# Computational Complexity of Discrete Problems 

Edited by<br>Martin Grohe ${ }^{1}$, Michal Koucký ${ }^{2}$, Rüdiger Reischuk ${ }^{3}$, and<br>Dieter van Melkebeek ${ }^{4}$

1 HU Berlin, DE, grohe@informatik.hu-berlin.de
2 Academy of Sciences - Prague, CZ, koucky@math.cas.cz
3 Universität zu Lübeck, DE, reischuk@tcs.uni-luebeck.de
4 University of Wisconsin - Madison, US, dieter@cs.wisc.edu


#### Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 11121 "Computational Complexity of Discrete Problems". The first section gives an overview of the topics covered and the organization of the meeting. Section 2 lists the talks given in chronological order. The last section contains the abstracts of the talks.

Seminar 20.-25. March, 2011 - www.dagstuhl.de/11121 1998 ACM Subject Classification F.1.3 Complexity Measures and Classes, F. 2 Analysis of Algorithms and Problem Complexity Keywords and phrases discrete problems, computational complexity, Turing machines, Boolean circuits, quantum computing, communication and query complexity, extractors, pseudorandomness, derandomization, approximation, coding cryptography, algorithmic learning Digital Object Identifier 10.4230/DagRep.1.3.42 Edited in cooperation with Michael Elberfeld


## 1 Executive Summary

Martin Grohe<br>Michal Koucky<br>Rüdiger Reischuk<br>Dieter van Melkebeek

License © (c) $\Theta$ Creative Commons BY-NC-ND 3.0 Unported license
© Martin Grohe, Michal Koucký, Rüdiger Reischuk, and Dieter van Melkebeek

## Introduction and Goals

Computational models like Turing machines and Boolean circuits work on discrete input data. Even quantum computation and communication studied in the recent past are mainly applied to solve discrete problems. Analysing the computational complexity of such problems with respect to these models is one of the central topics in the theory of computation. Researchers try to classify algorithmic problems according to complexity measures like time and space both in the uniform and in the nonuniform setting. A variety of specialized computational models have been developed in order to better measure the complexity of certain classes of discrete problems.

Randomness has turned out to be another fundamental measure and added a lot of new intricate questions. Performing probabilistic choices within an algorithm one can design solution strategies for a given computational problem for which there are no obvious

deterministic ones. Recently, large effort has been taken to remove randomness from probabilistic algorithms, so called derandomization. Here one tries to develop general techniques that can be applied to a wide range of discrete problems.

Information transfer is investigated according to the amount of communication necessary in different scenarios like 1-way channels or a bounded number of communication rounds. This is a basis for the design of efficient communication protocols. Furthermore, it has been observed that often ordinary computational problems given to a specific computational device can formally be analysed elegantly by concentrating on information flow aspects.

In addition, other computational processes arising in diverse areas of computer science have been studied, each with their own relevant complexity measures. Several of those investigations have evolved into substantial research areas, including:

- approximability (motivated by optimization),
- computational learning theory (motivated by artificial intelligence),
- query complexity (motivated by databases).

The analysis and relative power of basic models of computation remains a major challenge. New lower bound techniques for explicitly defined functions have brought the field a major step forward. For example, close connections have been discovered between circuit lower bounds for certain uniform complexity classes and the existence of pseudorandom generators and the possibility of efficient derandomization.

The seminar "Computational Complexity of Discrete Problems" has evolved out of the series of seminars entitled "Complexity of Boolean Functions," a topic that has been covered at Dagstuhl on a regular basis since the foundation of this research center. Over the years, the focus on nonuniform models has broadened to include uniform ones as well.

A salient feature of the current research in computational complexity is the interpenetration of ideas from different subareas of computational complexity and from other fields in computer science and mathematics. By organizing a generic seminar on computational complexity we have aimed to attract researchers from those various subareas and foster further fruitful interactions.

## Organization of the Meeting

47 researchers from all over the world including a good number of young scientists met in Dagstuhl for this seminar. Every day we started with a longer survey talk on recent advances in specific topics that had been selected in advance by the organizers. We thank our colleagues who agreed to prepare and give these presentations:

- Prahladh Harsha took the duty for threshold functions,
- Paul Beame for $A C^{0}$ circuits,
- Troy Lee for communication complexity,
- Eli Ben-Sasson for extractors, and
- Robin Moser for constraint satisfaction problems.

The surveys were followed by shorter talks on new results obtained by the participants. We could schedule 30 of such plenary talks such that enough additional time was left for discussions in smaller groups on a spontaneous basis. In addition, Tuesday evening was devoted to a rump session where everybody could present his favourite open problem.

The first evening the participants could also extend their knowledge and taste in a completely different area, namely arts. We took part in the vernisage of the art exhibit by Irene Zaharoff who presented her colorful paintings in the corridors of the new building.

Everybody got so excited that the spontaneous idea to select one of her paintings and support a donation to Dagstuhl was implemented on the spot.

## Topics and Achievements

We shortly review the main topics that have been discussed during the meeting. Further details as well as additional material can be found in the abstracts following.

## Randomized Computations, Derandomization, and Testing

The complexity of randomized computations and its theoretical foundation was a major issue of the seminar. It showed up in about half of all contributions. Eric Allender discussed the computational power of Kolmogorov-random strings, while Andrej Bogdanov showed how to construct pseudorandom generators for read-once formulas and Pavel Pudlák for read-once permutation branching programs. Improved pseudorandom generators for a special class of discrete functions called combinatorial checkerboards were given by Thomas Watson.

For randomness extractors improved constructions were presented by Eli Ben-Sasson for the case of two sources and by Xin Li for three sources. For restricted sources that are generated by circuits of constant depth extractors were designed by Emanuele Viola.

Markus Bläser discussed the randomized complexity of identity tests for sparse polynomials, while Beate Bollig did this for integer multiplication in the OBDD model generalizing her deterministic lower bound shown at the previous meeting.

Derandomization techniques were presented by Matthew Anderson for zero tests of multilinear arithmetic formulas and by Robin Moser for Schöning's satisfiability test of k-CNF formulas. Eldar Fischer considered property testing of monotone formulas.

## Communication Complexity

How many bits two parties have to exchange in order to compute a given function if the input is distributed among them? This is a fundamental question for the design of communication protocols. To determine the Hamming distance of two $n$-bit strings it has been well known that the trivial solution of one party sending his string to the other party is optimal. It was open for quite a while if this still holds if the two parties get the additional information that the distance of their inputs is either small or large (let's say not in the region between $[n / 2-\sqrt{n}, n / 2+\sqrt{n}]$. Oded Regev could resolve this question for general probabilistic protocols with unbounded rounds of communication by proving a linear lower bound.

Allowing the two parties also to exchange quantum bits leads to quantum protocols which - in contrast to quantum computers - are already used in practice. There are examples known that quantum bits can lead to an exponential decrease of the amount of communication. Oded Regev in his second contribution showed that such a separation can even be obtained when comparing 1 -way quantum protocols with 2 -way classical protocols.

Troy Lee investigated the query complexity of quantum states and a generalization of this problem called state conversion. He defined a new norm for the distance of quantum states and proved that this gives an appropriate measure.

Andrew Drucker showed how fault-tolerant protocols can be used to improve upon more complex objects called probabilistically checkable debate systems. This has implications for the approximability of problems in PSPACE.

## Complexity Classes

For classical complexity classes some progress was reported, too. Michael Elberfeld showed how graph problems restricted to instances of bounded tree width can be solved in logarithmic space, while Fabian Wagner was able to solve the isomorphism problem for such instances in LogCFL. Meena Mahajan presented a detailed investigation of arithmetic circuits of logarithmic depth and their relation to logspace.

For Boolean circuits the tradeoff between size and depth has been investigated from the very beginning. Anna Gál showed with the help of the pebble game how the bounds can be substantially improved for layered circuits. Or Meir took a closer lock at the breakthrough result $I P=$ PSPACE and showed an alternate proof that uses fairly general error-correcting codes instead of polynomials.

Another famous result that unbounded circuits of constant depth cannot compute the parity function was taken up by Paul Beame and Johan Håstad trying to get a finer quantitative statement of this property. Paul described a simulation of such circuits by decision trees which has implications how well $A C^{0}$ can approximate the parity function, while Johan presented a direct proof for an upper bound on the correlation between parity and functions computable in constant depth. Nicole Schweikardt gave a precise characterization of the locality of order-invariant first-order queries with arbitrary predicates, which are closely related to the complexity class $A C^{0}$.

Srikanth Srinivasan showed that computing the determinant over simple noncommutative rings is as hard as computing the permanent in the commutative case, thus establishing a huge complexity gap between commutative and noncommutative domains.

## Further Topics

Improving the construction of good error correcting codes by combining classical codes with outer codes was adressed by Amnon Ta-Shma. Matthias Krause presented a new technique to prove security properties of cryptographic hash functions. Philipp Woelfel considered random walks on a line towards a target where the searcher can fix an arbitrary distribution on his probabilistically chosen next movement. A lower bound on the first hitting time was shown matching previously known upper bounds for this problem. Jakob Nordström considered linear invariance properties in the realm of property testing. He investigated the problem to decide on the semantic difference for syntactically different descriptions of linear invariances.

Efficiently learning unknown concepts by queries or taking random samples is another topic of general applicability. An important measure in this respect is the VC-dimension which implies bounds on the minimal achievable additive error for any learning algorithm. Ilan Newman asked the same question for the multiplicative error and showed that the triangular rank of a set system gives a corresponding measure. Kristoffer Hansen considered the class of Boolean functions with a constant degree representation where each variable is used only a bounded number of times. He presented a deterministic polynomial time algorithm for this problem. For Boolean functions the notion of sensivity has turned to be an important measure although it seems to be hard to estimate in many cases. Prahladh Harsha considered polynomial threshold functions and showed the first nontrivial upper bound, which has also implications for the learning complexity of these functions.

## Conclusion

Investigating the complexity of discrete problems is one of the fundamental tasks in the theory of computation. On the one hand, new algorithmic techniques and new ways to look at a problem have led to better algorithms and protocols. On the other hand, typically more demanding is the task to prove lower bounds on the computational complexity of a concrete problem. Progress is still continuing, as seen for example in testing, derandomization and explicit constructions of combinatorial objects like extractors, that improves our knowledge considerably. Despite these significant steps forward that have been achieved in several subareas since our previous meeting three years ago, the general feeling among the participants was that we still have to work hard for many more years to get a good understanding what are the limits of efficient computation.

We like to thank the staff at Dagstuhl who - as usual - provided a marvellous surrounding to make this a successful meeting with ample space for undisturbed interactions between the participants.

## 2 Table of Contents

Executive Summary
Martin Grohe, Michal Koucký, Rüdiger Reischuk, and Dieter van Melkebeek ..... 42
Overview of Talks
A Survey of Recent Advances in Threshold Functions
Prahladh Harsha ..... 49
Bounding the Average and Noise Sensitivity of Polynomial Threshold Functions Prahladh Harsha ..... 49
Isomorphism and Canonization of Bounded Treewidth Graphs Fabian Wagner ..... 50
Counting Classes and the Fine Structure between NC $^{1}$ and DLOG Meena Mahajan ..... 50
The Hardness of the Noncommutative Determinant
Srikanth Srinivasan ..... 51
$\mathrm{IP}=\mathrm{PSPACE}$ using Error Correcting Codes
Or Meir ..... 51
Efficient Probabilistically Checkable Debates
Andrew Drucker ..... 51
Limits on the Computational Power of Random Strings Eric Allender ..... 52
How well do $\mathrm{AC}^{0}$ Circuits Approximate Parity? Approximating $\mathrm{AC}^{0}$ by "Small" Height Decision Trees
Paul Beame ..... 53
Randomized OBDDs for the Most Significant Bit of Multiplication Need Exponential Size
Beate Bollig ..... 53
The Size and Depth of Layered Boolean Circuits
Anna Gál ..... 54
Preimage Resistance Beyond the Birthday Barrier - The Case of Blockcipher Based Hashing
Matthias Krause ..... 54
Pseudorandom Generators for Group Products
Pavel Pudlák ..... 55
Pseudorandom Generators for Combinatorial Checkerboards Thomas W. Watson ..... 55
Pseudorandomness for Read-Once Formulas
Andrej Bogdanov ..... 55
Testing Assignments for Satisfying a Monotone Formula Eldar Fischer ..... 56
On the Semantics of Local Characterizations for Linear-Invariant Properties Jakob Nordström ..... 56
Quantum Query Complexity of State Generation Troy Lee ..... 57
Quantum One-Way Communication can be Exponentially Stronger Than Classical Communication Oded Regev ..... 58
An Optimal Lower Bound on the Communication Complexity of Gap-Hamming- Distance
Oded Regev ..... 58
From Affine to Two-Source Extractors via Approximate Duality Eli Ben-Sasson ..... 59
Improved Constructions of Three Source Extractors Xin Li ..... 59
Extractors for Circuit Sources
Emanuele Viola ..... 59
What Binary Codes can be Obtained by Concatenating AG Codes with Hadamard? Amnon Ta-Shma ..... 60
Derandomizing Polynomial Identity Testing for Multilinear Constant-Read Formulae Matthew Anderson ..... 60
Randomness Efficient Testing of Sparse Blackbox Identities of Unbounded Degree over the Reals Markus Bläser ..... 61
Learning Read-Constant Polynomials of Constant Degree Modulo Composites Kristoffer Arnsfelt Hansen ..... 61
Locality of $\mathrm{AC}^{0}$-Computable Graph Queries Nicole Schweikardt ..... 62
A Survey of Exponential Algorithms for Constraint Satisfaction Problems Robin Moser ..... 62
A Full Derandomization of Schöning's $k$-SAT Algorithm Robin Moser ..... 63
Algorithmic Meta Theorems Inside Logspace and Their Applications Michael Elberfeld ..... 63
Triangular Rank and Sampling With Multiplicative Errors Ilan Newman ..... 63
Tight Lower Bounds for Greedy Routing in Uniform Small World Rings Philipp Woelfel ..... 64
On the Correlation of Parity with Small Depth Circuits Johan Håstad ..... 65
Participants ..... 66

## 3 Overview of Talks

### 3.1 A Survey of Recent Advances in Threshold Functions

Prahladh Harsha (TIFR Mumbai, IN)
License © © $\bigodot$ Creative Commons BY-NC-ND 3.0 Unported license
© Prahladh Harsha
Threshold functions (halfspaces, intersection of halfspaces, polynomial threshold functions) commonly occur in various applications in learning theory, communication complexity etc. In the last two years, there has been a sequence of results in the area of threshold functions (eg., improved pseudorandom generators for various types of threshold functions, better bounds on certain quantitative functional parameters such as noise sensitivity, average sensitivity etc). Most of these results have been inspired by a better understanding of invariance principles from probability theory. In this talk, I'll give a survey of some these results related to threshold functions and the corresponding invariance principles.

### 3.2 Bounding the Average and Noise Sensitivity of Polynomial Threshold Functions

Prahladh Harsha (TIFR Mumbai, IN)
License © © $\odot$ Creative Commons BY-NC-ND 3.0 Unported license © Prahladh Harsha
Joint work of Harsha, Prahladh; Klivans, Adaml; Meka, Raghu
Main reference In Proc. 42nd ACM Symp. on Theory of Computing (STOC) (Cambridge, Massachusetts, 6-8 June), pages 543-552, 2010
URL http://arxiv.org/abs/0909.5175
In 1994, Gotsman and Linial posed the following question: "what is the maximum number of edges of the n-dimensional Boolean hypercube cut by any degree d polynomial surface?" Generalizing from the degree one case, they conjectured that the symmetric function slicing the middle d layers of the Boolean hypercube achieves this maximum. A restating of this conjecture is that the average sensitivity of a degree d polynomial threshold function (PTF) is at most $O(d \sqrt{n})$. A closely related (and in fact, equivalent) conjecture is that the noise sensitivity of a degree $d$ PTF (for noise rate $\delta$ ) is at most $O(d \sqrt{\delta})$.

In this work, we give the first nontrivial upper bounds on the average sensitivity and noise sensitivity of polynomial threshold functions. More specifically, we show that

- The average sensitivity of a $d$-PTF is at most $O\left(n^{1-1 /(4 d+6)}\right)$
- The noise sensitivity of $f$ with noise rate $\delta$ is at most $O\left(\delta^{1 /(4 d+6)}\right)$.

The Gotsman-Linial conjecture itself remains unresolved. Nevertheless, these bounds immediately yield (the first) polynomial time agnostic learning algorithms for the class of degree d PTFs.

# 3.3 Isomorphism and Canonization of Bounded Treewidth Graphs 

Fabian Wagner (Universität Ulm, DE)
License © © © Creative Commons BY-NC-ND 3.0 Unported license © Fabian Wagner
Main reference B. Das, J. Torán, F. Wagner: Restricted Space Algorithms for Isomorphism on Bounded Treewidth Graphs, in proceedings of STACS, pp. 227-238, 2010.
F. Wagner: Graphs of Bounded Treewidth can be Canonized in $\mathrm{AC}^{1}$, to appear in proceedings of CSR 2011, technical report: ECCC TR-032, 2011.

In two recent results we show that isomorphism testing of bounded treewidth graphs is in LogCFL [Das-Torán-Wagner'10] and canonization is in $\mathrm{AC}^{1}$ [Wagner'11], improving the previously known upper bounds of $\mathrm{TC}^{1}$ [Grohe-Verbitsky'06] and $\mathrm{TC}^{2}$ [Köbler-Verbitsky'08].

Both results extend in two different ways the techniques of canonization algorithms developed for restricted graph classes.

Most notably Lindells logspace algorithm for trees [Lindell'92] which was generalized to logspace algorithms for partial 2-trees [Arvind-Das-Köbler'08], $k$-trees [Köbler-Kuhnert'09], interval graphs [Köbler-Kuhnert-Laubner-Verbitsky'09], planar graphs [Datta-Limaye-Nimbhorkar-Thierauf-Wagner'09], $K_{3,3^{-}}$and $K_{5}$-minor free graphs [Datta-Nimbhorkar-Thierauf-Wagner'09].

In the talk I will present the proof techniques from both results [Das-Torán-Wagner'10] and [Wagner'11].

## References

1 B. Das, J. Toran, F. Wagner: Restricted Space Algorithms for Isomorphism on Bounded Treewidth Graphs, Proceedings of STACS'10, LIPIcs Vol. 5, pp. 227-238, 2010.
2 F. Wagner: Graphs of Bounded Treewidth can be Canonized in $\mathrm{AC}^{1}$, to appear in proceedings of CSR 2011, technical report: ECCC TR-032, 2011.

### 3.4 Counting Classes and the Fine Structure between NC $^{1}$ and DLOG

Meena Mahajan (The Institute of Mathematical Sciences - Chennai, IN)
License © © $\Theta$ Creative Commons BY-NC-ND 3.0 Unported license
© Meena Mahajan
Joint work of Mahajan, Meena; Datta, Samir; Rao, B. V. Raghavendra; Thomas, Michael; Vollmer, Heribert
Main reference Datta, Samir; Mahajan, Meenal; Rao, B. V. Raghavendra; Thomas, Michael; Vollmer, Heribert; "Counting classes and the fine structure between NC ${ }^{1}$ and L," Proc. 35th MFCS 2010 URL http://dx.doi.org/10.1007/978-3-642-15155-2_28

The class $\mathrm{NC}^{1}$ of problems solvable by bounded fan-in circuit families of logarithmic depth is known to be contained in logarithmic space DLOG, but not much about the converse is known. In this paper we examine the structure of classes in between $\mathrm{NC}^{1}$ and DLOG based on counting functions or, equivalently, based on arithmetic circuits. The classes $\mathrm{PNC}^{1}$ and $\mathrm{CNC}^{1}$, defined by a test for positivity and a test for zero, respectively, of arithmetic circuit families of logarithmic depth, sit in this complexity interval. We study the landscape of Boolean hierarchies, constant-depth oracle hierarchies, and logarithmic-depth oracle hierarchies over $\mathrm{PNC}^{1}$ and $\mathrm{CNC}^{1}$. We provide complete problems, obtain the upper bound DLOG for all these hierarchies, and prove partial hierarchy collapses. In particular, the constant-depth oracle hierarchy over PNC ${ }^{1}$ collapses to its first level $\mathrm{PNC}^{1}$, and the constant-depth oracle hierarchy over $\mathrm{CNC}^{1}$ collapses to its second level.

3.5 The Hardness of the Noncommutative Determinant<br>Srikanth Srinivasan (Institute for Advanced Study - Princeton, US)<br>License © © © Creative Commons BY-NC-ND 3.0 Unported license<br>(c) Srikanth Srinivasan<br>Joint work of Chien, Steve; Harsha, Prahladh; Sinclair, Alistair; Srinivasan, Srikanth<br>Main reference Steve Chien, Prahladh Harsha, Alistair Sinclair, Srikanth Srinivasan; "Almost Settling the Hardness of Noncommutative Determinant," STOC 2011, to appear.<br>URL http://arxiv.org/abs/1101.1169

We consider the complexity of the determinant over noncommutative domains and show that even in simple noncommutative settings such as the setting of 2 X 2 matrices, this problem is \#P-hard. This has applications to the analysis of a natural extension to the Godsil-Gutman estimator for the $0-1$ permanent and to arithmetic circuit complexity.

### 3.6 IP = PSPACE using Error Correcting Codes

Or Meir (Weizmann Institute - Rehovot, IL)
License © © $\Theta$ Creative Commons BY-NC-ND 3.0 Unported license
© Or Meir
Main reference Or Meir; "IP = PSPACE using Error Correcting Codes," ECCC TR10-137
URL http://eccc.hpi-web.de/report/2010/137/
The IP theorem, which asserts that IP = PSPACE (Lund et. al., and Shamir, in J. ACM $39(4)$ ), is one of the major achievements of complexity theory. The known proofs of the theorem are based on the arithmetization technique, which transforms a quantified Boolean formula into a related polynomial. The intuition that underlies the use of polynomials is commonly explained by the fact that polynomials constitute good error correcting codes. However, the known proofs seem tailored to the use of polynomials, and do not generalize to arbitrary error correcting codes.

In this work, we show that the IP theorem can be proved by using general error correcting codes. We believe that this establishes a rigorous basis for the aforementioned intuition, and sheds further light on the IP theorem.

### 3.7 Efficient Probabilistically Checkable Debates

Andrew Drucker (MIT - Cambridge, US)
License © $\odot \odot$ Creative Commons BY-NC-ND 3.0 Unported license
© Andrew Drucker
Main reference Andrew Drucker; "Efficient Probabilistically Checkable Debates," Electronic Colloquium on Computational Complexity (ECCC), TR11-073, 2011.
URL http://eccc.hpi-web.de/report/2011/073/
Probabilistically checkable debate systems (PCDSs) are debates between two competing provers, which a polynomial-time verifier inspects in $O(1)$ bits.

Condon et al. showed all PSPACE languages have PCDSs. This implies that the approximation versions of some natural PSPACE-complete problems are also PSPACEcomplete.

We give an improved construction: for a language $L$ with an ordinary debate system defined by uniform circuits of size $s=s(n)$, we give a PCDS for $L$ with debate bitlength
$s$-polylog $(s)$. This tightens the connection between the time complexities of PSPACE-complete problems and their approximation versions.

Our key ingredient is a novel application of error-resilient communication protocols (specifically, the Braverman-Rao protocol). By requiring ordinary debates to be resiliently encoded, we endow them with a useful "stability" property, which lets them be converted into PCDSs. Our main technical challenge is to enforce error-resilient encoding by the debaters.

### 3.8 Limits on the Computational Power of Random Strings

Eric Allender (Rutgers University - Piscataway, US)
License © (c) $\Theta$ Creative Commons BY-NC-ND 3.0 Unported license
© Eric Allender
Joint work of Allender, Eric; Friedman, Luke; Gasarch, William
Main reference Eric Allender, Luke Friedman, William Gasarch; "Limits on the Computational Power of Random Strings," ICALP, 2011
URL http://eccc.hpi-web.de/report/2010/139/
R , the set of Kolmogorov-random strings, is a central notion in the study of algorithmic information theory, and in recent years R has increasingly been studied in relation to computational complexity theory. This talk takes as its starting point three strange inclusions that have been proved since 2002: 1. NEXP is contained in the class of problems NP-Turingreducible to R. 2. PSPACE is contained in the class of problems poly-time Turing-reducible to R. 3. BPP is contained in the class of problems poly-time truth-table-reducible to R.
(These inclusions hold for both of the most widely-studied variants of Kolmogorov complexity: the plain complexity $\mathrm{C}(\mathrm{x})$ and the prefix-complexity $\mathrm{K}(\mathrm{x})$.

They also hold no matter which "universal" Turing machine is used in the definitions of the functions C and K.)

These inclusions are "strange" since R is not even computable! Thus it is not at all clear that these are meaningful upper bounds on the complexity of BPP, PSPACE, and NEXP, and indeed it is not at all clear that it is very interesting to consider efficient reductions to noncomputable sets such as R.

In this talk, I will try to convince you that the class of problems efficiently reducible to R is, indeed, a complexity class. The main theorems are that, if we restrict attention to prefix complexity K and the corresponding set of random strings $\mathrm{R}_{K}$, then the class of decidable problems that are in NP relative to $\mathrm{R}_{K}$ (no matter which universal machine is used to define K) lies in EXPSPACE, and the class of decidable problems that are poly-time truth-table reducible to $\mathrm{R}_{K}$ (no matter which universal machine is used to define K ) lies in PSPACE.

Thus we can "sandwich" PSPACE between the class of problems truth-table- and Turingreducible to $\mathrm{R}_{K}$, and the class of decidable problems that are in NP relative to $\mathrm{R}_{K}$ lies between NEXP and EXPSPACE. The corresponding questions for plain Kolmogorov complexity C are wide open; no upper bounds are known at all for the class of decidable problems efficiently reducible to $\mathrm{R}_{C}$.

These results also provide the first quantitative limits on the applicability of uniform derandomization techniques.

### 3.9 How well do AC $^{0}$ Circuits Approximate Parity? Approximating AC $^{0}$ by "Small" Height Decision Trees

Paul Beame (University of Washington - Seattle, US)
License © © $\Theta$ Creative Commons BY-NC-ND 3.0 Unported license © Paul Beame
Joint work of Beame, Paul; Impagliazzo, Russell; Srinivasan, Srikanth
We show that for every $C=C(n)>1$ and every family $F$ of $k$-DNF formulas in n variables one can build a single decision tree $T$ of height $h=n / C$ such that for all but a $2^{-h /\left(2^{O(k)} \log |F|\right)}$ fraction of paths $p$ in $T$, every formula in $F$ reduces to a $\left(2^{k} C \log |F|\right)^{O\left(k^{3}\right)}$ _ junta on assignments consistent with $p$. This improves a construction, due to Ajtai, which had an exponentially larger dependence on $k$.

As a consequence of this construction we show that every n-input $\mathrm{AC}^{0}$ circuit of size $S$ and depth $d$ can be approximated by a decision tree of height at most $n-B\{S, d\} n$, where $B\{S, d\}=2^{-2 d \log _{2}^{4 / 5}} S$, that is always correct but may not produce an answer on at most a $2^{-B\{S, d\} n}$ fraction of branches. It follows that any such $\mathrm{AC}^{0}$ circuit has correlation at most $2^{-B\{S, d\} n}$ with the $n$-bit Parity function.

Our proof is constructive and yields a deterministic algorithm running in time $2^{n-B\{S, d\} n} S^{O(1)}$ that exactly counts the number of satisfying assignments of any n-input $\mathrm{AC}^{0}$ circuit of size $S$ and depth $d$. Indeed, in the same running time we can deterministically construct a decision tree of size at most $2^{n-B\{S, d\} n}$ that exactly computes the function given by such a circuit.
(Our constructions more naturally yield randomized algorithms for these problems but deterministic algorithms follow because only limited independence is required in their analysis.)

### 3.10 Randomized OBDDs for the Most Significant Bit of Multiplication Need Exponential Size

Beate Bollig (Technische Universität Dortmund, DE)
License © © $\Theta$ Creative Commons BY-NC-ND 3.0 Unported license
© Beate Bollig
Joint work of Bollig, Beate; Gille, Marc
Main reference Beate Bollig and Marc Gille; "Randomized OBDDs for the most significant bit of multiplication need exponential size," Information Processing Letters 111, 151-155, 2011.
URL http://dx.doi.org/10.1016/j.ipl.2010.11.013
The basic arithmetic functions have been in the middle of several complexity theoretical investigations and ordered binary decision diagrams (OBDDs) are a popular dynamic data structure for Boolean functions.

Only in 2008 it has been shown that the size of deterministic OBDDs for the most significant bit of integer multiplication is exponential.

Since probabilistic methods have turned out to be useful in almost all areas of computer science, one may ask whether randomization can help to represent the most significant bit of multiplication in smaller size.

Here, it is proved that the randomized OBDD complexity is also exponential.

# 3.11 The Size and Depth of Layered Boolean Circuits 

Anna Gál (University of Texas at Austin, US)
License © © © Coreative Commons BY-NC-ND 3.0 Unported license
© Anna Gál
Joint work of Gál, Anna; Jang, Jing-Tang
We consider the relationship between size and depth for layered Boolean circuits, synchronous circuits and planar circuits as well as classes of circuits with small separators. In particular, we show that every layered Boolean circuit of size $s$ can be simulated by a layered Boolean circuit of depth $O(\sqrt{s \log s})$. For planar circuits and synchronous circuits of size $s$, we obtain simulations of depth $O(\sqrt{s})$. The best known result so far was by Paterson and Valiant, and Dymond and Tompa, which holds for general Boolean circuits and states that $D(f)=O(C(f) / \log C(f))$, where $C(f)$ and $D(f)$ are the minimum size and depth, respectively, of Boolean circuits computing $f$. The proof of our main result uses an adaptive strategy based on the two-person pebble game introduced by Dymond and Tompa. Improving any of our results by polylog factors would immediately improve the bounds for general circuits.

# 3.12 Preimage Resistance Beyond the Birthday Barrier - The Case of Blockcipher Based Hashing 

Matthias Krause (Universität Mannheim, DE)
License © © $\Theta$ Creative Commons BY-NC-ND 3.0 Unported license
© Matthias Krause
Joint work of Krause, Matthias; Armknecht, Frederik; Fleischmann, Ewan
Security proofs are an essential part of modern cryptography. Often the challenge is not to come up with appropriate schemes but rather to technically prove that these satisfy the desired security properties. We provide for the first time techniques for proving asymptotically optimal preimage resistance bounds for block cipher based double length, double call hash functions. More precisely, we consider for some blocklength n compression functions $H$ from $\{0,1\}^{3 n} \rightarrow\{0,1\}^{2 n}$ using two calls to an ideal block cipher with an n-bit block size. Optimally, an adversary trying to find a preimage for $H$ should require ? $\left(2^{2 n}\right)$ queries to the underlying block cipher. As a matter of fact there have been several attempts to prove the preimage resistance of such compression functions, but no proof did go beyond the ? $\left(2^{n}\right)$ "birthday" barrier, therefore leaving a huge gap when compared to the optimal bound.

In this paper, we introduce two new techniques on how to lift this bound to ? $\left(2^{2 n}\right)$. We demonstrate our new techniques for a simple and natural design of $H$, being the concatenation of two instances of the well-known Davies-Meyer compression function.

### 3.13 Pseudorandom Generators for Group Products

Pavel Pudlák (Acad. of Sciences - Prague, CZ)
License © © $\Theta$ Creative Commons BY-NC-ND 3.0 Unported license © Pavel Pudlák
Joint work of Koucký, Michal; Nimbhorkar, Prajakta; Pudlák, Pavel
Main reference M. Koucký, P. Nimbhorkar, P. Pudlák; "Pseudorandom Generators for Group Products," Proc. of the 2011 ACM STOC.
URL http://www.math.cas.cz/ pudlak/version-g.pdf
We proved that the pseudorandom generator introduced by Impagliazzo et al. in 1994 with proper choice of parameters fools group products of a given finite group $G$. The seed length is $O\left(|G|^{O(1)} \cdot \log n+\log n / \delta\right)$, where $n$ is the length of the word and $\delta$ is the allowed error. The result is equivalent to the statement that the pseudorandom generator with seed length $O\left(2^{O(w \log w)} \cdot \log n+\log n / \delta\right)$ fools read-once permutation branching programs of width $w$.

In the lecture I give a short sketch of the main ideas focusing on a geometric lemma that is one of the main technical parts.

### 3.14 Pseudorandom Generators for Combinatorial Checkerboards

Thomas W. Watson (University of California - Berkeley, US)
License $\propto \odot \odot$ Creative Commons BY-NC-ND 3.0 Unported license
© Thomas W. Watson
We define a combinatorial checkerboard to be a function $f:\{1, \ldots, m\}^{d} \rightarrow\{1,-1\}$ of the form $f\left(u_{1}, \ldots, u_{d}\right)=\prod_{i=1}^{d} f_{i}\left(u_{i}\right)$ for some functions $f_{i}:\{1, \ldots, m\} \rightarrow\{1,-1\}$. This is a variant of combinatorial rectangles, which can be defined in the same way but using $\{0,1\}$ instead of $\{1,-1\}$.

We consider the problem of constructing explicit pseudorandom generators for combinatorial checkerboards. This is a generalization of small-bias generators, which correspond to the case $m=2$.

We construct a pseudorandom generator that $\epsilon$-fools all combinatorial checkerboards with seed length $O\left(\log m+\log d \cdot \log \log d+\log ^{3 / 2} \frac{1}{\epsilon}\right)$. Previous work by Impagliazzo, Nisan, and Wigderson implies a pseudorandom generator with seed length $O\left(\log m+\log ^{2} d+\log d \cdot \log \frac{1}{\epsilon}\right)$. Our seed length is better except when $\frac{1}{\epsilon} \geq d^{\omega(\log d)}$.

### 3.15 Pseudorandomness for Read-Once Formulas

Andrej Bogdanov (Chinese University of Hong Kong, HK)
License © © © $\odot$ Creative Commons BY-NC-ND 3.0 Unported license
© Andrej Bogdanov
Joint work of Bogdanov, Andrej; Papakonstantinou, Periklis; Wan, Andrew
Main reference manuscript (unpublished)
We give an explicit construction of a pseudorandom generator for read-once formulas whose inputs can be read in arbitrary order. For formulas in $n$ inputs and arbitrary gates of fan-in at most $d=O(n / \log n)$, the pseudorandom generator uses $(1-\Omega(1)) n$ bits of randomness and produces an output that looks $2^{-\Omega(n)}$-pseudorandom to all such formulas.

Our analysis is based on the following lemma. Let $p r=M z+e$, where $M$ is the parity-check matrix of a sufficiently good binary error-correcting code of constant rate, $z$ is a random string, $e$ is a small-bias distribution, and all operations are modulo 2. Then for every pair of functions $f, g: B^{n / 2} \rightarrow B$ and every equipartition $(I, J)$ of $[n]$, the distribution $p r$ is pseudorandom for the pair $\left(f\left(\left.x\right|_{I}\right), g\left(\left.x\right|_{J}\right)\right)$, where $\left.x\right|_{I}$ and $\left.x\right|_{J}$ denote the restriction of $x$ to the coordinates in $I$ and $J$, respectively.

### 3.16 Testing Assignments for Satisfying a Monotone Formula

Eldar Fischer (Technion - Haifa, IL)
License © (c) $\Theta$ Creative Commons BY-NC-ND 3.0 Unported license
© Eldar Fischer
Joint work of Fischer, Eldar; Lachish, Oded; Nimbhorkar, Prajakta
Property Testing deals with the following question: Distinguish using as few queries to the input as possible, ideally with a number of queries independent of the input size, between inputs that satisfy a given property and inputs that are far from any possible input satisfying the property. In the massively parametrized model, a fixed part of the input is fully given to the algorithm in advance, on which the algorithm has to be exact (i.e. the approximation of "not being far from a satisfying input" can only be made for the input not given in advance).

In this talk we consider properties that relate to tree-like structures that are given in advance, and in particular to read-once monotone Boolean formulas. Such formulas are representable as trees with And/Or labels on their nodes, and the part of the input not given in advance is the assignment, i.e. the values at the leaves.

The main result is a test for the property of an assignment satisfying the given formula, whose number of queries does not depend on the input size at all. We also discuss some related questions, such as making the test tolerant, or alternatively reducing its number of queries to be quasi-polynomial in the approximation parameter.

### 3.17 On the Semantics of Local Characterizations for Linear-Invariant Properties

Jakob Nordström (KTH Stockholm, SE)

License © © $\Theta$ Creative Commons BY-NC-ND 3.0 Unported license
© Jakob Nordström
Joint work of Bhattacharyya, Arnab; Grigorescu, Elena; Nordström, Jakob; Xie, Ning
Main reference Arnab Bhattacharyya, Elena Grigorescu, Jakob Nordström, Ning Xie; "Separations of Matroid Freeness Properties," ECCC TR10-136
URL http://eccc.hpi-web.de/report/2010/136/
A property of functions on a vector space is said to be linear-invariant if it is closed under linear transformations of the domain. Linear-invariant properties are some of the most well-studied properties in the field of property testing. Testable linear-invariant properties can always be characterized by so-called local constraints, and of late there has been a rapidly developing body of research investigating the testability of linear-invariant properties in terms of their descriptions using such local constraints. One problematic aspect that has been largely ignored in this line of research, however, is that syntactically distinct local characterizations need not at all correspond to semantically distinct properties. In fact, there
are known fairly dramatic examples where seemingly infinite families of properties collapse into a small finite set that was already well-understood.

In this work, we therefore initiate a systematic study of the semantics of local characterizations of linear-invariant properties. For such properties the local characterizations have an especially nice structure in terms of forbidden patterns on linearly dependent sets of vectors, which can be encoded formally as matroid constraints. We develop techniques for determining, given two such matroid constraints, whether these constraints encode identical or distinct properties, and show for a fairly broad class of properties that these techniques provide necessary and sufficient conditions for deciding between the two cases. We use these tools to show that recent (syntactic) testability results indeed provide an infinite number of infinite strict hierarchies of (semantically) distinct testable locally characterized linear-invariant properties.

### 3.18 Quantum Query Complexity of State Generation

Troy Lee (National University of Singapore, SG)
License © © © $\Theta$ Creative Commons BY-NC-ND 3.0 Unported license
© Troy Lee © Troy Lee
Joint work of Lee, Troy; Mittal, Rajat; Reichardt, Ben; Spalek, Robert; Szegedy, Mario
Main reference Troy Lee, Rajat Mittal, Ben W. Reichardt, Robert Spalek; "An adversary for algorithms," arXiv:1011.3020v1
URL http://arxiv.org/abs/1011.3020
State-conversion generalizes query complexity to the problem of converting between two input-dependent quantum states by making queries to the input. We characterize the complexity of this problem by introducing a natural information-theoretic norm that extends the Schur product operator norm. The complexity of converting between two systems of states is given by the distance between them, as measured by this norm.

In the special case of function evaluation, the norm is closely related to the general adversary bound, a semi-definite program that lower-bounds the number of input queries needed by a quantum algorithm to evaluate a function. We thus obtain that the general adversary bound characterizes the quantum query complexity of any function whatsoever. This generalizes and simplifies the proof of the same result in the case of Boolean input and output. Also in the case of function evaluation, we show that our norm satisfies a remarkable composition property, implying that the quantum query complexity of the composition of two functions is at most the product of the query complexities of the functions, up to a constant. Finally, our result implies that discrete and continuous-time query models are equivalent in the bounded-error setting, even for the general state-conversion problem.

# 3.19 Quantum One-Way Communication can be Exponentially Stronger Than Classical Communication 

Oded Regev (Tel Aviv University, IL)

License © © $\Theta$ Creative Commons BY-NC-ND 3.0 Unported license
© Oded Regev
Joint work of Regev, Oded; Klartag, Bo'az
Main reference Bo'az Klartag, Oded Regev, "Quantum One-Way Communication is Exponentially Stronger Than Classical Communication," STOC 2011, to appear.
URL http://eccc.hpi-web.de/report/2010/143/
In STOC 1999, Raz presented a (partial) function for which there is a quantum protocol communicating only $O(\log n)$ qubits, but for which any classical (randomized, bounded-error) protocol requires poly $(n)$ bits of communication.

That quantum protocol requires two rounds of communication. Ever since Raz's paper it was open whether the same exponential separation can be achieved with a quantum protocol that uses only one round of communication. In other words, can quantum one-way communication be exponentially stronger than classical two-way communication? Here we settle this question in the affirmative.

Note: This talk is about lower bounds for classical communication complexity; no knowledge of quantum communication complexity is assumed or required.

### 3.20 An Optimal Lower Bound on the Communication Complexity of Gap-Hamming-Distance

Oded Regev (Tel Aviv University, IL)
License © © $\Theta$ Creative Commons BY-NC-ND 3.0 Unported license
© Oded Regev
Main reference Amit Chakrabarti, Oded Regev; "An Optimal Lower Bound on the Communication Complexity of Gap-Hamming-Distance," STOC 2011, to appear.
URL http://arxiv.org/abs/1009.3460
We consider the Gap Hamming Distance problem in communication complexity. Here, Alice receives an $n$-bit string $x$, and Bob receives an $n$-bit string $y$.

They are promised that the Hamming distance between x and y is either at least $n / 2+\sqrt{n}$ or at most $n / 2-\sqrt{n}$, and their goal is to decide which is the case.

The naive protocol requires $n$ bits of communication and it was an open question whether this is optimal. This was shown in several special cases, e.g., when the communication is deterministic [Woodruff'07] or when the number of rounds of communication is limited [Indyk-Woodruff'03, Jayram-Kumar-Sivakumar'07, Brody-Chakrabarti'09, Brody-Chakrabarti-Regev-Vidick-deWolf'09].

Here we settle this question by showing a tight lower bound of $\Omega(n)$ on the randomized communication complexity of the problem. The bound is based on a new geometric statement regarding correlations in Gaussian space, related to a result of C. Borell from 1985, which is proven using properties of projections of sets in Gaussian space.

# 3.21 From Affine to Two-Source Extractors via Approximate Duality 

Eli Ben-Sasson (Technion - Haifa, IL)
License © © © $\odot$ Creative Commons BY-NC-ND 3.0 Unported license © Eli Ben-Sasson
Joint work of Ben-Sasson, Eli; Zewi, Noga
Main reference Eli Ben-Sasson, Noga Zewi ; "From Affine to Two-Source Extractors via Approximate Duality," Proceedings of STOC 2011.
URL http://eccc.hpi-web.de/report/2010/144/
Two-source and affine extractors and dispersers are fundamental objects studied in the context of derandomization. (Two-source dispersers are equivalent to bipartite Ramsey graphs.) We show how to construct two-source extractors and dispersers (i.e., bipartite Ramsey graphs) for arbitrarily small min-entropy rate in a black-box manner from affine extractors with sufficiently good parameters. Our analysis relies on the study of approximate duality, a concept related to the polynomial Freiman-Ruzsa conjecture from additive combinatorics.

### 3.22 Improved Constructions of Three Source Extractors

Xin Li (University of Texas - Austin, US)
 © Xin Li
Main reference Xin Li; "Improved Constructions of Three Source Extractors," CCC 2011
URL http://eccc.hpi-web.de/report/2010/190/
This talk presents recent constructions of extractors for three independent weak random sources on $n$ bits with min-entropy $n^{1 / 2+\alpha}$, for any arbitrary constant $\alpha>0$. This improves the previous best result where at least one source is required to have min-entropy $n^{0.9}$. Other results include extractors for three independent sources with uneven lengths and extractors for two independent affine sources on $n$ bits with entropy $n^{1 / 2+\alpha}$.

### 3.23 Extractors for Circuit Sources

Emanuele Viola (Northeastern Univ. - Boston, US)
License © © © Creative Commons BY-NC-ND 3.0 Unported license
© Emanuele Viola
Main reference Emanuele Viola; "Extractors for circuit sources," ECCC Technical Report 2011-056
URL http://www.eccc.uni-trier.de/report/2011/056/
We obtain the first deterministic extractors for sources generated (or sampled) by small circuits of bounded depth. Our main results are:
(1) We extract $k(k / n d)^{O(1)}$ bits with exponentially small error from $n$-bit sources of min-entropy $k$ that are generated by functions $f:\{0,1\}^{\ell} \rightarrow\{0,1\}^{n}$ where each output bit depends on $\leq d$ input bits. In particular, we extract from $N C^{0}$ sources, corresponding to $d=O(1)$.
(2) We extract $k\left(k / n^{1+\gamma}\right)^{O(1)}$ bits with super-polynomially small error from $n$-bit sources of min-entropy $k$ that are generated by poly $(n)$-size $A C^{0}$ circuits, for any $\gamma>0$.

As our starting point, we revisit the connection by Trevisan and Vadhan (FOCS 2000) between circuit lower bounds and extractors for sources generated by circuits. We note that
such extractors (with very weak parameters) are equivalent to lower bounds for generating distributions (FOCS 2010; with Lovett, CCC 2011).

Building on those bounds, we prove that the sources in (1) and (2) are (close to) a convex combination of high-entropy "bit-block" sources. Introduced here, such sources are a special case of affine ones. As extractors for (1) and (2) one can use the extractor for low-weight affine sources by Rao (CCC 2009).

Along the way, we exhibit an explicit Boolean function $b:\{0,1\}^{n} \rightarrow\{0,1\}$ such that $\operatorname{poly}(n)$-size $A C^{0}$ circuits cannot generate the distribution $(x, b(x))$, solving a problem about the complexity of distributions.

Independently, De and Watson (ECCC TR11-037) obtain a result similar to (1) in the special case $d=o(\lg n)$.

### 3.24 What Binary Codes can be Obtained by Concatenating AG Codes with Hadamard?

Amnon Ta-Shma (Tel Aviv University, IL)
License © (®) $\bigodot$ Creative Commons BY-NC-ND 3.0 Unported license © Amnon Ta-Shma
Joint work of Ta-Shma, Amnon; Ben-Aroya, Avraham
Main reference Avraham Ben-Aroya, Amnon Ta-Shma; "Constructing Small-Bias Sets from Algebraic-Geometric Codes", pp. 191-197, FOCS 2009
URL http://dx.doi.org/10.1109/FOCS.2009.44

The currently best explicit constructions of binary error correcting codes of distance close to half work by concatenating a good outer code with Hadamard. When the outer code is RS the obtained code has length $n=O\left(k^{2} /\right.$ eps $\left.^{2}\right)$, while taking an AG code of degree larger than the genus gives $n=O\left(k /\right.$ eps $\left.^{3}\right)$, where $k$ is the code dimension, $1 / 2-$ eps is the distance and the O notation also hides logarithmic factors.

I show that the result can be improved by taking AG codes with degree *smaller* than the genus. Specifically, we obtain codes of length $n=O\left(k / e p s^{2}\right)^{5 / 4}$ which improves upon previous explicit constructions when eps is roughly (ignoring logarithmic factors) in the range $\left[k^{-1.5}, k^{-0.5}\right]$. We also discuss an argument by Voloch exposing the limitations of the technique.

### 3.25 Derandomizing Polynomial Identity Testing for Multilinear Constant-Read Formulae

Matthew Anderson (University of Wisconsin - Madison, US)
License © (c) $\Theta$ Creative Commons BY-NC-ND 3.0 Unported license © Matthew Anderson
Joint work of Anderson, Matthew; van Melkebeek, Dieter; Volkovich, Ilya
Main reference M. Anderson, D. van Melkebeek, and I. Volkovich; "Derandomizing Polynomial Identity Testing for Multilinear Constant-Read Formulae," Electronic Colloquium on Computational Complexity, Technical Report ECCC-TR 10-188, 2010.
URL http://eccc.hpi-web.de/report/2010/188/
We present a polynomial-time deterministic algorithm for testing whether constant-read multilinear arithmetic formulae are identically zero. In such a formula each variable occurs only a constant number of times and each subformula computes a multilinear polynomial. Our algorithm runs in time $s^{O(1)} \cdot n^{k^{O(k)}}$, where $s$ denotes the size of the formula, $n$ denotes
the number of variables, and $k$ bounds the number of occurrences of each variable. Before our work no subexponential-time deterministic algorithm was known for this class of formulae. We also present a deterministic algorithm that works in a blackbox fashion and runs in time $n^{k^{O(k)}+O(k \log n)}$ in general, and time $n^{k^{O\left(k^{2}\right)}+O(k \delta)}$ for depth $\delta$. Finally, we extend our results and allow the inputs to be replaced with sparse polynomials. Our results encompass recent deterministic identity tests for sums of a constant number of read-once formulae, and for multilinear depth-four formulae.

### 3.26 Randomness Efficient Testing of Sparse Blackbox Identities of Unbounded Degree over the Reals

Markus Bläser (Universität des Saarlandes, DE)
License © © $\odot$ Creative Commons BY-NC-ND 3.0 Unported license © Markus Bläser
Joint work of Bläser, Markus; Engels, Christian
Main reference Markus Blaeser and Christian Engels; "Randomness Efficient Testing of Sparse Black Box Identities of Unbounded Degree over the Reals," pp. 555-566, LIPIcs Vol. 9, STACS 2011. URL http://dx.doi.org/10.4230/LIPIcs.STACS.2011.555

We construct a hitting set generator for sparse multivariate polynomials over the reals. The seed length of our generator is $O\left(\log ^{2}(m n / \epsilon)\right)$ where $m$ is the number of monomials, $n$ is number of variables, and $1-\epsilon$ is the hitting probability. The generator can be evaluated in time polynomial in $\log m, n$, and $\log 1 / \epsilon$. This is the first hitting set generator whose seed length is independent of the degree of the polynomial.

The seed length of the best generator so far by Klivans and Spielman depends logarithmically on the degree.

From this, we get a randomized algorithm for testing sparse blackbox polynomial identities over the reals using $O\left(\log ^{2}(m n / \epsilon)\right.$ ) random bits with running time polynomial in $\log m, n$, and $\log \frac{1}{\epsilon}$.

We also design a deterministic test with running time $\tilde{O}\left(m^{3} n^{3}\right)$.
Here, the $\tilde{O}$-notation suppresses polylogarithmic factors.
The previously best determininstic test by Lipton and Vishnoi has a running time that depends polynomially on $\log \delta$, where $\delta$ is the degree of the blackbox polynomial.

### 3.27 Learning Read-Constant Polynomials of Constant Degree Modulo Composites

Kristoffer Arnsfelt Hansen (Aarhus University, DK)
License © © $\odot$ Creative Commons BY-NC-ND 3.0 Unported license
© Kristoffer Arnsfelt Hansen
Joint work of Chattopadhyay, Arkadev; Gavaldà, Ricard; Hansen, Kristoffer Arnsfelt; Thérien, Denis
Boolean functions that have constant degree polynomial representation over a fixed finite ring form a natural and strict subclass of the complexity class $\mathrm{ACC}^{0}$. They are also precisely the functions computable efficiently by programs over fixed and finite nilpotent groups. This class is not known to be learnable in any reasonable learning model.

In this paper, we provide a deterministic polynomial time algorithm for learning Boolean functions represented by polynomials of constant degree over arbitrary finite rings from
membership queries, with the additional constraint that each variable in the target polynomial appears in a constant number of monomials. Our algorithm extends to superconstant but low degree polynomials and still runs in quasipolynomial time.

### 3.28 Locality of AC $^{0}$-Computable Graph Queries

Nicole Schweikardt (Goethe-Universität Frankfurt am Main, DE)
License © $\odot \odot$ Creative Commons BY-NC-ND 3.0 Unported license (C) Nicole Schweikardt

Joint work of Anderson, Matthew; van Melkebeek, Dieter; Schweikardt, Nicole; Segoufin, Luc
Main reference Matthew Anderson, Dieter van Melkebeek, Nicole Schweikardt, Luc Segoufin, "Locality of queries definable in invariant first-order logic with arbitrary built-in predicates," pp. 368-379, LNCS Vol. 6756, ICALP 2011.
URL http://dx.doi.org/10.1007/978-3-642-22012-8__29
Our main theorem states that $\mathrm{AC}^{0}$-computable graph queries are $f$-local, for every function $f$ growing faster than a polylogarithmic function. Here, $f$-local means that for any graph of size $n$ and any two tuples of nodes $a$ and $b$ whose $f(n)$-neighborhoods are isomorphic, $b$ belongs to the query result if and only if $a$ does.

Our proof makes use of the known tight lower bounds for parity on constant-depth circuits. The size $f(n)$ of the neighborhoods is optimal, since for every polylogarithmic function $g$ we can find an $\mathrm{AC}^{0}$-computable graph query that is not $g$-local.

### 3.29 A Survey of Exponential Algorithms for Constraint Satisfaction Problems

Robin Moser (ETH Zürich, CH)
License © © © © Creative Commons BY-NC-ND 3.0 Unported license
In this talk, I surveyed the two most important currently competitive algorithms for k-SAT: Schöning's Algorithm and the PPSZ algorithm due to Paturi, Pudlák, Saks and Zane. There have been very recent news about both algorithms. In the case of Schöning, we were recently able with Scheder to provide a deterministic variant of essentially the same running time as the randomized one. In the case of PPSZ, a recent breakthrough result due to Timon Hertli shows that the success probability of the algorithm is no worse in the general case than in the case of a uniquely satisfying assignment, demonstrating that PPSZ is dramatically faster than was previously known.

### 3.30 A Full Derandomization of Schöning's $k$-SAT Algorithm

Robin Moser (ETH Zürich, CH)
License © © $\Theta$ Creative Commons BY-NC-ND 3.0 Unported license (C) Robin Moser

Joint work of Moser, Robin; Scheder, Dominik
Main reference Robin A. Moser, Dominik Scheder; "A Full Derandomization of Schoening's k-SAT Algorithm," submitted, available at arXiv:1008.4067
URL http://arxiv.org/abs/1008.4067
Schöning [1] presents a simple randomized algorithm for $k$-SAT with running time $a_{k}^{n} \cdot \operatorname{poly}(n)$ for $a_{k}=2(k-1) / k$. We give a deterministic version of this algorithm running in time $a_{k}^{n+o(n)}$.

## References

1 U. Schöning. A probabilistic algorithm for $k$-SAT and constraint satisfaction problems.
In FOCS '99: Proceedings of the 40th Annual Symposium on Foundations of Computer Science, page 410, Washington, DC, USA, 1999. IEEE CS.

### 3.31 Algorithmic Meta Theorems Inside Logspace and Their Applications

Michael Elberfeld (Universität Lübeck, DE)

 © Michael Elberfeld
Joint work of Jakoby, Andreas; Stockhusen, Christoph; Tantau, Till
Main reference M. Elberfeld, A. Jakoby, and T. Tantau; "Logspace versions of the Theorems of Bodlaender and Courcelle," Proceedings of FOCS 2010, pp. 143-152, 2010.
URL http://eccc.hpi-web.de/report/2010/062/
Bodlaender's Theorem states that for every $k$ there is a linear-time algorithm that decides whether an input graph has tree width $k$ and, if so, computes a width- $k$ tree decomposition. Courcelle's Theorem sets up on Bodlaender's Theorem and states that for every monadic second-order (MSO) formula $\phi$ and for every $k$ there is a linear-time algorithm that decides whether a given logical structure $\mathcal{A}$ of tree width at most $k$ satisfies $\phi$.

Recently we proved that the Theorems of Bodlaender and Courcelle also hold when "linear time" is replaced by "logarithmic space", yielding an algorithmic meta theorem that can be used to show deterministic logarithmic-space solvability for MSO-definable problems on logical structures of bounded tree width.

In the talk I outline the above results, and discussed current work on (1) their applications and (2) refined algorithmic meta theorems for circuit classes inside L .

### 3.32 Triangular Rank and Sampling With Multiplicative Errors

```
Ilan Newman (Haifa University,IL)
    License © © ¢ Creative Commons BY-NC-ND 3.0 Unported license
    C Ilan Newman
Joint work of Newman, Ilan; Rabinovich, Yuri
```

It is well known that if a family $F$ of subsets of a universe $U$ has VC-dimension $d$, then for every probability distribution $D$ over $U$ there exists a sample $S \subset U$ of size $d * \operatorname{poly}(1 / \epsilon)$
which faithfully represents $P$ on $F$ up to an $\epsilon$ additive error. Namely, for which $|(S \cap T) /|S|-$ $\operatorname{Pr}_{D}(T) \mid \leq \epsilon$ for every set $T$ in $F$.

We ask whether there exists a property of $F$ analogous to VC-dimension which would ensure the existence of a small sample faithfully representing $D$ on $F$ up to ( $1+\epsilon$ ) multiplicative error. The answer turns out to be positive, and the key parameter is the triangular rank of $F$. In particular, we show that if the triangular rank of $F$ is $t$, then there exists a sample of size $\min \left\{r \log |F| * \operatorname{poly}(1 / \epsilon), r^{2} \log r * \operatorname{poly}(1 / \epsilon)\right\}$ which faithfully represents $D$ on $F$ up to $(1+\epsilon)$ multiplicative factor.

One application of this is to show some upper bounds on the dimension reduction possibility for $\ell_{1}$ metrics.

### 3.33 Tight Lower Bounds for Greedy Routing in Uniform Small World Rings

Philipp Woelfel (University of Calgary, CA)
License © © $\Theta$ Creative Commons BY-NC-ND 3.0 Unported license © Philipp Woelfel
Joint work of Dietzfelbinger, Martin; Woelfel, Philipp
Main reference Martin Dietzfelbinger and Philipp Woelfel; "Tight Lower Bounds for Greedy Routing in Uniform Small World Rings," Proc. of 41st STOC, pp. 591-600, 2009.
URL http://dx.doi.org/10.1145/1536414.1536494
Consider the following game played on a board with $2 n+1$ spaces labeled $-n, \ldots,-1,0,1, \ldots, n$ (from left to right). Fix some probability distribution $\mu$ over $\{1, \ldots, n\}^{k}$, where $k=O(\log n)$. In the beginning, a token is placed on the board at a position chosen uniformly at random. Then, in each step the token is moved closer to its target, space 0 , according to the following random experiment: Suppose after the $i$-th step the token is located at position $x$. In the $(i+1)$-th step, $k$ distances $d_{1}, \ldots, d_{k}$ are chosen at random according to the probability distribution $\mu$. Then, the distance $d$ in $\left\{0, d_{1}, \ldots, d_{k}\right\}$ is applied that moves the token closest to its target. I.e., the token is moved position $x-d$, where $d \in\left\{0, d_{1}, \ldots, d_{k}\right\}$ minimizes $|x-d|$.

We are interested in the number of steps, $T$, it takes to move the token from its random start position to position 0 , for the best probability distribution $\mu$. The problem has been first studied in the context of Small World Graph routing [1, 2] and has applications in P2P Networks [3, 4] and Black Box Optimization [5].

Probability distributions $\mu$ for which $E[T]=O\left((\log n)^{2} / k\right)$ are well known. In this talk I sketch a proof that this upper bound is asymptotically tight. Previous lower bounds were only known for restricted versions of the problem.

## References

1 J.M. Kleinberg. Navigation in a small world. Nature, p. 845, 2000.
2 J.M. Kleinberg. The small-world phenomenon: An algorithmic perspective. 32nd STOC, 2000.

3 P. Ganesan and G. S. Manku. Optimal routing in chord. 15th SODA, 2004.
4 I. Stoica, R. Morris, D. Liben-Nowell, D. R. Karger, M. F. Kaashoek, F. Dabek, and H. Balakrishnan. Chord: A scalable peer-to-peer lookup protocol for internet applications. IEEE/ACM Transactions on Networking, 11:17-32, 2003.
5 M. Dietzfelbinger, J. E. Rowe, I. Wegener, and P. Woelfel. Tight bounds for blind search on the integers. 25th STACS, 2008.

### 3.34 On the Correlation of Parity with Small Depth Circuits

Johan Håstad (KTH Stockholm, SE)
License $\Subset \circledast \Theta$ Creative Commons BY-NC-ND 3.0 Unported license
© Johan Håstad
We prove that the correlation of the depth $d$ circuit of size $S$ with parity is bounded by $2^{-\Omega\left(n /(\log S)^{d-1}\right)}$. The result follows from applying the classical switching lemma together with some deterministic post-processing.

## Participants

- Eric Allender

Rutgers Univ. - Piscataway, US

- Matthew Anderson

University of Wisconsin Madison, US

- Paul Beame

University of Washington -
Seattle, US

- Eli Ben-Sasson

Technion - Haifa, IL

- Markus Bläser

Universität des Saarlandes, DE

- Andrej Bogdanov

Chinese Univ. of Hong Kong, HK

- Beate Bollig

Technische Universität
Dortmund, DE

- Holger Dell

HU Berlin, DE

- Martin Dietzfelbinger

TU Ilmenau, DE

- Andrew Drucker

MIT - Cambridge, US

- Michael Elberfeld

Universität Lübeck, DE

- Eldar Fischer

Technion - Haifa, IL

- Lance Fortnow

Northwestern University -
Evanston, US

- Anna Gál

University of Texas - Austin, US

- Martin Grohe

HU Berlin, DE

- Kristoffer Arnsfelt Hansen

Aarhus University, DK

- Prahladh Harsha

TIFR Mumbai, IN

- Johan Hastad

KTH Stockholm, SE

- Stasys Jukna

Univ. Frankfurt am Main, DE

- Valentine Kabanets

Simon Fraser University -
Burnaby, CA

- Michal Koucký

Acad. of Sciences - Prague, CZ

- Matthias Krause

Universität Mannheim, DE

- Troy Lee

National University of Singapore, SG

- Xin Li

University of Texas - Austin, US

- Meena Mahajan

The Institute of Mathematical
Sciences - Chennai, IN

- Pierre McKenzie

Université de Montréal, CA

- Or Meir

Weizmann Inst. - Rehovot, IL

- Peter Bro Miltersen

Aarhus University, DK

- Robin Moser

ETH Zürich, CH

- Ilan Newman

University of Haifa, IL

- Jakob Nordström

KTH Stockholm, SE

- Pavel Pudlák

Acad. of Sciences - Prague, CZ

- Oded Regev

Tel Aviv University, IL

- Rüdiger Reischuk

Universität Lübeck, DE

- Rahul Santhanam

University of Edinburgh, GB

- Georg Schnitger

Univ. Frankfurt am Main, DE

- Uwe Schöning

Universität Ulm, DE

- Nicole Schweikardt

Univ. Frankfurt am Main, DE

- Srikanth Srinivasan

Institute for Advanced Study -
Princeton, US

- Amnon Ta-Shma

Tel Aviv University, IL

- Till Tantau

Universität Lübeck, DE

- Dieter van Melkebeek

University of Wisconsin Madison, US

- Emanuele Viola

Northeastern Univ. - Boston, US

- Heribert Vollmer

Leibniz Univ. Hannover, DE

- Fabian Wagner

Universität Ulm, DE

- Thomas W. Watson

University of California -
Berkeley, US

- Philipp Wölfel

University of Calgary, CA


