09421 Abstracts Collection
Algebraic Methods in Computational Complexity
— Dagstuhl Seminar —

Manindra Agrawal[1], Lance Fortnow[2], Thomas Thierauf[3] and Christopher Umans[4]

[1] Indian Inst. of Technology - Kanpur, IND
[2] NW University - Evanston, USA
lance@fortnow.com
[3] Hochschule Aalen, D
Thomas.thierauf@HTW-Aalen.de
[4] CalTech - Pasadena, USA
umans@cs.caltech.edu

Abstract. From 11.10. to 16.10.2009, the Dagstuhl Seminar 09421 "Algebraic Methods in Computational Complexity " was held in Schloss Dagstuhl – Leibniz Center for Informatics. During the seminar, several participants presented their current research, and ongoing work and open problems were discussed. Abstracts of the presentations given during the seminar as well as abstracts of seminar results and ideas are put together in this paper. The first section describes the seminar topics and goals in general. Links to extended abstracts or full papers are provided, if available.

Keywords. Computational Complexity, Algebra

09421 Executive Summary – Algebraic Methods in Computational Complexity

The seminar brought together more than 50 researchers covering a wide spectrum of complexity theory. The focus on algebraic methods showed once again the great importance of algebraic techniques for theoretical computer science. We had almost 30 talks, most of them about 40 minutes leaving ample room for discussions. We also had a much appreciated open problem session.

The talks ranged over a broad assortment of subjects with the underlying theme of using algebraic techniques. It was very fruitful 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!

Keywords: Computational Complexity, Algebra

Joint work of: Agrawal, Manindra; Fortnow, Lance; Thierauf, Thomas; Umans, Christopher

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2010/2410

BQP and the Polynomial Hierarchy

Scott Aaronson (MIT - Cambridge, US)

The relationship between BQP and PH has been an open problem since the earliest days of quantum computing. We present new evidence that quantum computers can solve problems outside PH—and in the process, relate this question to frontier topics in Fourier analysis, pseudorandomness, and circuit complexity.

First, we show that there exists a black-box relational problem (i.e., a problem with many valid outputs) that is solvable in quantum polynomial time, but not in a relational version of PH. This also yields a relational problem that is solvable in quantum logarithmic time, but not in AC0.

Second, we show that a black-box decision problem separating BQP from PH (that is, an oracle relative to which BQP is not in PH) would follow from a natural generalization of the Linial-Nisan Conjecture. The original Linial-Nisan Conjecture was recently proved by Braverman, after being open for twenty years.

A Survey of Quantum Money

Scott Aaronson (MIT - Cambridge, US)

In a remarkable 1969 paper, Stephen Wiesner raised the possibility of money whose authenticity would be guaranteed by the laws of quantum physics. However, Wiesner's money can only be verified by the bank that printed it—and the natural question of whether one can have secure quantum money that anyone can verify has remained open for forty years. In this talk, I'll tell you about recent progress on this question.

- I'll show that no "public-key" quantum money scheme can have security based on quantum physics alone: like in most cryptography, one needs a computational hardness assumption.

- I'll show that one can have quantum money that remains hard to counterfeit, even if a counterfeiter gains black-box access to a device for checking the money.

- I'll describe a candidate quantum money scheme I proposed last spring, and how that scheme was recently broken by Farhi, Gosset, Hassidim, Kelner, Lutomirski, Shor, and me.

- I'll describe a new quantum money scheme we propose in the same work. The new scheme has the strange property that not even the bank can prepare the same bill twice.

A Communication Complexity Approach to the Superposition Problem

Farid Ablayev (Kazan State University, RU)

In function theory the superposition problem is known as the problem of representing a continuous function $f(x_1, \ldots, x_k)$ in k variables as the composition of "simpler" functions. This problem stems from the Hilbert's thirteenth problem. In computer science good formalization for the notion of composition of functions is formula.

In the paper we consider real-valued continuous functions in k variables in the cube $[0,1]^k$ from the class $\mathcal{H}^k_{\omega_p}$ with ω_p a special *modulus of continuity* (measure the smoothness of a function) defined in the paper. $\mathcal{H}^k_{\omega_p}$ is a superset of Hölder class of functions. We present an explicit function $f \in \mathcal{H}^k_{\omega_p}$ which is hard in the sense that it cannot be represented in the following way as a formula: zero level (input) gates associated with variables $\{x_1, \ldots, x_k\}$ (different input gates can be associated with the same variable $x_i \in \{x_1, \ldots, x_k\}$), on the first level of the formula, arbitrary number $s \geq 1$ of t variable functions from $\mathcal{H}^t_{\omega_p}$ for $t < k$ are allowed, while the second (output) level may compute any s variable Hölder function.

We apply communication complexity for constructing such hard explicit function. Notice that one can show the existence of such function using the "non constructive" proof method known in function theory as Kolmogorov's entropy method.

Keywords: Superposition problem of continuious functions, discrete approximation of continuious functions, communication complexity

Joint work of: Ablayev, Farid; Ablayeva Svetlana

Affine-invariant locally testable codes have exponentially small rate

Eli Ben-Sasson (Technion - Haifa, IL)

A linear code is said to be affine-invariant if the coordinates of the code can be viewed as a vector space and the code is invariant under an affine transformation of the coordinates. A code is said to be locally testable if proximity of a received word to the code can be tested by querying the received word in a few coordinates. It was recently pointed out by Kaufman and Sudan that affine-invariance explains a large class of natural codes that are locally testable. So far all known codes analyzed by this method had low rate. In this work we show that this weakness is an inherent limitation of affine-invariant codes. We show that any k-query affine-invariant codes is contained in an 2^k-query testable Reed-Muller code. In fact our result shows that any affine-invariant code that has a

k-local constraint (i.e., a weight k codeword in its dual), a necessary condition for k-query local testability, is contained in a Reed-Muller code that 2^k–locally characterized (i.e., its dual is spanned by words of weight at most 2^k).

The key technical ingredient of our analysis is showing that a certain class of homogeneous polynomial equations have no non-trivial solutions. Specifically we look at a system of equations of the form $\sum_{i=1}^{k} c_i x_i^d = 0$, for $d \in D$, and consider under what conditions on $c_1, \ldots, c_k$ and D can this system have a common zero where the x_i's are all distinct.

The need to study such systems of equations was already noted in previous work on affine invariant property testing, and we give a new sufficient condition on D under which this system has no such solutions (with distinct x_i's). We believe this result may be of independent interest.

Keywords: Locally testable codes

Joint work of: Ben-Sasson, Eli; Sudan, Madhu

Linear systems over composite moduli

Arkadev Chattopadhyay (University of Toronto, CA)

We study solution sets to systems of generalized linear equations of the form $\ell_i(x_1, x_2, \cdots, x_n) \in A_i \ (mod m)$ where $\ell_1, ..., \ell_t$ are linear forms in n Boolean variables, each A_i is an arbitrary subset of Z_m, and m is a composite integer that is a product of two distinct primes, like 6. Our main technical result is that such solution sets have exponentially small correlation, i.e. $exp(-\Omega(n))$, with the boolean function MOD_q, when m and q are relatively prime. This bound is independent of the number t of equations.

This yields progress on limiting the power of constant-depth circuits with modular gates.

We derive the first exponential lower bound on the size of depth-three circuits of type MAJ of AND of MOD_m (i.e. having a MAJORITY gate at the top, AND/OR gates at the middle layer and generalized MOD_m gates at the base with an arbitrary accepting set A), computing the function MOD_q.

This solves an open problem of Beigel and Maciel , for the case of such modulus m.

Our technique makes use of the work of Bourgain on estimating exponential sums involving a low-degree polynomial and ideas involving matrix rigidity from the work of Grigoriev and Razborov on arithmetic circuits over finite fields.

Joint work of: Chattopadhyay, Arkadev; Wigderson, Avi

Extensions to the method of multiplicities, with applications to kakeya sets and mergers

Zeev Dvir (Institute for Advanced Study - Princeton, US)

We extend the "method of multiplicities" to get the following results, of interest in combinatorics and randomness extraction.

(1) We show that every Kakeya set (a set of points that contains a line in every direction) in $\backslash F_q^n$ must be of size at least $q^n/2^n$. This bound is tight to within a $2 + o(1)$ factor for every n as $q \to \infty$, compared to previous bounds that were off by exponential factors in n.

(2) We give an improved construction of "randomness mergers".

Mergers are seeded functions that take as input Λ (possibly correlated) random variables in $\{0,1\}^N$ and a short random seed, and output a single random variable in $\{0,1\}^N$ that is statistically close to having entropy $(1-\delta) \cdot N$ when one of the Λ input variables is distributed uniformly. The seed we require is only $(1/\delta) \cdot \log \Lambda$-bits long, which significantly improves upon previous construction of mergers.

(3) Using our new mergers, we show how to construct randomness extractors that use logarithmic length seeds while extracting $1 - o(1)$ fraction of the min-entropy of the source. Previous results could extract only a constant fraction of the entropy while maintaining logarithmic seed length.

The "method of multiplicities", as used in prior work, analyzed subsets of vector spaces over finite fields by constructing somewhat low degree interpolating polynomials that vanish on every point in the subset *with high multiplicity*. The typical use of this method involved showing that the interpolating polynomial also vanished on some points outside the subset, and then used simple bounds on the number of zeroes to complete the analysis.

Our augmentation to this technique is that we prove, under appropriate conditions, that the interpolating polynomial vanishes *with high multiplicity* outside the set. This novelty leads to significantly tighter analyses. To develop the extended method of multiplicities we provide a number of basic technical results about multiplicity of zeroes of polynomials that may be of general use. For instance, we strengthen the Schwartz-Zippel lemma to show that the expected multiplicity of zeroes of a non-zero degree d polynomial at a random point in S^n, for any finite subset S of the underlying field, is at most $d/|S|$.

Keywords: Extractors, mergers, kakeya

Joint work of: Dvir, Zeev; Kopparty, Swastik; Saraf, Shubhangi; Sudan, Manhu

Full Paper:
http://eccc.hpi-web.de/report/2009/004/

Bounding Rationality by Discounting Time

Lance Fortnow (Northwestern University - Evanston, US)

Consider a game where Alice generates an integer and Bob wins if he can factor that integer. Traditional game theory tells us that Bob will always win this game even though in practice Alice will win given our usual assumptions about the hardness of factoring.

We define a new notion of bounded rationality, where the payoffs of players are discounted by the computation time they take to produce their actions.

We use this notion to give a direct correspondence between the existence of equilibria where Alice has a winning strategy and the hardness of factoring. Namely, under a natural assumption on the discount rates, there is an equilibrium where Alice has a winning strategy iff there is a linear-time samplable distribution with respect to which Factoring is hard on average.

Joint work of: Fortnow, Lance; Santhanam, Rahul

On the limitations of three query linear locally decodable codes

Anna Gal (Univ. of Texas at Austin, US)

On the limitations of 3-query linear locally decodable codes

Locally decodable codes were introduced by Katz and Trevisan in 2000.

These are error correcting codes with the extra property, that in order to retrieve just one bit of the original input with high probability, it is sufficient to read a constant number of bits of the corresponding (possibly corrupted) codeword.

A breakthrough result by Yekhanin showed that 3-query linear locally decodable codes may have subexponential length. However there is still a large gap between the known upper and lower bounds.

The known exponential lower bounds on the length of 2 query locally decodable codes hold for any code that achieves correctness $> 1/2$.

The construction of Yekhanin, and the constructions that followed, can achieve correctness only up to a certain limit. More precisely, so far the largest correctness for a subexponential size constant query code is achieved in a construction by Woodruff, and it is below 1 - 3 delta, where the adversary is allowed to corrupt up to delta fraction of the codeword.

We show that achieving somewhat larger correctness (as a function of delta) requires exponential size for 3-query linear codes.

Joint work with Andrew Mills (University of Texas at Austin)

Joint work of: Gal, Anna; Mills, Andrew

Learning Parities in the Mistake-Bound model

David Garcia-Soriano (CWI - Amsterdam, NL)

We study the problem of learning parity functions that depend on at most k variables (k-parities) attribute-efficiently in the mistake-bound model.

We design a simple, deterministic, polynomial-time algorithm for learning k-parities with mistake bound $O(n^{1-\frac{c}{k}})$, for any constant $c > 0$. This is the first polynomial-time algorithms that learns $\omega(1)$-parities in the mistake-bound model with mistake bound $o(n)$.

Using the standard conversion techniques from the mistake-bound model to the PAC model, our algorithm can also be used for learning k-parities in the PAC model. In particular, this implies a slight improvement on the results of Klivans and Servedio [KS04] for learning k-parities in the PAC model.

We also show that the $\widetilde{O}(n^{k/2})$ time algorithm from [KS04] that PAC-learns k-parities with optimal sample complexity can be extended to the mistake-bound model.

Keywords: Attribute-efficient learning, parities, mistake-bound

Joint work of: Buhrman, Harry; Garcia-Soriano, David; Matsliah, Arie

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2010/2417

What is an Explicit Construction?

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

The Prob. Method is often used to show that objects exist without saying how to construct them. We show that, if you assume some common HARDness assumptions used by people in the field of derandomization then these constructions can be made explicit.

We also give a general theorem that yields many such constructions.

This general theorem is a generalization of Robin Moser's STOC 2009 talk. I obtain both lower bounds on VDW numbers AND Robin Mosers result on k-CNF from this General Theorem. I then derandomize both using a HARDness assumption.

Keywords: Probabilistic Method, Ramsey Theory, randomization, derandomiazation

Collapsing and Separating Completeness Notions under Average-Case and Worst-Case Hypotheses

John Hitchcock (University of Wyoming, US)

We present the following results on sets that are complete for NP.

1. If there is a problem in NP that cannot be solved in worst-case subexponential time, then every many-one NP-complete set is complete under P/poly length-increasing reductions.

2. If there is a problem in coNP that cannot be solved by polynomial-size nondeterministic circuits, then every many-one NP-complete set is complete under P/poly length-increasing reductions.

3. If one-way permutations exist and there is a hard tally language in NP intersect coNP, then there is a Turing complete language for NP that is not many-one complete.

The first two results use worst-case hardness hypotheses. Earlier work relied on average-case or almost-everywhere hardness assumptions.

The use of average-case and worst-case hypotheses in the last result is unique as previous work used almost-everywhere hardness hypotheses.

This is joint work with Xiaoyang Gu and A. Pavan.

Joint work of: Gu, Xiaoyang; Hitchcock, John; Pavan, A.

An Axiomatic Approach to Algebrization

Valentine Kabanets (Simon Fraser University - Burnaby, CA)

Non-relativization of complexity issues can be interpreted as giving some evidence that these issues cannot be resolved by "black-box" techniques. In the early 1990's, a sequence of important non-relativizing results was proved, mainly using algebraic techniques. Two approaches have been proposed to understand the power and limitations of these algebraic techniques: (1) Fortnow gives a construction of a class of oracles which have a similar algebraic and logical structure, although they are arbitrarily powerful. He shows that many of the non-relativizing results proved using algebraic techniques hold for all such oracles, but he does not show, e.g., that the outcome of the "P vs. NP" question differs between different oracles in that class. (2) Aaronson and Wigderson give definitions of algebrizing separations and collapses of complexity classes, by comparing classes relative to one oracle to classes relative to an algebraic extension of that oracle. Using these definitions, they show both that the standard collapses and separations "algebrize" and that many of the open questions in complexity fail to "algebrize", suggesting that the arithmetization technique is close to its limits. However, it is unclear how to formalize algebrization of more complicated complexity statements than collapses or separations, and whether the algebrizing statements are, e.g., closed under modus ponens; so it is conceivable that several algebrizing premises could imply (in a relativizing way) a non-algebrizing conclusion.

Here, building on the work of Arora, Impagliazzo, and Vazirani [4], we propose an axiomatic approach to "algebrization", which complements and clarifies the approaches of Fortnow and Aaronso&Wigderson. We present logical theories formalizing the notion of algebrizing techniques so that most algebrizing results

are provable within our theories and separations requiring non-algebrizing techniques are independent of them.

Our theories extend the [AIV] theory formalizing relativization by adding an Arithmetic Checkability axiom.

We show the following: (i) Arithmetic checkability holds relative to arbitrarily powerful oracles (since Fortnow's algebraic oracles all satisfy Arithmetic Checkability axiom); by contrast, Local Checkability of [AIV] restricts the oracle power to $NP \cap co - NP$. (ii) Most of the algebrizing collapses and separations from [AW], such as IP = PSPACE, $NP \subset ZKIP$ if one-way functions exist, MA-EXP not in P/poly, etc., are provable from Arithmetic Checkability. (iii) Many of the open complexity questions (shown to require nonalgebrizing techniques in [AW]), such as "P vs. NP", "NP vs.

BPP", etc., cannot be proved from Arithmetic Checkability.

(iv) Arithmetic Checkability is also insufficient to prove one known result, NEXP = MIP.

Keywords: Oracles, arithmetization, algebrization

Joint work of: Impagliazzo, Russell; Kabanets, Valentine; Kolokolova, Antonina

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2010/2415

Direct Products: Decoding and Testing, with Applications

Valentine Kabanets (Simon Fraser University - Burnaby, CA)

K-wise direct product of a function f is a function f^k that takes k input strings and outputs the k-tuple of values of f on these input strings.

Encoding f with its k-wise direct product function has some error-correcting properties that have been very useful in complexity theory (hardness amplification); a famous example is Yao's XOR Lemma.

In this talk, I will describe the recent progress on the problems of decoding and testing such "direct product" codes. I will also show an application of our testing results to 2-query PCPs: we give a certain version of "parallel repetition" which can be used to reduce the soundness error of 2-query PCPs.

The talk is based on the joint work with Russell Impagliazzo, Ragesh Jaiswal, and Avi Wigderson [stoc'08, stoc'09].

Keywords: Direct product, error-correcting codes, decoding, testing, PCP

Joint work of: Impagliazzo, Russell; Jaiswal, Ragesh; Kabanets, Valentine; Wigderson, Avi

Random Graphs and the Parity Quantifier

Swastik Kopparty (MIT - Cambridge, US)

The classical zero-one law for first-order logic on random graphs says that for every first-order property φ in the theory of graphs and every $p \in (0,1)$, the probability that the random graph $G(n,p)$ satisfies φ approaches either 0 or 1 as n approaches infinity.

It is well known that this law fails to hold for any formalism that can express the parity quantifier: for certain properties, the probability that $G(n,p)$ satisfies the property need not converge, and for others the limit may be strictly between 0 and 1.

In this work, we capture the limiting behavior of properties definable in first order logic augmented with the parity quantifier, $FO[parity]$, over $G(n,p)$, thus eluding the above hurdles. Specifically, we establish the following "modular convergence law":

For every $FO[parity]$ sentence φ, there are two explicitly computable rational numbers a_0, a_1, such that for $i \in \{0,1\}$, as n approaches infinity, the probability that the random graph $G(2n+i,p)$ satisfies φ approaches a_i.

Our results also extend appropriately to $\backslash FO$ equipped with $\backslash Mod_q$ quantifiers for prime q.

In the process of deriving the above theorem, we explore a new question that may be of interest in its own right. Specifically, we study the joint distribution of the subgraph statistics modulo 2 of $G(n,p)$: namely, the number of copies, mod 2, of a fixed number of graphs $F_1, \ldots, F_\ell$ of bounded size in $G(n,p)$. We first show that every $FO[parity]$ property φ is almost surely determined by subgraph statistics modulo 2 of the above type.

Next, we show that the limiting joint distribution of the subgraph statistics modulo 2 depends only on $n \backslash mod 2$, and we determine this limiting distribution completely. Interestingly, both these steps are based on a common technique using multivariate polynomials over finite fields and, in particular, on a new generalization of the Gowers norm.

The first step above is analogous to the Razborov-Smolensky method for lower bounds for AC_0 with parity gates, yet stronger in certain ways. For instance, it allows us to obtain examples of simple graph properties that are exponentially uncorrelated with every $FO[parity]$ sentence, which is something that is not known for $AC_0[parity]$.

Joint work of: Kolaitis, Phokion; Kopparty, Swastik

Full Paper:
http://eccc.hpi-web.de/eccc-reports/2009/TR09-033/index.html

Affine Dispersers from Subspace Polynomials

Swastik Kopparty (MIT - Cambridge, US)

An affine disperser over F_2^n for sources of dimension d is a function $f : F_2^n - - > F_2$ such that for any affine subspace S in F_2^n of dimension at least d, we have $f(s) : sinS = F_2$. Affine dispersers have been considered in the context of deterministic extraction of randomness from structured sources of imperfect randomness. Previously, explicit constructions of affine dispersers were known for every $d = O(n)$, due to Barak-Kindler-Shaltiel-Sudakov-Wigderson and Bourgain (the latter in fact gives stronger objects called affine extractors).

In this talk, I will describe an explicit affine disperser for sublinear dimension. Specifically, the disperser works even when $d = O(n^{4/5})$. The main novelty in our construction lies in the method of proof, which uses elementary properties of simple-but-powerful algebraic objects called subspace polynomials. In contrast, the previous works mentioned above relied on sum-product theorems for finite fields.

Joint work of: Ben-Sasson, Eli; Kopparty, Swastik

Full Paper:
http://web.mit.edu/swastik/www/affine-disperser.pdf

Local Testing and List Decoding of Sparse Random Linear Codes from High Error

Swastik Kopparty (MIT - Cambridge, US)

We show that sparse random linear codes are locally testable and locally list decodable from $(1/2-\epsilon)$-fraction errors, for every constant $\epsilon > 0$. More precisely, we show that any linear code in F_2^n which is:

(1) sparse (i.e., has only poly(n) codewords) (2) unbiased (i.e., each nonzero codeword has Hamming weight $\in (1/2 - n^{-\gamma}, 1/2 + n^{-\gamma})$ for some constant $\gamma > 0$) can be locally tested and locally list decoded from $(1/2 - \epsilon)$-fraction errors using only poly<math>$(\frac{1}{\epsilon}) < /math >$ queries to the received word. This generalizes a result of Kaufman and Sudan, who gave a local tester and local (unique) decoder for such codes from some constant fraction of errors.

The running "time" of the tester and decoder is determined by the time complexity of uniformly sampling dual codewords of a given weight. For a particular widely studied family of codes in this class, the dual-BCH codes, we give a polylog(n) time algorithm for this task, extending a line of work by Litsyn, Grigorescu, Kaufman and Sudan.

Joint work of: Kopparty, Swastik; Shubhangi, Saraf

Optimal Testing of Reed-Muller Codes

Swastik Kopparty (MIT - Cambridge, US)

We consider the problem of testing if a given function $f : F_2^n \to F_2$ is close to any degree d polynomial in n variables, also known as the Reed-Muller testing problem.

Alon et al.[AKKLR] proposed and analyzed a natural 2^{d+1}-query test for this property and showed that it accepts every degree d polynomial with probability 1, while rejecting functions that are $\Omega(1)$-far with probability $\Omega(1/(d2^d))$.

We give an asymptotically optimal analysis of their test showing that it rejects functions that are (even only) $\Omega(2^{-d})$-far with $\Omega(1)$-probability (so the rejection probability is a universal constant independent of d and n).

Our proof works by induction on n, and yields a new analysis of even the classical Blum-Luby-Rubinfeld [BLR] linearity test, for the setting of functions mapping F_2^n to F_2. The optimality follows from a tighter analysis of counterexamples to the "inverse conjecture for the Gowers norm" constructed by [GT,LMS9].

Our result gives a new relationship between the $(d+1)^{\text{st}}$-Gowers norm of a function and its maximal correlation with degree d polynomials. For functions highly correlated with degree d polynomials, this relationship is asymptotically optimal.

Our improved analysis of the [AKKLR]-test also improves the parameters of an XOR lemma for polynomials given by Viola and Wigderson [VW].

Finally, the optimality of our result also implies a "query-hierarchy" result for property testing of linear-invariant properties: For every function $q(n)$, it gives a linear-invariant property that is testable with $O(q(n))$-queries, but not with $o(q(n))$-queries, complementing an analogous result of [GKNR08] for graph properties.

Joint work of: Bhattacharya, Arnab; Kopparty, Swastik; Schoenebeck, Grant; Sudan, Madhu; Zuckerman, David

A new characterization of ACC⁰ and probabilistic CC⁰.

Michal Koucky (Academy of Sciences - Prague, CZ)

Barrington, Straubing and Thérien (1990) conjectured that the Boolean AND function can not be computed by polynomial size constant depth circuits built from modular counting gates, i.e., by CC^0 circuits. In this work we show that the AND function can be computed by uniform probabilistic CC^0 circuits that use only $O(logn)$ random bits. This may be viewed as evidence contrary to the conjecture.

As a consequence of our construction we get that all of ACC^0 can be computed by probabilistic CC^0 circuits that use only $O(logn)$ random bits. Thus,

if one were able to derandomize such circuits, we would obtain a collapse of circuit classes giving $ACC^0 = CC^0$. We present a derandomization of probabilistic CC^0 circuits using AND and OR gates to obtain $ACC^0 = AND - OR - CC^0 = OR - AND - CC^0$. AND and OR gates of sublinear fan-in suffice.

Both these results hold for uniform as well as non-uniform circuit classes. For non-uniform circuits we obtain the stronger conclusion that $ACC^0 = rand - ACC^0 = rand - CC^0 = rand(logn) - CC^0$, i.e., probabilistic ACC^0 circuits can be simulated by probabilistic CC^0 circuits using only $O(logn)$ random bits.

As an application of our results we obtain a characterization of ACC^0 by constant width planar nondeterministic branching programs, improving a previous characterization for the quasi-polynomial size setting.

Joint work of: Arnsfelt Hansen, Kristoffer; Koucký, Michal

Small space analogues of Valiant's classes and the limitations of skew formula

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

In the uniform circuit model of computation, the width of a boolean circuit exactly characterises the "space" complexity of the computed function. Looking for a similar relationship in Valiant's algebraic model of computation, we propose width of an arithmetic circuit as a possible measure of space. We introduce the class VL as an algebraic variant of deterministic log-space L. In the uniform setting, we show that our definition coincides with that of VPSPACE at polynomial width.

Further, to define algebraic variants of non-deterministic space-bounded classes, we introduce the notion of "read-once" certificates for arithmetic circuits. We show that polynomial-size algebraic branching programs can be expressed as a read-once exponential sum over polynomials in VL, ie VBP $\in \Sigma^R \cdot$ VL.

We also show that $\Sigma^R \cdot$ VBP = VBP, ie VBPs are stable under read-once exponential sums. Further, we show that read-once exponential sums over a restricted class of constant-width arithmetic circuits are within VQP, and this is the largest known such subclass of poly-log-width circuits with this property.

We also study the power of skew formulas and show that exponential sums of a skew formula cannot represent the determinant polynomial.

Keywords: Algebraic circuits, space bounds, circuit width, nondeterministic circuits, skew formulas

Joint work of: Mahajan, Meena; Rao B V , Raghavendra

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2010/2412

Hilbert's 13th problem and circuit complexity

Peter Bro Miltersen (Aarhus University, DK)

We study the following question, communicated to us by Miklós Ajtai: Can all explicit (e.g., polynomial time computable) functions $f : (\{0,1\}^w)^3 \to \{0,1\}^w$ be computed by word circuits of constant size? A word circuit is an acyclic circuit where each wire holds a word (i.e., an element of $\{0,1\}^w$) and each gate G computes some binary operation $g_G : (\{0,1\}^w)^2 \to \{0,1\}^w$, defined for all word lengths w. We present an explicit function so that its w'th slice for any $w \geq 8$ cannot be computed by word circuits with at most 4 gates. Also, we formally relate Ajtai's question to open problems concerning ACC^0 circuits.

This is joint work with Kristoffer Arnsfelt Hansen and Oded Lachish.

Joint work of: Hansen, Kristoffer Arnsfelt; Lachish, Oded; Miltersen, Peter Bro

Full Paper:
http://www.daimi.au.dk/~bromille/Papers/hilbert.pdf

The Algebraic Proof For The Low Error PCP Theorem

Dana Moshkovitz (Princeton Inst. for Advanced Studies, US)

The PCP Theorem shows that any mathematical proof can be efficiently converted into a form that can be checked probabilistically by making only *two* queries to the proof.

The error of the checking can tend to 0 with n, the length of the proof.

The proof relies on algebraic techniques, like the [LFKN90] Sum-Check protocol, and Low Degree Testing, as well as combinatorial techniques for composition [M-Raz08, Dinur-Harsha09].

In the talk we will outline the (very elegant) proof.

Keywords: Probabilistically Checkable Proofs (PCP)

The cut dimension of ℓ_1 metrics

Ilan Newman (Haifa University, IL)

Dimension reduction is of great importance in the theory of geometric embedding of finite metric spaces, both in terms of potential algorithmic applications and from the structural point of view. The celebrated Johnson-Lindenstrauss Theorem [johnson-lindenstrauss] states that any Euclidian metric on n points can be approximated to any multiplicative $(1+\epsilon)$-factor by an embedding into $IR^{O(\log n)}$. The Theorem has huge number of applications, both algorithmic and mathematical.

The situation for ℓ_1 is, however different. The results of [brikman-charikar] and [lee-naor] show that one cannot expect dimension reduction better than $d = n^{\alpha}$ for some fixed $\alpha < 1$. On the other hand $O(n^2)$ dimensions suffices even for a perfect isometry (as will become clear in what follows).

The best upper bound for the smalleset dimension that still allows for $1 + e$ multiplicative approximation was that of Schechtman , showing that $O(n \log n)$ dimensions are enough.

The gap between the lower bound and Schetman upper bound was open at large.

A different, but quite related measure of dimensionality for ℓ_1 metrics is what we call here the *cut-dimension*. For a finite set of points V, and a subset $C \subset V$, the *cut metric* $\delta_C : V^2 \mapsto I\!R$ is defined by $\delta_C(x, y) = 1$ if $|\{x, y\} \cap S| = 1$ and 0 otherwise. It is known (and sometimes serves as the definition for ℓ_1 metric) that any ℓ_1 metric d on finite set V can be written as $d = \sum_{C \in \mathcal{C}} \alpha_C \cdot \delta_C$ where $\mathcal{C} \subseteq 2^V$ is a collection of cuts and $\alpha_C > 0$. Namely, any ℓ_1 metric d is a positive weighted combination of cut-metrics. For an ℓ_1 metric d, its cut-dimension is defined as the smallest number of cuts whose positive weighted sum is d. Thus, the notion of cut dimension is quite natural as it serves as a measure of the complexity of representing the metric. It is also of direct algorithmic interest; it measures of how succinct is a representation, and when the dimension is small enough it allows efficient algorithms for many problems that are not known to be tractable in general. In addition, it is known that the cut-dimension is an upper bound on the geometric dimension. Thus an upper bound on the cut dimension should be viewed as a 'dimension-reduction' result.

The main result here is that for any $\epsilon > 0$, any ℓ_1 metric (d, V) on n points has a $(1 + e)$-approxmation ℓ_1 metric d' that has *cut-dimension* $= O(n/\epsilon^2)$. In particular this implies that V can be embedded into $I\!R^{O(n)}$ so that the natural ℓ_1 distance distorts d by at most $1 + \epsilon$. Moreover, given a representation of an ℓ_1 metric as a positive combination of cuts, the family of $O(n/\epsilon^2)$ cuts that defines the approximating metric is a subset of the original family of cuts, and it can be found (along with the associated weights) efficiently by a randomized algorithm. We also show that this result is asymptotically best possible, namely there is an ℓ_1 metric on n points $d_{\mathcal{C}} = \sum_{C \in C} \delta_C$, where $\mathcal{C}$ is collection of cuts of size $O(n)$, and such that for any subfamily of cuts $\mathcal{C}' \subseteq \mathcal{C}$, with $|\mathcal{C}'| = o(n)$, the corresponding metric $d' = \sum_{C \in C'} \alpha_C \delta_C$ distorts $d_{\mathcal{C}}$ by $w(1)$, for any set of weights $\{\alpha_C\}_{C'}$.

The construction we use is based on an adaptation of methods that were used before in a completely different context but that, as we will show, lend themselves to our setting, and to more general setting as well. Our starting point is the results of Karger [karger] and Benczúr and Karger [karger-benczur]. Let $G = (V, E)$ be an undirected graph, for a cut defined by a subset of vertices $S \subseteq V$, the standard cut size is $c(S) = \{(x, y) \in E(G) |\ x \in S, y \notin S\}$. Benczúr et. al [karger-benczur] were interested in the following problem: Is there a graph $G' = (V, E')$ were $|E'|$ is considerably smaller than $|E|$ for which the corresponding cut sizes

$(1+e)$-approximate the corresponding sizes for G, namely such that for every $S \subseteq V$, $(1-\epsilon) \cdot c_G(S) \leq c_{G'}(S) \cdot \leq (1+\epsilon) c_G(S)$.

They proved that indeed for any graph and any $\epsilon > 0$, $O(n \log n/\epsilon^2)$ edges are enough. This result was latter generalized and strengthen by Splielmsn and Teng [spielman-teng-sparsification] and finally by Batson, Spielman and Srivastava [spielman-sparsifier] giving an optimal (disregarding dependence on e) $O(n/\epsilon^2)$ upper bound.

While this problem seems unrelated to our problem, it turns out the the methods in both papers extend (using the right generalization) to our setup yielding the results stated above. In view of this, one can ask how general are these methods ? We define a general notion of split systems and show that the corresponding 'sparsification' problem captures both the graph sparsification problem as well as the metric cut-reduction problem. We then exemplify another instance generalizing the metrics case which falls under this notion.

The structure of the paper is as follows: In Section **??** we lay out the basic notations as well as the basic metric preliminaries. In Section **??** we present our adaptation of the Karger-Benczúr method and the implication that $O(n \log n)$ cuts are enough. In Section **??** we generalize Batson et al. [spielman-sparsifier] results for semi-definite sparsification and show how it implies that $O(n)$ cuts are enough. Section **??** shows that the general upper bound is asymptotically optimal. Then in Section **??** we present a general setting of 'split' systems and observe that most of the Karger-Benczúr mechanism is applicable. Finally in Section **??** we introduce ℓ_1 volumes and show that sparsification for these objects, as well as Karger's problems for hypergraphs fall directly into our generalized framework.

Keywords: Metric spaces, sparsification

Joint work of: Newman, Ilan; Rabinovich, Yuri

Security Levels in Steganography

Ruediger Reischuk (Universität Lübeck, DE)

We take a fresh look at security notions for steganography – the art of encoding secret messages into unsuspicious covertexts such that an adversary cannot distinguish the resulting stegotexts from original covertexts.

Starting from the observation that the commonly used definition of (in)security does not help in quantifying the power of the adversary, we propose better alternatives.

The pitfalls with the security notion used so far is that the only known secure systems are quite inefficient.

Furthermore, as will be shown, one can construct stegosystems that are not secure, but also cannot be broken by an adversary.

This indicates that a different notion of security is needed which we call undetectability.

We investigate different variants of detectability and show that detectability on average clearly outperforms the others by giving the best results concerning an intuitive understanding of security in real life situations.

For this purpose, examples of steganographic channels and stegosystems are constructed that yield similar behaviour for all other security measures, but are well differentiated by the average measure.

As our main technical contribution we establish a close connection between the task of recognizing steganography and the task to distinguish pseudorandom functions from random functions.

Keywords: Steganography, security, algorithmic learning, games

Joint work of: Liskiewicz, Maciej; Reischuk, Rüdiger; Wölfel, Ulrich

Data Stream Algorithms for Codeword Testing

Atri Rudra (SUNY - Buffalo, US)

Motivated by applications in storage systems and the possibility of proving lower bounds for locally testable codes, we study data stream algorithms for local testing and tolerant testing of codes. Ideally, we would like to know whether there exist asymptotically good codes that can be local/tolerant tested with one-pass, poly-log space data stream algorithms.

Using an almost trivial extension of the fingerprinting method, we show that for the error detection problem (and hence, the local testing problem), there exists a one-pass, log-space randomized data stream algorithm for a broad class of asymptotically good codes, including the Reed-Solomon (RS) code and expander codes. In our technically more involved result, we give a one-pass, $O(e \log^2 n)$-space algorithm for RS (and related) codes with dimension k and block length n that can distinguish between the cases when the Hamming distance between the received word and the code is at most e and at least $\alpha \cdot e$ for some absolute constant $\alpha > 1$. For RS codes with random errors, we can obtain $e \leq O(n/k)$. For folded RS codes, we obtain similar results for worst-case errors as long as $e \leq (n/k)^{1-\epsilon}$ for any constant $\epsilon > 0$. These results follow by reducing the tolerant testing problem to the error detection problem using results from group testing and the list decodability of the code. We also show that using our techniques, the space requirement and the upper bound of $e \leq O(n/k)$ cannot be improved by more than logarithmic factors.

The result for random errors follows from our general result that for any code with distance d (over large alphabets), any Hamming ball of radius up to $d(1-\epsilon)$ for $\epsilon > 0$ contains only one codeword with high probability.

However, many interesting questions remain open.

Keywords: Sublinear algorithms, Locally Testable codes, Group testing, List decoding, Reed-Solomon codes, Random errors.

Joint work of: Rudra, Atri; Uurtamo, Steve

Unconditional Lower Bounds against Advice

Rahul Santhanam (University of Edinburgh, GB)

We show several unconditional lower bounds for exponential time classes against polynomial time classes with advice, including: (1) For any constant c, NEXP not in $P^{NP[n^c]}$ (2) For any constant c, MAEXP not in MA/n^c (3) BPEXP not in $BPP/n^{o(1)}$.

It was previously unknown even whether NEXP in $NP/n^{0.01}$. For the probabilistic classes, no lower bounds for uniform exponential time against advice were known before. We also consider the question of whether these lower bounds can be made to work on almost all input lengths rather than on infinitely many. We give an oracle relative to which NEXP in i.o.NP, which provides evidence that this is not possible with current techniques.

Keywords: Advice, derandomization, diagonalization, lower bounds, semantic classes

Joint work of: Buhrman, Harry; Fortnow, Lance; Santhanam, Rahul

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2010/2411

Rank Bounds for Depth-3 Identities

Nitin Saxena (Universität Bonn, DE)

We show that the rank of a depth-3 circuit (over any field) that is simple, minimal and zero is at most $O(k^3 logd)$. The previous best rank bound known was $2^{O(k^2)}(logd)^{k-2}$ by Dvir and Shpilka (STOC 2005).

Our main result almost resolves the rank question first posed by Dvir and Shpilka, as we also provide a simple and minimal identity of rank $\Omega(klogd)$.

Our rank bound significantly improves (dependence on k exponentially reduced) the best known deterministic black-box identity tests for depth-3 circuits by Karnin and Shpilka (CCC 2008). Our techniques also shed light on the factorization pattern of nonzero depth-3 circuits: the rank of linear factors of a simple, minimal and nonzero depth-3 circuit (over any field) is at most $O(k^3 logd)$.

The novel feature of this work is a new notion of maps between sets of linear forms, called ideal matchings, used to study depth-3 circuits. The proof involves decompositions of depth-3 identities into smaller identities using these techniques.

Joint work of: Saxena, Nitin; Seshadhri C.

Typically correct derandomization

Ronen Shaltiel (Haifa University, IL)

A typically-correct derandomization of a randomized algorithm A is a deterministic algorithm B (preferably of the same complexity as A) that agrees with A on "most inputs". This relaxed goal makes sense in cases where "derandomization on all inputs" is impossible (e.g. for Communication protocols, decision trees and streaming algorithms). The relaxed goal sometimes allows better derandomization than is known for "derandomization on all inputs" (specifically, it is possible to unconditionally simulate a randomized AC0 algorithm by a deterministic AC0 algorithm that succeeds on most inputs). It also allows polynomial time deterministic simulation of BPP under assumptions that are incomparable to those used in "hardness versus randomness tradeoffs".

I will discuss general approaches to achieve typically-correct derandomization in various algorithmic settings, and whether the relaxed goal of typically correct derandomization implies circuit lower bounds.

Joint work with Jeff Kinne and Dieter van Melkebeek

Keywords: Dearndomization, randomness extractors, pseudorandom generators, circuit lower bounds

On the Complexity of Boolean Functions in Different Characteristics

Amir Shpilka (Technion - Haifa, IL)

Every Boolean function on n variables can be expressed as a unique multivariate polynomial modulo p for every prime p. In this work, we study how the degree of a function in one characteristic affects its complexity in other characteristics. We establish the following general principle: functions with low degree modulo p must have high complexity in every other characteristic q. More precisely, we show the following results about Boolean functions $f : 0,1^n- > 0,1$ which depend on all n variables, and distinct primes p,q:

1. If f has degree $o(\log n)$ modulo p, then it must have degree $\Omega(n^{1-o(1)})$ modulo q. Thus a Boolean function has degree $o(\log n)$ in only one characteristic. This result is essentially tight as there exist functions that have degree $\log n$ in every characteristic.

2. If f has degree $d = o(\log n)$ modulo p, it cannot be computed correctly on more than $1 - p^{-O(d)}$ fraction of the hypercube by polynomials of degree $n^{1/2-\epsilon}$ modulo q.

As a corollary of the above results it follows that if f has degree $o(\log n)$ modulo p, then it requires super-polynomial size $AC_0[q]$ circuits. This gives a lower bound for a broad and natural class of functions.

Kolmogorov Complexity in Randomness Extraction

N. Variyam Vinodchandran (University of Nebraska, US)

We show that a computable function is an almost randomness extractor if and only if it is a Kolmogorov complexity extractor, thus establishing a fundamental equivalence between two forms of extraction studied in the literature: Kolmogorov extraction and randomness extraction. We present a distribution $\mathcal{M}_k$ based on Kolmogorov complexity that is complete for randomness extraction in the sense that a computable function is an almost randomness extractor if and only if it extracts randomness from $\mathcal{M}_k$.

Joint work of: J. Hitchcock, A. Pavan N. V. Vinodchandran

Planar Graph Isomorphism is in Log-space

Fabian Wagner (Universität Ulm, DE)

Graph Isomorphism is the prime example of a computational problem with a wide difference between the best known lower and upper bounds on its complexity. There is a significant gap between extant lower and upper bounds for planar graphs as well.

We bridge the gap for this natural and important special case by presenting an upper bound that matches the known log-space hardness [JKMT03]. In fact, we show the formally stronger result that planar graph canonization is in log-space. This improves the previously known upper bound of AC1 [MR91].

Our algorithm first constructs the biconnected component tree of a connected planar graph and then refines each biconnected component into a triconnected component tree. The next step is to log-space reduce the biconnected planar graph isomorphism and canonization problems to those for 3-connected planar graphs, which are known to be in log-space by [DLN08]. This is achieved by using the above decomposition, and by making significant modifications to LindellŠs algorithm for tree canonization, along with changes in the space complexity analysis.

The reduction from the connected case to the biconnected case requires further new ideas including a non-trivial case analysis and a group theoretic lemma to bound the number of automorphisms of a colored 3-connected planar graph.

Keywords: Planar Graphs, Graph Isomorphism, Logspace

Joint work of: Datta, Samir; Limaye, Nutan; Nimbhorkar, Prajakta; Thierauf, Thomas; Wagner, Fabian

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2010/2416

See also: Samir Datta, Nutan Limaye, Prajakta Nimbhorkar, Thomas Thierauf, Fabian Wagner, "Planar Graph Isomorphism is in Log-Space," ccc, pp.203-214, 2009 24th Annual IEEE Conference on Computational Complexity, 2009

Graph Algorithms from Group Algebra

Ryan Williams (IBM Almaden Center - San José, US)

I will outline a new method for exactly solving certain NP-hard search problems that was first proposed by Koutis in ICALP'08 and improved upon in later papers by myself and Koutis. The high-level idea is: encode a subset of potential solutions of a search problem with a multivariate polynomial that can be efficiently evaluated, then evaluate this polynomial on carefully chosen points over a group algebra that will "cancel out" all non-solutions and preserve some solutions with decent probability. This basic method has led to new randomized algorithms for several fundamental problems, most notably the longest path problem.

Deterministic approximation algorithms for the nearest codeword problem

Sergey Yekhanin (Microsoft Research - Mountain View, US)

The Nearest Codeword Problem (NCP) is a basic algorithmic question in the theory of error-correcting codes. Given a point v in F_2^n and a linear space L in F_2^n of dimension k NCP asks to find a point l in L that minimizes the (Hamming) distance from v.

It is well-known that the nearest codeword problem is NP-hard. Therefore approximation algorithms are of interest. The best effcient approximation algorithms for the NCP to date are due to Berman and Karpinski. They are a deterministic algorithm that achieves an approximation ratio of $O(k/c)$ for an arbitrary constant c; and a randomized algorithm that achieves an approximation ratio of $O(k/logn)$.

In this paper we present new deterministic algorithms for approximating the NCP that improve substantially upon the earlier work, (almost) de-randomizing the randomized algorithm of Berman and Karpinski.

We also initiate a study of the following Remote Point Problem (RPP). Given a linear space L in F_2^n of dimension k RPP asks to find a point v in F_2^n that is far from L. We say that an algorithm achieves a remoteness of r for the RPP if it always outputs a point v that is at least r-far from L. In this paper we present a deterministic polynomial time algorithm that achieves a remoteness of $\Omega(nlogk/k)$ for all $k < n/2$.

We motivate the remote point problem by relating it to both the nearest codeword problem and the matrix rigidity approach to circuit lower bounds in computational complexity theory.

Joint work of: Alon, Noga; Panigrahy, Rina; Yekhanin, Sergey

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2010/2413

Full Paper:
http://research.microsoft.com/en-us/um/people/yekhanin/Papers/NCP_approx.pdf

See also: Proceedings of the 13th Intl. Workshop on Randomization and Computation (RANDOM), pp. 339-351, 2009.