Report from Dagstuhl Seminar 12421

Algebraic and Combinatorial Methods in Computational Complexity

Edited by

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

1 **Indian Inst. of Technology – Kanpur, IN,** manindra@iitk.ac.in
2 **Hochschule Aalen, DE,** Thomas.thierauf@HTW-Aalen.de
3 **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 (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 PCP characterization of NP and the Agrawal-Kayal-Saxena polynomial-time primality test are two prominent examples.

Recently, there have been some works going in the opposite direction, giving alternative combinatorial proofs for results that were originally proved algebraically. These alternative proofs can yield important improvements because they are closer to the underlying problems and avoid the losses in passing to the algebraic setting. A prominent example is Dinur's proof of the PCP Theorem via gap amplification which yielded short PCPs with only a polylogarithmic length blowup (which had been the focus of significant research effort up to that point). We see here (and in a number of recent works) an exciting interplay between algebraic and combinatorial techniques.

This seminar aims to capitalize on recent progress and bring together researchers who are using a diverse array of algebraic and combinatorial methods in a variety of settings.

Seminar 14.–19. October, 2012 – www.dagstuhl.de/12421

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

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

Digital Object Identifier 10.4230/DagRep.2.10.60

Edited in cooperation with Thomas Thierauf

1 Executive Summary

Manindra Agrawal
Thomas Thierauf
Christopher Umans

The seminar brought together more than 50 researchers covering a wide spectrum of complexity theory. The focus on algebraic and combinatorial methods showed the great importance of such techniques for theoretical computer science. We had 30 talks, most of them lasting

Algebraic and Combinatorial Methods in Comp. Complexity, *Dagstuhl Reports*, Vol. 2, Issue 10, pp. 60–78
Editors: Manindra Agrawal, Thomas Thierauf, and Christopher Umans
DAGSTUHL REPORTS Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

about 40 minutes, leaving ample room for discussions. In the following we describe the major topics of discussion in more detail.

Circuit Complexity

is an area of fundamental importance to Complexity, which has resisted all efforts to prove strong lower bounds. We had several talks on circuit upper and lower bounds.

Valentine Kabanets considered the following compression problem: Given a truth table of an n-variate Boolean function f, find a Boolean circuit C of non-trivial size (less than $2^n/n$) that computes f. The motivation comes from the desire to understand "easy" functions (what property of their truth tables makes such functions compressible), and "hard" functions (once we understand which functions are compressible, we may be able to prove certain functions to require high circuit complexity). As an example, he showed that the class of functions computable by polysize AC^0-circuits, and linear-size de Morgan formulas are compressible.

The Shub and Smale's "tau-conjecture" states that 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 real version of the tau-conjecture in his talk. If this new conjecture is true, then the permanent polynomial cannot be computed by polynomial-size arithmetic circuits.

Fred Green showed that degree-d block-symmetric multivariate polynomials modulo any odd p correlate with parity exponentially better than degree-d symmetric polynomials, for certain values of d. The result is obtained through the development of a theory call spectral analysis of symmetric correlation, which originated in work of Cai, Green, and Thierauf.

Chaudhuri and Radhakrishnan used certifying polynomials to show that Approximate Majority cannot be computed by AC^0-circuits of size $n^{1+o(1)}$. In his talk, Swastik Kopparty extended their technique and showed that Approximate Majority cannot be computed by AC^0[parity]-circuits of size $n^{1+o(1)}$. This implies a separation between the power of AC^0[parity]-circuits of near-linear size and uniform AC^0[parity]-circuits of polynomial size.

Neeraj Kayal talked on the problem of computing the smallest formula for a polynomial given as a blackbox. The complexity of this problem is still unclear. It is conjectured that it is NP-hard. Neeraj presented his very impressive result, a randomized algorithm that given blackbox access to the polynomial f computed by an unknown/hidden arithmetic formula reconstructs, on the average, an equivalent or smaller formula in time polynomial in the size of its output . This is the strongest model of arithmetic computation for which a reconstruction algorithm is presently known, albeit efficient in a distributional sense rather than in the worst case.

Coding Theory

Error-correcting codes, particularly those constructed from polynomials, lie at the heart of many of the most significant results in Computational Complexity (e.g. interactive proofs, PCPS, hardness amplification, explicit constructions, derandomization, etc.) In many of these applications it is evident that the *local-testability/decodability* of the code is critical.

A q-query Locally Decodable Code (LDC) is an error-correcting code that allows to read any particular symbol of the message by reading only q symbols of the codeword. In a completely new approach, Klim Efremenko showed how to construct q-query LDCs from representation theory. Parikshit Gopalan showed an equivalence between locally testable codes and Cayley graphs with certain spectral properties. These Cayley graphs can be viewed as “derandomized hypercubes” which preserve several important properties of the Boolean hypercube such as small-set expansion, large threshold rank and hypercontractivity.

Shubhangi Saraf talked about the classical theorem of Sylvester-Gallai, which says that, if for every two points there is a third point on the line through them, then all points are on the same line. In the stable versions of the theorem, it is only guaranteed that many triples of points are approximately collinear. Configurations with many approximately collinear q-tuples of points also arise naturally in stable versions of Locally Correctable Codes over the complex numbers. She showed that that such stable codes with constant query complexity do not exist.

Explicit Constructions

Until recently the best-known construction of extractors (and their cousins, *condensers*) was a primarily combinatorial construction of Lu, Reingold, Vadhan, and Wigderson. Then Guruswami, Umans and Vadhan gave an entirely algebraic construction, utilizing the new polynomial error-correcting codes of Parvaresh and Vardy. Amnon Ta-Shma presented a new construction of condensers based on Parvaresh-Vardy codes. Amnons condensers have entropy rate $1 - \alpha$ for subconstant α (in contrast to GUV which required constant α) and suffer only sublinear entropy loss.

Ronen Shaltiel presented new constructions of zero-error seedless dispersers for bit-fixing sources and affine sources. Ronen used these dispersers to construct an algorithm for a problem related to the Write-Once-Memory (WOM) problem in which once we raise a storage cell from zero to one, it is stuck at this value. He gives the first explicit scheme with asymptotically optimal rate.

Anna Gál identified a new class of superconcentrator-like graphs with connectivity properties distinct from previously studied ones. Anna showed that any circuit computing good codes must satisfy such superconcentrator-like properties.

Probabilistic proof systems is a sub-field of complexity theory that investigates questions such as “how can we use randomness to prove and verify assertions?”, “what do we gain from using randomness in verification procedures?”, and “what assertions can be verified by probabilistic verification procedures?”. Research in this area began in the 1980, and has led to several of the most important achievements of complexity theory in those decades.

A line of research from the recent years is aimed at finding alternative “combinatorial” proofs for those key results, i.e., proofs that do not rely on algebra. This line of research is motivated by trying to gain more intuition of those results, as well as to understand the properties of polynomials that make them useful for such constructions. Or Meir gave a very interesting survey talk about this line of research.

Complexity

In a much appreciated talk, Joshua Grochow gave a very interesting survey-type talk on the Geometric Complexity Theory (GCT) program, which was introduced by Mulmuley and Sohoni to attack fundamental lower bound problems in complexity – such as P vs NP – using algebraic geometry and representation theory. Joshua succeeded in explaining very nicely some of the intuition behind the use of algebraic geometry and representation theory in complexity.

Michal Koucký gave a very interesting overview talk on the online labeling problem, where one receives n integers from the set $\{1, \ldots, r\}$ and has to store them in an array of size m. The integers are presented sequentially in an arbitrary order, and must be stored in the array in sorted order. The complexity measure is essentially the number of times an element has to be moved in to make space for a newly arrived item. Michal showed that various known algorithms in the literature solve the problem asymptotically optimal.

Perfect matching is in P but not known to be in NC. Counting the number of perfect matchings in a graph is #P-complete. In contrast, Vazirani showed that counting the number of perfect matchings in a planar graph is in NC. So in particular, the decision version of perfect matching in planar graphs is in NC. Hence one way to get perfect matching in NC could be to reduce perfect matching to perfect matching in planar graphs. An obvious approach to construct such a reduction is to come up with a *planarizing gadget*. Jochen Messner proved in his talk unconditionally that such a reduction is not possible for the perfect matching problem.

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. Recently, Daniel Grier, an undergrad at the University of South Carolina, has settled the problem and showed that determining the winner of a poset game is PSPACE-complete. The reduction shows, that the game is already PSPACE-complete when the poset has only 3 levels. The complexity of two-level poset games is still open. Steve presented a simple formula allowing one to compute the status for a large class of of two-level poset game.

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 Noncommutativity makes determinants hard

Markus Bläser (Universität des Saarlandes, DE)

We consider the complexity of computing the determinant over arbitrary finite-dimensional algebras. We first consider the case that A is fixed. We obtain the following dichotomy: If $A/\operatorname{rad} A$ is noncommutative, then computing the determinant over A is hard. "Hard" here means $\#P$-hard over fields of characteristic 0 and $ModP_p$-hard over fields of characteristic $p > 0$. If $A/\operatorname{rad} A$ is commutative and the underlying field is perfect, then we can compute the determinant over A in polynomial time.

We also consider the case when A is part of the input. Here the hardness is closely related to the nilpotency index of the commutator ideal of A. The commutator ideal $operatornamecom(A)$ of A is the ideal generated by all elements of the form $xy - yx$ with $x, y \in A$. We prove that if the nilpotency index of $operatornamecom(A)$ is linear in n, where $n \times n$ is the format of the given matrix, then computing the determinant is hard. On the other hand, we show the following upper bound: Assume that there is an algebra $B \subseteq A$ with $B = A/\operatorname{rad}(A)$. (If the underlying field is perfect, then this is always true.) The center $Z(A)$ of A is the set of all elements that commute with all other elements. It is a commutative subalgebra. We call an ideal J a complete ideal of noncommuting elements if $B + Z(A) + J = A$. If there is such a J with nilpotency index $o(n/\log n)$, then we can compute the determinant in subexponential time. Therefore, the determinant cannot be hard in this case, assuming the counting version of the exponential time hypothesis.

3.2 Limits of provable security for homomorphic encryptions

Andrej Bogdanov (Chinese University of Hong Kong, HK)

Joint work of Bogdanov, Andrej; Lee, Chin Ho
Main reference unpublished manuscript

We show that public-key bit encryption schemes that support weak homomorphic evaluation of parity (or majority) cannot be proved message indistinguishable beyond AM intersect coAM via general (adaptive) reductions, and beyond statistical zero-knowledge via reductions of constant query complexity.

Previous works on the limitation of reductions for proving security of encryption schemes make restrictive assumptions about the encryption algorithm (Brassard, Goldreich and Goldwasser, Akavia et al.) or about the reduction (Feigenbaum and Fortnow, Bogdanov and Trevisan, Akavia et al.) Our first result makes no assumptions of either sort.

Towards these results, we show that any homomorphic evaluator for parity or majority over sufficiently many inputs can be used to obtain statistical rerandomization of ciphertexts.

3.3 Testing of Boolean Function Isomorphism

Sourav Chakraborty (Chennai Mathematical Institute, IN)

Testing Isomorphism among various objects is a very important problem is Computer Science. We consider the problem of testing whether two given functions are isomorphic under permutation of the inputs. It is one of the most well studied problem in Property Testing and in the past couple of year we have made significant progress in understanding the problem. We know various classes of functions for which testing isomorphism can be done by looking at only a constant number of bits of the truth table. These new understanding on this problem also helps in testing of other function properties.

3.4 Regular Languages are Church-Rosser Congruential

Volker Diekert (Universität Stuttgart, DE)

Joint work of Diekert, Volker; Kufleitner, Manfred; Reinhardt, Klaus; Walter, Tobias
Main reference V. Diekert, M. Kufleitner, K. Reinhardt, T. Walter, "Regular Languages are Church-Rosser Congruential," arXiv:1202.1148v1 [cs.FL]; Proc. ICALP 2012, Warwick, UK, LNCS 7392, pp. 275–286, 2012.
URL http://arxiv.org/abs/1202.1148
URL http://dx.doi.org/10.1007/978-3-642-31585-5_19

I report on the solution to a long standing conjecture in formal language theory. It states that all regular languages are Church-Rosser congruential. The class of Church-Rosser congruential languages was introduced by McNaughton, Narendran, and Otto in 1988. A language L is Church-Rosser congruential, if there exists a finite confluent, and length-reducing semi-Thue system S such that L is a finite union of congruence classes modulo S. It was known that there are deterministic linear context-free languages which are not Church-Rosser congruential, but on the other hand it was strongly believed that all regular language are of this form.

The key step for the solution has been an algebraic proof for more general result about finite semigroups.

The talk is based on a joint paper with Manfred Kufleitner, Klaus Reinhardt, and Tobias Walter which was presented at ICALP 2012 (Best paper award, Track B).

3.5 From Irreducible Representations to Locally Decodable Codes

Klim Efremenko (Tel Aviv University, IL)

Main reference From Irreducible Representations to Locally Decodable Codes

Locally Decodable Code (LDC) is a code that encodes a message in a way that one can decode any particular symbol of the message by reading only a constant number of locations, even if a constant fraction of the encoded message is adversarially corrupted.

In this paper we present a new approach for the construction of LDCs. We show that if there exists an irreducible representation (ρ, V) of G and q elements $g_1, g_2, \ldots, g_q$ in G

such that there exists a linear combination of matrices $\rho(g_i)$ that is of rank one, then we can construct a q-query Locally Decodable Code $C: V \to F^G$.

We show the potential of this approach by constructing constant query LDCs of subexponential length matching the parameters of the best known constructions.

3.6 Two-level poset games

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

We consider the complexity of determining the winner of a game played on a finite two-level partially ordered set . This is a natural question, as it has been shown recently that determining the winner of a finite three-level poset game is PSPACE-complete. We give a simple formula allowing one to compute the status of a type of two-level poset game that we call, "parity-uniform." This class includes significantly more easily solvable two-level games than was known previously. We also establish general equivalences between various two-level games. This implies that for any n, only finitely many two-level posets with n minimal elements need be considered. We show a similar result for posets with n maximal elements.

3.7 Error-correcting codes vs. superconcentrator graphs

Anna Gál (University of Texas at Austin, US)

Joint work of Gál, Anna; Hansen, Kristoffer; Koucký, Michal; Pudlák, Pavel; Viola, Emanuele
Main reference A. Gál, K.A. Hansen, M. Koucký, P. Pudlák, E. Viola, "Tight bounds on computing error-correcting codes by bounded-depth circuits with arbitrary gates," STOC 2012: 479–494
URL http://dx.doi.org/10.1145/2213977.2214023

We prove tight bounds on the number of wires in constant depth (unbounded fan-in) circuits computing asymptotically good error-correcting codes. We show that quasilinear number of wires is sufficient for computing good codes already in depth 2 circuits with parity gates. This implies that a (necessarily dense) generator matrix for the code can be written as the product of two sparse matrices. For depth 2, our $\Omega(n(\log n/\log\log n)^2)$ lower bound gives the largest known lower bound for computing any linear map.

Furthermore, we identify a new class of superconcentrator-like graphs with connectivity properties distinct from previously studied ones. We show that any circuit computing good codes must satisfy such superconcentrator-like properties.

3.8 The Complexity of Grid Problems

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

Joint work of Gasarch, William; Lawler, Kevin

A c-coloring of an $n \times m$ grid is a mapping of $n \times m$ into $\{1, \ldots, c\}$ such that no four corners forming a rectangle have the same color. Consider the following problem: Given a partial c-coloring of an $n \times m$ grid, can it be extended to a full c-coloring? We show that this problem is NP-complete. We discuss algorithms for fixed c. We also phrase the statement "$n \times m$ is c-colorable' as a propositional formlua and show that, when its fails, any tree resolution proof of it takes size exponential in c.

3.9 Locally testable codes and Cayley graphs

Parikshit Gopalan (Microsoft Research – Mountain View, US)

Joint work of Gopalan, Parikshit; Boaz Barak; Johan Hastad; Raghu Meka; Prasad Raghavendra; David Steurer; Salil Vadhan; Yuan Zhou

We show an equivalence between locally testable codes and Cayley graphs with certain spectral properties. These Cayley graphs can be viewed as "derandomized hypercubes" which preserve several important properties of the Boolean hypercube such as small-set expansion and hypercontractivity.

3.10 Block-Symmetric Polynomials Correlate with Parity Better than Symmetric

Frederic Green (Clark University – Worcester, US)

Joint work of Green, Frederic; Kreymer, Daniel; Viola, Emenuele

We show that degree-d block-symmetric polynomials in n variables modulo any odd p correlate with parity exponentially better than degree-d symmetric polynomials, if $n > d^3$ and $0.98p^t <= d < p^t$ for some $t >= c$ where c is some constant. For these infinitely many degrees, our result solves an open problem raised by a number of researchers including Alon and Beigel (Computational Complexity Conference 2001). The only case for which this was previously known was $d = 2$ and $p = 3$ (Green, Computational Complexity Conference 2002).

The result is obtained through the development of a theory we call spectral analysis of symmetric correlation, which originated in works of Cai, Green, and Thierauf, MST 1996. In particular, our result follows from a detailed analysis of the correlation of symmetric polynomials, which is determined up to an exponentially small relative error when $d = p^t - 1$.

We give a partial complement to these results by showing that for degree $d = p^t$, p prime, block-symmetric polynomials correlate exponentially worse than symmetric, assuming that the blocks are large enough which is the case above. Moreover we show the same holds for every d in the case of polynomials modulo $p = 2$ vs. the Mod_3 function. In this setting we present computational evidence that symmetric polynomials may in fact be optimal.

This work builds on a study of correlation using computer search by the authors which gave unexpected results. The latter are here explained analytically. We advocate further use of computer search in complexity theory.

3.11 Introduction to Geometric Complexity Theory

Joshua A. Grochow (University of Toronto, CA)

The Geometric Complexity Theory (GCT) program was introduced by Mulmuley and Sohoni to attack fundamental lower bound problems in complexity – such as P vs NP – using algebraic geometry and representation theory. In addition to presenting the basic structure of the GCT program, I will discuss some of the intuition behind the use of algebraic geometry and representation theory in complexity. This is an expository talk; the only mathematical background presumed is a basic familiarity with group actions and polynomial rings.

3.12 Compression of Boolean functions

Valentine Kabanets (Simon Fraser University – Burnaby, CA)

We consider the following natural compression problem: Given a truth table of an n-variate Boolean function (from some class C of ‘easy” functions), we want to find a Boolean circuit C of non-trivial size (less than $2^n/n$) that computes f. For lossless compression, the circuit C must compute f everywhere. For lossy compression, we allow C to approximate f. The compression algorithm must be a deterministic algorithm running in time $\mathrm{poly}(2^n)$.

The motivation comes from the desire to understand “easy” functions (what property of their truth tables makes such functions compressible), and “hard” functions (once we understand which functions are compressible, we may be able to prove certain functions to require high circuit complexity).

We show that the class of functions computable by polysize AC^0 circuits, and linear-size de Morgan formulas are compressible. This uses ideas from the Circuit-SAT algorithms for the corresponding circuit classes, which in turn use the method of random restrictions. On the negative side, we show that for any circuit class $C \subseteq \mathrm{P/poly}$, any nontrivial compression of C implies the circuit lower bounds of the form $\mathrm{NEXP} \not\subseteq C$. However, we believe that the latter implication may be used to prove existing lower bounds (e.g., $\mathrm{NEXP} \not\subseteq \mathrm{ACC}^0$ of Williams) and new lower bounds.

3.13 Random Arithmetic Formulas Can be Reconstructed Efficiently

Neeraj Kayal (Microsoft Research India – Bangalore, IN)

Joint work of Gupta, Ankit; Kayal, Neeraj; Qiao, Youming
Main reference A. Gupta, N. Kayal, Y. Qiao, "Random Arithmetic Formulas can be Reconstructed Efficiently," in Electronic Colloquium on Computational Complexity (ECCC), Report No. 33 (2012), 33 pp.
URL http://eccc.hpi-web.de/report/2012/033/

Informally stated, we present here a randomized algorithm that given blackbox access to the polynomial f computed by an unknown/hidden arithmetic formula reconstructs, on the average, an equivalent or smaller formula in time polynomial in the size of its output .

Specifically, we consider arithmetic formulas wherein the underlying tree is a complete binary tree, the leaf nodes are labelled by affine forms (i.e. degree one polynomials) over the input variables and where the internal nodes consist of alternating layers of addition and multiplication gates. We call these alternating normal form (ANF) formulas. If a polynomial f can be computed by an arithmetic formula of size s, it can also be computed by an ANF formula, possibly of slightly larger size $s^{O(1)}$. Our algorithm gets as input blackbox access to the output polynomial f (i.e. for any point x in the domain, it can query the blackbox and obtain $f(x)$ in one step) of a random ANF formula of size s (wherein the coefficients of the affine forms in the leaf nodes of are chosen independently and uniformly at random from a large enough subset of the underlying field). With high probability (over the choice of coefficients in the leaf nodes), the algorithm efficiently (i.e. in time $s^{O(1)}$) computes an ANF formula of size s computing f. This then is the strongest model of arithmetic computation for which a reconstruction algorithm is presently known, albeit efficient in a distributional sense rather than in the worst case.

3.14 A Wronskian approach to the real tau-conjecture

Pascal Koiran (ENS – Lyon, FR)

Joint work of Koiran, Pascal; Portier, Natacha; Tavenas, Sébastien
Main reference P. Koiran, N. Portier, S. Tavenas, "A Wronskian Approach to the real ?-conjecture," arXiv:1205.1015v1 [cs.CC].
URL http://arxiv.org/abs/1205.1015v1

According to the real tau-conjecture, the number of real roots of a sum of products of sparse polynomials should be polynomially bounded in the size of such an expression. It is known that this conjecture implies a superpolynomial lower bound on the arithmetic circuit complexity of the permanent. In this paper, we use the Wronksian determinant to give an upper bound on the number of real roots of sums of products of sparse polynomials. The proof technique is quite versatile; it can in particular be applied to some sparse geometric problems that do not originate from arithmetic circuit complexity. The paper should therefore be of interest to researchers from these two communities (complexity theory and sparse polynomial systems).

3.15 Certifying Polynomials for AC0(parity) circuits, with applications

Swastik Kopparty (Rutgers Univ. – Piscataway, US)

Joint work of Kopparty, Swastik; Srikanth Srinivasan

I will talk about the method of "certifying polynomials" for proving AC^0[parity] circuit lower bounds.

We use this method to show that Approximate Majority cannot be computed by AC^0[parity] circuits of size $n^{1+o(1)}$. This implies a separation between the power of AC^0[parity] circuits of near-linear size and uniform AC^0[parity] (and even AC^0) circuits of polynomial size. This also implies a separation between randomized AC^0[parity] circuits of linear size and deterministic AC^0[parity] circuits of near-linear size.

Our proof using certifying polynomials extends the deterministic restrictions technique of Chaudhuri and Radhakrishnan, who showed that Approximate Majority cannot be computed by AC^0 circuits of size $n^{1+o(1)}$. At the technical level, we show that for every AC^0[parity] circuit C of near linear size, there is a low degree variety V over F_2 such that the restriction of C to V is constant.

We also prove other results exploring various aspects of the power of certifying polynomials. In the process, we show an essentially optimal lower bound of $(\log s)^{\Omega(d)} \log(1/epsilon)$ on the degree of epsilon-approximating polynomials for AC^0[parity] circuits of size s and depth d.

3.16 An Algebraic Version of Constant Depth Complexity

Klaus-Joern Lange (Universität Tübingen, DE)

Circuit classes of constant depth are known to be equivalent to first order formulas. Less well known is the equivalent transformation of these into an algebraic framework in terms of recognition of languages by morphisms. These connections are surprisingly tight as demonstrated for example by the equivalence of linear sized circuits to two variable logics and to the algebraic restriction of being weakly blocked.

The logical-algebraic approach does not relativize and enforces polynomial size on the circuit side. The algebraic formulation seems to be the most natural one since the underlying questions (like parity not in AC^0) are of an algebraic nature.

The talk tries to demonstate how depth reduction could look like in the algebraic formulation.

3.17 NC^0 proof systems

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

Joint work of Beyersdorff, Olaf; Datta, Samir; Krebs, Andreas; Mahajan, Meena; Scharfenberger-Fabian, Gido; Sreenivasaiah, Karteek; Thomas, Michael; Vollmer, Heribert
Main reference O. Beyersdorff, S. Datta, A. Krebs, M. Mahajan, G. Scharfenberger-Fabian, K. Sreenivasaiah, M.l Thomas, H. Vollmer, "Verifying Proofs in Constant Depth," in Electronic Colloquium on

Computational Complexity (ECCC), Report No. 79 (2012), 27 pp.
URL http://eccc.hpi-web.de/report/2012/079

Every language L in NP is expressible as the range of some honest P-computable function f. We can think of the argument to f as encoding a candidate string $w \in L$, and a proof x of the fact that w is indeed in L. The function f verifies the proof: if it is fine, then f outputs w, otherwise f outputs some default string in L. The function f is referred to as a proof system for L. We explore the situation where f is required to be computed in NC^0. This requires the proof to be, in a sense, "locally checkable" and "locally correctable". We attempt to understand what kind of languages have proofs possessing these properties. We show that languages with NC^0 proof systems slice vertically across complexity classes.

Based on joint work with Olaf Beyersdorff, Samir Datta, Andreas Krebs, Gido Scharfenberger-Fabian, Karteek Sreenivasaiah, Michael Thomas, and Heribert Vollmer, part of which appears as ECCC TR12-079 (preliminary version in MFCS 2011).

3.18 Themes in Algebraic and Combinatorial Constructions of Probabilistic Proof Systems

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

Joint work of Meir, Or; Dinur, Irit; Goldreich, Oded

Probabilistic proof systems is a sub-field of complexity theory that investigates questions such as "how can we use randomness to prove and verify assertions?", "what do we gain from using randomness in verification procedures?", and "what assertions can be verified by probabilistic verification procedures?". Research in this area began in the 1980, and has led to several of the most important achievements of complexity theory in those decades. Many of the key results in this area rely on sophisticated use of low degree polynomials.

A line of research from the recent years is aimed at finding alternative "combinatorial" proofs for those key results, i.e., proofs that do not rely on algebra. This line of research is motivated by trying to gain more intuition of those results, as well as to understand the properties of polynomials that make them useful for such constructions.

In this talk, we will survey this line of research, and focus on a few themes that are shared by this line of work and the algebraic constructions.

3.19 Planarizing Gadgets for Perfect Matching Do not Exist

Jochen Messner (Hochschule Aalen, DE)

Joint work of Gurjar, Rohit; Korwar, Arpita; Messner, Jochen; Straub, Simon; Thierauf, Thomas
Main reference R. Gurjar, A. Korwar, J. Messner, S. Straub, T. Thierauf, "Planarizing Gadgets for Perfect Matching Do not Exist," in Mathematical Foundations of Computer Science 2012. Springer, LNCS, Vol. 7464, pp. 478–490, 2012.
URL http://dx.doi.org/10.1007/978-3-642-32589-2_43

To reduce a graph problem to its planar version, a standard technique is to replace crossings in a drawing of the input graph by planarizing gadgets. We show unconditionally that such a reduction is not possible for the perfect matching problem and also extend this to other related problems like Mod_k-PM for $k \geq 3$.

3.20 One algorithm to rule them all: One join query at a time

Atri Rudra (SUNY – Buffalo, US)

Joint work of Ngo, Hung; Porat, Ely; Re, Christopher; Rudra, Atri
Main reference H.Q. Ngo, E. Porat, C. Ré, A. Rudra, "Worst-case optimal join algorithms," PODS 2012: 37–48.
URL http://dx.doi.org/10.1145/2213556.2213565

We present a recent algorithm (PODS 2012) that is the first provably optimal (worst-case) algorithm to compute database joins.

As a special case, we show that this join algorithm implies

(i) The first algorithmic versions of some well-known geometric inequalities due to Loomis and Whitney (and their generalizations by Bollobas and Thomason);

(ii) Algorithmically list recoverable codes that work with parameters that no known algorithmic list recovery result work with (e.g. those based on the Reed-Solomon codes) and an application of this result in designing sublinear time decodable compressed sensing schemes;

(iii) Worst-case optimal algorithm to list all occurrences of any fixed hypergraph H in a given large hypergraph G.

We believe that this algorithm should find many more applications.

This talk will focus on (i) and (ii) and is based on joint works with Gilbert, Ngo, Porat, Re and Strauss.

3.21 Lower Bounds against Weak Uniformity and Sublinear Advice

Rahul Santhanam (University of Edinburgh, GB)

Joint work of Santhanam, Rahul; Lance Fortnow; Ryan Williams

Hierarchy theorems give unconditional lower bounds for explicit problems against strongly (DLOGTIME) uniform circuits. There are a couple of natural ways of relaxing the uniformity condition - (i) Allowing a small amount of advice in the lower bound against strongly uniform circuits (ii) Using a weaker notion of uniformity (eg., P- uniformity).

We prove new circuit lower bounds for P and NP with these relaxed uniformity conditions. Among other results, we show that or every constant k

(i) NP is not in $\mathrm{NTIME}(n^k)/n^{o(1)}$

(ii) P does not have P-uniform deterministic circuits of size n^k.

(iii) NP does not have NP-uniform non-deterministic circuits of size n^k.

Based on joint works with Lance Fortnow and Ryan Williams.

3.22 Rank bound for design matrices and applications to incidence theorems and locally correctable codes

Shubhangi Saraf (Rutgers Univ. – Piscataway, US)

Consider a finite set of points in R^n. The classical theorem of Sylvester-Gallai says that, if for every two points there is a third point on the line through them, then all points are on the same line. In this talk I will describe several extensions to this theorem – quantitative versions, high dimensional versions, and average case versions. The main component of our proofs is an improved lower bound on the rank of design matrices, which are matrices over the complexes with certain zero-nonzero patterns. We use our improved lower bounds on the rank to get improved analyses for several questions in incidence geometry. These results build upon and extend a recent work of Barak, Dvir, Wigderson and Yehudayoff.

I will also talk about stable versions of the Sylvester-Gallai Theorem, where we are only guaranteed many triples of points which are approximately collinear. Configurations with many approximately collinear q-tuples of points also arise naturally in stable versions of Locally Correctable Codes over the complex numbers. We show that that such stable codes with constant query complexity do not exist. No impossibility results were known in any such local setting for more than 2 queries.

Based on joint works with Albert Ai, Zeev Dvir and Avi Wigderson

3.23 Invertible zero-error dispersers and defective memory with stuck-at errors

Ronen Shaltiel (University of Haifa, IL)

Joint work of Gabizon, Ariel; Shaltiel, Ronen
Main reference A. Gabizon, R. Shaltiel, "Invertible Zero-Error Dispersers and Defective Memory with Stuck-At Errors," in Proc. of the 16th Int'l Workshop on Randomization and Approximation Techniques in Computer Science, (RANDOM), pp. 553–564, 2012.
URL http://cs.haifa.ac.il/~ronen/online_papers/defects_full.pdf

Let $x = (x_1, \dots, x_n)$ be a memory with n bit cells where a subset $S \subseteq [n]$ containing at most s out of the n cells are 'stuck' at certain values and cannot be modified. The goal is to store a long string z in memory x, so that at a later point it would be possible to read x and retrieve z, even without knowing which of the cells are stuck. This problem is related to, and harder than, the Write-Once-Memory (WOM) problem (in which once we raise a cell x_i from zero to one, it is stuck at this value).

We give explicit schemes which store $n - s - o(n)$ bits (note that the trivial lower bound is $n - s$). This is the first explicit scheme with asymptotically optimal rate. We are able to guarantee the same rate even if following the encoding, the memory x is corrupted in $o(\sqrt{n})$ adversarially chosen positions.

Our approach utilizes a recent connection observed by Shpilka between the WOM problem and linear seeded extractors for bit-fixing sources. We generalize this observation and show that memory schemes for stuck-at memory are equivalent to zero-error seedless dispersers for bit-fixing sources. It turns out that explicitness of the disperser is not sufficient for the explicitness of the memory scheme. We also need that the disperser is efficiently invertible.

In order to construct our memory schemes, we give new constructions of zero-error seedless dispersers for bit-fixing sources and affine sources. These constructions improve upon previous work: For sources with min- entropy k, they

(i) achieve larger output length $m = (1 - o(1)) \cdot k$ whereas previous constructions did not, and

(ii) are efficiently invertible, whereas previous constructions do not seem to be easily invertible.

3.24 Better condensers and extractors from Parvaresh-Vardy codes

Amnon Ta-Shma (Tel Aviv University, IL)

We give a new construction of condensers based on Parvaresh-Vardy codes. Our condensers have entropy rate $1 - \alpha$ for subconstant α (in contrast to GUV which required constant α) and suffer only sublinear entropy loss.

Known extractors can be applied to the output to extract all but a subconstant fraction of the minentropy. The resulting (k, ϵ)-extractor has output length $m = (1 - \alpha)k$ with $\alpha = 1/\text{polylog}(n)$, and seed length $d = O(\log n)$ when $\epsilon > 1/2^{\log^{\beta} n}$ for any constant $\beta < 1$. Thus we achieve the same "world-record" extractor parameters as DKSS, with an (arguably) simpler construction, while being able to handle smaller error.

3.25 A perspective on arithmetic circuit lower bounds

Amir Yehudayoff (Technion – Haifa, IL)

We discussed general approaches for proving lower bounds for arithmetics circuits. We mainly focus on the following:

1. Prove a structural statement for arithmetic circuits, and
2. find weakness of structure to prove lower bound.

Several structural results are know for general circuits:

(i) Valiant el al. proved that they can be balanced to have depth order $\log(s)\log(r)$, where s is size and r is degree, and

(ii) this was used by Agrawal and Vinay to show a general non-trivial reduction to depth 4. We do not know, however, how to use these structural results to prove lower bounds.

For multilinear formulas, this approach turned out to be extremely useful. The structural theorem for multilinear formulas is that they can be written as a sum of highly-reducible, variable-disjoint polynomials. The main breakthrough in this context came in the work of Raz who identified a concrete weakness of multilinear formulas, that is based on this structure.

Finally, we discussed other approaches for proving lower bounds.

3.26 Pseudorandomness from Shrinkage

David Zuckerman (University of Texas at Austin, US)

Joint work of Impagliazzo, Russell; Meka, Raghu; Zuckerman, David
Main reference R. Impagliazzo, R. Meka, and D. Zuckerman, “Pseudorandomness From Shrinkage,” FOCS 2012.
URL http://eccc.hpi-web.de/report/2012/057/

One powerful theme in complexity theory and pseudorandomness in the past few decades has been the use of lower bounds to give pseudorandom generators (PRGs). However, the general results using this hardness vs. randomness paradigm suffer a quantitative loss in parameters, and hence do not give nontrivial implications for models where we don't know super-polynomial lower bounds but do know lower bounds of a fixed polynomial. We show that when such lower bounds are proved using random restrictions, we can construct PRGs that are essentially best possible without in turn improving the lower bounds.

More specifically, say that a circuit family has shrinkage exponent Γ if a random restriction leaving a p-fraction of variables unset shrinks the size of any circuit in the family by a factor of $p^{\Gamma+o(1)}$. Our PRG uses a seed of length $s^{1/(\Gamma+1)+o(1)}$ to fool circuits in the family of size s. By using this generic construction, we get PRGs with polynomially small error for the following classes of circuits of size s and with the following seed lengths:

1. For de Morgan formulas, seed length $s^{1/3+o(1)}$;
2. For formulas over an arbitrary basis, seed length $s^{1/2+o(1)}$;
3. For read-once de Morgan formulas, seed length $s^{0.234\ldots}$;
4. For branching programs of size s, seed length $s^{1/2+o(1)}$.

The previous best PRGs known for these classes used seeds of length bigger than $n/2$ to output n bits, and worked only when the size $s = O(n)$.

Participants

- Farid Ablayev
Kazan State University, RU
- Manindra Agrawal
Indian Inst. of Technology – Kanpur, IN
- Eric Allender
Rutgers Univ. – Piscataway, US
- Vikraman Arvind
The Institute of Mathematical Sciences – Chennai, IN
- David A. Mix Barrington
University of Massachusetts – Amherst, US
- 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
- Samir Datta
Chennai Mathematical Inst., IN
- Volker Diekert
Universität Stuttgart, DE
- Klim Efremenko
Tel Aviv University, IL
- Stephen A. Fenner
University of South Carolina, US
- Lance Fortnow
Georgia Inst. of Technology, US
- Anna Gál
University of Texas at Austin, US
- William Gasarch
University of Maryland – College Park, US
- Parikshit Gopalan
Microsoft Research – Mountain View, US
- Frederic Green
Clark University – Worcester, US
- Joshua A. Grochow
University of Toronto, CA
- Steve Homer
Boston University, US
- Valentine Kabanets
Simon Fraser University – Burnaby, CA
- Neeraj Kayal
Microsoft Research India – Bangalore, IN
- Pascal Koiran
ENS – Lyon, FR
- Swastik Kopparty
Rutgers Univ. – Piscataway, US
- Michal Koucký
Academy of Sciences – Prague, CZ
- Matthias Krause
Universität Mannheim, DE
- Klaus-Jörn Lange
Universität Tübingen, DE
- Sophie Laplante
University Paris-Diderot, FR
- Bruno Loff
CWI – Amsterdam, NL
- Meena Mahajan
The Institute of Mathematical Sciences – Chennai, IN
- Pierre McKenzie
University of Montreal, CA
- Or Meir
Institute of Advanced Study – Princeton, US
- Jochen Messner
Hochschule Aalen, DE
- Natacha Portier
ENS – Lyon, FR
- Atri Rudra
SUNY – Buffalo, US
- Chandan Saha
IISc – Bangalore, IN
- Rahul Santhanam
University of Edinburgh, GB
- Shubhangi Saraf
Rutgers Univ. – Piscataway, US
- Uwe Schöning
Universität Ulm, DE
- Rocco Servedio
Columbia University, US
- Ronen Shaltiel
University of Haifa, IL
- Simon Straub
Universität Ulm, DE
- Amnon Ta-Shma
Tel Aviv University, IL
- Thomas Thierauf
Hochschule Aalen, DE
- Jacobo Toran
Universität Ulm, DE
- Christopher Umans
CalTech – Pasadena, US
- Virginia Vassilevska Williams
Stanford University, US
- Nikolay K. Vereshchagin
Moscow State University, RU
- Ryan Williams
Stanford University, US
- Amir Yehudayoff
Technion – Haifa, IL
- David Zuckerman
University of Texas at Austin, US