not only to discover and improve these tradeoffs, but ideally to find tight lower bounds to match the solutions that have been found, and use such results in one of the models to inform results in the others. Despite decades of work on these problems, the answers to many foundational questions (such as $P$ vs $NP$, $P$ vs $BPP$, $NP$ vs $co-NP$) still remain out of reach.

For the 2019 instalment of the seminar series Computational Complexity of Discrete Problems – which evolved out of the seminar series Complexity of Boolean Functions that dates back to the founding of Dagstuhl – Anna Gál, Oded Regev, Rahul Santhanam, and Till Tantau invited 40 participants to Dagstuhl to work towards discovering new results in the field. The seminar started with the assembly of a large “graph of interests” that allowed
the participants both to present their own research interests and to see how these align with
the other present researchers. The bulk of the research work was then done in the form of,
on the one hand, talks in the morning and late afternoon and, on the other hand, break-out
sessions and small discussions in the afternoon by smaller groups.

A distinguishing feature of the seminar talks were the lively discussions during and after
the talk: given the often highly abstract and specialized topics presented by the experts in
the field, lively discussions are by no means a given and they proved to be both rewarding and
helpful for all participants. In the informal afternoon sessions, smaller groups of researchers
had ample time to tackle the open problems of the field; with some discussions still going
on after midnight. Two events – the traditional Wednesday hike and the traditional wine-
and-cheese party on Thursday – allowed everyone well-earned breaks from doing research on
computational complexity.

The range of topics covered by the participants during the seminar was broad and included
derandomization, lower bounds for specific problems, communication complexity, complexity
classes, graph algorithms, learning theory, coding theory, and proof complexity. Specific
selected results presented throughout include:

- A proof that the Log-Approximate-Rank Conjecture is false, yielding the first exponential
gap between the logarithm of the approximate rank and randomized communication
complexity for total functions.

- An oracle separation of $\text{BQP}$ and the polynomial hierarchy, showing a strong converse
to the Bennett et al. oracle relative to which $\text{BQP}$ cannot solve $\text{NP}$-complete problems
in sub-exponential time.

- Improved lower bounds for the Minimum Circuit Size Problem, including
  - $\text{MCSP} \not\in \text{AC}^0[p]$, 
  - $\text{MCSP}$ requires $N^{3-o(1)}$-size de Morgan formulas,
  - $\text{MCSP}$ requires $N^{2-o(1)}$-size general formulas,
  - $\text{MCSP}$ requires $2^{\Omega(N^{1/d+2.\alpha})}$-size depth-$d$ $\text{AC}^0$ circuits,
  where the first result is achieved by showing $\text{MCSP}$ can solve the coin problem and the
  others using properties of local pseudorandom generators.

Open problems were posed by Amit Chakrabarty, Alexander Golovnev, Or Meir, and
Omri Weinstein.

The organizers, Anna Gál, Oded Regev, Rahul Santhanam, and Till Tantau, would like
to thank all participants at this point for the many contributions they made, but we would
also like to especially thank the Dagstuhl staff for doing – as always – an excellent job and
helping with organizational matters and with making everyone feel welcome.
2 Table of Contents

Executive Summary
Anna Gál, Rahul Santhanam, and Till Tantau ............................ 64

Overview of Talks
Planarity, Exclusivity, and Unambiguity
Eric Allender .............................................. 68
Time-Space Tradeoffs for Learning Finite Functions from Random Evaluations, with Applications to Polynomials
Paul Beame .............................................. 68
Randomness and intractability in Kolmogorov complexity
Igor Carboni Oliveira ..................................... 69
Quantum Exact Learning of k-sparse functions and improved Chang’s Lemma for sparse Boolean functions
Sourav Chakraborty ...................................... 69
The Log-Approximate-Rank Conjecture is False
Arkadev Chattopadhyay .................................... 70
A Route Towards Advances on the BPL versus L problem
Gil Cohen .................................................. 71
Identifying low-dimensional functions in high-dimensional spaces
Anindya De ............................................... 71
Graph Communication Protocols
Lukáš Folwarczný .......................................... 71
Static Data Structure Lower Bounds Imply Rigidity
Alexander Golovnev ........................................ 72
Recent Applications of High Dimensional Expanders to Coding
Prabhlad Harsha ........................................... 72
New Circuit Lower Bounds for Minimum Circuit Size Problem
Valentine Kabanets ......................................... 73
An Optimal Space Lower Bound for Approximating MAX-CUT
Michael Kapralov .......................................... 73
Improved soundness for proving proximity to Reed-Solomon codes
Swastik Kopparty .......................................... 74
Stronger Lower Bounds for Online ORAM
Michal Koucký ............................................. 75
Improving OBDD-Attacks and Related Complexity-Theoretic Problems
Matthias Krause ............................................ 75
Building strategies into QBF proofs
Meena Mahajan ............................................ 76
Exponential Lower Bounds for Weak Pigeonhole Principle and Perfect Matching Formulas over Sparse Graphs
Jakob Nordström .......................................... 77
Extractors for small zero-fixing sources  
*Pavel Pudlák* 

Majority Quantifiers, Complexity Classes and Games  
*Rüdiger Reischuk* 

Computational Two Party Correlation  
*Ronen Shaltiel* 

Near-Optimal Erasure List-Decodable Codes  
*Amnon Ta-Shma* 

Oracle Separation of BQP and the Polynomial Hierarchy  
*Avishay Tal* 

Different methods to isolate a perfect matching in bipartite graphs  
*Thomas Thierauf* 

Lower Bounds for Matrix Factorization  
*Ben Lee Volk* 

Oblivious Lower Bounds for Near-Neighbor Search  
*Omri Weinstein* 

*Participants*
3 Overview of Talks

3.1 Planarity, Exclusivity, and Unambiguity

Eric Allender (Rutgers University – Piscataway, US)

We provide new upper bounds on the complexity of the s-t-connectivity problem in planar graphs, thereby providing additional evidence that this problem is not complete for NL. This also yields a new upper bound on the complexity of computing edit distance. Building on these techniques, we provide new upper bounds on the complexity of several other computational problems on planar graphs. All of these problems are shown to solvable in logarithmic time on a concurrent-read exclusive-write (CREW) PRAM. The new upper bounds are provided by making use of a known characterization of CREW algorithms in terms of “unambiguous” $\text{AC}^1$ circuits. This seems to be the first occasion where this characterization has been used in order to provide new upper bounds on natural problems.

Joint work with Archit Chauhan, Samir Datta, and Anish Mukherjee.

3.2 Time-Space Tradeoffs for Learning Finite Functions from Random Evaluations, with Applications to Polynomials

Paul Beame (University of Washington – Seattle, US)

We develop an extension of recent analytic methods for obtaining time-space tradeoff lower bounds for problems of learning Boolean functions from uniformly random labelled examples. With our methods we can obtain bounds for learning arbitrary concept classes of finite functions from random evaluations even when the sample space of random inputs can be significantly smaller than the concept class of functions and the function values can be from an arbitrary finite set.

To obtain our results, we reduce the time-space complexity of learning from random evaluations to the question of how much the corresponding evaluation matrix amplifies the 2-norms of ‘almost uniform’ probability distributions. To analyze the latter, we formulate it as a semidefinite program, and analyze its dual. (Similar results to ours using related but somewhat different techniques were independently shown by Garg, Raz, and Tal.)

As applications we show that any algorithm that learns an $n$-variate polynomial function of degree at most $d$ over any prime field $F_p$ with probability $p^{-O(n)}$, or with prediction advantage $p^{-O(n)}$ over random guessing, given evaluations on randomly chosen inputs either requires space $\Omega((nN/d) \log p)$ or time $p^{\Omega(n/d)}$ where $N = (n/d)^{\Theta(d)}$ is the dimension of the space of such polynomials. These bounds, which are based on new bounds on the bias of
polynomials over \( F_p \), are asymptotically optimal for polynomials of arbitrary constant degree and constant \( p \) since they match the tradeoffs achieved by natural learning algorithms for the problems.

### 3.3 Randomness and intractability in Kolmogorov complexity

**Igor Carboni Oliveira (University of Oxford, GB)**

We introduce randomized time-bounded Kolmogorov complexity (rKt), a natural extension of Levin’s notion of Kolmogorov complexity. A string \( w \) of low rKt complexity can be decompressed from a short representation via a time-bounded algorithm that outputs \( w \) with high probability.

This complexity measure gives rise to a decision problem over strings: \( \text{MrKtP} \) (The Minimum rKt Problem). We explore ideas from pseudorandomness to prove that \( \text{MrKtP} \) and its variants cannot be solved in randomized quasi-polynomial time. This exhibits a natural string compression problem that is provably intractable, even for randomized computations. Our techniques also imply that there is no \( n^{1-\epsilon} \)-approximate algorithm for \( \text{MrKtP} \) running in randomized quasi-polynomial time.

Complementing this lower bound, we observe connections between rKt, the power of randomness in computing, and circuit complexity. In particular, we present the first hardness magnification theorem for a natural problem that is unconditionally hard against a strong model of computation.

### 3.4 Quantum Exact Learning of k-sparse functions and improved Chang’s Lemma for sparse Boolean functions

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

We show how to exactly learn a \( k \)-Fourier-sparse \( n \)-bit Boolean function from \( O(k^{1.5} (\log k)^2) \) uniform quantum samples from that function. This improves over the bound of \( \Theta(kn) \) uniformly random classical examples [1]. Our main tool is an improvement of Chang’s lemma for sparse Boolean functions. This result appears in paper “Two new results about quantum exact learning” written jointly with Srinivasan Arunachalam, Troy Lee, Manaswi Paraashar and Ronald de Wolf.

**References**

1. Ishay Haviv, Oded Regev *The List-Decoding Size of Fourier-Sparse Boolean Functions*. Conference on Computational Complexity 2015: 58-71
3.5 The Log-Approximate-Rank Conjecture is False

Arkadev Chattopadhyay (TIFR – Mumbai, IN)

License © Creative Commons BY 3.0 Unported license © Arkadev Chattopadhyay

Joint work of Arkadev Chattopadhyay, Nikhil S. Mande, Suhail Sherif


We construct a simple and total XOR function $F$ on $2n$ variables that has only $O(\sqrt{n})$ spectral norm, $O(n^2)$ approximate rank and $n^{O(\log n)}$ approximate nonnegative rank. We show it has polynomially large randomized bounded-error communication complexity of $\Omega(\sqrt{n})$. This yields the first exponential gap between the logarithm of the approximate rank and randomized communication complexity for total functions. Thus $F$ witnesses a refutation of the Log-Approximate-Rank Conjecture (LARC) which was posed by Lee and Shraibman [5] as a very natural analogue for randomized communication of the still unresolved Log-Rank Conjecture for deterministic communication. The best known previous gap for any total function between the two measures is a recent 4th-power separation by Göös, Jayram, Pitassi and Watson [1].

Additionally, our function $F$ refutes Grolmusz’s Conjecture [2] and a variant of the Log-Approximate-Nonnegative-Rank Conjecture, suggested recently by Kol, Moran, Shpilka and Yehudayoff [3], both of which are implied by the LARC. The complement of $F$ has exponentially large approximate nonnegative rank. This answers a question of Lee [4] and Kol et al. [3], showing that approximate nonnegative rank can be exponentially larger than approximate rank. The function $F$ also falsifies a conjecture about parity measures of Boolean functions made by Tsang, Wong, Xie and Zhang [6]. The latter conjecture implied the Log-Rank Conjecture for XOR functions. Our result further implies that at least one of the following statements is true: (a) The Quantum-Log-Rank Conjecture is false; (b) The total function $F$ exponentially separates quantum communication complexity from its classical randomized counterpart.

References

3.6 A Route Towards Advances on the BPL versus L problem

Gil Cohen (Princeton University, US)

The BPL vs. L problem is a fundamental question in complexity theory. The best known result by Saks and Zhou from the late 90s puts BPL in L^{3/2} where the common belief is that BPL = L. In this talk, I’ll present a potential program towards improving the Saks-Zhou result to BPL ⊆ L^c for some constant c < 3/2. One step of this program was implemented in a joint work with Braverman and Garg. The missing step is related to a beautiful paper by Raz and Reingold.

3.7 Identifying low-dimensional functions in high-dimensional spaces

Anindya De (University of Pennsylvania – Philadelphia, US)

Motivated by the problem of feature selection in machine learning, the problem of testing juntas, i.e., checking if a Boolean function on the n-dimensional hypercube only depends on k << n coordinates, has attracted a lot of attention in theoretical computer science. However, in many settings, there is no obvious choice of a basis and a more meaningful question is to ask if a function only depends a k-dimensional subspace. We show that while such “linear juntas” are not testable with any finite number of queries, assuming an upper bound of s on their surface area, such functions can tested with poly(k, s) queries, i.e., independent of the ambient dimension n. We also show a poly(s) lower bound on the query complexity of any non-adaptive tester for linear-juntas showing that the dependence on s is tight up to polynomial factors. As a consequence of our upper bound, we show that intersections of a constant number of halfspaces (as well as several related concepts) are testable with constant query complexity.

3.8 Graph Communication Protocols

Lukáš Folwarczný (Charles University – Prague, CZ)

Graph communication protocols are a generalization of classical communication protocols to the case when the underlying graph is a directed acyclic graph. Motivated by potential applications in proof complexity, we study variants of graph communication protocols and relations between them.

Our results establish the following hierarchy: Protocols with disjointness are at least as strong as protocols with equality and protocols with equality are at least as strong as...
protocols with inequality. Furthermore, we establish that protocols with a conjunction of two inequalities have the same strength as protocols with equality. Lower bounds for protocols with inequality are known. Obtaining lower bounds for protocols higher in the hierarchy would directly lead to applications in proof complexity. In particular, lower bounds for resolution with parities (R(LIN)) and DNF-resolution (DNF-R) would be obtained this way.

3.9 Static Data Structure Lower Bounds Imply Rigidity

Alexander Golovnev (Harvard University – Cambridge, US)

License © Creative Commons BY 3.0 Unported license
Joint work of Zeev Dvir, Alexander Golovnev, Omri Weinstein

We show that static data structure lower bounds in the group (linear) model imply semi-explicit lower bounds on matrix rigidity. In particular, we prove that an explicit lower bound of $t \geq \omega(\log^2 n)$ on the cell-probe complexity of linear data structures in the group model, even against arbitrarily small linear space ($s = (1 + \epsilon)n$), would already imply a semi-explicit (P^NP) construction of rigid matrices with significantly better parameters than the current state of art [1]. Our results further assert that polynomial ($t \geq n^{\delta}$) data structure lower bounds against near-optimal space, would imply super-linear circuit lower bounds for log-depth linear circuits (a four-decade open question). In the succinct space regime ($s = n + o(n)$), we show that any improvement on current cell-probe lower bounds in the linear model would also imply new rigidity bounds. Our results rely on a new connection between the “inner” and “outer” dimensions of a matrix [2], and on a new reduction from worst-case to average-case rigidity, which is of independent interest.

References

3.10 Recent Applications of High Dimensional Expanders to Coding

Prahladh Harsha (TIFR – Mumbai, IN)

License © Creative Commons BY 3.0 Unported license

Expander graphs, over the last few decades, have played a pervasive role in almost all areas of theoretical computer science. Recently, various high-dimensional analogues of these objects have been studied in mathematics and even more recently, there have been some surprising applications in computer science, especially in the area of coding theory.

In this talk, we’ll explore these high-dimensional expanders from a spectral viewpoint and give an alternate characterization if terms of random walks. We will then see an application of high-dimensional expanders towards efficient list decoding.
3.11 New Circuit Lower Bounds for Minimum Circuit Size Problem

Valentine Kabanets (Simon Fraser University – Burnaby, CA)

Minimum Circuit Size Problem (MCSP) asks if a given truth table of an $n$-variate boolean function is computable by a boolean circuit of size at most $s$, for a given $s > 0$. While MCSP is believed to be outside of $\mathbf{P}$, it’s not known if MCSP is $\mathbf{NP}$-hard.

It is natural to ask for circuit lower bounds for MCSP against restricted circuit models. In this talk, I will show some new circuit lower bounds for MCSP against constant-depth circuits ($\mathbf{AC}^0$ and $\mathbf{AC}^0[p]$) and de Morgan formulas, essentially matching the known state-of-the-art lower bounds for the corresponding circuit models.

This talk is based on two joint works with Alexander Golovnev, Rahul Ilango, Russell Impagliazzo, Antonina Kolokolova, and Avishay Tal, as well as Mahdi Cheraghchi, Zhenjian Lu, and Dimitrios Myrisiotis.

3.12 An Optimal Space Lower Bound for Approximating MAX-CUT

Michael Kapralov (EPFL – Lausanne, CH)

We consider the problem of estimating the value of MAX-CUT in a graph in the streaming model of computation. At one extreme, there is a trivial 2-approximation for this problem that uses only $O(\log n)$ space, namely, count the number of edges and output half of this value as the estimate for the size of the MAX-CUT. On the other extreme, for any fixed $\epsilon > 0$, if one allows $O(n)$ space, a $(1 + \epsilon)$-approximate solution to the MAX-CUT value can be obtained by storing an $O(n)$-size sparsifier that essentially preserves MAX-CUT value.

Our main result is that any (randomized) single pass streaming algorithm that breaks the 2-approximation barrier requires $\Omega(n)$-space, thus resolving the space complexity of any non-trivial approximations of the MAX-CUT value to within polylogarithmic factors in the single pass streaming model. We achieve the result by presenting a tight analysis of the Implicit Hidden Partition Problem introduced by Kapralov et al. [1] for an arbitrarily large number of players. In this problem a number of players receive random matchings of $\Omega(n)$ size together with random bits on the edges, and their task is to determine whether the bits correspond to parities of some hidden bipartition, or are just uniformly random.
Unlike all previous Fourier analytic communication lower bounds, our analysis does not directly use bounds on the $\ell_2$ norm of Fourier coefficients of a typical message at any given weight level that follow from hypercontractivity. Instead, we use the fact that graphs received by players are sparse (matchings) to obtain strong upper bounds on the $\ell_1$ norm of the Fourier coefficients of the messages of individual players using their special structure, and then argue, using the convolution theorem, that similar strong bounds on the $\ell_1$ norm are essentially preserved (up to an exponential loss in the number of players) once messages of different players are combined. We feel that our main technique is likely of independent interest.

References
1. Michael Kapralov, Sanjeev Khanna, Madhu Sudan, Anayya Velingker: $(1 + \Omega(1))$-Approximation to MAX-CUT Requires Linear Space. SODA 2017: 1703-1722

3.13 Improved soundness for proving proximity to Reed-Solomon codes

Swastik Kopparty (Rutgers University – Piscataway, US)

License Creative Commons BY 3.0 Unported license
© Swastik Kopparty

Joint work of Eli Ben-Sasson, Lior Goldberg, Swastik Kopparty, Shubhangi Saraf


Given oracle access to some string $w$, we would like to verify (using few queries, with the aid of an interactive prover), that $w$ is a codeword of the Reed-Solomon code. An ingenious FFT-based protocol called FRI (Fast Reed-Solomon IOPP) was recently given by [1]. Follow-up work of [2] showed that FRI rejects any $w$ that is very far from the Reed-Solomon code with quite large probability.

We give an improved analysis for the soundness of FRI, and show that this is tight.

We then give a new protocol called *DEEP-FRI* which has both (a) a better name, and (b) further improved (and possibly optimal) soundness for this problem.

The list-decodability of Reed-Solomon codes plays an important role in these results.

References
3.14 Stronger Lower Bounds for Online ORAM

Michal Koucký (Charles University – Prague, CZ)

Oblivious RAM (ORAM), introduced in the context of software protection by Goldreich and Ostrovsky [1], aims at obfuscating the memory access pattern induced by a RAM computation. Ideally, the memory access pattern of an ORAM should be independent of the data being processed. Since the work of Goldreich and Ostrovsky, it was believed that there is an inherent \( \Omega(\log n) \) bandwidth overhead in any ORAM working with memory of size \( n \).

Larsen and Nielsen [2] were the first to give a general \( \Omega(\log n) \) lower bound for any online ORAM, i.e., an ORAM that must process its inputs in an online manner.

In this work, we revisit the lower bound of Larsen and Nielsen, which was proved under the assumption that the adversarial server knows exactly which server accesses correspond to which input operation. We give a \( \Omega(\log n) \) lower bound for the bandwidth overhead of any online ORAM even when the adversary has no access to this information. For many known constructions of ORAM this information is provided implicitly as each input operation induces an access sequence of roughly the same length. Thus, they are subject to the lower bound of Larsen and Nielsen. Our results rule out a broader class of constructions and specifically, they imply that obfuscating the boundaries between the input operations does not help in building a more efficient ORAM.

As our main technical contribution and to handle the lack of structure, we study the properties of access graphs induced naturally by the memory access pattern of an ORAM computation. We identify a particular graph property that can be efficiently tested and that all access graphs of ORAM computation must satisfy with high probability. This property is reminiscent of the Larsen-Nielsen property but it is substantially less structured; that is, it is more generic.

References
2 Kasper Green Larsen, Jesper Buus Nielsen: Yes, There is an Oblivious RAM Lower Bound! CRYPTO (2) 2018: 523-542

3.15 Improving OBDD-Attacks and Related Complexity-Theoretic Problems

Matthias Krause (Universität Mannheim, DE)

We present and discuss new algorithmic ideas for improving OBDD-attacks against stream ciphers. Standard OBDD-attacks compute the secret initial state behind a given piece of keystream by generating a sequence \( Q_1, Q_2, \ldots, Q_s \) of ordered binary decision diagrams.
(OBDDs), where $Q_1$ is small, the intermediate OBDDs become not larger than $2^{(1-a)/(1+a)n}$, and $Q_s$ contains the secret initial state behind $z$ as only satisfying assignment. Here, $n$ denotes the inner state length of the cipher, and $a \in (0,1)$ the compression rate, a constant defined by the cipher. The motivation of our research is to circumvent the bottleneck of standard OBDDs attack consisting in the huge storage of $2^{(1-a)/(1+a)n}$ needed for some of the intermediate OBDDs.

For reaching this goal we propose the following strategy

1. Generate in parallel two OBDDs $P$ and $Q$ of moderate size such that $P$ and $Q$ have only a few common satisfying assignments.
2. Compute these satisfying assignments, including the secret inner state, by a new breadth-first-search based algorithm.

We show at hand of experiments that this approach improves standard OBDD-attacks drastically. For understanding the theory behind this phenomenon we study in a first step the complexity of the Bounded Synthesis Problem (given two OBDDs $P$ and $Q$ for which it is known that they have only one common satisfying assignment, compute this assignment).

The question to discuss here is if there are algorithms for the Bounded Synthesis Problem which are asymptotically better than synthising and minimizing $P \land Q$.

### 3.16 Building strategies into QBF proofs

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

License © Creative Commons BY 3.0 Unported license

Joint work of Olaf Beyersdorff, Joshua Blinkhorn, Meena Mahajan


URL http://dx.doi.org/10.4230/LIPIcs.STACS.2019.14

Quantified Boolean Formulas (QBF) are a natural extension of the SAT problem, with more sophisticated semantics: functions witnessing the truth of a QBF can be interpreted as strategies in a two-player game. A lot has been written regarding the extraction of strategies from QBF proofs, in various proof systems. Here we devise a new system – Merge Resolution – in which strategies are built explicitly within the proofs themselves. We investigate some advantages of Merge Resolution over existing systems; in particular, we find that it lifts naturally to DQBF, a further extension of QBF.

Joint work with Olaf Beyersdorff and Joshua Blinkhorn. STACS 2019.
3.17 Exponential Lower Bounds for Weak Pigeonhole Principle and Perfect Matching Formulas over Sparse Graphs

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

We show exponential lower bounds on resolution proof length for pigeonhole principle (PHP) formulas and perfect matching formulas over highly unbalanced, sparse expander graphs, thus answering the challenge to establish strong lower bounds in the regime between balanced constant-degree expanders as in [1] and highly unbalanced, dense graphs as in [2], [3], and [4]. We obtain our results by revisiting Razborov’s pseudo-width method for PHP formulas over dense graphs and extending it to sparse graphs. This further demonstrates the power of the pseudo-width method, and we believe it could potentially be useful for attacking also other longstanding open problems for resolution and other proof systems.

This is joint work with Susanna F. de Rezende, Kilian Risse, and Dmitry Sokolov.

References

3.18 Extractors for small zero-fixing sources

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

A random variable $X$ is an $(n, k)$-zero-fixing source if for some subset $V \subset [n]$, $X$ is the uniform distribution on the strings $\{0, 1\}^n$ that are zero on every coordinate outside of $V$. An $\epsilon$-extractor for $(n, k)$-zero-fixing sources is a mapping $F: \{0, 1\}^n \to \{0, 1\}^m$, for some $m$, such that $F(X)$ is $\epsilon$-close in statistical distance to the uniform distribution on $\{0, 1\}^m$ for every $(n, k)$-zero-fixing source $X$. Zero-fixing sources were introduced by Cohen and Shinkar in [1] in connection with the previously studied extractors for bit-fixing sources. They constructed, for every $\mu > 0$, an efficiently computable extractor that extracts a positive fraction of entropy, i.e., $\Omega(k)$ bits, from $(n, k)$-zero-fixing sources where $k \geq (\log \log n)^{2+\mu}$.

We have found two different constructions of extractors for zero-fixing sources that are able to extract a positive fraction of entropy for $k$ essentially smaller than $\log \log n$. The first extractor works for $k \geq C \log \log \log n$, for some constant $C$. The second extractor extracts a positive fraction of entropy for $k \geq \log^{(i)} n$ for any fixed $i \in \mathbb{N}$, where $\log^{(i)}$ denotes $i$-times iterated logarithm. The fraction of extracted entropy decreases with $i$. The first extractor
is a function computable in polynomial time in \( \sim n \) (for \( \epsilon = o(1) \), but not too small); the second one is computable in polynomial time when \( k \leq \alpha \log \log n / \log \log \log n \), where \( \alpha \) is a positive constant.

In the talk we sketch the main idea of the first construction.
Joint work with Vojtech Rodl.

References

3.19 Majority Quantifiers, Complexity Classes and Games

Rüdiger Reischuk (Universität zu Lübeck, DE)

An overview is given on logical/syntactical descriptions of complexity classes based on quantifiers. Existential and universal quantifiers together with predicates in \( \mathbf{P} \) suffice to characterize the polynomial hierarchy, \( \mathbf{PSPACE} \) and 2 person full information games. Zachos and coauthors have investigated probabilistic quantifiers and shown that a pair of sequences of quantifiers can be used to characterize the classical probabilistic complexity classes and 2 person games involving randomness – Arthur Merlin games. We discuss technical tools to prove relations between these complexity classes based on such characterizations and to investigate hierarchies built on quantifier sequences. The essential technique here is swapping of quantifiers.

3.20 Computational Two Party Correlation

Ronen Shaltiel (University of Haifa, IL)

Let \( \pi \) be an efficient two-party protocol that (given security parameter \( \kappa \)) both parties output single bits \( X_\kappa \) and \( Y_\kappa \), respectively. We are interested in how \( (X_\kappa, Y_\kappa) \) “appears” to an efficient adversary that only views the transcript \( T_\kappa \). We make the following contributions:

- We develop new tools to argue about this loose notion, and show (modulo some caveats) that for every such protocol \( \pi \), there exists an efficient simulator such that the following holds: on input \( T_\kappa \), the simulator outputs a pair \( (X'_\kappa, Y'_\kappa) \) such that \( (X'_\kappa, Y'_\kappa, T_\kappa) \) is (somewhat) computationally indistinguishable from \( (X_\kappa, Y_\kappa, T_\kappa) \).
- We use these tools to prove the following dichotomy theorem: every such protocol \( \pi \) is:
  - either uncorrelated – it is (somewhat) indistinguishable from an efficient protocol whose parties interact to produce \( T_\kappa \), but then choose their outputs independently from some product distribution (that is determined in poly-time from \( T_\kappa \)),
  - or, the protocol implies a key-agreement protocol (for infinitely many \( \kappa \)'s).
Uncorrelated protocols are uninteresting from a cryptographic viewpoint, as the correlation between outputs is (computationally) trivial. Our dichotomy shows that every protocol is either completely uninteresting or implies key-agreement.

3.21 Near-Optimal Erasure List-Decodable Codes

Amnon Ta-Shma (Tel Aviv University, IL)

A code \( C \) is \((1 - \tau, L)\) erasure list-decodable if for every word \( w \), after erasing any \( 1 - \tau \) fraction of the symbols of \( w \), the remaining \( \tau \)-fraction of its symbols have at most \( L \) possible completions into codewords of \( C \).

Non-explicitly, there exist binary \((1 - \tau, L)\) erasure list-decodable codes having rate \( O(\tau) \) and tiny list-size \( L = O(\log 1/\tau) \). Achieving either of these parameters explicitly is a natural open problem (see, e.g., [5],[3],[4]). While partial progress on the problem has been achieved, no prior explicit construction achieved rate better than \( \Omega(\tau^2) \) or list-size smaller than \( \Omega(1/\tau) \).

Furthermore, Guruswami showed no linear code can have list-size smaller than \( \Omega(1/\tau) \) [3]. We construct an explicit binary \((1 - \tau, L)\) erasure list-decodable code having rate \( \tau^{1+\gamma} \) (for any constant \( \gamma > 0 \) and small \( \tau \) and list-size \( \text{poly}(\log 1/\tau) \), answering simultaneously both questions, and exhibiting an explicit non-linear code that provably beats the best possible linear code.

The binary erasure list-decoding problem is equivalent to the construction of explicit, low-error, strong dispersers outputting one bit with minimal entropy-loss and seed-length. For error \( \epsilon \), no prior explicit construction achieved seed-length better than \( 2\log 1/\epsilon \) or entropy-loss smaller than \( 2\log 1/\epsilon \), which are the best possible parameters for extractors. We explicitly construct an \( \epsilon \)-error one-bit strong disperser with near-optimal seed-length \( (1 + \gamma)\log 1/\epsilon \) and entropy-loss \( O(\log \log 1/\epsilon) \).

The main ingredient in our construction is a new (and almost-optimal) unbalanced two-source extractor. The extractor extracts one bit with constant error from two independent sources, where one source has length \( n \) and tiny min-entropy \( O(\log \log n) \) and the other source has length \( O(\log n) \) and arbitrarily small constant min-entropy rate. When instantiated as a balanced two-source extractor, it improves upon Raz’s extractor [7] in the constant error regime. The construction incorporates recent components and ideas from extractor theory with a delicate and novel analysis needed in order to solve dependency and error issues that prevented previous papers (such as [6],[1],[2]) from achieving the above results.

References
In their seminal paper, Bennett, Bernstein, Brassard, and Vazirani [2] showed that relative to an oracle, quantum algorithms are unable to solve \( \text{NP} \)-complete problems in sub-exponential time (i.e., that Grover’s search is optimal in this setting).

In this work, we show a strong converse to their result. Namely, we show that, relative to an oracle, there exist computational tasks that can be solved efficiently by a quantum algorithm but require exponential time for any algorithm in the polynomial hierarchy (that captures \( \text{P} \), \( \text{NP} \), and \( \text{co-NP} \) as its first levels).

The tasks that exhibit this “quantum advantage” arise from a pseudo-randomness approach initiated by Aaronson [1]. Our core technical result is constructing a distribution over Boolean strings that “look random” to constant-depth circuits of quasi-polynomial size, but can be distinguished from the uniform distribution by very efficient quantum algorithms.

References

1. Scott Aaronson: \( \text{BQP and the polynomial hierarchy} \). STOC 2010: 141-150

3.23 Different methods to isolate a perfect matching in bipartite graphs

Thomas Thierauf (Hochschule Aalen, DE)

We give different proofs of our result that the perfect matching problem for bipartite is in \( \text{quasi-NC} \). In particular, we present three different ways how to construct a weight function that isolates the minimum weight perfect matching. Each method yields different parameters for the size of the weights. We think that is interesting to see different methods because still it is an open problem to improve our result to \( \text{NC} \).
3.24 Lower Bounds for Matrix Factorization

Ben Lee Volk (Caltech – Pasadena, US)

License Creative Commons BY 3.0 Unported license
© Ben Lee Volk
Joint work of Mrinal Kumar, Ben Lee Volk

We consider the problem of constructing explicit matrices which cannot be expressed as a product of a few sparse matrices. In addition to being a natural mathematical question, this problem appears in various areas in computer science, such as algebraic complexity, data structures, and machine learning.

We outline an approach for proving improved lower bounds through a certain derandomization problem, and use this approach to prove asymptotically optimal quadratic lower bounds for natural special cases, which generalize many of the common matrix decompositions.

We then discuss some open problems related to this approach.

3.25 Oblivious Lower Bounds for Near-Neighbor Search

Omri Weinstein (Columbia University – New York, US)

License Creative Commons BY 3.0 Unported license
© Omri Weinstein
Joint work of Kasper Green Larsen, Tal Malkin, Omri Weinstein, Kevin Yeo

We prove an $\Omega(d \log n / (\log \log n)^2)$ lower bound on the dynamic cell-probe complexity of statistically oblivious approximate-near-neighbor search (ANN) over the $d$-dimensional Hamming cube. For the natural setting of $d = \Theta(\log n)$, our result implies an $\tilde{\Omega}(\log^2 n)$ lower bound, which is a quadratic improvement over the highest (non-oblivious) cell-probe lower bound for ANN. This is the first super-logarithmic unconditional lower bound for ANN against general (non black-box) data structures. We also show that any oblivious static data structure for decomposable search problems (like ANN) can be obliviously dynamized with $O(\log n)$ overhead in update and query time, strengthening a classic result of Bentley and Saxe ([1]).

References
Participants

- Eric Allender
  Rutgers University – Piscataway, US
- Paul Beame
  University of Washington – Seattle, US
- Harry Buhrman
  CWI – Amsterdam, NL
- Igor Carboni Oliveira
  University of Oxford, GB
- Katrin Casel
  Hasso-Plattner-Institut – Potsdam, DE
- Amit Chakrabarti
  Dartmouth College – Hanover, US
- Sourav Chakraborty
  Indian Statistical Institute – Kolkata, IN
- Arkadev Chattopadhyay
  TIFR – Mumbai, IN
- Gil Cohen
  Princeton University, US
- Anindya De
  University of Pennsylvania – Philadelphia, US
- Lukáš Folwarczný
  Charles University – Prague, CZ
- Lance Fortnow
  Georgia Institute of Technology – Atlanta, US
- Anna Gál
  University of Texas – Austin, US
- Alexander Golovnev
  Harvard University – Cambridge, US
- Kristoffer Arnsfelt Hansen
  Aarhus University, DK
- Prabhakar Harsha
  TIFR – Mumbai, IN
- Johan Hastad
  KTH Royal Institute of Technology, SE
- Valentine Kabanets
  Simon Fraser University – Burnaby, CA
- Michael Kapralov
  EPFL – Lausanne, CH
- Mathew Katzman
  University of Oxford, GB
- Antonina Kolokolova
  Memorial University of Newfoundland – St. John’s, CA
- Swastik Kopparty
  Rutgers University – Piscataway, US
- Michal Koucký
  Charles University – Prague, CZ
- Matthias Krause
  Universität Mannheim, DE
- Meena Mahajan
  Institute of Mathematical Sciences – Chennai, IN
- Or Meir
  University of Haifa, IL
- 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
- Rüdiger Reischuk
  Universität zu Lübeck, DE
- Michael E. Saks
  Rutgers University – Piscataway, US
- Rahul Santhanam
  University of Oxford, GB
- Or Meir
  University of Haifa, IL
- Amnon Ta-Shma
  Tel Aviv University, IL
- Thomas Thierauf
  Hochschule Aalen, DE
- Jacobo Torán
  Universität Ulm, DE
- Ben Lee Volk
  Caltech – Pasadena, US
- Omri Weinstein
  Columbia University – New York, US