Dagstuhl Seminar

on

Complexity of Boolean Functions

17.03. – 22.03.2002

organized by

D. A. M. Barrington (Amherst),

J. Håstad (Stockholm),

M. Krause (Mannheim),

R. Reischuk (Lübeck)

Contents

Scientific Report on the Dagstuhl Seminar "Complexity of Boolean Functions"

organized by
David Mix Barrington, Amherst, USA
Johan Håstad, Stockholm, Sweden
Matthias Krause, Mannheim
Rüdiger Reischuk, Lübeck

Summary of the Proceedings Many talks of the seminar dealt with new techniques for analyzing the computational power of basic models to compute Boolean functions. In particular, branching programs were dicussed most extensively. At the first day we had a keynote talk in the morning and an evening discussion on time-space tradeoff results on the level of branching programs (Beame). Several talks on refined lower bound methods for nondeterministic and randomized free BDDs (Okol'nishnikova, Žák, Sauerhoff, Wölfel) and the approximability of Boolean functions by OBDDs (Wegener) followed. Other important topics were new results concerning distributed computing of Boolean functions (Jakoby) and communication complexity (Forster, Thérien, and several BDD talks). One highlight here was the presentation of and the discussions on Forsters technique to prove almost optimal lower bounds on the unbounded error probabilistic communication complexity of particular Boolean functions (Forster, Simon). Further talks considered the comparison of classical models and related quantum models for computing Boolean functions (Sieling, Klauck, van Melkebeek, Buhrman, Kerntopf). In addition, besides presenting his own results, Klauck discussed Razborov's very recent solution to a long open problem on deterministic versus probabilistic quantum communication complexity.
Other talks of the seminar dealt with methods for better determining the complexity of hardware relevant Boolean functions (like integer multiplication) with respect to models used as data structures in hardware verification (Bollig, Wölfel), the computational power of decision lists (Krause), and new results on the power of span programs (Gál). Efficient algorithms was another main topic, especially concerning restricted types of circuits and branching programs as data structures for manipulating, minimizing and learning Boolean functions. Here we had several interesting talks about latest progress in SAT algorithms (Hofmeister, Goerdt, Alekhnovich), new developments in proof complexity (Ben-Sasson, Alekhnovich), new positive and negative results on the learnability of DNFs and AND-decision lists (Maruoka, Krause), and fixed-parameter tractability (Ragde).
Further talks were concerned with relations between Boolean complexity topics and uniform complexity theory, especially with the complexity of derandomizing probabilistic algorithms (Allender, Kabanets), and the closely connected topics of characterizing logspace-classes (Thierauf) and the uniform complexity of reachability problems

(Koucký, Barrington). Several talks stressed, at least implicitely, cryptographic implications of structural and complexity-theoretic results on Boolean functions, especially from the viewpoint of design and security criterions for cryptographic primitives like pseudorandom functions and permutations and S-Box functions (Golic, Lucks).
The contributions of this seminar showed that several new trends in Boolean complexity have gained increased consideration, in particular proof complexity and computing with quantum bits. We have discussed in detail how far our current proof methods have brought us to precisely determine the computational complexity of Boolean functions for general computational models.
The seminar had a number of younger European researchers who for the first time had a chance to take part in such a detailed discussion on current research topics in Boolean complexity. About half of the presentations were given by participants from outside the European Union. The research on Boolean functions is conducted in a broad international exchange. We felt that this meeting at the IFBI was quite productive for all participants concerning their own future research.

Public Outreach To determine the complexity of Boolean functions with respect to various hardware models – like Boolean circuits, branching programs or constant layer feedforward neural networks – is one of the central and classical topics in the theory of computation. This includes the search for efficient implementations of hardware relevant functions, like address functions and arithmetic and logical operations. On the other hand, we strive for establishing lower bounds on the computational complexity showing that a certain function cannot be computed if a certain amount of resources is not available. In this respect, a lot of interesting and surprising results have been obtained, which in many cases are based on the development of elegant, highly nontrivial mathematical proof techniques. However, in spite of enormous efforts, there still seems to be quite a long way to go before getting tight characterizations of the complexity of important functions for general types of circuits and branching programs. Methods originally designed to analyze the complexity of Boolean functions turned out to have interesting implications in other areas like hardware verification, computational intelligence and cryptography.
The aim of this seminar was to collect the leading experts of Boolean complexity theory and to present the latest results in this area. One main focus was to discuss successfull applications of Boolean complexity methods in other more applied fields like hardware design and verification, algorithmic learning, neural computing, proof complexity theory, quantum computing, design of cryptographic primitives, and cryptoanalysis of block and stream ciphers.

Seminar Program

Monday, March 18th, 2002

9.00 – 9.45	**Paul Beame, Washington** Time-Space Tradeoffs and Multiparty Communication Complexity
9.45 – 10.30	**Beate Bollig, Dortmund** Exponential Lower Bounds for Integer Multiplication Using Universal Hashing
10.45 – 11.30	**Philipp Wölfel, Dortmund** On k-wise l-mixed Boolean Functions
11.30 – 12.15	**Elizabeta Okol'nishnikova, Novosibirsk** On one Lower Bound for Branching Programs
14.45 – 15.30	**Stanislav Žák** Information Flow in Read-once Branching Programs
15.45 – 16.30	**Jürgen Forster** Bounds on the Dimension and Margin of Arrangements of Half Spaces
16.30 – 17.15	**Hans Ulrich Simon, Bochum** Some Observations Concerning the Ridigity of Matrices
17.15 – 18.00	**Denis Thérien, Montréal** Communication Complexity of Regular Languages

Tuesday, March 19th, 2002

9.00	**Eric Allender, Piscataway** Derandomization Through the Lens of Kolmogorov Complexity – Random Strings are Hard
9.45 – 10.30	**Michal Kouck** Universal Exploration Sequences
10.45 – 11.30	**Valentine Kabanets, San Diego** The Witness Complexity of Exponential Time
11.30 – 12.15	**David A. Mix Barrington, Amherst** Grid Graph Reachability Problems
14.45 – 15.30	**Stefan Lucks, Mannheim** On the Role of Complexity Theory in Cryptography
15.45 – 16.30	**Jovan Golic, Rome** Low Order Structures and Approximations of Boolean Functions
16.30 – 17.15	**Anna Gál** On the Size of Self-Avoiding Families – Lower Bounds for Monotone Span Programs

Wednesday, March 20th, 2002

9.00 – 9.45	**Akira Maruoka, Tohoku** Derandomization of a Learning Algorithm for DNFs
9.45 – 10.30	**Eli Ben-Sasson, Cambridge** Hard Examples for Bounded Depth Frege
10.45 – 11.30	**Thomas Hofmeister, Dortmund** 3-SAT Algaorithms with Running Time 1.3302^n
11.30 – 12.15	**Andreas Gördt, Chemnitz** Special Unsatisfiability Algorithms on Random Instances
16:00 – 16:45	**Thomas Thierauf, Ulm** On the Minimal Polynomial of a Matrix
16:45 – 17:30	**Harry Buhrman, Amsterdam** Quantum Fingerprinting
17:30 – 18:15	**Detlef Sieling, Dortmund** Quantum Branching Programs: Simulations and Upper and Lower Bounds

Thursday, March 21st, 2002

9.00 – 9.45	**Dieter van Melkebeek, Madison** On the Quantum Black-Box Complexity of Majority
9.45 – 10.30	**Hartmut Klauck, Amsterdam** Lower Bounds on Quantum Communication Complexity
10.45 – 11.30	**Martin Sauerhoff, Dortmund** Separating Randomness from Nondeterminism for Read-once Branching Programs
11.30 – 12.15	**Prabhakar Ragde, Waterloo** Fast Fixed-Parameter-Tractable Algorithms for Nontrivial Generalizations of Vertex Cover

Friday, March 22nd, 2002

9.00 – 9.45	**Pawel Kerntopf, Warsaw** Reversible Logic Circuits
9.45 – 10.30	**Andreas Jakoby** On the Number of Random Bits to Compute Parity on a k-Connected Network
10.45 – 11.30	**Matthias Krause, Mannheim** On Boolean Decisions Lists
11.30 – 12.15	**Ingo Wegener, Dortmund** On the Non-Approximability of Boolean Functions by OBDDs

Time-Space Tradeoffs and Multiparty Communication Complexity

Paul Beame (University of Washington, USA)

(Joint work with Erik Vee.)

Recently, the first non-trivial time-space tradeoff lower bounds have been shown for decision problems using non-uniform algorithms. These results have used ideas such as embedded rectangles that are derived from two-party communication complexity. We extend these techniques using ideas from multiparty communication complexity.
Using these arguments, for inputs from large domains we prove larger time-space tradeoffs than previously known for general branching programs, yielding time lower bounds of the form $T = \Omega(n \log^2 n)$ when space $S = n^{1-\epsilon} \log |D|$ where D is the domain size for the computation of a certain multilinear form. This bound is as large as the best that is known for oblivious branching programs.
We also prove a separation between the power of oblivious and general branching programs for computing 1-GAP, the out-degree 1 graph accessibility function; we show that oblivious branching programs require $T = \Omega\big(n \log^2\big(\frac{n}{s}\big)\big)$ whereas $T = n$, $S = 2 \log_2 n$ suffices for general branching programs.

Exponential Lower Bounds for Integer Multiplication Using Universal Hashing

Beate Bollig (Universität Dortmund, Germany)

(Joint work with Philipp Wölfel.)

Branching Programs (BPs) are a well-established computation and representation model for Boolean functions. Especially read-once branching programs (BP1s) have been studied intensively. Exponential lower bounds on the deterministic and nondeterministic BP1 complexity of explicitly defined functions have been known for a long time. Nevertheless the proof of exponential lower bounds on the BP1 size of selected functions is sometimes difficult. Furthermore, the problem of proving superpolynomial lower bounds for parity BP1s is still open.
Motivated by applications the BP1 complexity of fundamental functions is of interest. Ponzio (1998) has proved the first exponential lower bound on the size of deterministic BP1s representing integer multiplication. Combining results and methods for universal hashing with lower bound techniques for BP1s the first exponential lower bound for integer multiplication is presented. Using a new proof technique this lower bound can be generalized for restricted nondeterministic and parity BP1s. In addition more insight into the structure of integer multiplication is yielded.

On k-wise l-mixed Boolean Functions

Philipp Wölfel (Universität Dortmund, Germany)

A new lower bound technique for two types of restricted branching programs (BPs) is presented, namely for read-once BPs (BP1s) with restricted amount of nondeterminism and for $(1, +k)$-BPs. For this technique, the notion of *(strictly) k-wise ℓ-mixed* Boolean functions is introduced, which generalizes the concept of ℓ-mixedness defined by Jukna in 1988. It is proven that if a Boolean function f is (strictly) k-wise l-mixed, then any nondeterministic BP1 with at most $k-1$ nondeterministic nodes and any $(1, +k)$-BP representing f has a size of at least $2^{\Omega(\ell)}$. While leading to new exponential lower bounds of well-studied functions (e.g. linear codes), the lower bound technique also shows that the polynomial size hierarchy for BP1s with respect to the available amount of nondeterminism is strict. More precisely, a class of functions is introduced, which can be represented by polynomial size BP1s with k nondeterministic nodes, but requires superpolynomial size if only $k-1$ nondeterministic nodes are available (for $k = o(n^{1/3}/\log^{2/3} n)$). This is the first hierarchy result of this kind where the BP1 does not obey any further restrictions. Finally, it is shown that the polynomial size hierarchy for $(1, +k)$-BPs with respect to k is strict for $k = o(\sqrt{n/\log n})$. This extends the hierarchy result of Savický and Žák (2000), where k was bounded above by $n^{1/6}/(2\log^{1/3} n)$.

On One Lower Bound for Branching Programs

Elizabeta Okol'nishnikova (Sobolev Institute of Mathematics, Novosibirsk, Russia)

The method of obtaining nonlinear lower bounds on the complexity of Boolean functions for nondeterministic branching programs is proposed. A lower bound $\Omega(n \log n/\log\log n)$ on the complexity of characteristic functions of Reed-Muller codes for nondeterministic branching programs is obtained.

Information Flow in Read-once Branching Programs

Stanislav Žák (Academy of Sciences, Prague, Czech Republic)

(Joint work with Stasys Jukna.)

We describe a lower bounds argument for read-once branching programs which is not just a standard cut-and-paste. The argument is based on a more subtle analysis of the information flow during the individual computations. Although the same lower bound can be also obtained by standard arguments, our proof may be promising because (unlike the cut-and-paste argument) it can potentially be extended to more general models.

Bounds on the Dimension and Margin of Arrangements of Half Spaces

Jürgen Forster (Ruhr-Universität Bochum, Germany)

The main mathematical result of the talk may be stated as follows: Given a matrix $M \in \{-1,1\}^{n\times n}$ and any matrix $\tilde{M} \in \mathsf{R}^{n\times n}$ such that $\operatorname{sign}(\tilde{M}_{i,j}) = M_{i,j}$ for all i,j, then $\operatorname{rank}(\tilde{M}) \geq n/\|M\|$. Here $\|M\|$ denotes the spectral norm of the matrix M.
This implies a general lower bound on the complexity of unbounded error probabilistic communication protocols. As a simple consequence we obtain the first linear lower bound on the complexity of unbounded error probabilistic communication protocols for the functions defined by Hadamard matrices. This solves a long standing open problem stated by Paturi and Simon [1].
We also give an upper bound on the margin of any embedding of a concept class in half spaces. Such bounds are of interest to problems in learning theory. Concept classes can canonically be represented by matrices with entries 1 and -1. We used the singular value decomposition of this matrix to determine the optimal margins of embeddings of the concept classes of singletons and of half intervals in homogeneous Euclidean half spaces. For these concept classes the singular value decomposition can be used to construct optimal embeddings and also to prove the corresponding best possible upper bounds on the margin. We show that the optimal margin for embedding n singletons is $\frac{n}{3n-4}$ and that the optimal margin for half intervals over $\{1,\ldots,n\}$ is $\frac{\pi}{2\ln n} + \Theta(\frac{1}{(\ln n)^2})$.

[1] Paturi, R., and Simon, J. (1986). Probabilistic communication complexity. *Journal of Computer and System Sciences*, *33*, 106–123.

Some Observations Concerning the Rigidity of Matrices

Hans Ulrich Simon (Ruhr-Universität Bochum, Germany)

We are interested in lower bounds on the rank of matrices A' that are modifications of a given matrix A. We discuss mainly two types of transformations:

I. Replace s entries of A by new entries.

II. Apply a sign-preserving transformation, i.e., replace each entry by a new-one without changing the sign.

The question is how small the rank of the transformed matrix can possibly be. In the talk, we sketch some new observations that build on previous work of various other people. Some details follow.

Jürgen Forster has shown recently the remarkable result that, if A' is a sign-preserving transformation of an $m \times n$ matrix A satsfying $|a_{i,j}| \geq 1$, then the rank of A' is at least $\sqrt{mn}/\|A\|$, where $\|A\|$ denotes the spectral norm of A. In particular for the Hadamard matrix $H_n \in \{-1,+1\}^{2^n \times 2^n}$, he gets $\text{rank}(H'_n) \geq 2^{n/2}$. It is well known that $\|A\|$ coincides with largest singular value of A. We derive an improved bound that uses the full spectrum of all $r = \text{rank}(A)$ many non-trivial singular values, say $\sigma_1 \geq \cdots \geq \sigma_r$, of A: if A' is a sign-preserving transformation of an $m \times n$ matrix A, then the rank d of A' satisfies $d(\sigma_1^2 + \cdots + \sigma_d^2) \geq mn$. The new bound collapses to the old-one if $\sigma_1 = \cdots = \sigma_d$, and is a strict improvement otherwise.

According to a result of Kashin and Razborov, there exists a constant $c > 0$ such that for all sufficiently large N and for all $s \geq 2cN$ the following holds: if s entries of a (generalized) $N \times N$ Hadamard-matrix H are changed, then the rank of the resulting matrix H' is at least cN^2/s. We consider the case, where transformations of both types, I and II, are allowed: you may first change s entries and then apply a sign-preserving transformation on top of that. We show that, for all m, n and all $m \times n$ matrices $A \in \{-1,+1\}^{m \times n}$, the following holds: if s entries of A are changed and a sign-preserving transformation is applied afterwards, then the rank of the resulting matrix A'' is at least $\frac{\sqrt{mn}}{\|A\|+2\sqrt{s}}$. For $s = 0$, this collapses to the aforementioned bound of Forster. If we substitute the $N \times N$ Hadamard matrix H for A, we get $\text{rank}(H'') \geq \frac{N}{\sqrt{N}+2\sqrt{s}}$. This is at least $\frac{1}{3}N/\sqrt{s}$ if $s \geq \sqrt{N}$.

Forster, Krause, Lokam, Mubarakzjanov, Schmitt, and Simon have shown recently the following result. If the inner-product modulo-2 function $\oplus_{i=1}^n x_i y_i$ is computed by a threshold circuit of depth 2, where the weights of the hidden units are polynomially bounded and the weights of the output unit are unbounded, then the number of hidden units must be exponential in n. We generalize this result, by showing that the lower bound on the number of hidden units remains exponential in n, when the circuit must only compute an "approximation" of the inner-product modulo-2 function. "Approximation" means that a fraction $2^{-\varepsilon n}$ of the 2^{2n} function values may be computed

incorrectly. The proof is an easy application of our result concerning transformations of types I,II (mentioned above).

Communication Complexity of Regular Languages

Denis Thérien (McGill University, Montréal, Canada)

We look at the problem of determining the communication complexity of regular languages, both in the 2-party and in the multi-party setting. In all cases, this complexity depends on the algebraic structure of the minimal monoid recognizing the language. In the 2-player case, it is found that the communication complexity of a regular language is either constant, logarithmic or linear, and the question is completely resolved. We also determine which languages can be recognized in constant complexity with a constant number of players.

Derandomization Through the Lens of Kolmogorov Complexity – Random Strings are Hard

Eric Allender (Rutgers University, Piscataway, USA)

(Joint work with Michal Koucký and Detlef Ronneburger.)

This talk has the following goals:

- To survey some of the recent developments in the field of derandomization.
- To introduce a new notion of time-bounded Kolmogorov complexity (KT), and show that it provides a useful tool for understanding advances in derandomization, and for putting various results in context.
- To present new classes of complete sets for EXP and PSPACE, defined in terms of time- and space-bounded Kolmogorov complexity. These sets are complete under non-uniform (P/poly) truth-table reductions, but are not complete under uniform poly-time truth-table reductions, and thus seem to be quite different than other ”natural” complete problems for these complexity classes.
- To pose some promising directions for future research.

Universal Exploration Sequences

Michal Koucký (Rutgers University, Piscataway, USA)

Deciding whether two vertices s and t are connected in a graph belongs to the class of fundamental algorithmic problems. The question, we are interested in, is how much space do we need to decide this problem. It is known that s-t-connectivity can be decided in non-deterministic logarithmic space and hence, by Savitch's Theorem in deterministic space $O(\log^2 n)$. Surprisingly, s-t-connectivity in a graph that is undirected can be solved in randomized log-space and as was subsequently shown in deterministic space $O(\log^{4/3} n)$. It is widely believed that s-t-connectivity in undirected graph can in fact be decided in deterministic logarithmic space.
A tool to study undirected s-t-connectivity is the notion of universal traversal sequences proposed by Cook [AKL+'79]. Closely related to traversal sequences are exploration sequences. In the talk we will give the definition of universal exploration sequences, show their basic properties, and give some explicit constructions. Further, we will show an explicit relation between universal exploration sequences and universal traversal sequences (joint work with Howard Karloff and Omer Reingold,) and pose some open problems.

The Witness Complexity of Exponential Time

Valentine Kabanets (University of California, San Diego, USA)

(Joint work with Russell Impagliazzo.)

We define the witness complexity of a polytime relation $R : \{0,1\}^n \times \{0,1\}^{2^n}$ to be bounded by a function $s : N \to N$ if, for all sufficiently large strings x we have

$$\exists y R(x,y) \text{ implies } \exists y' R(x,y') \text{ and } size(y') < s(|x|),$$

where size(y) is the Boolean circuit complexity of the string y. We show that circuit upper bounds on the complexity classes ZPE, BPE, and NE$\cap$ coNE imply upper bounds on the witness complexity of the polytime relations corresponding to these complexity classes. We also show that circuit upper bounds for BPE and ZPE imply derandomization of these classes. Finally, we prove that derandomization of MAE (MAE=NE) implies that MA is in NSUBEXP i.o. Our proofs rely on the techniques from derandomization (hardness-randomness tradeoffs).

Grid Graph Reachability Problems

David A. Mix Barrington (University of Massachusetts, Amherst, USA)

Imagine a Manhatten-like street grid where some streets are two-way, some one-way, and some closed entirely. Given such a directed graph and two vertices s and t, is there a path from s to t? We consider this grid graph reachability problem and several of its variants.
A grid graph might be undirected, limited to out-degree 1, limited to both in-degree and out-degree one, and/or be levelled. We present a hierarchy of eight grid graph reducibility problems, all of them in NL and most (all but the general and general-levelled versions) in L. We show that the easiest problem (levelled, in-degree and out-degree one) is TC^0 hard and that all the others are NC^1-hard. But these are the best lower bounds known – we invite further work on improving either them or the L and NL upper bounds.

On the Role of Complexity Theory in Cryptography

Stefan Lucks (Universität Mannheim, Germany)

This talk describes the complexity-theoretical approach in cryptography. An example deals with Rabin's trapdoor one-way function, which is provably secure if factoring large integers is hard. The talk concentrates on pseudorandom functions and permutations, and on the construction of secure pseudorandom functions from secure pseudorandom permutations. If s and t are two independent random permutations over $\{0,1\}^n$, the functions f and F: $\{0,1\}^n \to \{0,1\}^n$ are defined by $f(x) = s(x) + t(x)$ and $F(x) = s(t(x) + x)$ (here, "+" denotes a group operation in $\{0,1\}^n$). Both f and F are significantly more secure as pseudorandom functions than when a random permutation, such as s or t, is used directly. The talk also introduces the problem of constructing pseudorandom functions with an improved efficiency when used in counter mode.

Low Order Structures and Approximations of Boolean Functions

Jovan Golic (Rome CryptoDesign Center, Gemplus, Italy)

Zero-order and first-order linear structures of Boolean functions are introduced and a number of interesting properties, characterizations, and enumerations are presented. An overview of different algorithms for finding low-order approximations to Boolean functions is given and some open problems are highlighted. Some applications in cryptology are also discussed. A possible speed-up of finding linear approximations by using quantum computing algorithms is proposed. A problem of finding linear structured approximations to Boolean functions is also pointed out.

On the Size of Self-Avoiding Families – Lower Bounds for Monotone Span Programs

Anna Gál (University of Texas at Austin, USA)

This talk is about the limitations of the current lower bound methods for monotone span programs. The largest known lower bounds on the monotone span program complexity of explicit Boolean functions are of the form $n^{\Omega(logn)}$. A method for proving lower bounds on the size of monotone span programs, introduced by Beimel, Gál, Paterson in 1995, is based on identifying a subset of minterms of the function, that forms a self-avoiding family. All superpolynomial lower bounds obtained so far, can be derived based on this criterion.

It has been an open question, whether exponential size self-avoiding families exist. In a recent paper, Pavel Pudlak presented a generalization of the above method, and asked if it can lead to larger than $n^{\Omega(logn)}$ lower bounds. We show that the answer to this question is no. This implies that the size of self-avoiding families of subsets of an n element universe is at most $n^{O(\log n)}$.

On derandomization of an algorithm to learn DNF

Akira Maruoka (Tohoku University, Sendai, Japan)

(Joint work with Kazuyuki Amano.)

We give a derandomized version of the weak learning algorithm, due to Jackson, for DNF formulas with membership queries under the uniform distribution which produces large Fourier coefficients of a target function, where by "large" coefficients we mean the ones of magnitude exceeding some threshold. The algorithm to do so is based upon the following statement which is obtained by extending a theorem due to Luby *et al* :

$$\forall f \in t\text{-DNF}\ \forall A \subseteq [n] \text{ s.t.} |A| = k\ \forall D : (l+k)\text{-wise } \delta\text{-dependent distribution}$$
$$|\ \Pr_U[f(x) = \bigoplus_{i \in A} x_i] - \Pr_D[f(x) = \bigoplus_{i \in A} x_i]\ | \leq e^{-\frac{l}{t2^t}} + 2^{l+k}\delta,$$

where U denotes the uniform distribution and t-DNF denotes the class of DNF formulas consisting of terms of length at most t. Since the Fourier coefficient $\hat{f}(A)$ is equal to $2\Pr_U[f(x) = \bigoplus_{i \in A} x_i] - 1$, the statement above claims that Fourier coefficients can be approximated by $2\Pr_D[f(x) = \bigoplus_{i \in A} x_i] - 1$, which is calculated by exhaustive search trying all the points corresponding to the probabilistic distribution D with limited amount of independency.

Hard Examples for Bounded Depth Frege

Eli Ben-Sasson (Harvard University, Cambridge, USA)

We prove exponential lower bounds on the size of a bounded depth Frege proof of a Tseitin graph-based contradiction, whenever the underlying graph is an expander. This is the first example of a contradiction, naturally formalized as a 3-CNF, that has no short bounded depth Frege proofs. Previously, lower bounds of this type were known only for the pigeonhole principle, and for Tseitin contradictions based on *complete* graphs.

Our proof is a novel reduction of a Tseitin formula of an expander graph to the pigeonhole principle, in a manner resembling that done by Fu and Urquhart for complete graphs.

In the proof we introduce a general method for removing extension variables without significantly increasing the proof size, which may be interesting in its own right.

3-SAT Algorithms with Running Time 1.3302^n

Thomas Hofmeister (Universität Dortmund, Germany)

(Joint work with Uwe Schöning, Rainer Schuler, and Osamu Watanabe.)

In [1], Schöning proposed a simple yet efficient randomized algorithm for solving the k-SAT problem. In the case of 3-SAT, the algorithm has an expected running time of poly$(n) \cdot (4/3)^n = O(1.3334^n)$ when given a formula F on n variables. This was the up to now best running time known for an algorithm solving 3-SAT. In this talk, we describe an algorithm which improves upon this time bound by combining an improved version of the above randomized algorithm with other randomized algorithms. Our new expected time bound for 3-SAT is $O(1.3302^n)$.

[1] U. Schöning, A probabilistic algorithm for k-SAT and constraint satisfaction problems, in *Proc. of the 40th Ann. IEEE Sympos. on Foundations of Comp. Sci.* (FOCS'99), IEEE, 410–414, 1999.

Special Unsatisfiability Algorithms on Random Instances

Andreas Goerdt (Technische Universitt Chemnitz, Germany)

The investigation of random k-Sat instances is a current topic of Theoretical Computer Science. This is in part due to the interesting threshold behaviour in that there exist $c_k = c_k(n)$ such that random k-Sat instances with asymptotically less than $c_k n$ random clauses are satisfiable with high probability (i.e. with probability tending to 1 when n goes to infinity) whereas for more than $c_k n$ random clauses we have unsatisfiability with high probability.
We are interested in what we call "efficient certification" of unsatisfiability of a random k-Sat instance. That is we look for an efficient, deterministic algorithm which, given a propositional formula as input, either gives an inconclusive answer or states that the input formula is unsatisfiable. We require the algorithm to be *correct* in that the unsatisfiable answer implies that the input formula is really unsatisfiable. Assume we are given a family of probability spaces of random inputs which are unsatisfiable with high probability. "Efficient certification" requires in addition that an unsatisfiability algorithm as above is *complete* for the probability space in question. That is it answers ,,unsatisfiable" with high probability for inputs from this space. Note that this does not mean that it answers unsatisfiable on all unsatisfiable inputs, but only on most of them.

The best known result of this kind shows that one can efficiently certify unsatisfiability for random k-Sat instances with $n^{\varepsilon} \cdot n^{k/2}$ k-clauses. Recall that probabilistically we know that random k-Sat instances with cn clauses (for large enough constant c) are unsatisfiable with high probability. It is thus an obvious program to lower the bound of $n^{\varepsilon} \cdot n^{k/2}$.
We look at the following specialized satisfiability problems: For l-Out-Of-k-Sat we require that at least l literals per clause must be $true$ in order that the formula is satisfied. The ususal satsfiability problem has $l = 1$. For $l = 2$ and $k = 4$ we can certify unsatisfiability for $n^{\varepsilon} \cdot n^{3/2}$ random 4-clauses. This is better than the satisfiability bound of $n^{\varepsilon} \cdot n^2$ which we have. The same bound applies for $l = 2$ and $k = 5$ even better when compared to the satisfiability bound of $n^{\varepsilon} \cdot n^{5/2}$. To obtain our results we make some observations concerning the efficient certification of "discrepancy properties" of random 3-uniform hypergraphs. These observations may be of independent interest.
Moreover we look at the Not-All-Equal-3-Sat problem. We show that unsatisfiability in this case can in fact be certified already for a linear number of 3-clauses. We apply an approximation algorithm proposed by Kann, Lagergren and Panconesi (IPL 1996) to get our result. To the best of the author's knowledge approximation algorithms have by now not been used in this way to certify properties of random structures. Note that this result is particularly interesting in view of the fact that in upcoming paper by Feige (STOC 2002) the following hypothesis is put forward: For the classical 3-Sat problem efficient certification of unsatisfiability for a linear number of random clauses is not possible.

Satisfiability and Bandwidth

Mikhail V. Alekhnovitch (MIT, Cambridge, USA)

For CNF τ, let $w_b(\tau)$ be the branch-width of the underlying hypergraph of τ. In this paper we design an algorithm solving SAT in time $n^{O(1)}2^{w_b(\tau)}$. This in particular implies a polynomial algorithm for testing satisfiability on instances with branch-width $O(\log n)$.
Our algorithm is a modification of width based automated theorem prover (WBATP) which is a popular heuristic for finding resolution refutations of unsatisfiable CNFs. We show that instead of the exhaustive enumeration of all provable clauses, one can do a better search based on the Robertson-Seymour algorithm for approximating the branch-width of a graph. Moreover, as opposed to WBATP, it always produces regular refutations. We call the resulting procedure Branch-Width Based Automated Theorem Prover (BWBATP).

In the second part of the paper we investigate the behaviour of BWBATP on a well-studied class of Tseitin Tautologies. We argue that in this case BWBATP is better than WBATP. Namely, we show that its running time on any Tseitin tautology τ is $|\tau|^{O(1)} \cdot 2^{O(w(\tau \vdash \emptyset))}$, as opposed to the obvious bound $n^{O(w(\tau \vdash \emptyset))}$ provided by WBATP. This in particular implies that Resolution is automatizable on those Tseitin tautologies for which we know the relation $w(\tau \vdash \emptyset) \leq O(\log S(\tau))$. We identify one such subclass and prove partial results towards establishing this relation for larger classes of graphs.

On the Minimal Polynomial of a Matrix

Thomas Thierauf (Universität Ulm, Germany)

(Joint work with Thanh Minh Hoang.)

We investigate the complexity of the degree and the constant term of the minimal polynomial of a matrix. We show that the degree of the minimal polynomial behaves as the matrix rank, and if the constant term of the minimal polynomial of a matrix is reducible to the determinant then the *exact counting in logspace* class $\mathbf{C_=L}$ is closed under complement.
Furthermore, we improve the upper bound of the decision whether a matrix is diagonalizable, namely we show that this problem is complete for $\mathbf{AC}^0(\mathbf{C_=L})$, the $\mathbf{AC}^0$-*closure of* $\mathbf{C_=L}$.

Quantum Fingerprinting

Harry Buhrman (CWI & University of Amsterdam, The Netherlands)

(Joint work with Richard Cleve, John Watrous, and Ronald de Wolf.)

Classical fingerprinting associates with each string a shorter string (its fingerprint), such that any two distinct strings can be distinguished with small error by comparing their fingerprints alone. The fingerprints cannot be made exponentially smaller than the original strings unless the parties preparing the fingerprints have access to correlated random sources. We show that fingerprints consisting of quantum information can be made exponentially smaller than the original strings without any correlations or entanglement between the parties. This implies an exponential quantum/classical gap

for the equality problem in the simultaneous message passing model of communication complexity.

Quantum Branching Programs: Simulations and Upper and Lower Bounds

Detlef Sieling (Universität Dortmund, Germany)

(Joint work with Martin Sauerhoff.)

For the quantum analogs of branching programs and OBDDs (ordered binary decision diagrams) the following results are proven.

1. Quantum branching programs of polynomial size can simulate quantum Turing machines with logarithmic space restriction and vice versa (where for the latter direction the simulation is only done approximately). This justifies the definition of quantum branching programs and shows that they can be used to study space-bounded quantum computation.

2. It is observed that the known fingerprinting technique which allows to construct small randomized OBDDs for certain deterministically hard functions can be transferred to quantum OBDDs, for which an example is shown. On the other hand, an exponential lower bound on the size of quantum OBDDs for an explicitly defined function is proved, for which deterministic OBDDs have linear size.

3. Finally, extended quantum OBDDs are investigated which allow to carry out superoperators instead of unitary operations as in usual quantum OBDDs. These quantum OBDDs with superoperators can simulate randomized OBDDs with small overhead. They are thus provably more powerful than quantum OBDDs with unitary operations. On the other hand, it is shown that even quantum OBDDs with superoperators require exponential size for so-called k-stable functions.

On the Quantum Black-Box Complexity of Majority

Dieter van Melkebeek (University of Wisconsin, Madison, USA)

(Joint work with T. Hayes and S. Kutin.)

We describe a quantum black-box network computing the majority of N bits with zero-sided error eps using only $\frac{2}{3}N + O\big(\sqrt{N \log \frac{\log N}{\epsilon}}\big)$ queries: the algorithm returns the correct answer with probability at least $1 - \epsilon$, and "I don't know" otherwise. Our algorithm is given as a randomized "XOR decision tree" for which the number of queries on any input is strongly concentrated around a value of at most $\frac{2}{3}N$. We provide a nearly matching lower bound of $\frac{2}{3}N - O(N)$ on the expected number of queries on a worst-case input in the randomized XOR decision tree model with zero-sided error $o(1)$. Any classical randomized decision tree computing the majority on N bits with zero-sided error $\frac{1}{2}$ has cost N.

Lower Bounds on Quantum Communication Complexity

Hartmut Klauck (CWI, Amsterdam, The Netherlands)

We prove new lower bounds for bounded error quantum communication complexity. Our methods are based on the Fourier transform of the considered functions. First we generalize a method for proving classical communication complexity lower bounds developed by Raz to the quantum case. Applying this method we give an exponential separation between bounded error quantum communication complexity and nondeterministic quantum communication complexity. We develop several other Fourier based lower bound methods, notably showing that $\sqrt{\bar{s}(f)/\log n}$, for the average sensitivity $\bar{s}(f)$ of a function f, yields a lower bound on the bounded error quantum communication complexity of $f(xANDyXORz)$, where x is a Boolean word held by Alice and y, z are Boolean words held by Bob. We then prove the first large lower bounds on the bounded error quantum communication complexity of functions, for which a polynomial quantum speedup is possible. For all the functions we investigate, the only previously applied general lower bound method based on discrepancy yields bounds that are $O(\log n)$. The full version of the paper is available under `www.arXiv.org/abs/quant-ph/0106160`.

Separating Randomness from Nondeterminism for Read-once Branching Programs

Martin Sauerhoff (Universität Dortmund, Germany)

We prove that the "weighted sum function" WS_n due to Savický and Žák, which is defined for inputs $(x_1, \ldots, x_n) \in \{0,1\}^n$ by $\mathrm{WS}_n(x_1, \ldots, x_n) = x_s$, where $s = \left(\sum_{i=1}^{n} i x_i\right) \bmod p$, p the smallest prime greater than n, requires strongly exponential size $2^{\Omega(n)}$ for approximating and randomized read-once branching programs with two-sided error bounded by an arbitrary constant smaller than $1/2$. Since WS_n and its complement have polynomial size for nondeterministic read-once branching programs, this result implies that "NP $\cap$ coNP $\not\subseteq$ BPP" as well as "RP $\not\subseteq$ NP" for analogs of the standard complexity classes defined in terms of polynomial read-once branching program size.

Fast Fixed-Parameter-Tractable Algorithms for Nontrivial Generalizations of Vertex Cover

Prabhakar Ragde (University of Waterloo, Canada)

This talk covered joint work with Naomi Nishimura and Dimitrios Thilikos concerning graph recognition algorithms. Given a graph family closed under minors and with a bound on maximum degree, we demonstrate an algorithm for recognizing graphs "within k vertices" of the family that runs in time linear in the size of the graph plus a factor $(ck)^k$, where the constant c depends on properties of the graph. Since graphs with a k-vertex cover are within k vertices of an edgeless graph, and graphs with a k-vertex feedback set are within k vertices of a forest, this approach may lead to efficient algorithms for NP-complete problems whose natural parameter k is fixed. Correctness of the algorithm depends on a Ramsey-style theorem limiting the size of any obstruction (minor-minimal excluded graph) for the class of graphs within k vertices of the base family, thereby providing a nice illustration of how existential techniques commonly used in lower bounds can lead to good algorithms. The talk concluded with a survey of the state of the art in parameterized complexity and an appeal for lower bounds and structured models of computation appropriate to this area.

Reversible Logic Circuits

Pawel Kerntopf (Warsaw University of Technology, Poland)

A circuit (a gate) is said to be reversible if there is a one-to-one mapping between input vectors and output vectors, i.e. not only the output vector can be uniquely determined from the input vector but also the input vector can be reconstructed from the output vector. Reversible computing is a fast developing area of research due to its increasing importance to future computer technologies. It gives an attractive perspective of constructing digital devices that are almost energy lossless (i.e. without heat dissipation). A number of low-power arithmetic circuits and processor chips have already been implemented using CMOS circuits. Design of reversible logic circuits is quite different from that of conventional irreversible logic circuits. For realization of majority of Boolean functions (namely, the so-called unbalanced functions) it is necessary to apply constant signals to some of the circuit inputs and create additional outputs ("garbage") to preserve reversibility. Moreover, at least one gate is needed to duplicate (fanout) any signal (in contrast, in conventional circuits duplication of some signals is always possible "for free"). A survey of main results and some open problems concerning reversible gates and synthesis of reversible logic circuits will be presented.

On the Number of Random Bits to Compute Parity on a k-connected Network

Andreas Jakoby (Med. Universität zu Lübeck, Germany)

(Joint work with Markus Bläser, Maciej Liśkiewicz, and Bodo Siebert.)

We have studied the following problem: Given a network G connecting n players $P_1, \ldots, P_n$ of unrestricted computational power. Each player P_i knows an individual secret x_i and can use a random string R_i. The players can exchange some data with other players using the bidirectional links given by the edges of the network. The goal is to compute a function f over all secrets, such that no player learns anything about the input of the other players that cannot be derived from the result of the function, i.e. if x and y are two inputs with $x_i = y_i$ and $f(x) = f(y)$ then for each player P_i and for each communication string c_i the probability that P_i sees c_i on input x is exactly the same as that P_i sees c_i on input y.
In this talk we will investigate the number of random bits that are needed to compute the parity function over n bits with a private protocol if the communication network is k-connected. It is well known, that parity can be computed privately on a Hamiltonian graph by using only one random bit. We will show that computing parity on a $K_{k,n-k}$

with $2k \leq n$ requires at least $\frac{n-2}{k-1} - 1$ random bits. On the other hand, we will present a protocol for computing parity on an arbitrary k-connected network that uses at most $\frac{n-2}{k-1} - 1$ random bits.

On Boolean Decision Lists

Matthias Krause (Universität Mannheim, Germany)

We study the computational power of decision lists over AND-functions versus threshold-parity circuits. AND-decision lists are a natural generalization of formulas in disjunctive or conjunctive normal form. We show that, in contrast to CNF- and DNF-formulas, there are functions with small AND-decision lists which need exponential size unbounded weight threshold-parity circuits. This implies that it Jackson's polynomial learning algorithm for DNFs which is based on the efficient simulation of DNFs by polynomial weight threshold-parity circuits, cannot be app lied to AND-decision lists. A further result is that for all k the complexity class defined by polynomial length AC^0_k-decision lists lies *strictly* between AC^0_{k+1} and AC^0_{k+2}.

On the Non-Approximability of Boolean Functions by OBDDs

Ingo Wegener (Universität Dortmund, Germany)

People in machine learning and genetic programming have used OBDDs to represent a training set of data ($(x, f(x))$ for polynomially many x). In order to generalize the training set, based on Occam's razor theorem, the idea is to minimize the OBDD size while still presenting the training set correctly. This approach only works if some good approximation of the unknown function f has a small OBDD representation. Therefore, we are interested in lower bounds of approximations of boolean functions. The most general model where we can prove non-approximability results for error size $1/2 - o(1)$ are syntactic read-k times BPs. Since OBDDs are used in applications we also consider OBDD lower bounds for functions which are easy for correct representations and slightly more general models than OBDDs. For the hidden weighted bit function we prove such a non-approximability result which is based on a result on the distributional one-way communication complexity of the index function where the value of the index is binomially distributed.