Report from Dagstuhl Seminar 14121

Computational Complexity of Discrete Problems

Edited by

Anna Gal[1], Michal Koucký[2], Oded Regev[3], and Rüdiger Reischuk[4]

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

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 14121 "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 chronological order. The last section contains the abstracts of the talks.

Seminar March 16–21, 2014 – http://www.dagstuhl.de/14121
1998 ACM Subject Classification F.1.3 Complexity Measures and Classes, F.2 Analysis of Algorithms and Problem Complexity
Keywords and phrases discrete problems, computational complexity, Turing machines, Boolean circuits, arithmetic circuits, quantum computing, communication complexity, pseudorandomness, derandomization, approximation, data streams
Digital Object Identifier 10.4230/DagRep.4.3.62
Edited in cooperation with Omri Weinstein

1 Executive Summary

Anna Gal
Michal Koucký
Oded Regev
Rüdiger Reischuk

Introduction and goals

Computational complexity aims to answer what is efficiently solvable and what is not on various computational models. This means providing upper and lower bounds on the necessary resources such as time, space or communication, and establishing connections among the different models.

There are intricate connections between complexity measures in different computational models. For instance, circuit size is closely related to computation time, whereas circuit depth and branching program size are closely related to computation space. Breaking the current barriers of our understanding in any of these models would have major consequences in several of the other models as well.

Investigating the connections between the various computational models and subareas of computational complexity has already led to many exciting results. In recent years several novel techniques have been introduced in computational complexity, resulting in a number

Computational Complexity of Discrete Problems, *Dagstuhl Reports*, Vol. 4, Issue 3, pp. 62–84
Editors: Anna Gal, Michal Koucký, Oded Regev, and Rüdiger Reischuk
Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

of breakthroughs, some of which are still actively investigated. In particular, information-theoretic techniques have led to tremendous progress in our understanding of communication complexity, such as new methods to compress interactive communication, very efficient ways to immunize protocols against corruption of the communication by an adversary, and a better understanding of so-called direct product questions. This progress in turn led to progress in our understanding of the streaming model, in which one needs to process massive amounts of received data without being able to store it. Semi-definite programming, a technique originally used in optimization and in the design of approximation algorithms, has led to a tight and very elegant characterization of quantum query complexity. In the area of hardness of approximation, new approaches to prove the Unique Game Conjecture (which is one of the most central open questions in the area) have been suggested. Finally, a recent breakthrough separation of the class NEXP (nondeterministic exponential time) from the class ACC^0 (bounded depth circuits with counting) rests on a new technique that derives a lower bound for a non-uniform model from an upper bound on satisfiability in the uniform setting; this technique opens up a new range of possible connections between uniform and non-uniform models.

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. A salient 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. By organizing a generic seminar on computational complexity we have aimed to attract researchers from those various subareas and foster further fruitful interactions.

Organization of the meeting

43 researches from around the world participated in the seminar including a substantial number of young researchers. Each day, Monday to Thursday, we started by a longer talk surveying recent results in specific areas that were chosen beforehand. We had the following survey talks:

- Shubhangi Saraf: Recent developments in arithmetic circuits
- Subhash Khot: On the unique games conjecture and the approximation resistance of predicates.
- Mark Braverman: Recent progress on interactive error correction: an overview.
- Ankur Moitra: Extended formulations and information complexity.

Additionally, on Friday we started with a survey on recent progress in algorithms for matrix multiplication presented by Chris Umans. The tutorials were followed by shorter talks by other participants. Afternoons were reserved for discussions in impromptu groups. In late afternoon on Monday, Tuesday and Thursday we had several additional short talks. On Wednesday evening we organized a rump session where everyone could present an open problem or announce a new result. One of the open problems from this session on the relationship between information cost and communication complexity presented by Omri Weinstein was very recently resolved.

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.

Circuit complexity

One of the goals in circuit complexity is to prove strong lower bounds on the size of circuits computing explicit functions. Even in the case of bounded depth circuits the known lower bounds deteriorate quickly with depth. Oded Goldreich discussed approaches to prove strong lower bounds of almost the type $2^{\Omega(n)}$ in such a setting by focusing on certain kinds of multilinear functions.

Another approach to proving lower bounds was presented by Anup Rao, who showed new lower bounds for bounded-depth circuits with arbitrary gates when the fan-in of gates is strictly smaller than n.

Valentine Kabanets considered the interplay between Boolean formulas and harmonic analysis of functions computed by Boolean formulas. He showed that functions represented by sub-quadratic formulas over the basis AND, OR and NOT have constrained Fourier coefficients. Among other things, this fact leads to new learning algorithms for such functions.

Shubhangi Saraf reviewed recent progress towards separating Valiant's classes VP and VNP, the arithmetic analogues of P and NP.

Eric Allender in his talk focused on another aspect of circuit complexity by providing improved upper bounds on the level of counting hierarchy in which certain problems involving arithmetic circuits lie.

Beside proving lower bounds several talks also focused on algorithmic aspects of circuits. Kristoffer Arnsfelt Hansen discussed the circuit complexity of several graph problems when the graphs have bounded cut-width, and Swastik Kopparty showed in his talk an efficient way of indexing irreducible polynomials over finite fields which may serve as a useful tool in designing efficient arithmetic circuits.

Amir Yehudayoff studied the growth rate of symmetric polynomials with possible applications in pseudorandomness.

Communication complexity and its applications

The classical theory of error correcting codes addresses mainly the question of one-way communication over unreliable channel. In communication complexity the main issue is to minimize the amount of communication between two interacting parties whose goal is to evaluate some joint function of their respective inputs. In this scenario the communication goes both ways. Mark Braverman gave a summary of results on error correcting techniques when the two parties communicate over unreliable channel.

Pavel Pudlák presented approaches to constructing good error correcting codes for interactive communication (so-called tree codes) based on properties of certain matrices.

Another popular research topic in communication complexity is information complexity. This topic was discussed by Omri Weinstein. He showed a new technique to estimate interactively the amount of information leaked by the two players about their inputs during a two party communication. This might have applications for secure communication.

Hartmut Klauck presented an interplay between quantum and classical communication, and established that in certain setting quantum communication can be replaced by classical messages.

Mike Saks provided a surprisingly simple protocol for certain class of functions in the number-on-the-forehead multi-party model.

Ankur Moitra presented a survey on recent results regarding extended formulation approach to solving hard combinatorial problems. In this context he also successfully applied techniques from communication complexity.

Communication complexity is a major tool in the analysis of data stream algorithms, algorithms that can process huge data sets while utilizing only little memory. David Woodruff presented a surprising fundamental result showing that a large class of streaming algorithms can be simulated using only linear sketches of the data stream. This could simplify design of data stream algorithms.

Amit Chakrabarti considered a model for processing large data streams with the help of an untrusted but powerful helper (e.g. cloud service). He discussed a relationship between this model and Arthur Merlin communication protocols.

Inapproximability

When we lack efficient algorithms for various problems that are NP-complete we may try to solve them approximately. In some cases, even that is hard as demonstrated by Prahladh Harsha in his talk on inapproximability of coloring of hypergraphs.

On the other hand, Johan Håstad presented a new algorithm for finding a satisfying solution to a CNF formula when all clauses in the formula can simultaneously be satisfied by majority of their literals. When the formula does not have such a property the problem becomes NP-complete.

Irit Dinur discussed her results on testing whether a given function is a direct product of some function with application to parallel repetition, and Eli Ben-Sasson explained his result on constructing linear-size probabilistically checkable proofs (PCP) that can be checked using n^ϵ queries.

Pseudorandomness

Construction of pseudorandom generators for Boolean circuits is currently reasonably well understood. However, in non-Boolean setting such as in the case of multi-output functions or arithmetic circuits we still lack good understanding of the problem. Ronen Shaltiel presented pseudorandom generators with optimal seed length for multi-output functions computed by polynomial size circuits, and Amnon Ta-Shma presented a new construction of hitting set generators for low-degree polynomials.

A central problem for which we know a very efficient randomized algorithm but no deterministic one is the problem of testing whether a polynomial is identically zero. Meena Mahajan considered the problem of testing whether a polynomial represented by an arithmetic formula that reads each variable at most three times is zero or not. She provided a deterministic algorithm for this problem.

Amir Shpilka presented a new algorithm for the closely related problem of testing whether two polynomials are the same up to a linear transformation of variables.

Other models

Harry Buhrman presented a new model of computation, catalytic space, in which in addition to the usual limited work space we have essentially unlimited amount of extra space which is however full of data that have to be preserved. He exhibited the surprising power of this extra space that allows one to compute functions that we do not know how to compute using only the limited work space.

Matthias Krause discussed the issue of cryptographic authentication by devices with limited resources which are not able to evaluate the standard cryptographic primitives like RSA and AES. He proposed solutions for those situations and reported on an actual implementation.

Jaikumar Radhakrishnan considered the bit-probe complexity of a data structure for storing sets (set-membership problem). He presented a very elegant and more efficient solution for this problem.

Thomas Thierauf presented an algorithm to compute the number of perfect matchings in K_5-free graphs. In general graphs this problem is considered to be hard.

Till Tantau talked about parallel algorithms in the context of fixed parameter tractability. He defined the notion and presented parallel algorithms in that context.

Chris Umans presented an overview of recent progress on matrix multiplication.

Conclusion

Understanding the computational complexity of various problems is the primary goal of theory of computing. In the past several years there has be tremendous progress in various areas of complexity for example, in communication complexity, arithmetic circuit complexity and derandomization. This progress brings us closer to the goal of understanding computation. Yet, as we have seen new relevant concepts and models emerge, e.g., information cost and catalytic computation. Despite all the progress that have been achieved since our previous meeting three years ago, and in the light of the new developments, there is a general consensus among the participants of the seminar that there is still long way ahead of us before we gain a good understanding of limits of efficient computation and resolve many of the central problems in computational complexity.

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.

2 Table of Contents

3 Overview of Talks

3.1 Small circuits and big numbers; Better bounds on computing the bits of arithmetic circuits

Eric Allender (Rutgers University – Piscataway, US)

Joint work of Allender, Eric; Balaji, Nikhil; Datta, Samir
Main reference E. Allender, N. Balaji, S. Datta, "Low-depth Uniform Threshold Circuits and the Bit-Complexity of Straight Line Programs," ECCC TR13-177, 2013.
URL http://eccc.hpi-web.de/report/2013/177/

Earlier work had shown that, given an arithmetic circuit C and a number i, the problem of computing the i-th bit of the number represented by C lies in the counting hierarchy – *way up* in the counting hierarchy. We knock one level off of that bound, and show that several other problems lie in the same level. The talk won't focus on the details, which can be found in [ECCC TR13-177]. Instead, the talk will present lots of intriguing open questions, and will also attempt to explain why it is interesting to consider the complexity of problems that deal with computing the bits of very big numbers.

3.2 Constant rate PCPs for circuit-SAT with sublinear query complexity

Eli Ben-Sasson (Technion – Haifa, IL)

Joint work of Ben-Sasson, Eli; Kaplan, Yohay; Kopparty, Swastik; Meir, Or; Stichtenoth, Henning
Main reference E. Ben-Sasson, Y. Kaplan, S. Kopparty, O. Meir, H. Stichtenoth, "Constant Rate PCPs for Circuit-SAT with Sublinear Query Complexity," in Proc. of the 54th Annual IEEE Symp. on Foundations of Computer Science (FOCS'13), pp. 320–329, IEEE CS, 2013.
URL http://dx.doi.org/10.1109/FOCS.2013.42

The PCP theorem (Arora et. al., J. ACM 45(1,3)) says that every NP-proof can be encoded to another proof, namely, a probabilistically checkable proof (PCP), which can be tested by a verifier that queries only a small part of the PCP. A natural question is how large is the blow-up incurred by this encoding, i.e., how long is the PCP compared to the original NP-proof. The state-of-the-art work of Ben-Sasson and Sudan (SICOMP 38(2)) and Dinur (J. ACM 54(3)) shows that one can encode proofs of length n by PCPs of length $n \log^{O(1)} n$ that can be verified using a constant number of queries. In this work, we show that if the query complexity is relaxed to n, then one can construct PCPs of length $O(n)$ for circuit-SAT, and PCPs of length $O(t \log t)$ for any language in NTIME(t).

More specifically, for any $\epsilon > 0$ we present (non-uniform) probabilistically checkable proofs (PCPs) of length $2^{O(1/\epsilon)}n$ that can be checked using n^ϵ queries for circuit-SAT instances of size n. Our PCPs have perfect completeness and constant soundness. This is the first constant-rate PCP construction that achieves constant soundness with nontrivial query complexity ($o(n)$).

Our proof replaces the low-degree polynomials in algebraic PCP constructions with tensors of transitive algebraic geometry (AG) codes. We show that the automorphisms of an AG code can be used to simulate the role of affine transformations which are crucial in earlier high-rate algebraic PCP constructions. Using this observation we conclude that any asymptotically good family of transitive AG codes over a constant-sized alphabet leads to a family of constant-rate PCPs with polynomially small query complexity. Such codes are constructed in the appendix to this paper for the first time for every message length, after they have been constructed for infinitely many message lengths by Stichtenoth [Trans. Information Theory 2006].

3.3 Recent progress on interactive error correction: an overview

Mark Braverman (Princeton University, US)

Classical error-correcting codes deal with the problem of data transmission over a noisy channel. There are efficient error-correcting codes that work even when the noise is adversarial. In the interactive setting, the goal is to protect an entire conversation between two (or more) parties from adversarial errors. The area of interactive error correcting codes has experienced a substantial amount of activity in the last few years. In this talk we will introduce the problem of interactive error-correction and discuss some of the recent exciting progress towards its resolution.

3.4 Catalytic space

Harry Buhrman (CWI – Amsterdam, NL)

Joint work of Buhrman, Harry; Cleve, Richard; Koucký, Michal; Loff, Bruno; Speelman, Florian

We define the notion of a *catalytic-space* computation. This is a computation that has a small amount of clean space available and is equipped with additional auxiliary space, with the caveat that the additional space is initially in an arbitrary, possibly incompressible, state and must be returned to this state when the computation is finished. We show that the extra space can be used in a nontrivial way, to compute uniform $TC1$-circuits with just a logarithmic amount of clean space. The extra space thus works analogously to a catalyst in a chemical reaction. $TC1$- circuits can compute for example the determinant of a matrix, which is not known to be computable in logspace.

In order to obtain our results we study an algebraic model of computation, a variant of straight-line programs. We employ register machines with input registers $x_1, \ldots, x_n$ and work registers $r_1, \ldots, r_m$. The instructions available are of the form $r_i := r_i \pm u \cdot v$, with u, v registers (distinct from r_i) or constants. We wish to compute a function $f(x_1, \ldots, x_n)$ through a sequence of such instructions. The working registers have some arbitrary initial value $r_i = t_i$, and they may be altered throughout the computation, but by the end all registers must be returned to their initial value t_i, except for, say, r_1 which must hold $t_1 + f(x_1, \ldots, x_n)$. We show that all of Valiant's class VP, and more, can be computed in this model. This significantly extends the framework and techniques of Ben-Or and Cleve.

Upper bounding the power of catalytic computation we show that catalytic logspace is contained in ZPP. We further construct an oracle world where catalytic logpace is equal to PSPACE, and show that under the exponential time hypothesis (ETH), SAT can not be computed in catalytic sub-linear space.

3.5 Arthur, Merlin, and data stream computation

Amit Chakrabarti (Dartmouth College – Hanover, US)

Joint work of Chakrabarti, Amit; Cormode, Graham; McGregor, Andrew; Thaler, Justin; Venkatasubramanian, Suresh
Main reference A. Chakrabarti, G. Cormode, A. McGregor, J. Thaler, "Annotations in Data Streams," ECCC TR12-022, 2012.
URL http://eccc.hpi-web.de/report/2012/022/

A series of recent works have developed a theory of computation wherein a space-limited algorithm tasked with answering questions about a massive data stream gets to interact with a powerful space-unbounded helper, thereby expanding its computational power. The streaming verifier is unwilling to blindly trust answers returned by the helper. How can we design a suitable protocol that allows the helper to not just supply an answer to the verifier but convince her that the answer is correct?

We shall describe a few of the most important algorithms in this model developed to date. We shall see that for several well-studied data stream problems, access to the helper results in significant space savings for the verifier: sometimes quadratic, sometimes even exponential.

We shall then turn to lower bounds in this model, which will naturally lead us to Arthur-Merlin communication complexity. Our work gives a number of new results about this kind of communication. In particular, we bring out the importance of the amount of interactivity between Arthur and Merlin.

3.6 Direct product testing

Irit Dinur (Weizmann Institute, IL)

Joint work of Dinur, Irit; Steurer, David
Main reference I. Dinur, D. Steurer, "Direct Product Testing," in Proc. of the 2014 IEEE Conf. on Computational Complexity (CCC'14), to appear; pre-print available as ECCC TR13-179 (2013).
URL http://eccc.hpi-web.de/report/2013/179/

The k-fold direct product of a function $f : [n] \to \{0,1\}$ is a new function that gives the local evaluation of the original function on all k-windows; $F : [n]^k \to \{0,1\}^k$ defined by $F(x_1, ..., x_k) = (f(x_1), ..., f(x_k))$. The direct product testing question is to test whether a given function F is (close to) an honest direct product. The test is simple: choose two local windows that intersect, and check consistency on the intersection. Surprisingly, the analysis is very tricky.

Proving that this test works entails lifting locally-consistent substrings to a globally consistent one. We prove that such lifting works in a comprehensive parameter setting, allowing non-trivial lifting already when the local consistency is above the minimum threshold of $exp(-k)$.

We also discuss connections of this question to parallel repetition through the "confuse and compare" game.

3.7 Boolean circuits of depth three and arithmetic circuits with arbitrary gates

Oded Goldreich (Weizmann Institute, IL)

Joint work of Goldreich, Oded; Wigderson, Avi
Main reference O. Goldreich, A. Wigderson, "On the Size of Depth-Three Boolean Circuits for Computing Multilinear Functions," ECCC TR13-043, 2013.
URL http://eccc-preview.hpi-web.de/report/2013/043/

This paper introduces and initiates a study of a new model of arithmetic circuits coupled with new complexity measures. The new model consists of multilinear circuits *with arbitrary multilinear gates*, rather than the standard multilinear circuits that use only addition and multiplication gates. In light of this generalization, the *arity of gates* becomes of crucial importance and is indeed one of our complexity measures. Our second complexity measure is the *number of gates* in the circuit, which (in our context) is significantly different from the number of wires in the circuit (which is typically used as a measure of size). Our main *complexity measure*, denoted C, is the maximum of these two measures (i.e., the maximum between the arity of the gates and the number of gates in the circuit). We also consider the depth of such circuits, focusing on depth-two and unbounded depth.

Our initial motivation for the study of this arithmetic model is the fact that the two main variants (i.e., depth-two and unbounded depth) yield natural classes of depth-three Boolean circuits for computing multi-linear functions. The resulting circuits have size that is exponential in the new complexity measure. Hence, lower bounds on the new complexity measure yield lower bounds on a restricted class of depth-three Boolean circuits (for computing multi-linear functions). Such lower bounds are a sanity check for our conjecture that multilinear functions of relatively low degree over $GF(2)$ are good candidates for obtaining exponential lower bounds on the size of constant-depth Boolean circuits (computing explicit functions). Specifically, we propose to move gradually from linear functions to multilinear ones, and conjecture that, for any $t \geq 2$, some explicit t-linear functions $F : (\{0,1\}^n)^t \to \{0,1\}$ require depth-three circuits of size $\exp(\Omega(tn^{t/(t+1)}))$.

Letting C_2 denote the complexity measure C, when minimized over all depth-two circuits of the above type, our main results are as follows.

1. For every t-linear function F, it holds that $C(F) \leq C_2(F) = O((tn)^{t/(t+1)})$.
2. For almost all t-linear function F, it holds that $C_2(F) \geq C(F) = \Omega((tn)^{t/(t+1)})$.
3. There exists a bilinear function F such that $C(F) = O(\sqrt{n})$ but $C_2(F) = \Omega(n^{2/3})$.

The main open problem posed in this paper is proving a result analogous to (2) for an explicit function F. For starters, we seek lower bound of $\Omega((tn)^{0.51})$ for an explicit t-linear function F, preferably for constant t. We outline an approach that reduces this challenge (for $t = 3$) to a question regarding matrix rigidity.

3.8 Circuit complexity of properties of graphs with constant planar cutwidth

Kristoffer Arnsfelt Hansen (Aarhus University, DK)

Joint work of Hansen, Kristoffer Arnsfelt; Komarath, Balagopal; Sarma M. N., Jayalal; Skyum, Sven; Talebanfard, Navid

We study the complexity of several of the classical graph decision problems in the setting of bounded cutwidth and how imposing planarity affects the complexity. We show that for 2-coloring, for bipartite perfect matching, and for several variants of disjoint paths the straightforward NC^1 upper bound may be improved to $\mathsf{AC}^0[2]$, ACC^0, and AC^0 respectively for bounded planar cutwidth graphs. On the other hand we show that 3-coloring and Hamilton cycle remain hard for NC^1, analogous to the NP-completeness for general planar graphs. We also show that 2-coloring and (non-bipartite) perfect matching are hard for certain subclasses of $\mathsf{AC}^0[2]$. In particular this shows that our bounds for 2-coloring are quite close.

3.9 Improved inapproximability results for hypergraph coloring

Prahladh Harsha (TIFR Mumbai, IN)

Joint work of Guruswami, Venkat; Harsha, Prahladh; Håstad, Johan; Srinivasan, Srikanth; Varma, Girish
Main reference V. Guruswami, J. Håstad, P. Harsha, S. Srinivasan, G. Varma, "Super-polylogarithmic hypergraph coloring hardness via low-degree long codes," arXiv:1311.7407v1 [cs.CC], 2013.
URL http://arxiv.org/abs/1311.7407v1

Despite the tremendous progress in understanding the approximability of several problems, the status of approximate coloring of constant colorable (hyper)graphs is not resolved and in fact, there is an exponential (if not doubly exponential) gap between the best known approximation algorithms and inapproximability results. The best known approximation algorithms which are a combination of combinatorial and semi-definite programming methods, require at least n^δ colors to color a 2 colorable 4-uniform hypergraph for some constant delta in (0,1). On the contrary, till recently, the best known hardness results could rule out at best coloring a 2-colorable hypergraph with polylog n colors (if not polyloglog n colors in some cases).

Recently, with the discovery of the low-degree polynomial long code (aka short code of Barak et al [FOCS 2012]), there has been a super-polynomial (and in some cases, exponential) improvement in the inapproximability results. In particular, we prove quasi-NP-hardness of the following problems on n-vertex hypergraphs:

- Coloring a 2-colorable 8-uniform hypergraph with $2^{2^{\sqrt{\log\log n}}}$ colors.
- Coloring a 4-colorable 4-uniform hypergraph with $2^{2^{\sqrt{\log\log n}}}$ colors
- Coloring a 3-colorable 3-uniform hypergraph with $(\log n)^{1/\log\log\log n}$ colors.

These results are obtained using the low-degree polynomial code and the techniques proposed by Dinur and Guruswami [FOCS 2013] to incorporate this code for inapproximability results.

In this talk, I'll explain the bottleneck in obtaining improved coloring inapproximability results using the long code and how derandomizations of the long code (the short code in our setting) can be used to improve the inapproximability factors.

3.10 $(2+\epsilon)$-SAT is NP-hard

Johan Håstad (KTH Royal Institute of Technology, SE)

Main reference P. Austrin, V. Guruswami, J. Håstad, "$(2+\epsilon)$-SAT is NP-hard, ECCC TR13-159, 2013.
URL http://eccc.hpi-web.de/report/2013/159/

We prove the following hardness result for a natural promise variant of the classical CNF-satisfiability problem: Given a CNF-formula where each clause has width w and the guarantee that there exists an assignment satisfying at least $g < w/2$ literals in each clause, it is NP-hard to find a satisfying assignment to the formula (that sets at least one literal to true in each clause). On the other hand, when g is at least $w/2$, it is easy to find a satisfying assignment via simple generalizations of the algorithms for 2-Sat.

3.11 Small de Morgan formulas make low-frequency sound: Fourier concentration from shrinkage

Valentine Kabanets (Simon Fraser University – Burnaby, CA)

Joint work of Impagliazzo, Russell; Kabanets, Valentine
Main reference R. Impagliazzo, V. Kabanets, "Fourier concentration from shrinkage," in Proc. of the 2014 IEEE Conf. on Computational Complexity (CCC'14), to appear.

A standard complexity-theoretic way to measure the complexity of a Boolean function is via the size of a smallest algorithm (circuit or formula) computing (or approximating) the function. Another way to measure the complexity of a function is via the sparsity of its Fourier decomposition, e.g., the concentration of its Fourier mass on some subset of frequencies. The celebrated result of Linial, Mansour, and Nisan (1993) was the first to establish a connection between circuit complexity and Fourier complexity: they showed that the class of Boolean functions computable by polysize AC0 circuits (generalization of CNF/DNFs to arbitrary constant depth) exhibit sharp concentration of the Fourier spectrum over the set of low frequencies (of polylogarithmic weight).

In this talk, I will present analogous results for the class of Boolean functions computable by de Morgan formulas (using AND, OR, and NOT gates) of sub-quadratic size. The Fourier concentration for such functions is over the frequencies related to the *shrinkage exponent*: the quantity measuring how much the formulas reduce in size when hit with random restrictions of the variables. Namely, we show for an n-variate Boolean function f computable by a formula of size s, that the Fourier mass of f over the frequencies higher than $s^{1/\Gamma+\epsilon}$ is at most $exp(-n^{\epsilon/3})$, where Γ is the shrinkage exponent for the corresponding class of formulas: $\Gamma = 2$ for general formulas, and $\Gamma =\approx 3.27$ for read-once formulas. We prove that this Fourier concentration is essentially optimal.

As an application, we get that subquadratic-size formulas have negligible correlation with parity, and are learnable under the uniform distribution, and also lossily compressible, in subexponential time. We also prove tight bounds on the average sensitivity of read-once formulas.

3.12 Two results about quantum messages

Hartmut Klauck (Nanyang TU – Singapore, SG)

Joint work of Klauck, Hartmut; Podder, Supartha
Main reference H. Klauck, S. Podder, "Two Results about Quantum Messages," arXiv:1402.4312v2 [quant-ph], 2014.
URL http://arxiv.org/abs/1402.4312v2

We show two results about the relationship between quantum and classical messages. Our first contribution is to show how to replace a quantum message in a one-way communication protocol by a deterministic message, establishing that for all partial Boolean functions $f : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}$ we have $D^{A\to B}(f) \leq O(Q^{A\to B,*}(f) \cdot m)$. This bound was previously known for total functions, while for partial functions this improves on results by Aaronson, in which either a log-factor on the right hand is present, or the left hand side is $R^{A\to B}(f)$, and in which also no entanglement is allowed.

In our second contribution we investigate the power of quantum proofs over classical proofs. We give the first example of a scenario, where quantum proofs lead to exponential savings in computing a Boolean function. The previously only known separation between the power of quantum and classical proofs is in a setting where the input is also quantum.

We exhibit a partial Boolean function f, such that there is a one-way quantum communication protocol receiving a quantum proof (i.e., a protocol of type QMA) that has cost $O(\log n)$ for f, whereas every one-way quantum protocol for f receiving a classical proof (protocol of type QCMA) requires communication $\Omega(\sqrt{n}/\log n)$.

3.13 Indexing irreducible polynomials over finite fields

Swastik Kopparty (Rutgers University – Piscataway, US)

Joint work of Kopparty, Swastik; Kumar, Mrinal; Saks, Michael

Let S be the set of degree n irreducible polynomials over the finite field F_q. We show that there exists circuits of size $poly(n, \log q)$ which compute a bijection from $\{1, 2, ..., |S|\}$ to S.

3.14 On ultralightweight authentication

Matthias Krause (Universität Mannheim, DE)

In many application areas for ultra-lightweight devices, like passively powered RFIDs, there is a need of authenticity. However, most standard cryptographic algorithms like AES and RSA are not suited for implementation on such devices. This motivated an intense search for new approaches to ultra-lightweight authentication in the last years. It is known that Challenge-Response Protocols based on ultra-lightweight blockciphers like PRESENT solve this task sufficiently good w.r.t. to area, communication complexity and energy consumption. We study the question whether other approaches like HB-protocols or linear protocols can be used to obtain better solutions and get partially a positive answer. Moreover, we present a stream cipher based approach to ultralightweight authentication called Double Streaming, which is provable secure in a generic scenario, and which has the potential to beat existing solutions.

3.15 Testing read-restricted formulas.

Meena Mahajan (The Institute of Mathematical Sciences, IN)

Joint work of Mahajan, Meena; Rao, B. V. Raghavendra; Sreenivasaiah, Karteek
Main reference M. Mahajan, B. V. R. Rao, K. Sreenivasaiah, "Monomials, Multilinearity and Identity Testing in Simple Read-Restricted Circuits," Theoretical Computer Science, Vol. 524, pp. 90–102, 2014.
URL http://dx.doi.org/10.1016/j.tcs.2014.01.005

How do we test whether a given arithmetic circuit computes the identically zero polynomial? Efficient algorithms are known for special types of bounded-depth formulas, and special types of read-restricted multilinear formulas. We describe how to test read-twice or read-thrice formulas without any depth or multilinearity restrictions. We also describe an approach for testing the sum of two unbounded products of read-once formulas; this approach works over the integers but can hopefully be extended to other rings.

This is joint work with B V Raghavendra Rao and Karteek Sreenivasaiah, and is reported in papers in Theoretical Computer Science 524:90–102, 2014 (preliminary version in MFCS 2012) and in COCOON 2014.

Funded by an IMPECS project.

3.16 Extended formulations and information complexity

Ankur Moitra (MIT – Cambridge, US)

Joint work of Braverman, Mark; Moitra, Ankur
Main reference M. Braverman, A. Moitra, "An Information Complexity Approach to Extended Formulations," in Proc. of the 45th Annual ACM Symp. on Theory of Computing (STOC'13), pp. 161-170, ACM, 2013; pre-print available as ECCC TR12-131 (2012).
URL http://dx.doi.org/10.1145/2488608.2488629
URL http://eccc.hpi-web.de/report/2012/131/

We survey some of the recent lower bounds for extended formulations. Our emphasis is on the underlying techniques, and parallels to the techniques used in lower bounds for communication complexity.

3.17 Tree codes and triangular totally nonsingular matrices

Pavel Pudlák (Academy of Sciences – Prague, CZ)

Main reference P. Pudlák, "Linear tree codes and the problem of explicit constructions," arXiv:1310.5684v3 [cs.IT], 2014.
URL http://arxiv.org/abs/1310.5684v3

We reduce the problem of constructing asymptotically good tree codes to the construction of triangular totally positive matrices over fields with polynomially many elements.

3.18 Set membership with two bit probes

Jaikumar Radhakrishnan (TIFR Mumbai, IN)

Joint work of Garg, Mohit; Radhakrishnan, Jaikumar
Main reference N. Alon, U. Feige, "On the power of two, three and four probes," in Proc. of the 20th Annual ACM-SIAM Symp. on Discrete Algorithms (SODA'09), pp. 346–354, SIAM, 2009.
URL http://dx.doi.org/10.1137/1.9781611973068.39

We will consider the bit-probe complexity of the set membership problem, where a set S of size at most n from a universe of size m is to be represented as a short bit vector in order to answer membership queries of the form "Is x in S?" by adaptively probing the bit vector at t places. Let $s(m, n, t)$ be the minimum number of bits of storage needed for such a scheme. Alon and Feige showed that for $t = 2$ (two bit probes), such schemes can be obtained from dense graphs with large girth. In particular, they showed that for $n < \log m$,

$$s(m, n, 2) = O(mn \log((\log m)/n)/ \log m).$$

We improve their analysis and obtain a better upper bound; by modelling two-probe schemes as graphs and considering their girth, we obtain a corresponding lower bound.

(a) There is a constant $C > 0$, such that for all large m,

$$s(m, n, 2) \leq C \cdot m^{1-\frac{1}{4n+1}}.$$

(b) There is a constant $D > 0$, such that for $n \geq 4$ and all large m, we have

$$s(m, n, 2) \geq D \cdot m^{1-\frac{1}{\lfloor n/4 \rfloor}}.$$

References

1 Noga Alon, Uriel Feige: On the power of two, three and four probes. SODA 2009: 346–354.
2 Harry Buhrman, Peter Bro Miltersen, Jaikumar Radhakrishnan, Srinivasan Venkatesh: Are Bitvectors Optimal? SIAM J. Comput. 31(6):1723–1744, 2002.

3.19 Circuits with medium fan-in

Anup Rao (University of Washington – Seattle, US)

Main reference P. Hrubes, A. Rao, "Circuits with Medium Fan-In," ECCC TR14-020, 2014.
URL http://eccc.hpi-web.de/report/2014/020/

We consider boolean circuits in which every gate may compute an arbitrary boolean function of k other gates, for a parameter k. We give an explicit function $f : \{0,1\}^n \to \{0,1\}^n$ that requires at least $\Omega(\log^2 n)$ non-input gates when $k = 2n/3$. When the circuit is restricted to being layered and depth 2, we prove a lower bound of $n^{\Omega(1)}$ on the number of non-input gates. When the circuit is a formula with gates of fan-in k, we give a lower bound $\Omega(n^2/k \log n)$ on the total number of gates.

Our model is connected to some well known approaches to proving lower bounds in complexity theory. Optimal lower bounds for the Number-On-Forehead model in communication complexity, or for bounded depth circuits in AC_0, or extractors for varieties over small fields would imply strong lower bounds in our model. On the other hand, new lower bounds for our model would prove new time-space tradeoffs for branching programs and impossibility results for (fan-in 2) circuits with linear size and logarithmic depth. In particular, our lower bound gives a different proof for a known time-space tradeoff for oblivious branching programs.

3.20 The power of a superlogarithmic number of players

Michael Saks (Rutgers University – Piscataway, US)

Main reference A. Chattopadhyay, M. Saks, "The Power of Super-logarithmic Number of Players," ECCC TR14-064, 2014.
URL http://www.eccc.hpi-web.de/report/2014/064/

L

In the 'Number-on-Forehead' (NOF) model of multiparty communication, the input is a $k \times m$ boolean matrix A (where k is the number of players) and Player i sees all bits except those in the i-th row, and the players communicate by broadcast in order to evaluate a specified function f at A. We discover new computational power when k exceeds $\log m$. We give a protocol with communication cost poly-logarithmic in m, for block composed functions with limited block size. These are functions of the form $f \circ g$ where f is a symmetric b-variate function, and g is a kr-variate function and $f \circ g(A)$ is defined, for a $k \times br$ matrix to be $f(g(A^1), \ldots, g(A^b))$ where A^i is the i-th $k \times r$ block of A. Our protocol works provided that $k > 1 + \ln b + 2^r$. Ada, Chattopadhyay, Fawzi and Nguyen [1] previously obtained *simultaneous* and deterministic efficient protocols for composed functions of block-width $r = 1$. The new protocol is the first to work for block composed functions with $r > 1$. Moreover, it is simultaneous, with vanishingly small error probability, if public coin randomness is allowed. The deterministic and zero-error version barely uses interaction.

References

1 A. Ada, A. Chattopadhyay, O. Fawzi, and P. Nguyen. *The NOF multiparty communication complexity of composed functions*, *International Colloquium on Automata, Programming and Languages (ICALP)*, pages 13–24, 2012.

3.21 Survey on recent progress on lower bounds for arithmetic circuits

Shubhangi Saraf (Rutgers University – Piscataway, US)

In the last few years there have been several exciting results related to depth reduction of arithmetic circuits and strong lower bounds for bounded depth arithmetic circuits. I will survey these results and highlight some of the main challenges and open directions in this area.

3.22 Pseudorandom generators with optimal seed length for non-boolean poly-size circuits

Ronen Shaltiel (University of Haifa, IL)

Joint work of Artemenko, Sergei; Shaltiel, Ronen
Main reference S. Artemenko, R. Shaltiel, "Pseudorandom generators with optimal seed length for non-boolean poly-size circuits," in Proc. of the 46th Annual ACM Symp. on Theory of Computing (STOC'14), pp. 99–108, ACM, 2014.
URL http://doi.acm.org/10.1145/2591796.2591846

A sampling procedure for a distribution P over $\{0,1\}^\ell$, is a function $C : \{0,1\}^n \longrightarrow \{0,1\}^\ell$ such that the distribution $C(U_n)$ (obtained by applying C on the uniform distribution U_n) is the "desired distribution" P. Let $n > r \geq \ell = n^{\Omega(1)}$. An *nb-PRG* (defined by Dubrov and Ishai (STOC 2006)) is a function $G : \{0,1\}^r \longrightarrow \{0,1\}^n$ such that for every $C : \{0,1\}^n \longrightarrow \{0,1\}^\ell$ in some class of "interesting sampling procedures", $C'(U_r) = C(G(U_r))$ is close to $C(U_n)$ in *statistical distance*.

We construct poly-time computable nb-PRGs with $r = O(\ell)$ (which is best possible) for poly-size circuits. Previous nb-PRGs of Dubrov and Ishai have $r = \Omega(\ell^2)$. We rely on the assumption that: there exists $\beta > 0$, and a problem L in $\mathit{EE} = \mathit{DTIME}(2^{O(n)})$ such that for every large enough n, nondeterministic circuits of size $2^{\beta n}$ that have NP- gates cannot solve L on inputs of length n. This assumption is a scaled nonuniform analogue of (the widely believed) $\mathit{EXPT} \neq \Sigma_2^{PT}$, and similar assumptions appear in various contexts in derandomization. The nb-PRGs of Dubrov and Ishai are based on very strong cryptographic assumptions, or alternatively, on non-standard assumptions regarding incompressibility of functions on random inputs.

When restricting to poly-size circuits $C : \{0,1\}^n \longrightarrow \{0,1\}^\ell$ with Shannon entropy $H(C(U_n)) \leq k$, for $\ell > k = n^{\Omega(1)}$, our nb- PRGs have $r = O(k)$ which is best possible. The nb-PRGs of Dubrov and Ishai use seed length $r = \Omega(k^2)$ and require that the probability distribution of $C(U_n)$ is efficiently computable.

Our nb-PRGs follow from a notion of "conditional PRGs" which may be of independent interest. These are PRGs where $G(U_r)$ remains pseudorandom even when conditioned on a "large" event $\{A(G(U_r)) = 1\}$, for an arbitrary poly-size circuit A. A related notion was considered by Shaltiel and Umans (CCC 2005) in a different setup, and our proofs use ideas from that paper, as well as ideas of Dubrov and Ishai.

We also give an unconditional construction of a poly-time computable nb-PRGs for $\mathit{poly}(n)$-size, depth d circuits $C : \{0,1\}^n \longrightarrow \{0,1\}^\ell$ with $r = O(\ell \cdot \log^{d+O(1)} n)$. This improves upon the previous work of Dubrov and Ishai that has $r \geq \ell^2$. Our nb-PRGs can be implemented by a uniform family of poly-size constant depth circuits (with slightly larger, but still almost linear seed length). The nb-PRG of Dubrov and Ishai computes large parities and cannot be computed in poly-size and constant depth.

This result follows by adapting a recent PRG construction of Trevisan and Xue (CCC 2013) to the case of nb-PRGs, and implementing it by constant-depth circuits.

3.23 Testing equivalence of polynomials under shifts

Amir Shpilka (Technion – Haifa, IL)

Joint work of Dvir, Zeev;Mendes de Oliveira, Rafael; Shpilka, Amir
Main reference Z. Dvir, R. Oliveira, A. Shpilka, "Testing Equivalence of Polynomials under Shifts," in Proc. of the 41st Int'l Colloquium on Automata, Languages, and Programming (ICALP'14), LNCS, Vol. 8572, pp. 417–428, Springer, 2014; pre-print available from author's webpage.
URL http://dx.doi.org/10.1007/978-3-662-43948-7_35
URL http://www.cs.technion.ac.il/~shpilka/publications/DvirOliveiraShpilka14.pdf

Two polynomials $f, g \in \mathbb{F}[x_1, \dots, x_n]$ are called shift-equivalent if there exists a vector $a \in \mathbb{F}^n$ such that the polynomial identity $f(x_1 + a_1, \dots, x_n + a_n) \equiv g(x_1, \dots, x_n)$ holds. Our main result is a new randomized algorithm that tests whether two given polynomials are shift equivalent. Our algorithm runs in time polynomial in the circuit size of the polynomials to which it is given black box access. This complements a previous work of Grigoriev who gave a deterministic algorithm running in time roughly n^d for degree d polynomials.

Our algorithm uses randomness only to solve instances of the Polynomial Identity Testing (PIT) problem. Hence, if one could derandomize PIT a derandomization of our algorithm would follow. This establishes an equivalence between derandomising shift-equivalence testing and derandomizing PIT.

3.24 A simple approach for construction of HSG for low-degree multivariate polynomials based on AG codes

Amnon Ta-Shma (Tel Aviv University, IL)

Constructing pseudorandom generators for low degree polynomials has received a considerable attention in the past decade. Viola [CC 2009], following an exciting line of research, constructed a pseudorandom generator for degree d polynomials in n variables, over any prime field. The seed length used is $O(d \log n + d2^d)$, and thus this construction yields a non-trivial result only for $d = O(\log n)$. Bogdanov [STOC 2005] presented a pseudorandom generator with seed length $O(d^4 \log n)$. However, it is promised to work only for fields of size $\Omega(d^{10} \log^2 n)$. The work of Lu [CCC 2012], combined with that of Bogdanov, yields a pseudorandom generator with seed length $O(d^4 \log n)$ for fields of size $\Omega(d^{6+c})$ – independent of n, where c is an arbitrarily small constant.

In this work we show that for any d, a random sub-code (with a proper dimension) of any good algebraic geometry code, is a hitting set for degree d polynomials. By derandomizing this assertion, together with the work of Bogdanov, we obtain a construction of a pseudorandom generator for degree d polynomials over fields of size $\Omega(d^{12})$ – independent of n, and seed length $O(d^4 \log n)$.

Although quantitatively our result does not match Lu's parameters, our construction is clean mathematically and conceptually simple. We consider the proof technique to be the main contribution of this paper, and believe it will find other applications in complexity theory. In the heart of our proofs is a reduction from the problem of assuring independence between monomials to the much simpler problem of avoiding collisions over the integers. Our reduction heavily relies on the Riemann-Roch theorem.

3.25 Fixed-parameter parallelism

Till Tantau (Universität Lübeck, DE)

Joint work of Elberfeld, Michael; Stockhusen, Christoph; Tantau, Till
Main reference C, Stockhusen, T. Tantau, "Completeness Results for Parameterized Space Classes," in Proc. of the 8th Int'l Symp. on Parameterized and Exact Computation (IPEC'13), LNCS, Vol. 8246, pp. 335–347, Springer, 2013.
URL http://dx.doi.org/10.1007/978-3-319-03898-8_28

The talk presented some recent findings on fpt algorithms that can be parallelized. It was shown that the vertex cover problem can be solved in constant time using "fpt many processors" and that the feedback vertex set can be solved by an fpt algorithm that needs only slicewise logarithmic space, which in turn yields a parallel program. These results are part of a larger study of fixed parameter parallelism for which appropriate classes and models must be defined and their relationships investigated.

3.26 Counting the number of perfect matchings in K_5-free graphs

Thomas Thierauf (Hochschule Aalen, DE)

Counting the number of perfect matchings in arbitrary graphs is a #P-complete problem. However, for some restricted classes of graphs the problem can be solved efficiently. In the case of planar graphs, and even for $K_{3,3}$-free graphs, Vazirani showed that it is in NC^2. The technique there is to compute a *Pfaffian orientation* of a graph.

In the case of K_5-free graphs, this technique will not work because some K_5-free graphs do not have a Pfaffian orientation. We circumvent this problem and show that the number of perfect matchings in K_5-free graphs can be computed in polynomial time, in fact in NC.

3.27 Approaches to bounding the exponent of matrix multiplication

Christopher Umans (CalTech, US)

Joint work of Umans, Chris; Alon, Noga; Cohn, Henry; Kleinberg, Bobby; Shpilka,Amir; Szegedy, Balazs
Main reference H. Cohn, C. Umans, "Fast matrix multiplication using coherent configurations," arXiv:1207.6528v2 [math.NA], 2012; pre-print also available from author's webpage.
Main reference http://arxiv.org/abs/1207.6528v2
URL http://www.cs.caltech.edu/~umans/papers/CU12.pdf

We begin by describing the ideas behind the state-of-the-art bounds on omega, the exponent of matrix multiplication.

We then present the "group-theoretic" approach of Cohn and Umans as an alternative to these methods, and we generalize this approach from group algebras to general algebras. We identify adjacency algebras of coherent configurations as a promising family of algebras in the generalized framework. We prove a closure property involving symmetric powers of adjacency algebras, which enables us to prove nontrivial bounds on ω using commutative coherent configurations, and suggests that commutative coherent configurations may be sufficient to prove $\omega = 2$.

Along the way, we introduce a relaxation of the notion of tensor rank, called s-rank, and show that upper bounds on the s-rank of the matrix multiplication tensor imply upper bounds on the ordinary rank. In particular, if the "s-rank exponent of matrix multiplication" equals 2, then the (ordinary) exponent of matrix multiplication, ω, equals 2.

Finally, we will mention connections between several conjectures implying $\omega = 2$, and variants of the classical sunflower conjecture of Erdos and Rado.

No special background is assumed.

Based on joint works with Noga Alon, Henry Cohn, Bobby Kleinberg, Amir Shpilka, and Balazs Szegedy.

3.28 An interactive information odometer and applications

Omri Weinstein (Princeton University, US)

Joint work of Braverman, Mark; Weinstein, Omri
Main reference M. Braverman, O. Weinstein, "An Interactive Information Odometer with Applications," ECCC TR14-047, 2014.
URL http://eccc.hpi-web.de/report/2014/047/

We introduce a novel technique which enables two players to maintain an estimate of the internal information cost of their conversation in an online fashion without revealing much extra information. We use this construction to obtain new results about communication complexity and information- theoretically secure computation.

As a first corollary, we prove a strong direct product theorem for communication complexity in terms of information complexity: If I bits of information are required for solving a single copy of f under μ with probability 2/3, then any protocol attempting to solve n independent copies of f under μ^n using $o(n \cdot I)$ communication, will succeed with probability $2^{-\Omega(n)}$. This is the best one can hope for, as Braverman and Rao [FOCS '11] previously showed that $O(n \cdot I)$ communication suffice to succeed with probability $\sim (2/3)^n$.

We then show how the information odometer can be used to achieve information-theoretic secure communication between two untrusted parties: If the players' goal is to compute a function $f(x, y)$, and f admits a protocol with information cost is I and communication cost C, then our odometer can be used to produce a "robust" protocol which: (i) Assuming both players are honest, computes f with high probability, and (ii) Even if one party is malicious, then for any $k \in \mathbb{N}$, the probability that the honest player reveals more than $O(k \cdot (I + \log C))$ bits of information to the other player is at most $2^{-\Omega(k)}$.

Finally, we outline a potential approach which uses our odometer as a proxy for braking state of the art interactive compression results: any progress on interactive compression in the regime where $I = O(\log C)$ will lead to new *general* compression results in all regimes. In particular, any improvement on the dependence on I in the $2^{O(I)}$- compression result of Braverman [STOC '12] will lead to improved compression and new direct sum and product theorems in communication complexity.

3.29 Turnstile streaming algorithms might as well be linear sketches

David P. Woodruff (IBM Almaden Center, US)

Joint work of Li, Yi; Nguyen, Huy; Woodruff, David
Main reference Y. Li, H. L. Nguyen, D. P. Woodruff, "Turnstile streaming algorithms might as well be linear sketches," in Proc. of the 46th Annual ACM Symp. on Theory of Computing (STOC'14), pp. 174–183, ACM, 2014.
URL http://doi.acm.org/10.1145/2591796.2591812

Abstract: In the turnstile model of data streams, an underlying vector x in $\{-m, -m+1, \ldots, m-1, m\}$ is presented as a long sequence of arbitrary positive and negative integer updates to its coordinates. A randomized algorithm seeks to approximate a function $f(x)$ with constant probability while only making a single pass over this sequence of updates and using a small amount of space. All known algorithms in this model are linear sketches: they sample a matrix A from a distribution on integer matrices in the preprocessing phase, and maintain the linear sketch Ax while processing the stream. At the end of the stream, they output an arbitrary function of Ax. One cannot help but ask: are linear sketches universal?

In this work we answer this question by showing that any 1-pass constant probability streaming algorithm for approximating an arbitrary function f of x in the turnstile model can also be implemented by sampling a matrix A from the uniform distribution on $O(n \log m)$ integer matrices, with entries of magnitude $poly(n)$, and maintaining the linear sketch Ax. Furthermore, the logarithm of the number of possible states of Ax, as x ranges over $\{-m, -m+1, \ldots, m-1, m\}^n$, plus the amount of randomness needed to store A, is at most a logarithmic factor larger than the space required of the space-optimal algorithm. Our result shows that to prove space lower bounds for 1-pass streaming algorithms, it suffices to prove lower bounds in the simultaneous model of communication complexity, rather than the stronger 1-way model. Moreover, the fact that we can assume we have a linear sketch with polynomially-bounded entries further simplifies existing lower bounds, e.g., for frequency moments we present a simpler proof of the $\tilde{\Omega}(n^{1-2/k})$ bit complexity lower bound without using communication complexity.

3.30 Growth rates of elementary symmetric polynomials

Amir Yehudayoff (Technion – Haifa, IL)

Joint work of Gopalan, Parikshit; Yehudayoff, Amir
Main reference P. Gopalan, A. Yehudayoff, "Inequalities and tail bounds for elementary symmetric polynomials," ECCC TR14-019, 2014.
URL http://eccc.hpi-web.de/report/2014/019/

We shall discuss the growth of elementary symmetric polynomials S_k, $k \in [n]$, over the reals. We shall see that if $|S_1(a)|, |S_2(a)|$ are small then $|S_k(a)|$ is small for all k. Some motivation to study this comes from pseudorandomness, and also from properties of real univariate polynomials.

Participants

- Eric Allender
Rutgers Univ. – Piscataway, US
- Eli Ben-Sasson
Technion – Haifa, IL
- Beate Bollig
TU Dortmund, DE
- Mark Braverman
Princeton University, US
- Harry Buhrman
CWI – Amsterdam, NL
- Amit Chakrabarti
Dartmouth College – Hanover, US
- Arkadev Chattopadhyay
TIFR Mumbai, IN
- Irit Dinur
Weizmann Institute, IL
- Lance Fortnow
Georgia Inst. of Technology, US
- Anna Gál
University of Texas – Austin, US
- Oded Goldreich
Weizmann Institute, IL
- Kristoffer Arnsfelt Hansen
Aarhus University, DK
- Prahladh Harsha
TIFR Mumbai, IN
- Johan Hastad
KTH Royal Institute of Technology, SE
- Valentine Kabanets
Simon Fraser University – Burnaby, CA
- Subhash Khot
New York University, US
- Hartmut Klauck
Nanyang TU – Singapore, SG
- Swastik Kopparty
Rutgers Univ. – Piscataway, US
- Michal Koucký
Charles University – Prague, CZ
- Matthias Krause
Universität Mannheim, DE
- Meena Mahajan
The Institute of Mathematical Sciences, IN
- Pierre McKenzie
University of Montreal, CA
- Peter Bro Miltersen
Aarhus University, DK
- Ankur Moitra
MIT – Cambridge, US
- Pavel Pudlák
Academy of Sciences – Prague, CZ
- Jaikumar Radhakrishnan
TIFR Mumbai, IN
- Anup Rao
University of Washington – Seattle, US
- Oded Regev
New York University, US
- Rüdiger Reischuk
Universität Lübeck, DE
- Michael Saks
Rutgers Univ. – Piscataway, US
- Rahul Santhanam
University of Edinburgh, GB
- Shubhangi Saraf
Rutgers Univ. – Piscataway, US
- Nicole Schweikardt
Goethe-Universität Frankfurt am Main, DE
- Ronen Shaltiel
University of Haifa, IL
- Amir Shpilka
Technion – Haifa, IL
- Amnon Ta-Shma
Tel Aviv University, IL
- Till Tantau
Universität Lübeck, DE
- Thomas Thierauf
Hochschule Aalen, DE
- Christopher Umans
CalTech, US
- Dieter van Melkebeek
University of Wisconsin – Madison, US
- Omri Weinstein
Princeton University, US
- David P. Woodruff
IBM Almaden Center, US
- Amir Yehudayoff
Technion – Haifa, IL