Report from Dagstuhl Seminar 16411

Algebraic and Combinatorial Methods in Computational Complexity

Edited by

Valentine Kabanets[1], Thomas Thierauf[2], Jacobo Tóran[3], and Christopher Umans[4]

1 **Simon Fraser University, CA,** kabanets@cs.sfu.ca
2 **Aalen University, DE,** thomas.thierauf@uni-ulm.de
3 **Ulm University, DE,** jacobo.toran@uni-ulm.de
4 **CalTech – Pasadena, US,** umans@cs.caltech.edu

Abstract

Computational Complexity is concerned with the resources that are required for algorithms to detect properties of combinatorial objects and structures. It has often proven true that the best way to argue about these combinatorial objects is by establishing a connection (perhaps approximate) to a more well-behaved algebraic setting. Indeed, many of the deepest and most powerful results in Computational Complexity rely on algebraic proof techniques. The Razborov-Smolensky polynomial-approximation method for proving constant-depth circuit lower bounds, the PCP characterization of NP, and the Agrawal-Kayal-Saxena polynomial-time primality test are some of the most prominent examples.

The algebraic theme continues in some of the most exciting recent progress in computational complexity. There have been significant recent advances in algebraic circuit lower bounds, and the so-called chasm at depth 4 suggests that the restricted models now being considered are not so far from ones that would lead to a general result. There have been similar successes concerning the related problems of polynomial identity testing and circuit reconstruction in the algebraic model (and these are tied to central questions regarding the power of randomness in computation).

Another surprising connection is that the algebraic techniques invented to show lower bounds now prove useful to develop efficient algorithms. For example, Williams showed how to use the polynomial method to obtain faster all-pair-shortest-path algorithms. This emphases once again the central role of algebra in computer science.

The seminar aims to capitalize on recent progress and bring together researchers who are using a diverse array of algebraic methods in a variety of settings. Researchers in these areas are relying on ever more sophisticated and specialized mathematics and this seminar can play an important role in educating a diverse community about the latest new techniques, spurring further progress.

Seminar Oktober 9–14, 2016 – http://www.dagstuhl.de/16411

1998 ACM Subject Classification F.1.3 Complexity Measures and Classes, F.2 Analysis of Algorithms and Problem Complexity.

Keywords and phrases Computational Complexity, lower bounds, approximation, pseudo-randomness, derandomization, circuits

Digital Object Identifier 10.4230/DagRep.6.10.13

Algebra in Computational Complexity, *Dagstuhl Reports*, Vol. 6, Issue 10, pp. 13–32
Editors: Valentine Kabanets, Thomas Thierauf, Jacobo Tóran, and Christopher Umans
DAGSTUHL REPORTS Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Executive Summary

Valentine Kabanets
Thomas Thierauf
Jacobo Tóran
Christopher Umans

The seminar brought together more than 40 researchers covering a wide spectrum of complexity theory. The focus on algebraic methods showed the great importance of such techniques for theoretical computer science. We had 25 talks, most of them lasting about 40 minutes, leaving ample room for discussions. In the following we describe the major topics of discussion in more detail.

Circuit Complexity

This is an area of fundamental importance to Complexity. Circuit Complexity was one of the main topics in the seminar. Still it remains a big challenge to prove strong upper and lower bounds. Also Polynomial Identity Testing (PIT) plays a central role.

The seminar started with a talk by *Steve Fenner*. In a breakthrough result, he showed how to solve the perfect matching problem in bipartite graphs (almost) efficiently in parallel, by circuits of quasi-polynomial size and $O(\log^2 n)$ depth (in quasi-NC). This solves a problem open since more than 30 years. *Rohit Gurjar* showed how to extend the result even further to *linear matroid intersection*, where bipartite perfect matching is a special case of.

Both of the above results can be read as a singularity test of certain symbolic matrices. We had several talks dealing with determining singularity or computing the rank of a symbolic matrix. *Rafael Oliveira* presented an efficient algorithm for the symbolic singularity problem in the *non-commutative* setting. In the *commutative* setting, the complexity is a major open problem. Many other important problems reduce to it. *Markus Bläser* presented an *approximation algorithm* (PTAS) for the rank of a symbolic matrix. Surprisingly, this is achieved with a greedy-algorithm. *Kristoffer Hansen* showed a different kind of approximation for low rank binary matrices.

We have seen some great work on *Polynomial Identity Testing* (PIT) and circuit lower bounds recently, in particular on depth-3 and depth 4 circuits, and on arithmetic branching programs, which has brought us very close to statements that are known to imply $\mathrm{VP} \neq \mathrm{VNP}$, the analogue of the P vs. NP question in the arithmetic world. With respect to PIT, an ambitious goal is to come up with a hitting set construction for a specific model. A hitting set is a set of instances such that every non-zero polynomial in the model has a non-root in the set. This would solve the PIT problem in the *black box* model.

PIT is known to be efficiently solvable by *randomized* algorithms, for example when we consider arithmetic circuits. Things get a bit different when we consider *noncummutative* circuits. Now the standard test cannot be directly applied because the polynomials can have exponential degree, and hence doubly exponentially many monomials. *V. Arvind* presented a randomized polynomial identity test for noncommutative arithmetic circuits for the case when the polynomial has only exponentially many monomials.

One of the most successful methods for proving lower bounds for arithmetic circuits is to consider the dimension of the span of the *partial derivatives* of a polynomial. *Pascal Koiran* considered the complexity of the problem to compute this dimension. He showed that it is #P-hard. It remained open whether the problem is #P-complete.

Another important notion when proving lower bounds is the *algebraic independence* of arithmetic circuits. In 2015, Kumar and Saraf presented lower bounds and hitting sets for a class of depth-4 circuits that have low algebraic rank. Unfortunately, their technique requires base fields of characteristic zero, or at least exponentially large characteristic. *Nitin Saxena* closed this gap and showed how to make the approach work over *every* field.

Michael Forbes showed that lower bounds for certain algebraic circuits imply lower bounds in proof complexity.

Or Meir talked on one of the major open problems in complexity theory: proving super-polynomial lower bounds on the size of formulas. Karchmer, Raz, and Wigderson suggested an approach to this problem. The *KRW-conjecture* states that the formula complexity of two functions f and g roughly adds up when we consider the composed function $g \circ f$. They showed that the conjecture implies super-polynomial formula lower bounds In his talk, Or Meir did a step to prove the conjecture: he proved a special case, namely when f is the parity-function. His proof uses techniques from communication complexity.

Valiant introduced the arithmetic analogue of classes P and NP. Very roughly, the class VP contains all multivariate polynomials that can be computed (non-uniformly) by polynomial-size arithmetic circuits, and the class VNP contains all multivariate polynomials that have coefficients computable by VP-circuits. The question whether VP is different from VNP plays the role of the P-NP question in algebraic complexity theory. Valiant showed that the permanent is complete for VNP. But for VP, only artificially constructed functions were known to be complete. In her talk, *Meena Mahajan* described several polynomial families complete for VP and for VNP, based on the notion of graph homomorphism polynomials.

Complexity

Since the famous AKS-primality test, prime numbers can be recognized efficiently. The *construction* of prime numbers is still a challenging task. The best known deterministic algorithm have only exponential running time. *Rahul Santhanam* presented a randomized subexponential time algorithm that outputs primes, and only primes, with high probability, and moreover, the output is mostly the same prime. This is called a *zero-error pseudo-deterministic* algorithm.

Since the famous Isolation Lemma of Mulmuley, Vazirani, Vazirani, researchers recognized the power of isolation. For example, the bipartite perfect matching and the matroid intersection algorithms mentioned above, both rely on isolating a minimum weight solution, *Nutan Limaye* studied the problem of isolating an s-t-path in a directed graph. She proved that a randomized logspace algorithm that isolates such a path can be used to show NL $\subseteq$ L/poly.

Derandomization is an area where there are tight connections between lower bounds and algorithms. Strong enough circuit lower bounds can be used to construct pseudo-random generators that can then be used to simulate randomized algorithms with only polynomial overhead. The polynomial overhead is fine for algorithms running in polynomial time. However, in case of subexponential randomized algorithms, this overhead makes the resulting deterministic algorithm more or less useless. *Ronen Shaltiel* showed how to overcome this problem by achieving a more modest overhead. He needs, however, stronger lower bounds to begin with. Further talks on pseudo-random generators and randomness extractors were given by *Amnon Ta-Shma* and *William Hoza*.

Chris Umans gave an evening talk presenting a recent breakthrough in additive combinatorics, the resolution of the so-called *cap-set conjecture* by Ellenberg and Gijswijt. This result has implications for the Cohn-Umans group-theoretic approach for matrix multiplication, and elsewhere in Complexity.

Coding Theory

Error-correcting codes, particularly those constructed from polynomials, i.e. Reed-Solomon codes or Reed-Muller codes, lie at the heart of many significant results in Computational Complexity. *Shubhangi Saraf* gave a talk on locally-correctable and locally-testable codes. *Swastik Kopparty* generalized the well known decoding algorithm for Reed-Solomon codes to higher dimensions. He presented an efficient algorithm to decode Reed-Muller codes when the evaluation points are an arbitrary product set S^m, for some m, when S is larger than the degree of the polynomials.

Quantum Complexity

Complexity issues arising in the context of quantum computation are an important area in complexity theory since several decades. In the workshop, we had two talks related to quantum complexity. *Farid Ablayev* talked bout the notion of quantum hash function and how to construct such functions. He also explained some of its applications for constructing quantum message authentication codes. *Ryan O'Donnel* explained about the *quantum tomography problem* and how this special case of *quantum spectrum estimation* can be solved combinatorially by understanding certain statistics of random words.

Conclusion

As is evident from the list above, the talks ranged over a broad assortment of subjects with the underlying theme of using algebraic and combinatorial techniques. It was a very fruitful meeting and has hopefully initiated new directions in research. Several participants specifically mentioned that they appreciated the particular focus on a common class of *techniques* (rather than end results) as a unifying theme of the workshop. We look forward to our next meeting!

2 Table of Contents

Executive Summary

Overview of Talks

3 Overview of Talks

3.1 Quantum Fingerprinting and Quantum Hashing. Computational and Cryptographical Aspects

Farid Ablayev (Kazan State University, RU)

Joint work of Farid Ablayev, Marat Ablayev, Alexander Vasiliev, Mansur Ziatdinov
Main reference F. Ablayev, M. Ablayev, A. Vasiliev, and M. Ziatdinov, "Quantum Fingerprinting and Quantum Hashing. Computational and Cryptographical Aspects", Baltic J. Modern Computing, Vol. 4(4), pp. 860-–875, 2016.
URL http://dx.doi.org/10.22364/bjmc.2016.4.4.17

Rusins Freivalds was one of the first researchers who introduced methods (later called fingerprinting) for constructing effective randomized algorithms (which are more effective than any deterministic algorithm) (Freivalds, 1977, 1979). In quantum case, fingerprinting is a procedure that maps classical data to a quantum state that identifies the original data (with high probability). One of the first applications of the quantum fingerprinting method is due to Ambainis and Freivalds (1998): for a specific language they have constructed a quantum finite automaton with an exponentially smaller size than any classical randomized automaton. An explicit definition of the quantum fingerprinting was introduced by Buhrman et al. in (2001) for constructing effective quantum communication protocol for equality testing.

We define a notion of quantum hash function which is quantum one-way function and quantumly collision resistant function. We show that one-way property and collision resistance property are correlated for a quantum hash function. The more the function is one-way the less it is collision resistant and vice versa. We show that such a correlation can be balanced.

We present an approach for quantum hash function constructions by establishing a connection with small biased sets (Naor & Naor, 1990) and quantum hash function constructions: we prove that small sized ϵ-biased sets allow to generate balanced quantum hash functions. Such a connection adds to the long list of small-biased sets? applications. In particular it was observed in (Naor & Naor, 1990; Ben-Sasson et al., 2003) that the ϵ-bias property is closely related to the error-correcting properties of linear codes. Note that the quantum fingerprinting function from (Buhrman et al., 2001) is based on a binary error-correcting code and so it solves the problem of constructing quantum hash functions for the binary case. For the general case, ϵ-bias does not correspond to Hamming distance. Thus, in contrary to the binary case, an arbitrary linear error correcting code cannot be used directly for quantum hash functions.

Next, recall that any ϵ-biased set gives rise to a Cayley expander graph (Alon & Roichman, 1994). We show how such graphs generate balanced quantum hash functions. Every expander graph can be converted to a bipartite expander graph. The generalization of these bipartite expander graphs is the notion of extractor graphs. Such point of view gives a method for constructing quantum hash functions based on extractors.

This construction of quantum hash functions is applied to define the notion of keyed quantum hash functions. The latter is used for constructing quantum hash-based message authentication codes (QMAC). The security proof of QMAC is based on using strong extractors against quantum storage developed by Ta-Shma (2009).

3.2 PIT for noncommutative circuits

Vikraman Arvind (The Institute of Mathematical Sciences, IN)

Joint work of Vikraman Arvind, Partha Mukhopadhyay, S. Raja
Main reference V. Arvind, P. Mukhopadhyay, S. Raja, "Randomized Polynomial Time Identity Testing for Noncommutative Circuits", ECCC TR16-89, 2016.
URL http://eccc.hpi-web.de/report/2016/089/

In this talk we show that the black-box polynomial identity testing for noncommutative polynomials $f \in \mathbb{F}\langle z_1, z_2, \cdots, z_n\rangle$ of degree D and sparsity t, can be done in randomized poly$(n, \log t, \log D)$ time. As a consequence, if the black-box contains a circuit C of size s computing $f \in \mathbb{F}\langle z_1, z_2, \cdots, z_n\rangle$ which has at most t non-zero monomials, then the identity testing can be done by a randomized algorithm with running time polynomial in s and n and $\log t$. This makes significant progress on a question that has been open for over ten years.

The earlier result by Bogdanov and Wee [BW05], using the classical Amitsur-Levitski theorem, gives a randomized polynomial-time algorithm only for circuits of polynomially bounded syntactic degree. In our result, we place no restriction on the degree of the circuit.

Our algorithm is based on automata-theoretic ideas introduced in [AMS08,AM08]. In those papers, the main idea was to construct deterministic finite automata that isolate a single monomial from the set of nonzero monomials of a polynomial f in $\mathbb{F}\langle z_1, z_2, \cdots, z_n\rangle$. In the present paper, since we need to deal with exponential degree monomials, we carry out a different kind of monomial isolation using nondeterministic automata.

3.3 A deterministic PTAS for the commutative rank of a symbolic matrix

Markus Bläser (Universität des Saarlandes, DE)

Joint work of Markus Bläser, Gorav Jindal, Anurag Pandey
Main reference M. Bläser, G. Jindal, A. Pandey, "Greedy Strikes Again: A Deterministic PTAS for Commutative Rank of Matrix Spaces", ECCC TR16-145, 2016.
URL http://eccc.hpi-web.de/report/2016/145/

We present a deterministic PTAS for computing the commutative rank of a symbolic matrix or equivalently, of a given matrix space B. More specifically, given a matrix space $B \subseteq F^{n\times n}$ and a rational number $\epsilon > 0$, we give an algorithm that runs in time $O(n^{4+3/\epsilon})$ and computes a matrix A such that the rank of A is at least $(1-\epsilon)$ times the commutative rank of B. The algorithm is the natural greedy algorithm. It always takes the first set of k matrices that will increase the rank of the matrix constructed so far until it does not find any improvement, where the size of the set k depends on ϵ.

3.4 Non-algebraic methods for (and against) secret sharing

Andrej Bogdanov (The Chinese University of Hong Kong, HK)

When we talk about secret sharing things that come to mind are algebraic objects like finite fields, polynomials, codes, etc. We take on a probabilistic viewpoint and use analytic, combinatorial, and game-theoretic tools to rediscover some old connections and answer questions about the complexity of secret sharing and prove new lower bounds on share size in threshold schemes.

3.5 An Efficient Deterministic Simulation Theorem

Arkadev Chattopadhyay (Tata Institute of Fundamental Research – Mumbai, IN)

Joint work of Arkadev Chattopadhyay, Michal Koucky, Bruno Loff, Sagnik Mukhopadhyay

Recently, proving theorems of the form that the communication complexity of a composed function $f \circ g$ is essentially of the order of the decision tree complexity of f times the communication complexity of g has received a lot of attention. In particular, Goos-Pitassi-Watson (2015) simplified the proof of such a theorem for deterministic complexity due to Raz-McKenzie (1997) that worked only when g is the Indexing function. They used this theorem to settle a longstanding open problem in communication complexity. The Raz-Mckenzie theorem needs the size of the Indexing gadget to be at least n^{20}, where n is the number of instances of Index.

We identify a simple sufficient condition for g to be satisfied to prove such deterministic simulation theorems. Using this, we show that $CC(f \circ IP) = \Omega(DT(f) \cdot m)$, provided $m = \Omega(\log n)$, where IP is the inner-product function. This gives an exponential improvement over the gadget size of Raz and McKenzie.

3.6 Bipartite Perfect Matching is in quasi-NC

Stephen A. Fenner (University of South Carolina, US)

Joint work of Stephen A. Fenner, Rohit Gurjar, Thomas Thierauf
Main reference S. A. Fenner, R. Gurjar, T. Thierauf , "Bipartite Perfect Matching is in quasi-NC", ECCC TR16-177, 2015.
URL http://eccc.hpi-web.de/report/2015/177/

We show that the bipartite perfect matching problem is in QuasiNC^2. That is, it has uniform circuits of quasi-polynomial size $n^{O(\log n)}$, and $O(\log^2 n)$ depth. Previously, only an exponential upper bound was known on the size of such circuits with poly-logarithmic depth.

We obtain our result by an almost complete derandomization of the famous Isolation Lemma when applied to yield an efficient randomized parallel algorithm for the bipartite perfect matching problem.

3.7 Proof Complexity Lower Bounds from Algebraic Circuit Complexity

Michael Forbes (Stanford University, US)

Joint work of Michael Forbes, Amir Shpilka, Iddo Tzameret, Avi Wigderson
Main reference M. Forbes, A. Shpilka, I. Tzameret, A. Wigderson, "Proof Complexity Lower Bounds from Algebraic Circuit Complexity", ECCC TR16-98, 2016.
URL http://eccc.hpi-web.de/report/2016/098/

Proof complexity studies the complexity of mathematical proofs, with the aim of exhibiting (true) statements whose proofs are always necessarily long. One well-known proof system is Hilbert's Nullstellensatz, which shows that if the family $F = \{f_1, \ldots, f_m\}$ of n-variate polynomials have no common solution to the system $f_1 = \cdots = f_m = 0$, then there is a proof of this fact of the following form: there are polynomials $G = \{g_1, \ldots, g_m\}$ such that $f_1 \cdot g_1 + \cdots + f_m \cdot g_m = 1$ is an identity. From the perspective of computer science, it is most natural to assume that the *boolean axioms* $x_i^2 - x_i$ are among the polynomials F, and to ask how succinctly one can express the proof G. Assuming $NP \neq coNP$, there must be systems F such that any proof G requires super-polynomial size to write down, and the goal is to furnish such systems F unconditionally.

Substantial work on the Nullstellensatz system has measured the complexity of G in terms of their degree or sparsity, and obtained the desired lower bounds for these measures. Grochow and Pitassi have recently argued that it is natural to measure the complexity of G by the size needed to express them as algebraic circuits, as this can be exponentially more succinct than counting monomials. They called the resulting system the Ideal Proof System (IPS), and showed that it captures the power of well-known strong proof systems such as the Frege proof system, as well as showing that certain natural lower bounds for the size of IPS proofs would imply $VP \neq VNP$, an algebraic analogue of $P \neq NP$. This is in contrast to other proof systems, where direct ties to computational lower bounds are often lacking.

Motivated by their work, we study the IPS proof system further. We first show that weak subsystems of IPS can be quite powerful. We consider the *subset-sum axiom*, that $x_1 + \cdots + x_n + 1$ is unsatisfiable over the boolean cube. In prior work, Impagliazzo, Pudlak, and Sgall showed that any proof of unsatisfiability requires exponentially many monomials to write down. Here, we give an efficient proof even in restricted subclasses of the IPS proof system, showing that the proof can be expressed as a polynomial-size read-once oblivious algebraic branching program (roABP) or depth-3 multilinear formula.

We then consider lower bounds for subclasses of IPS. We obtain certain extensions to existing lower bound techniques, obtaining *functional lower bounds* as well as *lower bounds for multiples.* Using these extensions, we show that variants of the subset-sum axiom require super-polynomially large proofs to prove their unsatisfiability when the size of the algebraic circuits are measured as roABPs, sums of powers of low-degree polynomials, or multilinear formulas.

3.8 Linear Matroid Intersection is in quasi-NC

Rohit Gurjar (Aalen University, DE)

Joint work of Rohit Gurjar, Thomas Thierauf

Given two matroids on the same ground set, their intersection is the collection of common independent sets. Matroid intersection problem asks to find the maximum cardinality of a common independent set. The problem is in P [Edmonds], and is in RNC for linear matroids [Lovász]. The RNC algorithm is via the isolation lemma, which we derandomize to get a quasi-NC algorithm.

Another way to present the result: we get a quasi-polynomial time blackbox identity testing for the family of polynomials computed by $\det(A_1 z_1 + A_2 z_2 + \cdots + A_m z_m)$, where A_i's are rank 1 matrices.

3.9 On Low Rank Approximation of Binary Matrices

Kristoffer Arnsfelt Hansen (Aarhus University, DK)

Joint work of Chen Dan, Kristoffer Arnsfelt Hansen, He Jiang, Liwei Wang, Yuchen Zhou
Main reference C. Dan, K. A. Hansen, H. Jiang, L. Wang, Y. Zhou, "On Low Rank Approximation of Binary Matrices", arXiv:1511.01699v1 [cs.CC], 2015.
URL https://arxiv.org/abs/1511.01699v1

We consider the problem of low rank approximation of binary matrices. Here we are given a $d \times n$ binary matrix $\mathbf{A}$ and a small integer $k < d$. The goal is to find two binary matrices $\mathbf{U}$ and $\mathbf{V}$ of sizes $d \times k$ and $k \times n$ respectively, so that the Frobenius norm of $\mathbf{A} - \mathbf{UV}$ is minimized. There are two models of this problem, depending on the definition of the product of binary matrices: The GF(2) model and the Boolean semiring model. Previously, the only known results are 2-approximation algorithms for the special case $k = 1$ (where the two models are equivalent).

In this paper, we present algorithms for GF(2) and Boolean models respectively. For the GF(2) model, we give a $(\frac{k}{2} + 1 + \frac{k}{2(2^k-1)})$-approximation algorithm, which runs in time $O(dn^{k+1})$. For $k = 1$, the approximation ratio is 2. For the Boolean model, we give an algorithm which achieves $(2^{k-1} + 1)$-approximation and runs in time $O((2^k + 2)! n^{2^k} d)$. We also show that the low rank binary matrix approximation problem is NP-hard for $k = 1$.

3.10 Targeted Pseudorandom Generators, Simulation Advice Generators, and Derandomizing Logspace

William Hoza (University of Texas – Austin, US)

Joint work of William Hoza, Chris Umans
Main reference W. M. Hoza, C. Umans, "Targeted Pseudorandom Generators, Simulation Advice Generators, and Derandomizing Logspace", arXiv:1610.01199v3 [cs.CC], 2016.
URL https://arxiv.org/abs/1610.01199v3

We consider two generalizations of the concept of a pseudorandom generator against logspace. A targeted pseudorandom generator against logspace takes as input a short uniform random seed and a finite automaton; it outputs a long bitstring which looks random to that particular automaton. (Targeted pseudorandom generators were introduced by Goldreich in the BPP setting.) A simulation advice generator for logspace stretches a small uniform random seed into a long advice string; the requirement is that there is some logspace algorithm which, given a finite automaton and this advice string, simulates the automaton reading a long uniform random input. We prove that the intersection over all $\alpha > 0$ of promise-BPSPACE($\log^{1+\alpha} n$) is equal to the corresponding deterministic class if and only if every targeted pseudorandom generator against logspace can be transformed into a comparable simulation advice generator for logspace. In particular, if every derandomization of logspace yields a comparable (ordinary) pseudorandom generator, then BPL is contained in DSPACE($\log^{1+\alpha} n$) for every $\alpha > 0$. We also observe that in the uniform setting, targeted pseudorandom generators against logspace can be transformed into comparable simulation advice generators.

3.11 The complexity of partial derivatives

Pascal Koiran (ENS – Lyon, FR)

Joint work of Pascal Koiran, Ignacio Garcia-Marco, Timothée Pecatte, Stéphan Thomassé
Main reference P. Koiran, I. Garcia-Marco, T. Pecatte, S. Thomassé, "On the complexity of partial derivatives", arXiv:1607.05494v1 [cs.CC], 2016.
URL https://arxiv.org/abs/1607.05494v1

The method of partial derivatives is one of the most successful lower bound methods for arithmetic circuits. It uses as a complexity measure the dimension of the span of the partial derivatives of a polynomial. In this paper, we consider this complexity measure as a computational problem: for an input polynomial given as the sum of its nonzero monomials, what is the complexity of computing the dimension of its space of partial derivatives?

We show that this problem is #P-hard and we ask whether it belongs to #P. We analyze the *trace method*, recently used in combinatorics and in algebraic complexity to lower bound the rank of certain matrices. We show that this method provides a polynomial-time computable lower bound on the dimension of the span of partial derivatives, and from this method we derive closed-form lower bounds. We leave as an open problem the existence of an approximation algorithm with reasonable performance guarantees.

3.12 Decoding Reed-Muller codes over product sets

Swastik Kopparty (Rutgers University, US)

Joint work of Swastik Kopparty, John Kim
Main reference J. Y. Kim, S. Kopparty, "Decoding Reed-Muller Codes Over Product Sets", in Proc. of the 31st Conf. on Computational Complexity (CCC 2016), LIPICs, Vol. 50, pp. 11:1–11:28, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2016.
URL http://dx.doi.org/10.4230/LIPIcs.CCC.2016.11

We give a polynomial time algorithm to decode multivariate polynomial codes of degree d up to half their minimum distance, when the evaluation points are an arbitrary product set S^m, for every $d < |S|$. Previously known algorithms can achieve this only if the set S has some very special algebraic structure, or if the degree d is significantly smaller than $|S|$. We also give a near-linear time randomized algorithm, which is based on tools from list-decoding, to decode these codes from nearly half their minimum distance, provided $d < (1 - \epsilon)|S|$ for constant $\epsilon > 0$.

Our result gives an m-dimensional generalization of the well known decoding algorithms for Reed-Solomon codes, and can be viewed as giving an algorithmic version of the Schwartz-Zippel lemma.

3.13 Lower Bounds for Elimination via Weak Regularity

Michal Koucký (Charles University, CZ)

Joint work of Michal Koucký, Arkadev Chattopadhyay, Pavel Dvorak, Bruno Loff, and Sagnik Mukhopadhyay
Main reference A. Chattopadhyay, P. Dvorak, M. Koucký, B. Loff, S. Mukhopadhyay, "Lower Bounds for Elimination via Weak Regularity", ECCC TR16-156, 2016.
URL http://eccc.hpi-web.de/report/2016/165/

We consider the problem of elimination in communication complexity, that was first raised by Ambainis et al. (2001) and later studied by Beimel et al. (2014) for its connection to the famous direct sum question. In this problem, let $f : \{0,1\}^n \to \{0,1\}$ be any boolean function. Alice and Bob get k inputs $x_1, \ldots, x_k$ and $y_1, \ldots, y_k$ respectively, with $x_i, y_i \in \{0,1\}^n$. They want to output a k-bit vector v, such that there exists one index i for which $v_i \neq f(x_i, y_i)$. We prove a general result lower bounding the randomized communication complexity of the elimination problem for f using its discrepancy. Consequently, we obtain strong lower bounds for functions Inner-Product and Greater-Than, that work for exponentially larger values of k than the best previous bounds.

To prove our result, we use a pseudo-random notion called regularity that was first used by Raz and Wigderson (1989). We show that functions with small discrepancy are regular. We also observe that a weaker notion, that we call weak-regularity, already implies hardness of elimination. Finally, we give a different proof, borrowing ideas from Viola (2015), to show that Greater-Than is weakly regular.

3.14 Isolation Lemma for Directed Reachability and NL vs. L

Nutan Limaye (Indian Institute of Technology – Mumbai, IN)

Joint work of Nutan Limaye, Vaibhav Krishan
Main reference V. Krishan, N. Limaye, "Isolation Lemma for Directed Reachability and NL vs. L", ECCC TR16-155, 2016.
URL http://eccc.hpi-web.de/report/2016/155/

In this work we study the problem of efficiently isolating witnesses for the complexity classes NL and LogCFL, which are two well-studied complexity classes contained in P. We prove that if there is a L/poly randomized procedure with success probability at least 2/3 for isolating an s-t path in a given directed graph with a source sink pair (s, t), then NL is contained in L/poly. By isolating a path we mean outputting a new graph on the same set of nodes such that exactly one s-t path from the original graph survives. Such an isolating procedure will naturally imply a UL/poly algorithm for reachability, but we prove that in fact this implies an L/poly algorithm. We also prove a similar result for the class LogCFL.

3.15 Enumerator polynomials: Completeness and Intermediate Complexity

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

Joint work of Nitin Saurabh
Main reference M. Mahajan, N. Saurabh, "Some Complete and Intermediate Polynomials in Algebraic Complexity Theory", ECCC TR16-38, 2016.
URL http://eccc.hpi-web.de/report/2016/038/

VNP, VP, VBP are central complexity classes in algebraic complexity theory. The notions of reductions and completeness are central to understanding the relationships between them. This talk will describe

1. polynomial families based on graph homomorphisms and complete for each of these classes,
2. polynomial families based on basic combinatorial NP-complete problems, and unless PH collapses, provably *intermediate* in nature,
3. a lower bound showing that to express the clique polynomial as a monotone projection of the permanent polynomial, exponential *blow-up* is required.

3.16 Toward the KRW Composition Conjecture: Cubic Formula Lower Bounds via Communication Complexity

Or Meir (University of Haifa, IL)

Joint work of Or Meir, Irit Dinur
Main reference Irit Dinur, Or Meir, "Toward the KRW Composition Conjecture: Cubic Formula Lower Bounds via Communication Complexity", in Proc. of the 31st Conf. on Computational Complexity (CCC 2016), LIPIcs, Vol. 50, pp. 3:1–3:51, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2016.
URL http://dx.doi.org/10.4230/LIPIcs.CCC.2016.3

One of the major challenges of the research in circuit complexity is proving super-polynomial lower bounds for de-Morgan formulas. Karchmer, Raz, and Wigderson suggested to approach this problem by proving that formula complexity behaves *as expected* with respect to the composition of functions. They showed that this conjecture, if proved, would imply super-polynomial formula lower bounds.

We prove a special case of this conjecture, in which one composes an arbitrary function with the parity function.

While this special case of the KRW conjecture was already proved implicitly in Hastad's work on random restrictions, our proof seems more likely to be generalizable to other cases of the conjecture. In particular, our proof uses an entirely different approach, based on communication complexity technique of Karchmer and Wigderson.

3.17 Efficient Quantum Tomography and Longest Increasing Subsequences

Ryan O'Donnell (Carnegie Mellon University – Pittsburgh, US)

Joint work of Ryan O'Donnell, John Wright

In quantum mechanics, the state ρ of a d-dimensional particle is given by a $d \times d$ PSD matrix of trace 1. The *quantum tomography problem* is to estimate ρ accurately using as few *copies* of the state as possible. The special case of *quantum spectrum estimation* involves just estimating the eigenvalues $\alpha_1, \ldots, \alpha_d$ of ρ, which form a probability distribution. By virtue of some representation theory, understanding these problems mostly boils down to understanding certain statistics of random words with i.i.d. letters drawn from the α_i distribution. These statistics involve longest increasing subsequences, and more generally, the shape of Young tableaus produced by the Robinson-Schensted-Knuth algorithm. In this talk we will discuss new probabilistic, combinatorial, and representation-theoretic tools for these problems, and the consequent new upper and lower bounds for quantum tomography.

3.18 Operator Scaling and Applications to Algebraic Complexity, Mathematics and Optimization

Rafael Oliveira (Princeton University, US)

Joint work of Rafael Oliveira, Ankit Garg, Leonid Gurvits, Avi Wigderson

In this talk we shall explore the *non-commutative symbolic singularity problem*, and its myriad incarnations in commutative and non-commutative algebra, computational complexity, optimization and quantum information theory. We will describe an efficient algorithm solving all these related problems, and how its analysis combines ideas from all these areas. The problem these algorithms solve is non-convex, and we hope they will have many other applications.

3.19 On the Complexity of Generating Primes

Rahul Santhanam (University of Oxford, GB)

Joint work of Igor Carboni Oliveira, Rahul Santhanam

The question of whether n-bit primes can be generated deterministically in time poly(n) (or even subexp(n)) is a fundamental one in computational number theory. Despite much work on this problem, including the Polymath 4 project, no deterministic algorithm running in time better than $2^{n/2}$ is known.

We consider a relaxation of this question: *pseudo-deterministic* constructions, as defined and studied recently by Shafi Goldwasser and others. A zero-error pseudo-deterministic construction of primes in time $T(n)$ is a randomized algorithm, which for all large enough n, on input 1^n, halts in expected time $T(n)$ and outputs a *fixed* prime p_n (which does not depend on the randomness of the algorithm).

We show that either there is a deterministic sub-exponential time construction of infinitely many primes or there is a zero-error pseudo-deterministic construction of primes in sub-exponential time. In particular, this implies an unconditional zero-error pseudo-deterministic construction of infinitely many primes in sub-exponential time. The construction can be made deterministic under the assumption that ZPP=P, partially answering a question of the Polymath 4 project.

3.20 High rate locally-correctable and locally-testable codes with sub-polynomial query complexity

Shubhangi Saraf (Rutgers University – Piscataway, US)

Joint work of Shubhangi Saraf, Swastik Kopparty, Or Meir, Noga Ron-Zewi
Main reference S. Kopparty, O. Meir, N. Ron-Zewi, S. Saraf, "High rate locally-correctable and locally-testable codes with sub-polynomial query complexity", ECCC TR15-68, 2016.
URL http://eccc.hpi-web.de/report/2015/068/

We study locally correctable and locally testable codes in the high rate regime. The tradeoff between the rate of a code and the locality/efficiency of its decoding and testing algorithms has been studied extensively in the past decade, with numerous applications to complexity theory and pseudorandomness.

In this talk I will discuss some recent results giving efficient sub-polynomial query decoding and testing algorithms for high rate error correcting codes. will also highlight some of the most interesting challenges that remain.

3.21 Algebraic independence over positive characteristic: New criterion and applications to locally low algebraic rank circuits

Nitin Saxena (Indian Institute of Technology – Kanpur, IN)

Joint work of Nitin Saxena, Anurag Pandey, Amit Sinhababu
Main reference A. Pandey, N. Saxena, A. Sinhababu, "Algebraic Independence over Positive Characteristic: New Criterion and Applications to Locally Low Algebraic Rank Circuits", in Proc. of the 41st Int'l Symposium on Mathematical Foundations of Computer Science (MFCS 2016), LIPIcs, Vol. 58, pp. 74:1–74:15, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2016.
URL http://dx.doi.org/10.4230/LIPIcs.MFCS.2016.74

The motivation for this work comes from two problems – test algebraic independence of arithmetic circuits over a field of small characteristic, and generalize the structural property of algebraic dependence used by (Kumar, Saraf CCC'16) to arbitrary fields.

It is known that in the case of zero, or large characteristic, using a classical criterion based on the Jacobian, we get a randomized poly-time algorithm to test algebraic independence. Over small characteristic, the Jacobian criterion fails and there is no subexponential time algorithm known. This problem could well be conjectured to be in RP, but the current best algorithm puts it in $\mathrm{NP}^{\#\mathrm{P}}$ (Mittmann, Saxena, Scheiblechner Trans. AMS'14). Currently, even the case of two bivariate circuits over F_2 is open. We come up with a natural generalization of Jacobian criterion, that works over all characteristic. The new criterion is efficient if the underlying inseparable degree is promised to be a constant. This is a modest step towards the open question of fast independence testing, over finite fields, posed in (Dvir, Gabizon, Wigderson FOCS'07).

In a set of linearly dependent polynomials, any polynomial can be written as a linear combination of the polynomials forming a basis. The analogous property for algebraic dependence is false, but a property approximately in that spirit is named as *functional dependence* in (Kumar, Saraf CCC'16) and proved for zero or large characteristic. We show that functional dependence holds for arbitrary fields, thereby answering the open questions in (Kumar, Saraf CCC'16). Following them we use the functional dependence lemma to prove the first exponential lower bound for locally low algebraic rank circuits for arbitrary fields (a model that strongly generalizes homogeneous depth-4 circuits). We also recover their quasipoly-time hitting-set for such models, for fields of characteristic smaller than the ones known before.

Our results show that approximate functional dependence is indeed a more fundamental concept than the Jacobian as it is field independent. We achieve the former by first picking a *good* transcendence basis, then translating the circuits by new variables, and finally approximating them by truncating higher degree monomials. We give a tight analysis of the *degree* of approximation needed in the criterion. To get the locally low algebraic rank circuit applications we follow the known shifted partial derivative based methods.

3.22 Pseudorandomness when the odds are against you

Ronen Shaltiel (University of Haifa, IL)

Joint work of Ronen Shaltiel, Sergei Artemenko, Russel Impagliazzo, Valentine Kabanets
Main reference S. Artemenko, R. Impagliazzo, V. Kabanets, R. Shaltiel, "Pseudorandomness when the odds are against you", ECCC TR16-37, 2016.
URL http://eccc.hpi-web.de/report/2016/037/

A celebrated result by Impagliazzo and Wigderson is that under complexity theoretic hardness assumptions, every randomized algorithm can be transformed into one that uses only logarithmically many bits, with polynomial slowdown. Such algorithms can then be completely derandomized, with polynomial slowdown. In the talk I will discuss recent work attempting to extend this approach to:

1. Randomized algorithms that err with probability $1-\epsilon$ for small ϵ. (Here, the goal is to minimize the number of random bits/slowdown as a function of ϵ).
2. Known SAT-solving randomized algorithms. (Here, polynomial slowdown is a deal breaker as it gives trivial algorithms that run in super exponential time).
3. Randomized algorithms that sample from probability distributions. (Here, the goal is to sample a statistically-close distribution using only few random bits).

3.23 Explicit two-source extractors for near-logarithmic min-entropy

Amnon Ta-Shma (Tel Aviv University, IL)

Joint work of Amnon Ta-Shma, Avraham Ben-Aroya, Dean Doron
Main reference A. Ben-Aroya, D. Doron, A. Ta-Shma , "Explicit two-source extractors for near-logarithmic min-entropy", ECCC TR16-88, 2016.
URL http://eccc.hpi-web.de/report/2016/088/

We explicitly construct extractors for two independent n-bit sources of $(\log n)^{1+o(1)}$ min-entropy. Previous constructions required either polylog(n) min-entropy [CZ15] or five sources [Cohen16].

Our result extends the breakthrough result of Chattopadhyay and Zuckerman [CZ15] and uses the non-malleable extractor of Cohen [Cohen16]. The main new ingredient in our construction is a somewhere-random condenser with a small entropy gap, used as a sampler.

We construct such somewhere-random condensers using the error reduction mechanism of Raz et al. [RRV99] together with the high-error, constant degree dispersers of Zuckerman [Zuc06].

Using our framework and results Cohen and independently Li constructed 2-source extractors for even smaller min-entropies with the world record currently being $O(\log n \log\log n)$.

3.24 A one-sided error randomized protocol for Gap Hamming Distance problem

Nikolay K. Vereshchagin (NRU Higher School of Economics – Moscow, RU)

Assume that Alice has a binary string x and Bob a binary string y, both of length n. Their goal is to output 0, if x and y are at least L-close in Hamming distance, and output 1, if x and y are at least U-far in Hamming distance, where $L < U$ are some integer parameters known to both parties. If the Hamming distance between x and y lies in the interval (L, U), they are allowed to output anything. This problem is called the Gap Hamming Distance (GHD). We study public-coin one-sided error communication complexity of this problem. The error with probability at most $1/2$ is allowed only for pairs at Hamming distance at least U. We establish the upper bound $O((L^2/U)\log L)$ and the lower bound $\Omega(L^2/U)$ for this complexity. These bounds differ only by a $O(\log L)$ factor.

The best upper bounds for communication complexity of GHD known before are the following. The upper bounds $O(L \log n)$ for one-sided error complexity and $O(L \log L)$ for two-sided error complexity, which do not depend on U and hold for all $U > L$. Our bound is better than these two bounds in the case when the ratio U/L is not bounded by a constant. The other known upper bound $O(L^2/(U-L)^2)$ holds for two-sided error complexity of GHD. If U is greater than $L + \sqrt{L}$ then this bound is better than ours, however it is for two-sided error. It is worth to note that all mentioned protocols run in one round.

From technical viewpoint, our achievement is a new protocol to prove that x, y are far on the basis of a large difference between distances from x and y to a randomly chosen string.

Our lower bound $\Omega(L^2/U)$ (for the one-sided error communication complexity of GHD) generalizes the lower bound $\Omega(U)$ for $U = O(L)$ known before.

3.25 Pointer chasing via triangular discrimination

Amir Yehudayoff (Technion – Haifa, IL)

Main reference A. Yehudayoff, "Pointer chasing via triangular discrimination", ECCC TR16-151, 2016.
URL http://eccc.hpi-web.de/report/2016/151/

We prove an essentially sharp $\tilde{\Omega}(n/k)$ lower bound on the k-round distributional complexity of the k-step pointer chasing problem under the uniform distribution, when Bob speaks first. This is an improvement over Nisan and Wigderson's $\tilde{\Omega}(n/k^2)$ lower bound. The proof is information theoretic, and a key part of it is using triangular discrimination instead of total variation distance; this idea may be useful elsewhere.

Participants

- Farid Ablayev
Kazan State University, RU
- Vikraman Arvind
The Institute of Mathematical Sciences, India, IN
- Markus Bläser
Universität des Saarlandes, DE
- Andrej Bogdanov
The Chinese University of Hong Kong, HK
- Arkadev Chattopadhyay
Tata Institute of Fundamental Research – Mumbai, IN
- Samir Datta
Chennai Mathematical Institute, IN
- Stephen A. Fenner
University of South Carolina – Columbia, US
- Michael A. Forbes
Stanford University, US
- Anna Gál
University of Texas – Austin, US
- Frederic Green
Clark University – Worcester, US
- Rohit Gurjar
Aalen University, DE
- Kristoffer Arnsfelt Hansen
Aarhus University, DK
- William Hoza
University of Texas – Austin, US
- Valentine Kabanets
Simon Fraser University – Burnaby, CA
- Marek Karpinski
Universität Bonn, DE
- Neeraj Kayal
Microsoft Research India – Bangalore, IN
- Pascal Koiran
ENS – Lyon, FR
- Swastik Kopparty
Rutgers University – Piscataway, US
- Arpita Korwar
University Paris-Diderot, FR
- Michal Koucký
Charles University – Prague, CZ
- Andreas Krebs
Universität Tübingen, DE
- Sophie Laplante
University Paris-Diderot, FR
- Nutan Limaye
Indian Institute of Technology – Mumbai, IN
- Meena Mahajan
The Institute of Mathematical Sciences, India, IN
- Pierre McKenzie
University of Montréal, CA
- Or Meir
University of Haifa, IL
- David A. Mix Barrington
University of Massachusetts – Amherst, US
- Ryan O'Donnell
Carnegie Mellon University – Pittsburgh, US
- Rafael Oliveira
Princeton University, US
- Chandan Saha
Indian Institute of Science – Bangalore, IN
- Rahul Santhanam
University of Oxford, GB
- Shubhangi Saraf
Rutgers University – Piscataway, US
- Nitin Saxena
Indian Institute of Technology – Kanpur, IN
- Uwe Schöning
Universität Ulm, DE
- Ronen Shaltiel
University of Haifa, IL
- Amnon Ta-Shma
Tel Aviv University, IL
- Thomas Thierauf
Hochschule Aalen, DE
- Jacobo Torán
Universität Ulm, DE
- Christopher Umans
CalTech – Pasadena, US
- Nikolay K. Vereshchagin
NRU Higher School of Economics – Moscow, RU
- Amir Yehudayoff
Technion – Haifa, IL
- Jeroen Zuiddam
CWI – Amsterdam, NL