Report from Dagstuhl Seminar 14391

Algebra in Computational Complexity

Edited by

Manindra Agrawal[1], Valentine Kabanets[2], Thomas Thierauf[3], and Christopher Umans[4]

1 **Indian Institute of Technology – Kanpur, IN,** manindra@iitk.ac.in
1 **Simon Fraser University, CA,** kabanets@cs.sfu.ca
3 **Aalen University, DE,** thomas.thierauf@htw-aalen.de
4 **CalTech – Pasadena, US,** umans@cs.caltech.edu

Abstract

At its core, much of Computational Complexity is concerned with combinatorial objects and structures. But it has often proven true that the best way to prove things about these combinatorial objects is by establishing a connection 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. Representation theory has emerged as an important tool in three separate lines of work: the "Geometric Complexity Theory" approach to P vs. NP and circuit lower bounds, the effort to resolve the complexity of matrix multiplication, and a framework for constructing locally testable codes. Coding theory has seen several algebraic innovations in recent years, including multiplicity codes, and new lower bounds.

This seminar brought together researchers who are using a diverse array of algebraic methods in a variety of settings. It plays an important role in educating a diverse community about the latest new techniques, spurring further progress.

Seminar September 21–26, 2014 – http://www.dagstuhl.de/14391
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, approximazation, pseudorandomness, derandomization, circuits
Digital Object Identifier 10.4230/DagRep.4.9.85

Algebra in Computational Complexity, *Dagstuhl Reports*, Vol. 4, Issue 9, pp. 85–105
Editors: Manindra Agrawal, Valentine Kabanets, Thomas Thierauf, and Christopher Umans

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

1 Executive Summary

Manindra Agrawal
Valentine Kabanets
Thomas Thierauf
Christopher Umans

The seminar brought together almost 50 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. However, the speakers reported amazing progress in various directions.

Or Meir talked on one of the major open problems in complexity theory: proving super-logarithmic lower bounds on the depth of circuits. That is, separating the log-depth circuit class NC^1 from polynomial time, P. Karchmer, Raz, and Wigderson suggested an approach to this problem. The *KRW-conjecture* states that the circuit depth of two functions f and g adds up when we consider the composed function $g \circ f$. They showed that the conjecture implies a separation of NC^1 from P. In his talk, Or Meir presented a natural step in this direction, which lies between what is known and the original conjecture: he showed that an analogue of the conjecture holds for the composition of a function with a universal relation. The main technical tool is to use information complexity to analyze certain communication problems.

A core theme in circuit complexity is *depth-reduction*: very roughly, these are techniques to reduce the depth of a given circuit without increasing its size too much. The classic work of Valiant, Skyum, Berkowitz and Rackoff shows that any polynomial size arithmetic circuit has an equivalent circuit of polynomial size and $\log^2 n$ depth, where n is the number of input variables. Further impedus was given by Agrawal and Vinay who pushed the depth reduction to constant depth, thereby establishing the *chasm at depth* 4. It states that exponential lower bounds for circuits of depth 4 already give such bounds for general circuits. This was further improved by Koiran and by Tavenas.

Ramprasad Saptharishi gave a slightly different proof of the depth reduction of Tavenas in his talk. Thereby he was able to apply the technique to homogeneous formulas and constant depth formulas.

Chandan Saha presented a very strong result: an exponential lower bound for homogeneous depth-4 circuits that comes close to the chasm-barrier. His techniques also yield exponential lower bounds for certain nonhomogeneous depth-3 circuits. Having the parameters so close to the bounds coming from depth reduction make these results really exciting.

Depth reduction is also an crucial ingredient in Pascal Koirans talk. He presented a new version of the *τ-conjecture* for Newton polygons of bivariate polynomials. The τ-conjecture was originally stated by Shub and Smale:

> *the number of integer roots of a univariate polynomial should be polynomially bounded in the size of the smallest straight-line program computing it.*

Pascal Koiran proposed a new version of the τ-conjecture in his talk:

> *when a bivariate polynomial is expressed as a sum of products of sparse polynomials, the number of edges of its Newton polygon is polynomially bounded in the size of such an expression.*

If this new conjecture is true, then the permanent polynomial cannot be computed by polynomial-size arithmetic circuits.

Spurred by the depth reduction results, we have seen some great work on *Polynomial Identity Testing* (PIT) recently, in particular on depth-3 and depth 4 circuits, and on arithmetic branching programs. The most ambitious goal here 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 solves the PIT problem in the *black box* model.

Rohit Gurjar and Arpita Korwar gave a joint talk on PIT for read-once arithmetic branching programs. They presented a new technique called *basis isolating weight assignment*. These weight assignments yield a hitting set in quasi-polynomial time.

Michael Forbes considered the question whether the hitting set constructions running in quasi-polynomial time can be improved to polynomial time. He showed that in the case of depth-3 powering circuits (sums of powers of linear polynomials) one can obtain a hitting set of size $\text{poly}(s)^{\log\log s}$ for circuits of size s, which is pretty close to resolving the black-box identity testing problem for this class in polynomial time.

Swastik Kopparty showed the computational equivalence of factoring multivariate polynomials and PIT. For both problems we have efficient randomized algorithms. The question whether these algorithms can be derandomized are central in arithmetic complexity. Swastik established that they are equivalent.

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 natural complete polynomials for VP, based on the notion of graph homomorphism polynomials.

Eric Allender defined a class called ΛP which is in some sense dual to VP. Over finite fields, VP can be characterized by SAC^1, the class of logarithmic depth, polynomial-size semi-unbounded fan-in circuits (with bounded fan-in multiplication gates and unbounded fan-in addition gates). Eric defined the dual class ΛP in the same way, but with unbounded fan-in multiplication gates and bounded fan-in addition gates. He showed new characterizations of the complexity classes ACC^1 and TC^1 based on ΛP.

Klaus-Joern Lange defined a completeness notion on families of languages, called *densely complete*. He showed that the context-free languages are densely complete in SAC^1 via many-one AC^0-reductions.

Complexity

Ryan Williams once again demonstrated a fruitful interplay between algorithms and complexity. In his famous ACC-paper, he showed how to use fast algorithms for circuit satisfiability to

prove lower bounds with respect to the class ACC. In his present talk, Ryan reversed the direction and showed how to exploit techniques from complexity to obtain faster algorithms for the all-pairs shortest paths problem (APSP). He improved the running time from $n^3/\log^2 n$ previously to $n^3/2^{\Omega(\sqrt{\log n})}$. The big question here is whether one can improve the running time to $n^{3-\epsilon}$ for some $\epsilon > 0$. A crucial role in the new algorithm plays the *polynomial method* of Razborov and Smolensky, originally conceived for proving low-depth circuit lower bounds.

Michal Koucký talked on a model of computation he calls *catalytic computation*. In this model, a machine has only limited memory available, but has additionally access to almost unlimited amount of disk space, the *catalytic memory*. This disk is however already full of data. The machine has read-write access to the disk so that it can modify the content of the disk. However, at the end of a computation, the content of the catalytic memory has to be in its original state. The question now is whether the catalytic memory is of any use. Michal showed that a logspace bounded machine with a catalytic memory can do all of nondeterministic logspace. Hence, surprisingly, the catalytic memory really helps, unless L = NL.

Amnon Ta-Shma talked on the problem of *approximating* the eigenvalues of stochastic Hermitian matrices. In an earlier paper he had shown that this is possible in probabilistic logspace in the quantum model of computation, i.e. in BQL. In this talk, Amnon was asking whether this is also possible in probabilistic logspace in the classic world, i.e. in BPL. He showed that how to achieve approximations with *constant* accuracy. To bring the problem into BPL, one would have to approximate the eigenvalues with polynomially small accuracy. This remains open for now.

Venkatesan Guruswami condidered the following promise version of the satisfiability problem: Given a k-SAT instance with the promise that there is an assignment satisfying at least t out of k literals in each clause, can one efficiently find a satisfying assignment? Because 3-SAT is NP-hard, the promise problem is NP-hard for $t \leq k/3$. On the other hand, 2-SAT is efficiently solvable. Extensions of the 2-SAT algorithm show that the promis problem is efficiently solvable for $t \geq k/2$. Venkatesan showed a sharp borderline for the promise problem: it is NP-hard for $t < k/2$. The proof uses part of the PCP-machinery.

Communication Complexity

Amir Yehudayoff talked on communication complexity in the number on the forehead model. He considered the disjointness problem: there are k players, each having a set of numbers from $[n]$. A player can see the numbers of all the other players, but not his own numbers. The task of the payers is to determine, whether there is a number common to all sets. Amir showed a lower bound for the deterministic communication complexity of order $n/4^k$. This is quite amazing since it nearly matches the known upper bound, which is of order $k^2n/2^k$.

Arkadev Chattopadhyay talked on a communication model, where the inputs are distributed among the vertices of an undirected graph. The vertices coorespond to processors, each processor can send messages only to its neighbors in the graph. Arkadev showed lower bounds on the communication cost for computing certain functions in this model.

Rahul Santhanam considered a communication model called *compression game*. There are two players, Alice and Bob. Alice receives the whole input x and is computationally bounded, by $\mathrm{AC}^0[p]$ in this case, for some prime p. Bob has no information about x and is computationally unbounded. The communication cost of some function f is the number of bits Alice sent to Bob until they agree on the value $f(x)$. Rahul showed a lower bound on the communication complexity of the Mod_q-function, for any prime $q \neq p$.

Coding Theory

Error-correcting codes, particularly those constructed from polynomials, lie at the heart of many significant results in Computational Complexity. Usually, error correcting codes are studied with respect to the Hamming distance. Another model is that of random errors. Amir Shpilka in his talk considered the behaviour of Reed-Muller codes in the Shannon model of random errors. He showed that the rate for Reed-Muller codes with either low- or high-degree achieves (with high probability) the capacity for the Binary-Erasure-Channel

David Zuckerman talked on the relatively new concept of *non-malleable codes* which was introduced by Dziembowski, Pietrzak, and Wichs in 2010. Informally, a code is non-malleable if the message contained in a modified codeword is either the original message, or a completely unrelated value. Non-malleable codes provide an elegant algorithmic solution to the task of protecting hardware functionalities against "tampering attacks". David showed how to construct efficient non-malleable codes in the so-called C-split-state model that achieve constant rate and exponentially small error.

Game Theory

Steve Fenner considered the following two-player game on a finite partially odered set (poset) S: each player takes turns picking an element x of S and removes all $y > x$ from S. The first one to empty the poset wins. Daniel Grier showed that determining the winner of a poset game is PSPACE-complete. Steve considered the *black-white version* of the game, where each player and each element of S is assigned a color, black or white. Each player is only allowed to remove elements of their own color. He showed that also this black-white version of the poset game is PSPACE-complete. This is the first PSPACE-hardness result known for a purely numerical game. Another interesting result was that the game NimG, a generalization of both Nim and Geography, is polynomial-time solvable when restricted to undirected, bipartite graphs, whereas NimG is known to be PSPACE-complete for general graphs, both directed and undirected.

Bill Gasarch talked on a variant of classical NIM, where there is only one pile of stones and and a given set $\{a_1, a_2, \ldots, a_k\}$ of numbers. A move consists of choosing a number a_i from the set and then removing a_i stones from the pile. The first player who cannot move loses the game. This game has already been well studied. Bill considered an extension of the game where each player starts out with a number of dollars. Now each player has to spend a dollars to remove a stones. He presented some surprising results on the winning conditions for the extended game.

Cryptography

Farid Ablayev generalized classical universal hashing to the quantum setting. He defined the concept of a quantum hash generator and offer a design, which allows one to build a large number of different quantum hash functions. One of the important points here is to use unly few quantum bits. Farid proved that his construction is optimal with respect to the number of qubits needed.

Matthias Krause talked on approaches for designing authentication protocols for ultra-light weight devices as for example RFID chips. He proposed a new approach based on key stream generators as the main building block.

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

3 Overview of Talks

3.1 Quantum hashing via classical ϵ-universal hashing constructions

Farid Ablayev (Kazan State University, RU)

Joint work of Farid Ablayev, Marat Ablayev

Quantum computing is inherently a very mathematical subject, and discussions of how quantum computers can be more efficient than classical computers in breaking encryption algorithms have started since Peter Shor invented his famous quantum algorithm. The reaction of a cryptography community is a "Post-quantum cryptography", which refers to the research of problems (usually public-key cryptosystems) that are not efficiently breakable using quantum computers. Currently post-quantum cryptography includes different approaches, in particular, hash-based signature schemes such as Lamport signature and Merkle signature scheme.

Hashing itself is an important basic concept of computer science. The concept known as "universal hashing" was invented by Carter and Wegman in 1979.

In our research we define a quantum hashing as a quantum generalization of classical hashing. We define the concept of a quantum hash generator and offer a design, which allows one to build a large number of different quantum hash functions. The construction is based on composition of a classical ϵ-universal hash family and a given family of functions – quantum hash generators.

The relationship between epsilon-universal hash families and error-correcting codes give possibilities to build a large amount of different quantum hash functions. In particular, we present quantum hash function based on Reed-Solomon code, and we proved, that this construction is optimal in the sense of number of qubits needed.

Using the relationship between epsilon-universal hash families and Freivalds' fingerprinting schemas we present explicit quantum hash function and prove that this construction is optimal with respect to the number of qubits needed for the construction.

3.2 Dual VP classes

Eric Allender (Rutgers University, US)

Joint work of Eric Allender, Anna Gal, Ian Mertz
Main reference E. Allender, A. Gal, I. Mertz, "Dual VP Classes," ECCC, TR14-122, 2014.
URL http://eccc.hpi-web.de/report/2014/122/

We consider arithmetic complexity classes that are in some sense dual to the classes VP that were introduced by Valiant. This provides new characterizations of the complexity classes ACC^1 and TC^1, and also provides a compelling example of a class of high-degree polynomials that can be simulated via arithmetic circuits of much lower degree.

3.3 Asymptotic spectra of tensors

Markus Bläser (Universität des Saarlandes, DE)

Joint work of Manuel Arora, Markus Bläser

Asymptotic spectra were studied by Strassen to understand the asymptotic complexity of tensors, in particular of matrix multiplication. The (equivalence classes of) tensors are embedded into an ordered ring and then results by Stone, Kadison, and Dubois are applied to represent tensors by nonnegative continuous functions on some Hausdorff space.

In the first part of the talk, we give an introduction to asymptotic spectra and the work by Strassen. In the second part of the talk, we introduce a new order on the equivalence classes of tensors and study the resulting new spectra.

3.4 Topology matters in communication

Arkadev Chattopadhyay (TIFR, IN)

Joint work of Arkadev Chattopadhyay, Jaikumar Radhakrishnan, Atri Rudra

We consider the communication cost of computing functions when inputs are distributed among the vertices of an undirected graph. The communication is assumed to be point-to-point: a processor sends messages only to its neighbors. The processors in the graph act according to a pre-determined protocol, which can be randomized and may err with some small probability. The communication cost of the protocol is the total number of bits exchanged in the worst case. Extending recent work that assumed that the graph was the complete graph (with unit edge lengths), we develop a methodology for showing lower bounds that are sensitive to the graph topology. In particular, for a broad class of graphs, we obtain a lower bound of the form k^2n, for computing a function of k inputs, each of which is n-bits long and located at a different vertex. Previous works obtained lower bounds of the form kn.

This methodology yields a variety of other results including the following:

- A tight lower bound (ignoring poly-log factors) for Element Distinctness, settling a question of Phillips, Verbin and Zhang (SODA'12);
- a distributed XOR lemma;
- a lower bound for composed functions, settling a question of Phillips et al.;
- new topology-dependent bounds for several natural graph problems considered by Woodruff and Zhang (DISC'13).

To obtain these results we use tools from the theory of metric embeddings and represent the topological constraints imposed by the graph as a collection of cuts, each cut providing a setting where our understanding of two-party communication complexity can be effectively deployed.

3.5 Some new results on combinatorial game complexity

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

Joint work of Daniel Grier, Stephen A. Fenner Daniel, Jochen Messner, Luke Schaeffer, Thomas Thierauf

We give new hardness and easiness results for determining the winner in certain two-player games with perfect information. On the hardness side, we show that Black-White-Poset-Games (BWPG) and a generalized version of the game Col are both PSPACE-complete (via reductions from variants of TQBF). The BWPG result is the first PSPACE-hardness result known for a purely numerical game. On the easiness side, we show that NimG (a generalization of both Nim and Geography) is polynomial-time computable when restricted to undirected, bipartite graphs. (NimG is known to be PSPACE-complete for general graphs, both directed and undirected). We also show that Toads and Frogs is polynomial-time computable when each row is restricted to one toad and one frog.

3.6 Hitting Sets for Depth-3 Powering Circuits

Michael Forbes (University of California – Berkeley, US)

Joint work of Michael Forbes, Ramprasad Saptharishi, Amir Shpilka

A recent line of research has constructed hitting sets for various read-once and set-multilinear models of computation, as such hitting sets yield black-box polynomial identity testing algorithms. Despite the fact that these models all have a "white-box" identity testing algorithm that runs in polynomial-time (due to Raz and Shpilka), the black-box algorithms all run in quasipolynomial time. Improving these algorithms seems challenging, especially as these algorithms can be viewed as algebraic analogues of pseudorandom generators for RL (which have been stuck at $RL \subset L^2$ for 25 years).

In this work, we identify a particularly simple subclass of the above models, known as depth-3 powering circuits (sums of powers of linear polynomials). In fact, this is the simplest complete algebraic circuit class for which we do not have explicit polynomial-size hitting sets. We show how to combine two different hitting set constructions, each of size $\text{poly}(s)^{\log s}$ for size s circuits, to obtain a hitting set of size $\text{poly}(s)^{\log\log s}$, which is tantalizingly close to resolving the black-box identity testing problem for this class.

3.7 NIM with Cash

William Gasarch (University of Maryland – College Park, US)

Joint work of William Gasarch, John Purtilo, Doug Ulrich
Main reference W. Gasarch, J. Purtilo, "NIM with Cash," University of Maryland Computer Science Department, CS-TR-5015, 2012.
URL http://hdl.handle.net/1903/12908

$\text{NIM}(a_1, \ldots, a_k; n)$ is a 2-player game where initially there are n stones on the board and the players alternate removing either a_1 or $\ldots$ a_k stones. The first player who cannot move loses. This game has been well studied. For example, it is known that for $\text{NIM}(1, 2, 3; n)$

Player II wins if and only if n is divisible by 4. This game is interesting because even small sets $\{a_1, \ldots, a_k\}$ lead to interesting win conditions.

We investigate an extension of the game where Player I starts out with d_1 dollars and Player II starts out with d_2 dollars, and a player has to spend a dollars to remove a stones. For several choices of $a_1, \ldots, a_k$ we determine for all (n, d_1, d_2) which player wins. The win condition depend on *both* what n is congruent to mod some M *and* on how d_1 and d_2 relate. This game is interesting because even small sets $\{a_1, \ldots, a_k\}$ lead to interesting and complicated win conditions.

Some of our results are surprising. For example, there are cases where both players are poor, yet the one with less money wins.

3.8 Hitting Set for Read-Once Arithmetic Branching Programs

Rohit Gurjar and Arpita Korwar (IIT Kanpur, IN)

Joint work of Manindra Agrawal, Rohit Gurjar, Arpita Korwar, Nitin Saxena
Main reference M. Agrawal, R. Gurjar, A. Korwar, N. Saxena, "Hitting-sets for ROABP and Sum of Set-Multilinear circuits," ECCC, TR14-085, 2014.
URL http://eccc.hpi-web.de/report/2014/085/

In the march towards a deterministic solution for the polynomial identity testing problem, recently there has been a considerable amount of work on depth-3 set-multilinear circuits and read once arithmetic branching programs (ROABP). Continuing in this direction, we have given a $(n\delta)^{O(\log n)}$-time blackbox PIT algorithm for unknown-order, n-variate, individual degree δ ROABP, improving the previously known $n^{O(\delta \log^2 n)}$-time algorithm.

In this talk, we will look at a new idea "Basis Isolating Weight Assignment" for designing a hitting set for depth-3 circuits. This idea has been applied to read-once arithmetic branching programs (RO-ABPs) to get a $n^O(\log n)$ time hitting set.

3.9 (2+eps)-SAT is NP-hard

Venkatesan Guruswami (Carnegie Mellon University , US)

Joint work of Per Austrin, Venkatesan Guruswami, Johan Håstad
Main reference P. Austrin, V. Guruswami, J. Håstad, "$(2+\epsilon)$-SAT is NP-hard," ECCC, TR13-159, 2013/2014; peer-reviewed version to appear in Proc. of the 55th IEEE Symp. on Foundations of Computer Science (FOCS'14).
URL http://eccc.hpi-web.de/report/2013/159/

Given a k-SAT instance with the promise that there is an assignment satisfying at least t out of k literals in each clause, can one efficiently find a satisfying assignment (setting at least one literal to true in every clause)? The NP-hardness of 3-SAT implies that this problem is NP-hard when $t \leq k/3$, and extensions of some 2-SAT algorithms give efficient solutions when $t \geq k/2$.

We prove that for $t < k/2$, the problem is NP-hard. Thus, satisfiability becomes hard when the promised density of true literals falls below 1/2. One might thus say that the transition from easy to hard in 2-SAT vs. 3-SAT takes place just after two and not just before three.

The talk will sketch most of the proof, which is based on the fact that the only functions passing a natural dictatorship test are "juntas" depending on few variables. We will briefly mention the general "universal-algebraic" principle (based on the lack of certain *polymorphisms*) that underlies hardness of constraint satisfaction.

A strengthening of the k-SAT result shows that given a $(2t+1)$-uniform hypergraph that can be 2-colored such that each edge has near-perfect balance (at most $t+1$ vertices of each color), it is NP-hard to even find a 2-coloring that avoids a monochromatic edge. This shows extreme hardness of discrepancy minimization for systems of bounded-size sets.

(Subsequent work with Euiwoong Lee, available as ECCC TR14-043 and to appear at SODA 2015, in fact rules out coloring with any constant number of colors for the case of $2k$-uniform hypergraphs with discrepancy 2, and shows further extensions to hypergraphs admitting a near-balanced rainbow coloring with more than two colors.)

3.10 A τ-conjecture for Newton polygons

Pascal Koiran (ENS – Lyon, FR)

Joint work of Pascal Koiran, Natacha Portier, Sébastien Tavenas, Stéphan Thomassé
Main reference P. Koiran, N. Portier, S. Tavenas, S. Thomassé, "A tau-conjecture for Newton polygons," arXiv:1308.2286v2 [cs.CC], 2014.
URL http://arxiv.org/abs/1308.2286v2

One can associate to any bivariate polynomial $P(X,Y)$ its Newton polygon. This is the convex hull of the points (i,j) such that the monomial X^iY^j appears in P with a nonzero coefficient. We conjecture that when P is expressed as a sum of products of sparse polynomials, the number of edges of its Newton polygon is polynomially bounded in the size of such an expression. We show that this "τ-conjecture for Newton polygons," even in a weak form, implies that the permanent polynomial is not computable by polynomial size arithmetic circuits. We make the same observation for a weak version of an earlier "real τ-conjecture." Finally, we make some progress toward the τ-conjecture for Newton polygons using recent results from combinatorial geometry.

3.11 Equivalence of polynomial identity testing and multivariate polynomial factorization

Swastik Kopparty (Rutgers University, US)

Joint work of Swastik Kopparty, Shubhangi Saraf, Amir Shpilka
Main reference S. Kopparty, S. Saraf, A. Shpilka, "Equivalence of Polynomial Identity Testing and Deterministic Multivariate Polynomial Factorization," ECCC, TR14-001, 2014.
URL http://eccc.hpi-web.de/report/2014/001/

In this work, we show that the problem of deterministically factoring multivariate polynomials reduces to the problem of deterministic polynomial identity testing. Specifically, we show that given an arithmetic circuit (either explicitly or via black-box access) that computes a polynomial $f(X_1,\ldots,X_n)$, the task of computing arithmetic circuits for the factors of f can be solved deterministically, given a deterministic algorithm for the polynomial identity

testing problem (we require either a white-box or a black-box algorithm, depending on the representation of f).

Together with the easy observation that deterministic factoring implies a deterministic algorithm for polynomial identity testing, this establishes an equivalence between these two central derandomization problems of arithmetic complexity. Previously, such an equivalence was known only for multilinear circuits (Shpilka and Volkovich, ICALP 2010).

3.12 Catalytic computation

Michal Koucký (Charles University, CZ)

Joint work of Harry Buhrman, Richard Cleve, Michal Koucký, Bruno Loff, Florian Speelman
Main reference H. Buhrman, R. Cleve, M. Koucky, B. Loff, F. Speelman, "Computing with a full memory: Catalytic space," ECCC, TR14-053, 2014.
URL http://www.eccc.hpi-web.de/report/2014/053/

The known hierarchy theorems hold in a vacuum. However, our computation happens in a wider context. Although we may have only limited memory to carry out our computation we have access to almost unlimited amount of disk space provided at the end of the computation the disk contains exactly the same content as at the beginning. This naturally leads to a question: what can be computed in space s when we have access to read-write "catalytic" memory that we can use provided at the end of the computation the content of the catalytic memory is at its original, possibly incompressible, state. Is there any advantage in having this extra catalytic memory?

We provide affirmative answer to this question (assuming NL differs from L). We show that in space s with catalytic memory we can compute deterministically functions computable in non-deterministic space s. We can extend the results even further. The main techniques come from a special form of reversible computation that we call transparent computation.

3.13 Sharp Security Bounds for Authentication with Key Stream Generators

Matthias Krause (Mannheim University, DE)

In the last years, various approaches for designing authentication protocols for ultralight weight devices (e.g., RFIDs) have been intensively studied (HB-type protocols, Linear protocols, block cipher based solutions etc.) We propose an new approach which uses a key stream generators (KSG) as the main building block. The usage of KSGs appears advantageous in this context, as several well analyzed ultralight weight practical designs are available.

We propose a new mode of operation for KSGs which leads to an encryption function $E = E(x)$ of type $E(x) = F(P(x + k_1) + k_2)$, where F denotes a pseudo-random function, P a pseudo-random permutation and k_1, k_2 secret keys of length n.

We show a sharp information theoretic bound of $\frac{2}{3}n$ for the effective key length of this construction w.r.t. to an attacker of unbounded computational power which has access to E-, F- and P, P^{-1}-oracles.

3.14 Dense Completeness

Klaus-Joern Lange (Universität Tübingen, DE)

A family of formal languages F is said to be *densely complete* in a complexity class $\mathcal{C}$, iff F is contained in $\mathcal{C}$ and for each $L \in \mathcal{C}$ there exists some $L' \in F$ such that both L is reducible to L' and L' is reducible to L, i.e., L and L' have the same complexity modulo the chosen notion of reducibility.

Using many-one reductions computable in AC^0, it can be shown that the context-free languages are densely complete in SAC^1, the one-counter languages in $\mathrm{Nspace}(\log n)$, and the indexed languages in NP. On the other, hand the regular languages are not densely complete in NC^1. This result is now extended to the nonregular family of visibly one-counter languages.

3.15 Homomorphism polynomials complete for VP

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

Joint work of Arnaud Durand, Meena Mahajan, Guillaume Malod, Nicolas de Rugy-Altherre, Nitin Saurabh

The VP versus VNP question, introduced by Valiant, is probably the most important open question in algebraic complexity theory. Thanks to completeness results, a variant of this question, VBP versus VNP, can be succintly restated as asking whether the permanent of a generic matrix can be written as a determinant of a matrix of polynomially bounded size. Strikingly, this restatement does not mention any notion of computational model. To get a similar restatement for the original and more fundamental question, and also to better understand the class itself, we need a complete polynomial for VP. Ad hoc constructions yielding complete polynomials were known, but not natural examples in the vein of the determinant. This talk describes several variants of natural complete polynomials for VP, based on the notion of graph homomorphism polynomials.

3.16 Toward Better Formula Lower Bounds: An Information Complexity Approach to the KRW Composition Conjecture

Or Meir (Institute of Advanced Study – Princeton, US)

Joint work of Dmitry Gavinsky, Or Meir, Omri Weinstein, Avi Wigderson
Main reference D. Gavinsky, O. Meir, O. Weinstein, A. Wigderson, "Toward Better Formula Lower Bounds: An Information Complexity Approach to the KRW Composition Conjecture," ECCC, TR13-190, 2013/2014.
URL http://www.eccc.hpi-web.de/report/2013/190/

One of the major open problems in complexity theory is proving super-logarithmic lower bounds on the depth of circuits (i.e., $\mathbf{P} \not\subseteq \mathbf{NC}^1$). This problem is interesting for two reasons:

first, it is tightly related to understanding the power of parallel computation and of small-space computation; second, it is one of the first milestones toward proving super-polynomial circuit lower bounds.

Karchmer, Raz, and Wigderson suggested to approach this problem by proving the following conjecture: given two boolean functions f and g, the depth complexity of the composed function $g \circ f$ is roughly the sum of the depth complexities of f and g. They showed that the validity of this conjecture would imply that $\mathbf{P} \not\subseteq \mathbf{NC}^1$.

As a starting point for studying the composition of functions, they introduced a relation called ?the universal relation?, and suggested to study the composition of universal relations. This suggestion proved fruitful, and an analogue of the KRW conjecture for the universal relation was proved by Edmonds et. al. An alternative proof was given later by Håstad and Wigderson. However, studying the composition of functions seems more difficult, and the KRW conjecture is still wide open.

In this work, we make a natural step in this direction, which lies between what is known and the original conjecture: we show that an analogue of the conjecture holds for the composition of a function with a universal relation. We also suggest a candidate for the next step and provide initial results toward it.

Our main technical contribution is developing an approach based on the notion of information complexity for analyzing KW relations – communication problems that are closely related to questions on circuit depth and formula complexity. Recently, information complexity has proved to be a powerful tool, and underlined some major progress on several long-standing open problems in communication complexity. In this work, we develop general tools for analyzing the information complexity of KW relations, which may be of independent interest.

3.17 A Geometric Resolution-based Framework for Joins

Atri Rudra (SUNY – Buffalo, US)

Joint work of Mahmoud Abo Khamis, Hung Ngo, Dung Nguyen, Chris Re, Atri Rudra

We present a simple geometric framework for the relational join. Using this framework, we design an algorithm that achieves the fractional hypertree-width bound, which generalizes classical and recent worst-case algorithmic results on computing joins. In addition, we use our framework and the same algorithm to show a series of what are colloquially known as beyond worst-case results. The framework allows us to prove results for data stored in Btrees, multidimensional data structures, and even multiple indices per table. A key idea in our framework is formalizing the inference one does with an index as a type of geometric resolution; transforming the algorithmic problem of computing joins to a geometric problem. Our notion of geometric resolution can be viewed as a geometric analog of logical resolution.

In this talk, I will focus on our geometric interpretation of joins and give a flavor of our beyond worst-case results. In particular, I will present the main (very simple!) algorithmic ideas behind our upper bounds and clarify the actual model of resolution that we use. I will end with some open questions on lower bounds and some algebraic versions of the join problem that we do not know much about.

3.18 Lower bounds for (homogeneous) depth-4 and (nonhomogeneous) depth-3 arithmetic circuits

Chandan Saha (Indian Institute of Science – Bangalore, IN)

Joint work of Neeraj Kayal, Chandan Saha, Srikanth Srinivasan, Nutan Limaye

An approach to proving a super-polynomial lower bound for arithmetic circuits reduces the problem to proving "strong enough" lower bounds for small depth circuits, in particular (nonhomogeneous) depth-3 circuits and (homogeneous) depth-4 circuits. Depth of a circuit is the number of layers of gates in it.

In the talk, we plan to discuss an exponential lower bound for (homogeneous) depth-4 circuits that comes close to being 'strong enough'. More precisely, we give an explicit family of polynomials of degree d on N variables (with $N = d^3$ in our case) with $0,1$-coefficients such that for any representation of a polynomial f in this family of the form

$$f = \sum_i \prod_j Q_{ij},$$

where the Q_{ij}'s are homogeneous polynomials (recall that a polynomial is said to be homogeneous if all its monomials have the same degree), it must hold that

$$\sum_{i,j} (\text{Number of monomials of } Q_{ij}) \quad \geq \quad 2^{\Omega(\sqrt{d} \cdot \log N)}.$$

The above mentioned family, which we refer to as the Nisan-Wigderson design-based family of polynomials, is in the complexity class VNP. Our work builds on several recent lower bound results and the techniques also yield exponential lower bounds for certain (nonhomogeneous) depth-3 circuits, in particular depth-3 circuits with low bottom fanin which also answers a question posed by Shpilka and Wigderson (CCC'99).

3.19 Lower Bounds on $\mathrm{AC}^0[p]$-Compression Games

Rahul Santhanam (University of Edinburgh, GB)

Joint work of Igor Carboni Oliveira, Rahul Santhanam

Given a class of circuits $\mathcal{C}$, a $\mathcal{C}$-compression game to compute a Boolean function f is a 2-player game played as follows. Alice is a computationally bounded player who receives the input x, and whose next-message function is computable in $\mathcal{C}$. Bob is a computationally unbounded player who has no information about x before communication happens. Alice and Bob communicate until they agree on the value of $f(x)$. The cost of a compression protocol is the number of bits communicated from Alice to Bob. Compression games hybridize computational complexity and communication complexity. They generalize the notion of instance compression due to Harnik & Naor and Bodlaender, Downey, Fellows & Hermelin, and have applications in cryptography, parameterized complexity and circuit complexity.

We prove new lower bounds for $\mathcal{C}$-compression games where $\mathcal{C} = \mathrm{AC}^0[p]$ for some prime p. We show that the Mod_q function requires deterministic compression cost $\Omega(n/\mathrm{polylog}(n))$, and randomised compression cost $\Omega(\sqrt{n}/\mathrm{polylog}(n))$, whenever q is a prime different from p.

We also define and study multi-player compression games, where Alice communicates in parallel with several unbounded players Bob_1, $\text{Bob}_2, \ldots, \text{Bob}_k$ (which cannot communicate with each other), and the cost of the protocol is the maximum amount of communication from Alice to any fixed Bob_i. We show compression cost lower bound $n^{\Omega(1)}$ for constant-round multi-player $\text{AC}^0[p]$-compression games computing the Mod_q function when $q \neq p$, even when $k = \text{poly}(n)$. As an application, we strengthen the known $\text{AC}^0[p]$ lower bounds of Razborov and Smolensky to the setting of oracle circuits with arbitrary oracle gates, with some mild restrictions on the number of layers and fan-in of the oracle gates.

Finally we obtain a stronger version of the round separation result of Chattopadhyay & Santhanam for AC^0-compression games.

3.20 Depth Reduction for Arithmetic Circuits

Ramprasad Saptharishi (Microsoft Research India – Bangalore, IN)

Joint work of Saptharishi, Ramprasad; Vinay, V.

Almost all attempts to prove lower bounds for subclasses arithmetic circuits proceed by addressing a "depth four analogue" of the subclass. This talk shall give a slightly different proof of the depth reduction of Tavenas, and enable us to study this for homogeneous formulas and constant depth formulas.

3.21 Reed-Muller codes with respect to random errors and erasures

Amir Shpilka (Technion – Haifa, IL)

Joint work of Emmanuel Abbe, Amir Shpilka, Avi Wigderson

In TCS we usually study error correcting codes with respect to the Hamming metric, i.e. we study their behaviour with respect to worst case errors. However, in coding theory a more common model is that of random errors, where Shannon's results show a much better tradeoff between rate and decoding radius.

We consider the behaviour of Reed-Muller codes in the Shannon model of random errors. In particular, we show that RM codes with either low- or high-degree (degree $n^{1/2}$ or $n - n^{1/2}$, respectively), with high probability, can decode from an $1 - R$ fraction of random erasures (where R is the rate). In other words, for this range of parameters RM codes achieve capacity for the Binary-Erasure-Channel. This result matches experimental observations that RM codes can achieve capacity for the BEC, similarly to Polar codes. We also show that RM-codes can handle many more random errors than the minimum distance, i.e. roughly $n^{r/2}$ errors for codes of degree $n - r$ (where the minimum distance is only 2^r).

We show that the questions regarding the behaviour of Reed-Muller codes wrt random errors are tightly connected to the following question. Given a random set of vectors in $\{0,1\}^n$, what is the probability the their r^{th} tensor products are linearly independent? We obtain our results by giving answer to this question for certain range of parameters.

3.22 On the problem of approximating the eigenvalues of undirected graphs in probabilistic logspace

Amnon Ta-Shma (Tel Aviv University, IL)

We focus on the problem of *approximating* the eigenvalues of stochastic Hermitian operators in small space, which is a natural and important problem. The ultimate goal is solving the problem in full in BPL, i.e., with polynomially-small accuracy. In this paper, however, we only achieve approximations with *constant* accuracy. Our technique is new. We also show that going beyond constant accuracy requires a new idea.

3.23 Faster All-Pairs Shortest Paths Via Circuit Complexity

Ryan Williams (Stanford University, US)

I presented an algorithm for solving the all-pairs shortest paths problem on n-node graphs with edge weights in $[0, n^k]$ (for arbitrary k) running in $n^3/2^{(\log n)^\delta}$ time for an unspecified $\delta > 0$. In the full paper, I give an algorithm for solving the all-pairs shortest paths problem on n-node real-weighted graphs in the "real RAM" model, running in $n^3/2^{\Omega(\sqrt{\log n})}$ time.

Both algorithms apply the *polynomial method* of Razborov and Smolensky, originally conceived for proving low-depth circuit lower bounds. We show how low-depth circuits can compute a so-called "min-plus inner product" of two vectors, then show how to evaluate such low-depth circuits efficiently on many pairs of vectors by randomly reducing the circuit to a low-degree polynomial over $\mathbb{F}_2$ and using fast rectangular matrix multiplication.

3.24 Lower bounds on the multiparty communication complexity of disjointness

Amir Yehudayoff (Technion – Haifa, IL)

We give a proof of order $n/4^k$ lower bound for the deterministic communication complexity of set disjointness with k players in the number on the forehead model. This is the first lower bound that is linear in n, and it nearly matches the known upper bound. We discuss Sherstov's proof of an order $n^{1/2}/(k2^k)$ lower bound on the randomized complexity.

3.25 Non-Malleable Codes Against Constant Split-State Tampering

David Zuckerman (University of Texas at Austin, US)

Joint work of Eshan Chattopadhyay, David Zuckerman
Main reference E. Chattopadhyay, D. Zuckerman, "Non-Malleable Codes Against Constant Split-State Tampering," ECCC, TR14-102, 2014.
URL http://eccc.hpi-web.de/report/2014/102/

Non-malleable codes were introduced by Dziembowski, Pietrzak and Wichs as an elegant generalization of the classical notion of error detection, where the corruption of a codeword is viewed as a tampering function acting on it. Informally, a non-malleable code with respect to a family of tampering functions $\mathcal{F}$ consists of a randomized encoding function Enc and a deterministic decoding function Dec such that for any m, $\mathrm{Dec}(\mathrm{Enc}(m)) = m$. Further, for any tampering function $f \in \mathcal{F}$ and any message m, $\mathrm{Dec}(f(\mathrm{Enc}(m)))$ is either m or is ϵ-close to a distribution D_f independent of m, where ϵ is called the error.

Of particular importance are non-malleable codes in the C-split-state model. In this model, the codeword is partitioned into C equal sized blocks and the tampering function family consists of functions $(f_1, \ldots, f_C)$ such that f_i acts on the i^{th} block. For $C = 1$ there cannot exist non-malleable codes. For $C = 2$, the best known explicit construction is by Aggarwal, Dodis and Lovett who achieve rate $= \Omega(n^{-6/7})$ and error $= 2^{-\Omega(n^{-1/7})}$, where n is the block length of the code.

In our main result, we construct efficient non-malleable codes in the C-split-state model for $C = 10$ that achieve constant rate and error $= 2^{-\Omega(n)}$. These are the first explicit codes of constant rate in the C-split-state model for any $C = o(n)$, that do not rely on any unproven assumptions. We also improve the error in the explicit non-malleable codes constructed in the bit tampering model by Cheraghchi and Guruswami.

Our constructions use an elegant connection found between seedless non-malleable extractors and non-malleable codes by Cheraghchi and Guruswami. We explicitly construct such seedless non-malleable extractors for 10 independent sources and deduce our results on non-malleable codes based on this connection. Our constructions of extractors use encodings and a new variant of the sum-product theorem.

Participants

- Farid Ablayev
Kazan State University, RU
- Manindra Agrawal
IIT – Kanpur, IN
- Eric Allender
Rutgers Univ. – Piscataway, US
- Vikraman Arvind
The Institute of Mathematical Sciences, IN
- Markus Bläser
Universität des Saarlandes, DE
- Andrej Bogdanov
Chinese Univ. of Hong Kong, HK
- Harry Buhrman
CWI – Amsterdam, NL
- Sourav Chakraborty
Chennai Mathematical Inst., IN
- Arkadev Chattopadhyay
TIFR Mumbai, IN
- Stephen A. Fenner
University of South Carolina – Columbia, US
- Michael Forbes
University of California – Berkeley, US
- Lance Fortnow
Georgia Inst. of Technology, US
- Anna Gál
University of Texas – Austin, US
- William Gasarch
University of Maryland, US
- Frederic Green
Clark University – Worcester, US
- Rohit Gurjar
IIT – Kanpur, IN
- Venkatesan Guruswami
Carnegie Mellon University, 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 Univ. – Piscataway, US
- Arpita Korwar
IIT – Kanpur, IN
- Michal Koucký
Charles University – Prague, CZ
- Matthias Krause
Universität Mannheim, DE
- Klaus-Jörn Lange
Universität Tübingen, DE
- Sophie Laplante
University Paris-Diderot, FR
- Meena Mahajan
The Institute of Mathematical Sciences, IN
- Or Meir
Institute of Advanced Study – Princeton, US
- Peter Bro Miltersen
Aarhus University, DK
- Natacha Portier
ENS – Lyon, FR
- Atri Rudra
SUNY – Buffalo, US
- Chandan Saha
Indian Institute of Science – Bangalore, IN
- Rahul Santhanam
University of Edinburgh, GB
- Ramprasad Saptharishi
Microsoft Research India – Bangalore, IN
- Uwe Schöning
Universität Ulm, DE
- Ronen Shaltiel
University of Haifa, IL
- Amir Shpilka
Technion – Haifa, IL
- Florian Speelman
CWI – Amsterdam, NL
- Amnon Ta-Shma
Tel Aviv University, IL
- Thomas Thierauf
Hochschule Aalen, DE
- Jacobo Torán
Universität Ulm, DE
- Christopher Umans
CalTech, US
- Nikolay K. Vereshchagin
Moscow State University, RU
- Ryan Williams
Stanford University, US
- Amir Yehudayoff
Technion – Haifa, IL
- David Zuckerman
University of Texas – Austin, US