Dagstuhl Seminar
on
The Complexity of Boolean Functions

David Mix Barrington, University of Massachusetts
Noam Nisan, Hebrew University
Rüdiger Reischuk, Med. Universität zu Lübeck
Ingo Wegener, Universität Dortmund

Schloß Dagstuhl, March 10. – March 14. 1997

Contents

Summary of the Dagstuhl Seminar

"The Complexity of Boolean Functions"

One of the most fundamental problems in computer science is to estimate the complexity of Boolean functions with respect to different models and complexity measures. It is frustrating that several central problems have remained open for a long time, such as proving (1) nonlinear size lower bounds for circuits of logarithmic depth, (2) nonpolynomial size lower bounds for formulas, or (3) nonpolynomial size lower bounds for threshold circuits of depth three. Nevertheless, there has been a lot of progress on some of the classical research problems. Also, new methods such as communication complexity are now available, and new applications (such as hardware verification) pose new problems which can be answered by those people active in this area.

The organizers (David Mix Barrington, Noam Nisan, Rüdiger Reischuk, and Ingo Wegener) are happy that 40 researchers came to the Dagstuhl seminar, only 14 of them from Germany (including three guests from India and Lithuania) with the others from the USA (10), Israel (5), Czech Republic (3), Austria, Canada, Denmark, Hungary, the Netherlands, Russia, Spain, and Sweden.

The 31 talks captured many of the aspects of Boolean function complexity: lower bounds for different types of circuits and branching programs, the average delay of circuits, the power of restrictions, communication complexity, applications to neural nets, and structural results on circuit-based complexity classes. It was discussed whether some lower bound proofs, including proofs that are not "natural" in the sense of Razborov and Rudich, are even possible. Furthermore, some talks considered related areas such as the PCP theorem, Yao's XOR lemma, visual cryptography, PRAM complexity, and hashing.

A lively problem session was organized, where 13 open problems were presented. There was also an open discussion on the future of this research topic.

Needless to say, the participants took advantage of the Dagstuhl facilities and the excellent atmosphere to hold many informal discussions as well.

The organizers
David Mix Barrington, Noam Nisan, Rüdiger Reischuk, and Ingo Wegener

Seminar Programme

Monday, 10. March 1997

9.05	-	9.45	Ramamohan Paturi: *Exponential Lower Bounds for Depth-3 Boolean Circuits*
9.45	-	10.25	Wolfgang Maass: *On the Computation Power of Models for Biological Neural Computation*
10.50	-	11.30	Eric Allender: *Characterization of* TC^0 *in Term of #AC*
11.30	-	12.10	Stephan Waack: *On Parity OBDDs*

Afternoon Session: chair Pierre McKenzie

15.30	-	16.05	Georg Schnitger: *Las Vegas Versus Determinism for One-way Communication Complexity, Finite Automata, and Polynomial-time Computations*
16.05	-	16.40	Lance Fortnow: *Nondeterministic Polynomial Time versus Nondeterministic Logspace*
16.50	-	17.25	Vince Grolmusz: *Set Systems and MOD m Polynomials*
17.25	-	18.00	Thomas Hofmeister: *Contrast-Optimal k out of n Secret Sharing Schemes in Visual Cryptography*

Tuesday, 11. March 1997

Morning Session: chair Noam Nissan

9.00	-	9.40	Jehoshua Bruck: *LTM: Multiple Threshold Logic*
9.45	-	10.20	Pavel Pudlak: *The Number of Isolated Points of a k-CNF*
10.50	-	11.30	Hans-Jürgen Prömel: *Size and Structure of Random OBDDs*
11.30	-	12.10	Christoph Meinel: *A Reducibility Concept for Problems Defined in Terms of Ordered Binary Decision Diagrams*

Afternoon Session: chair Eric Allender

15.30	-	16.05	Andreas Jakoby: *On the Average Circuit Complexity of Semigroups*
16.05	-	16.40	Christian Schindelhauer: *Lower Bounds in Average Circuit Complexity*
16.50	-	17.25	Howard Straubing: *Languages Defined with Modular Quantifiers and the ACC Conjecture*
17.25	-	18.00	Richard Beigel: *Boolean Circuits over PP*
20.00	-	21.30	Open Problem Session

Wednesday, 12. March 1997

Morning Session: chair Ingo Wegener

9.00	-	9.40	Alexander Andreev: *Hitting Sets and Derandomization*
9.45	-	10.20	Armin Haken: *Prospects for "Unnatural" Proofs Using "Customized" Approximations*
10.50	-	11.30	Matthias Krause: *On Computing Boolean Functions by Polynomials and Related Types of Threshold Circuits*
11.30	-	12.10	Noam Nisan: *Pointer Jumping Requires Concurrent Read*

Thursday, 13. March 1997

Morning Session: chair Pavel Pudlak

9.00	-	9.40	Paul W. Beame: *Restriction Methods for Bounded Depth Circuit Complexity*
9.45	-	10.20	Petr Savicky: *On P versus NP ∩ coNP for Decision Trees and Read-Once Branching Programs*
10.50	-	11.30	Stasys Jukna: *Lower Bound Criterion for Real Monotone Circuits*
11.30	-	12.10	Rüdiger Reischuk: *The Strong Fault-Tolerance of Threshold Circuits Is Weak*

Afternoon Session: chair Wolfgang Maass

15.30	-	16.05	Ran Raz: *Sub-Constant Error PCP Characterization of NP*
16.05	-	16.40	Peter Bro Miltersen: *Fine-Grained Properties of Hashing by Linear Transformations*
16.50	-	17.25	Gyvrgy Turan: *Remarks on Analog Circuits and Threshold Circuits*
17.25	-	18.00	David A. Mix Barrington: *Boolean Function Complexity: What Next? (Discussion)*

Friday, 14. March 1997

Morning Session: chair David A. Mix Barrington

9.00	-	9.35	Klaus-Jörn Lange: *Circuit Representaions of Complexity Classes*
9.35	-	10.10	Pierre McKenzie: *Reversible Space = Deterministic Space*
10.40	-	11.40	Avi Wigderson: *P=BPP unless E has Sub-Exponential Circuits: Derandomizing the XOR Lemma*
11.40	-	12.15	Ingo Wegener: *On the Power of Restricted Nondeterministic Branching Programs*
12.15			end of Seminar

Abstracts of Presentation

Exponential Lower Bounds for Depth-3 Boolean Circuits

Ramamohan Paturi
University of California, San Diego, USA

We consider the class Σ_3^k of unbounded fan-in depth-3 boolean circuits, for which the bottom fan-in is limited by k and the top gate is an OR. It is known that the smallest such circuit computing the parity function has $\Omega(2^{\varepsilon n/k})$ gates (for $k = O(n^{1/2})$) for some $\varepsilon > 0$, and this was the best lower bound known for explicit (P-time computable) functions. In this paper, for $k = 2$, we exhibit functions in uniform NC^1 that requires $2^{n-o(n)}$ size depth 3 circuits. The main tool is a theorem that shows that any Σ_3^2 circuit on n variables that accepts a inputs and has size s must be constant on a projection (subset defined by equations of the form $x_i = 0$, $x_i = 1$, $x_i = x_j$ or $x_i = \bar{x}_j$) of dimension at least $\frac{\log(a/s)}{\log n}$.

Joint work with Michael E. Saks and Francis Zane.

On the Computational Power of Models for Biological Neural Computation

Wolfgang Maass
Technische Universitaet Graz, Austria

We consider two formal models for neural computation involving temporal coding:

- a model for analog computation in networks of integrate-and-fire neurons with coding of analog variables through delays of neuronal firing
- a model for analog computation in a higher-level model that reflects salient properties of computations with firing rates and firing correlations.

For both models we analyze their computational power and prove rigorous results which distinguish their computational power from that of common models for artificial neural networks.
As a consequence of our proofs we also derive two new results for traditional models for artificial neural nets: we improve the largest known lower bound for the size of a sigmoidal neural net needed to compute a concrete function, and we derive stronger separation results between high-order and first-order sigmoidal neural nets.

Characterizations of TC^{υ} in terms of $\#AC^{\upsilon}$

Eric Allender
Rutgers University, USA

Continuing a line of investigation that has studied the function classes #P, $\#SAC^1$, #L, and $\#NC^1$, we study the class of functions $\#AC^0$. One way to define $\#AC^0$ is as the class of functions computed by constant-depth polynomial-size arithmetic circuits of unbounded fan-in addition and multiplication gates. In contrast to the preceding function classes, for which we know no nontrivial lower bounds, lower bounds for $\#AC^0$ follow easily from established circuit lower bounds.

One of our main results is a characterization of TC^0 in terms of $\#AC^0$: A language A is in TC^0 if and only if there is a $\#AC^0$ function f and a number k such that x in A iff $f(x) = 2^{|x|^k}$. Using established naming conventions, this yields: $TC^0 = PAC^0 = C_{=AC^0}$ Another restatement of this characterization is that TC^0 can be simulated by constant-depth arithmetic circuits, with a single threshold gate. We hope that perhaps this characterization of TC^0 in terms of AC^0 circuits might provide a new avenue of attack for proving lower bounds.

Our characterization differs markedly from earlier characterizations of TC^0 in terms of arithmetic circuits over finite fields. Using our model of arithmetic circuits, computation over finite fields yields ACC^0.

Joint work with Manindra Agrawal and Samir Datta.

On Parity OBDDs

Stephan Waack
Universität Gottingen, Germany

I consider a data structure for Boolean functions which is motivated by the formul circuit design, called Parity-OBDDs. they combine the mice algorithmic properties of the well-known OBDDs, the State-of-the-art data structure, with a consideralby layer descriptive power. Beginning from an algebraic characterization of the Parity-OBDD complexity I sketched in my talk the algorithm which minimizes the number of nodes of a given Parity-OBDD. The running time is $O(nSIZE(B)^3)$, if Gaussian eliminetion is used. An equivalence test algorithm can be constructed easily now.Finally, I described the basic ideas of an equivalence test for different variable orderings.

Las Vegas Versus Determinism for One-way Communication Complexity, Finite Automata, and Polynomial-time Computations

Georg Schnitger
Johann Wolfgang Goethe–Universität
Frankfurt am Main, Germany

We investigate the power of Las Vegas computation for the complexity measures of one-way communication, finite automata and polynomial-time relativized Turing machine computation.

(i) For the one-way communication complexity of two-party protocols we show that Las Vegas communication can save at most one half of the deterministic one-way communication complexity.

We also present a language for which this gap is almost achieved.

(ii) For the size (i.e., the number of states) of finite automata we show that the size of Las Vegas finite automata recognizing a language L is at least the root of the size of the minimal deterministic finite automaton recognizing L. Using a specific language we verify the optimality of this lower bound.

(iii) It is known that Las Vegas may be more powerful than determinism in a relativized world. We strengthen this result by showing for polynomial-time relativized computations that Las Vegas may be even more powerful than nondeterminism with at most $f(n)$ advice bits for any function f bounded by a polynomial.

On the other hand, for any polynomial-time constructible function h growing faster than $\log_2 n$, there exists an oracle B such that polynomial-time nondeterministic computations with oracle B and at most $h(n)$ advice bits are more powerful than polynomial-time two-sided error Monte Carlo probabilistic computations with oracle B and an unbounded number of random bits.

Since Monte Carlo computations may be exchanged for Las Vegas computations in the last result, these results solve an open problem of Diaz and Torán.

Joint work with Pavol Ďuriš Juraj Hromkovič and José D. P. Rolim

Nondeterministic Polynomial Time versus Nondeterministic Logspace

Lance Fortnow
CWI, The Netherlands

We discuss the possibility of using the relatively old technique of diagonalization to separate complexity classes, in particular NL from NP. We show several results in this direction.

- Any nonconstant level of the polynomial-time hierarchy strictly contains NL.
- $\overline{SAT} \notin NL \cap NTIME(n^{1+o(1)})$. This yields the first nontrivial time-space tradeoffs for SAT on general Turing machines.
- On the negative side, we present a relativized world where P = NP but any nonconstant level of the polynomial-time hierarchy differs from P.

Set Systems and MOD m Polynomials

Vince Grolmusz
Eötvös University, Budapest, Hubgary

Let S be a set of n elements, and let $\mathcal{H}$ be a set-system on S, which satisfies that the size of any element of $\mathcal{H}$ is divisible by m, but the intersection of any two elements of $\mathcal{H}$ is not divisible by m. If m is a prime or prime-power, then the famous *Frankl–Wilson theorem* implies that $|\mathcal{H}| = O(n^{m-1})$, i.e. for fixed m, its size is at most polynomial in n. This theorem has numerous applications in combinatorics and also in geometry, (c.f. the disproof of *Borsuk's conjecture* by *Kahn* and *Kalai* in 1992, or explicit constructions of Ramsey graphs, or other geometric applications related to the Hadwiger–problem.) *Frankl* and *Wilson* asked whether an analogous upper bound existed for *non–prime power, composite moduli*. Here we show a surprising construction of a *superpolynomial–sized* uniform set-system $\mathcal{H}$ satisfying the intersection–property, for every non–prime–power, composite m, negatively settling a related conjecture of *Babai* and *Frankl*. The proof uses a polynomial–construction of *Barrington, Beigel* and *Rudich*, and a new method for constructing set-systems from multivariate polynomials. An improved upper bound for this polynomial construction would imply a better Ramsey-graph construction than is currently known.
A preliminary version of this paper is available at
http://www.cs.elte.hu/∼grolmusz

Contrast-Optimal k out of n Secret Sharing Schemes in Visual Cryptography

Thomas Hofmeister
Universität Dortmund, Germany

Visual cryptography and (k, n)–visual secret sharing schemes are notions introduced by Naor and Shamir in [NaSh95]. A sender wishing to transmit a secret message distributes n transparencies among n recipients, where the transparencies contain seemingly random pictures.
A (k, n)-scheme is designed to achieve the following situation: If any k recipients stack their transparencies together, then a secret message is revealed visually. On the other hand, if only $k-1$ recipients stack their transparencies, or analyze them by any other means, they are not able to obtain any information about the secret message.
The important measures of how good a scheme is, are given by its contrast, i.e., the clarity with which the message becomes visible, and the number of subpixels needed to encode one pixel of the original secret picture.
Naor and Shamir constructed (k, k)–schemes which achieve contrast $2^{-(k-1)}$ with the minimal number of subpixels. By an intricate result from [LiNi90], they were also able to prove that this was the optimal contrast. Using hashing strategies and small biased probability spaces they also proved that for all fixed $k \leq n$, there are (k, n)–schemes with contrast only depending on k (i.e., $(2e)^{-k}/\sqrt{2\pi k}$ – for $k = 2, 3$ and $k = 4$ the contrast is approximately 1/105, 1/698 and 1/4380, respectively.)
In this paper, we show that by solving a simple linear program, one is able to compute *exactly* the best contrast achievable in any (k, n)-scheme. The solution of the linear program also provides a representation of the corresponding scheme. This yields e.g. $(3, n)$–schemes of contrast larger than 1/16 and $(4, n)$–schemes of contrast larger than 1/64 for all n.
For small values of k as well as for $k = n$, we are able to analytically solve the linear program and get a much shorter proof of the optimality of Naor's and Shamir's (k, k)–schemes. In the case $k = 2$, we are able to use a different approach via coding theory which allows us to prove a number of optimal tradeoffs between contrast and number of subpixels. In particular, we construct $(2, n)$–schemes with a nearly optimal number of subpixels and with optimal contrast $\frac{n}{4(n-1)}$. Further we show that for all n and $\alpha < \frac{1}{4}$ there are $(2, n)$–schemes of contrast α with subpixel number $O(\log n)$.
Joint work with Matthias Krause and Hans U. Simon.

[LiNi90] N. Linial, N. Nisan, *Approximate inclusion-exclusion,* Combinatorica 10, p. 349-365, 1990.

[NaSh95] M. Naor, A. Shamir, *Visual Cryptography,* in "Advances in Cryptology - Eurocrypt 94." Springer, pages 1-12, 1995.

LTM: Multiple Threshold Logic

Jehoshua Bruck
California Institute of Technology Pasadena, USA

We introduce a new Boolean computing element related to the Linear Threshold (LT) element. Instead of the sign function in the LT element it computes an arbitrary (with polynomialy many transitions) Boolean function of the weighted sum of its inputs. We call the new computing element an LTM element, which stands for Linear Threshold with Multiple transitions. Our main contributions related to the study of LTM include:

(i) the creation of efficient designs of LTM circuits for the addition of a multiple number of integers and the product of two integers. In particular, we show how to compute the addition of m integers with a single layer of LTM elements.

(ii) the characterization of the computing power of LTM relative to LT circuits. Specifically, we prove that LTM is strictly contained in the class of Boolean functions computed by depth-2 polynomial size LT circuits with small weights.

Joint work with Vincent Bohossian.

The Number of Isolated Points of a k-CNF

Pavel Pudlak
Czech Academy of Science, Czech Republic

An isolated point of a k-CNF is a satisfying assignment such that no assignment of Hamming distance 1 satisfies the formula. We prove an optimal upper bound $2^{n-n/k}$. This result (more precisely the proof technique) has the following applications:

1. a precise bound $\Theta(n^{1/4}2^{\sqrt{n}})$ on the minimal size of a depth three circuits computing the parity of n variables;
2. a probabilistic algorithm producing a satisfying assignment for a satisfiable k-CNF in expected time $n^{O(1)}2^{n-n/k}$.

Joint work with R. Paturi and F. Zane.

Size and Structure of Random OBDD's

Hans Jürgen Prömel
Humboldt-Universität zu Berlin, Germany

In 1994 I. Wegener proved that for almost every n it is true that almost all Boolean functions on n variables allow only OBDD's of worst possible size which is, depending on n, between $\frac{2^n}{n}(1+o(1))$ and $\frac{2^n}{n}(2+o(1))$. It is said that for these n the strong Shannon effect holds. We give a complete description of those n for which the strong Shannon effect holds showing that this effect does hold for some n if and only if n is "sufficiently far" from any number which admits a representation as $2^h + h$ for some h. In particular, for $n = 2^h + h$ the strong Shannon effect does not hold.
Moreover, we show that the probability that the size of a random OBDD with n levels deviates more than $n \cdot 2^{\frac{1+c}{2}n}$ from the worst case is less than $e^{-2^{cn}}$ for arbitrary $c > 0$. This is to say that the weak Shannon effect holds with probability which tends double exponentially fast to 1. The proof of this last result invokes Azuma's unequality for matingales.

Joint work with C. Gröpl and A. Srivastav.

A Reducibility Concept for Problems Defined in Terms of Ordered Binary Decision Diagrams

Christoph Meinel
Universit"at Trier, Germany

Reducibility concepts are fundamental in complexity theory. Usually, they are defined as follows: A problem Π is reducible to a problem Σ if Π can be computed using a program or device for Σ as a subroutine. However, this approach has its limitations if restricted computational models are considered. In the case of ordered binary decision diagrams (OBDDs), it allows merely to use the almost unmodified original program for the subroutine.
Here we propose a new reducibility concept for OBDDs: We say that Π is reducible to Σ if an OBDD for Π can be constructed by applying a sequence of elementary operations to an OBDD for Σ. In contrast to traditional reducibility notions, the newly introduced reduction is able to reflect the real needs of a reducibility concept in the context of OBDD-based complexity classes: it allows to reduce those problems to each other which are computable with the same amount of OBDD-resources and it gives a tool to carry over lower and upper bounds.

Joint work with Anna Slobodov'a.

On the Average Circuit Complexity of Semigroups

Andreas Jakoby
Med. Universität zu Lübeck, Germany

We analyse the average complexity of evaluating all prefixes of an input vector over a given semigroup. As computational model circuits over the semigroup are used and a complexity measure for the average delay of such circuits, called *time*, is introduced. Based on this notion, we then define the average case complexity of a computational problem for arbitrary strict positive input distributions.
For highly nonuniform distributions the average case complexity turns out to be as large as the worst case complexity. Thus, in order to make the average case analysis meaningful we also develop a complexity measure for distributions.
We give a complete characterization of the average complexity of the parallel prefix problem with respect to the underlying semigroup. By considering a related reachability problem for finite automata it is shown that the complexity only depends on two properties of the semigroup: the *confluence* and the *diffluence*. Our analysis yields that only three different cases can arise for the reachability question. We show that the parallel prefix problem either can be solved with a constant average delay, with a average delay of an oder $\log\log n$, that means with an exponential speedup compared to the worst case, or in case of nonconfluent semigroups that no speedup is possible. Circuit designs are presented that for confluent semigroups achieve the optimal delay while keeping the circuit size linear.
The analysis and results are illustrated at some concrete functions. For the n-ary Boolean `OR` and `PARITY`, for example, the average case circuit delay is determined exactly up to small constant factors for arbitrary distributions.

Lower Bounds in Average Circuit Complexity

Christian Schindelhauer
Med. Universität zu Lübeck, Germany

In contrast to machine models like Turing machines or random access machines, circuits are a static computational model. The internal information flow of a computation is fixed in advance, independent of the actual input. Therefore, the size and the depth are natural and simple measures for circuits and provide a worst case measure. We consider a model where an internal gate is evaluated as soon as its result is determined by the already available input. So we obtain a dynamic notion of delay. In STOC94 we have defined an average case measure for the time complexity of circuits. Using this notion tight upper and lower

bounds could be obtained for the average case complexity of several basic Boolean functions.
Here, we will examine the asymptotic average case complexity of the set of all n-ary Boolean functions. In contrast to worst case analysis a simple counting argument does not work. We prove that almost all Boolean function require at least $n - \log n - \log\log n$ expected time even for the uniform probability distribution. On the other hand, there are significant subsets of functions that can be computed with a constant average delay.
Finally, we compare worst case and average case complexity of Boolean functions. We show that for each function that is not computable by circuits of depth less than d, the expected time complexity will be at least $d - \log n - \log d$ with respect to an explicitely defined probability distribution. In addition, a nontrivial upper bound on the complexity of such a distribution will be obtained.

Joint work with Andreas Jakoby and Rüdiger Reischuk.

Languages Defined with Modular Quantifiers and the ACC Conjecture

Howard Straubing
Boston College, USA

An outstanding conjecture in circuit complexity is that the class ACC is strictly contained in NC^1. This conjecture has a nice model-theoretic formulation. We use formulas of generalized first-order logic to describe properties of strings over a finite alphabet A. The variables of the formula range over the positions $1, .., |w|$ of the string w. There are two kinds of atomic formulas: If $a \in A$ then $Q_a x$ is interpreted to mean 'the letter in position x is a'. The other kind of atomic formula we call a numerical predicate. This is a relation on positions in a string, such as '$x < y$', or 'x is prime', that depends only on the positions, and not the letters that appear in those positions. A regular numerical predicate is a first-order formula in which the atomic formulas are all of the form '$x < y$' and '$x \equiv 0(modq)$'. We introduce a new kind of quantifier $\exists(i, s, t)$. We interpret

$$\exists^{(i,s,t)} x \phi(x)$$

to mean that the number of positions that satisfy ϕ is congruent to i modulo t, and either greater than or equal to s, or equal to i.
We can extend this quantifier to quantify k-tuples of positions instead of single positions. We call a formula of the form

$$\exists^{(i,s,t)}(x_1, ..., x_k)\phi(x_1, ..., x_k),$$

where ϕ is quantifier-free, a generalized Σ_1 sentence.
The conjecture that ACC is strictly contained in NC^1 is equivalent to: Every sentence defined with these modular quantifiers is satisfied by the same set of strings as such a sentnece in which only numerical predicates appear.
Our main result proves this conjecture in the case of boolean combinations of generalized Σ_1 sentences: Everly language defined by a boolean combination of generalized Σ_1 sentences is defined by such a boolean combination of Σ_1 sentences, with the same quantifiers, in which only numerical predicates appear. The proof uses a combination of finite semigroup theory and Ramsey's theorem.

Boolean Circuits over PP

Richard Beigel
Univ. of Maryland at College Park, USA

Wilson's [Wils85] model of oracle gates provides a framework for considering reductions whose strength is intermediate between truth-table and Turing. Improving on a stream of results by Beigel, Reingold, Spielman, Fortnow, and Ogihara [BeRS95, FoRe96, Ogih96], we prove that PL and PP are closed under NC^1 reductions. This answers an open problem of Ogihara [Ogih96]. More generally, we show that $\mathrm{NC}^{\mathrm{PP}}_{k+1} = \mathrm{AC}^{\mathrm{PP}}_k$ and $\mathrm{NC}^{\mathrm{PL}}_{k+1} = \mathrm{AC}^{\mathrm{PL}}_k$ for all $k \geq 0$. On the other hand, we construct an oracle A such that $\mathrm{NC}^{\mathrm{PP}^A}_k \neq \mathrm{NC}^{\mathrm{PP}^A}_{k+1}$ for all integers $k \geq 1$. Slightly weaker than NC_1 reductions are Boolean formula reductions. We ask whether PL and PP are closed under Boolean formula reductions. This is a nontrivial question despite $\mathrm{NC}^1 = \mathrm{BF}$, because that equality is easily seen not to relativize. We prove that $\mathrm{P}^{\mathrm{PP}}_{\log^2 n/\log\log n\text{-T}} \subseteq \mathrm{BF}^{\mathrm{PP}} \subseteq \mathrm{PTIME}(n^{O(\log n)})$. Because $\mathrm{P}^{\mathrm{PP}}_{\log^2 n/\log\log n\text{-T}} \not\subseteq \mathrm{PP}$ relative to an oracle, we think it is unlikely that PP is closed under Boolean formula reductions.

[Wils85] Christopher B. Wilson,*Relativized Circuit Complexity*, JCSS, Vol. 31, No. 2, 1985, p. 169-181.

[BeRS95] Richard Beigel and Nick Reingold and Daniel Spielman, *PP is closed under intersection*, JCSS, Vol. 50, No. 2, 1995, p. 191-202.

[FoRe96] Lance Fortnow and Nick Reingold, *PP is closed under truth-table reductions*, I& C, Vol. 124, No. 1, 1996, p. 1-6.

[Ogih96] M. Ogihara, *The PL Hierarchy Collapses*, FOCS'96

Hitting Sets and Derandomization

Alexander E. Andreev
Moscow University, Russia

We show that hitting sets can derandomize *any* BPP-algorithm. This gives a positive answer to a fundamental open question in probabilistic algorithms.
More precisely, we present a polynomial time deterministic algorithm which uses any given hitting set to approximate the fractions of 1's in the output of any boolean circuit of polynomial size. This new algorithm implies that if a quick hitting set generator with logarithmic price exists then $BPP = P$.
The existence of quick hitting set generators is thus a new weaker sufficient condition to obtain $BPP = P$; this can be considered as another strong indication that the gap between probabilistic and deterministic computational power is not large.
We show how to simulate any BPP algorithm using a weak random source of min-entropy r^γ for any $\gamma > 0$. This follows from a more general result about *sampling* with weak random sources. Our result matches an information-theoretic lower bound and solves a question that has been open for some years. The previous best results were a polynomial time simulation of RP and a $n^{\log^{(k)} n}$-time simulation of BPP for fixed k.
Departing significantly from previous related works, we do not use extractors; instead, we use the OR-disperser in combination with a tricky use of hitting sets.
We present the worst-case hardness conditions on the circuit complexity of EXP functions which are sufficient to obtain $P = BPP$ and $NC = BPNC$. In particular, we show that from such hardness conditions it is possible to construct quick Hitting Sets Generators with logarithmic prize and depth. As proved by as, such generators can efficiently derandomize any BPP and NC algorithm.

Joint work with Andrea E. F. Clementi, José D. P. Rolim, and Luca Trevisan

Prospects for "Unnatural" Proofs Using "Customized" Approximations

Armin Haken
DIMACS, USA

Is there hope for circuit loer bounds against NC^1 and more powerful models? By the work on natural proofs by Razborov and Rudich, all currently known lower bound proofs are *naturalizable*, and a naturalizable super-polynomial lower

bound for NC^1 is not to be expected (as long as we believe in pseudo-random generators).
This talk argues that a lower bound proof for CLIQUE, if one could be found, would likely not be naturalizable. The proof would have to make use of either the monotonicity of the function or of an NP condition on acceptance of a "typical" input.
The lower bound arguments for CLIQUE on monotone circuits cannot prove good non-monotone bounds due to a result by Razborov. However an extension of the method called *customized* approximation is not ruled out by that negative result. In customized approximation, the approximators to gates depend on only one specific circuit that is to be proved large.
Some (vague) ideas are given for how to customize the monotone-circuit arguments to the circuit and make use of the monotonicity of the function being bounded.

On Computing Boolean Functions by Polynomials and Related Types of Threshold Circuits

Matthias Krause
Universität Manheim, Germany

We investigate the computational power of threshold–AND circuits versus threshold–XOR circuits. Starting from the observation that small weight threshold–AND circuits can be simulated by small weight threshold–XOR circuits we pose the question whether a similar simulation exists for small size unbounded weight circuits. The answer to this question is no. We present a function with small threshold–AND circuits for which all threshold–XOR circuits have exponentially many nodes. This gives a solution to the following basic problem on separating subsets of the hypercube by hypersurfaces induced by sparse real polynomials: Is it generally better to choose domain $\{=1,-1\}$ or are there functions having more compact polynomials over $\{0,1\}$? We prove our result by a new lower bound argument which, we hope, contributes to a better understanding of the computational limitations of small depth threshold circuits.

Joint work with pavel Pudlák.

Pointer Jumping Requires Concurrent Read

Noam Nisan
Hebrew University of Jerusalem, Israel

We consider the well known problem of determining the k'th vertex reached by chasing pointers in a directed graph of out-degree 1. The famous "pointer doubling" technique provides an $O(\log k)$ parallel time algorithm on a Concurrent-Read Exclusive-Write (CREW) PRAM. We prove that this problem requires $\Omega(k)$ steps on an Exclusive-Read Exclusive-Write (EREW) PRAM, for every $k < c\sqrt{(}\log n)$, where n is the number of vertices and c is a constant.
This yields a boolean function which can be computed in $O(\log \log n)$ time on a CREW PRAM, but requires $\Omega(\sqrt{(}\log n))$ time on even an "ideal" EREW PRAM. This is the first separation known for boolean functions between the power of EREW and CREW PRAMs. Previously, separations between EREW and CREW PRAMs were only known for functions on "huge" input domains, or for restricted types of EREW PRAMs.

Joint work with Ziv Bar-Yossef.

Restriction Methods for Bounded Depth Circuit Complexity

Paul W. Beame
University of Washington, USA

We survey recent improvements in restriction methods for proving lower bounds for AC^0 circuits. The power of these methods is based on switching lemmas which convert RNF formulas with short terms into decision trees of small height. The first improvement we discuss is a substantial simplification in the proofs of bounds in the switching lemmas based on term by term canonical conversion of the formulas into decision trees. These methods which originate in the work of Yao and Håstad give the best lower bounds for almost all problems for AC circuits. A notable exception is distance-k-bounded st. connectivity for $k \leq \log n$ for which Ajtai gave $\Omega(\log^* k)$ depth lower bounds for polynomial size using an independent-set based switching lemma technique which originated in the work of Furst, Saxe, Sipser and Aitai. We develop a new swiching lemma technique that is based on a somewhat different use of independent sets by combining the features of both previous techniques. From this we obtain an improved $\Omega(\log \log k)$ depth lower bound for the k-st. connectivity problem.

Joint work with Russel Impaglizzo and Toniann Pitassi.

On P versus NP $\cap$ co-NP for Decision Trees and Read-Once Branching Programs

P. Savicky
Academy of Sciences of the Czech Republic, Czech Republic

It is known that if a Boolean function f in n variables has a DNF and a CNF of size at most N then f also has a (deterministic) decision tree of size $\exp(O(\log n \log^2 N))$. We show that this simulation cannot be made polynomial: we exhibit explicit Boolean functions f that require deterministic trees of size $\exp(\Omega(\log^2 N))$ where N is the total number of monomials in minimal DNFs for f and $\neg f$. Moreover, we exhibit new examples of explicit Boolean functions that require deterministic read-once branching programs of exponential size whereas both the functions and their negations have small nondeterministic read-once branching programs. One example results from the Bruen-Blokhuis bound on the size of nontrivial blocking sets in projective planes: it is remarkably simple and combinatorially clear. Whereas other examples have the additional property that f is in AC^0.

Joint work with S. Jukna, A. Razborov, and I. Wegener.

Lower Bounds Criterion for Real Monotone Circuits

S. Jukna
Universität Trier, Germany

We consider the following general model of monotone *real* computations: gates may be arbitrary non-decreasing real-valued functions $\phi : \mathbf{R}^m \to \mathbf{R}$ ($m \geq 1$). We do not bound the fanin m. Rather, we require that these functions have bounded "degree". The degree of a gate does not exceed the fanin but may be much smaller. In particular, a Boolean gate $\phi : \{0,1\}^m \to \{0,1\}$ has degree $\leq d$ if either all minterms or all maxterms (or both) have length at most d. For example, unbounded fanin AND and OR gates have degree 1. The degree of a threshold gate $T_s^m(x_1, \ldots, x_m)$ does not exceed threshold value $\min\{s, m-s+1\}$. Our main result is the following general combinatorial lower bounds criterion for bounded degree unbounded fanin monotone real circuits.

Criterion: *Let C be a monotone real circuit computing a monotone Boolean function f. If all the gates of C have degree at most d then, for any integers $a, b \geq 1$ and random vectors u, v in $\{0,1\}^n$, C has size at least the minimum of*

$$\frac{\mathrm{Min}_b\,[u,0]}{(db)^a \cdot \mathrm{Max}_a\,[u,0]} \quad \textit{and} \quad \frac{\mathrm{Min}_a\,[v,1]}{(da)^d \cdot \mathrm{Max}_b\,[v,1]}$$

where

$$\begin{aligned} \mathrm{Min}_k\,[u,\varepsilon] &= \min_{|S|\le k} \mathrm{Prob}[f(u)=\varepsilon \text{ and } u(S)\equiv \varepsilon\oplus 1]\,, \\ \mathrm{Max}_k\,[u,\varepsilon] &= \max_{|S|\ge k} \mathrm{Prob}[f(u)=\varepsilon \text{ and } u(S)\equiv \varepsilon]\,. \end{aligned}$$

The proof is relatively simple and direct, and combines the bottlenecks counting approach of Haken with the idea of finite limit due to Sipser. Apparently this is the first combinatorial lower bounds criterion for monotone computations. It is symmetric and yields (in a uniform and easy way) exponential lower bounds.

The Strong Fault Tolerance of Threshold Circuits is Weak

Rüdiger Reischuk
Med. Universität zu Lübeck, Germany

For ordinary circuits with a fixed upper bound on the maximal fanin of gates it has been shown that logarithmic redundancy is necessary and sufficient to overcome random hardware faults. We consider the same question for threshold circuits with gates of unbounded fanin. Wires, resp. gates may give wrong results with some error probablity that is not known exactly. As a main result it is shown that for circuits of depth d threshold gates of fanin larger than $O(d \log d)$ are useless for fault-tolerant computations. This implies that such circuits can only compute functions that depend on at most $O(\exp(d \log d))$ many variables and that almost all Boolean functions require depth $\Omega(\log n / \log\log n)$.

Sub-Constant Error PCP Characterization of NP

Ran Raz
Weizmann Institute, Israel

We introduce a new low-degree–test, one that uses the restriction of low-degree polynomials to planes (i.e., affine sub-spaces of dimension 2), rather than the restriction to lines (i.e., affine sub-spaces of dimension 1). We prove the new test to be of a very small error-probability (in particular, much smaller than constant).
The new test enables us to prove a low-error characterization of NP in terms of PCP. Specifically, our theorem states that, for any given $\epsilon > 0$, membership in any NP language can be verified with $O(1)$ accesses, each reading logarithmic number of bits, and such that the error-probability is $2^{-\log^{1-\epsilon} n}$. Our results are in fact stronger.

One application of the new characterization of NP is that approximating SET-COVER to within a logarithmic factors is NP-hard.
Previous analysis for low-degree–tests, as well as previous characterizations of NP in terms of PCP, have managed to achieve, with constant number of accesses, error-probability of, at best, a constant. The proof for the small error-probability of our new low-degree–test is, nevertheless, significantly simpler than previous proofs. In particular, it is combinatorial and geometrical in nature, rather than algebraic.

Joint work with S. Safra.

Fine-Grained Properties of Hashing by Linear Transformations

Peter Bro Miltersen
University of Aarhus BRICS, Denmark

Consider the set $\mathcal{H}$ of all linear (or affine) transformations between two vector spaces over a finite field F. We study how good $\mathcal{H}$ is as a class of hash functions, namely we consider hashing a set S of size n into a range having the same cardinality n by a randomly chosen function from $\mathcal{H}$ and look at the expected size of the largest hash bucket. $\mathcal{H}$ is a universal class of hash functions for any finite field, but with respect to our measure different fields behave differently.
If the finite field F has n elements then there is a bad set $S \subset F^2$ of size n with expected maximal bucket size $\Omega(n^{1/3})$. If n is a perfect square then there is even a bad set with largest bucket size *always* at least $\sqrt{n}$. (This is worst possible, since with respect to a universal class of hash functions every set of size n has expected largest bucket size below $\sqrt{n} + 1/2$.)
If, however, we consider the field of two elements then we get much better bounds. The best previously known upper bound on the expected size of the largest bucket for this class was $O(2^{\sqrt{\log n}})$. We reduce this upper bound to $O(\log n \log\log n)$. Note that this is not far from the guarantee for a random function. There, the average largest bucket would be $\Theta(\log n / \log\log n)$.
In the course of our proof we develop a tool which may be of independent interest. Suppose we have a subset S of a vector space D over $\mathbf{Z}_2$, and consider a random linear mapping of D to a smaller vector space R. If the cardinality of S is larger than $c_\varepsilon |R| \log |R|$ then with probability $1-\varepsilon$, the image of S will cover all elements in the range.

Joint work with Noga Alon, Martin Dietzfelbinger, Erez Petrank, and Gabor Tardos.

Remarks on Analog Circuits and Threshold Circuits

Gyorgy Turan
University of Illinois at Chicago, USA

Analog circuits are built of gates that compute functions of real-valued inputs. We discuss the computational power of analog circuits for computing Boolean functions. In some cases the lower bound techniques for Boolean circuits can be extended to analog circuits (for example, for the size of arithmetic threshold formulas, and, as shown by Pudlak, and Haken and Cook, for the size of monotone real circuits). It is noted that the information theoretic argument used to prove lower bounds for planar circuits does not work in the analog case, and in fact, planar arithmetic threshold circuits can be more powerful than planar Boolean circuits.
Proving an exponential lower bound for depth 2 threshold circuits with unrestricted weights is an open problem. We prove an exponential lower bound for depth 2 threshold circuits for which the weights of edges entering the final gate are +-1, +-2, +-4,... (thus, this is a class of circuits with exponentially large weights on the last level). This model corresponds to the class of neural networks constructed by the partition algorithms of Rujan and Marchand, or to the class of decision lists with linear tests. It can also be viewed as a generalization of the multiple threshold logic unit discussed by Bruck at this workshop (it is not known whether linear decision lists can actually be stronger).

Joint work with Farrokh Vatan.

Boolean Function Complexity: What Next?

David Mix Barrington
University of Massachusetts, USA

To promote a general discussion, I listed three results from the mid-1980's:

- Beame, Cook, Hoover: Division in P-uniform TC^0
- Smolensky: Lower Bounds for $ACC^0[p]$, p prime
- Hajnal et al.: Lower Bounds for depth-2 Threshold Circuits, even with unbounded weights.

Each suggested a direction for further results on which this community has made little progress. I asked whether we should be satisfied with this. I also invited discussion on possible inherent limits to such progress, such as the bounds on the power of "natural proofs".
Lance Fortnow reminded us of the rush of major circuit complexity results in 1985-7, and bemoaned what he saw as a proliferation of newly-defined models and complexity classes, which have distracted us from what should be our main goal, the P versus NP question. He offered a US$500 cash reward for a proof that NP is different from NC^1.
Avi Wigderson spoke more approvingly of the community's progress, and set two challenges to it:

1. Resolve the RP versus EXPTIME question.

2. Prove that a depth-3 sum-product-sum circuit, over a general field with gates for constants, needs superpolynomnial size to compute the permanent or determinant.

Circuit Representaions of Complexity Classes

Klaus-Jörn Lange
Tübingen, Germany

An overview is given about characterizations of PRAMs in terms of Boolean circuits. These results have been obtained by or in cooperation with R. Niedermeier,I. Niepel, K. Reinhardt, and P. Rossmanith. While the relations between concurrent access and nondeterminism, resp. exclusive access and unambiguity, are easy to handle, the case of owner access and determinism is a bit more difficult. Using *multiplex–* and *demultiplex–*gates characterizations of CROW- and OROW-PRAMs have been obtained. Recently, Klaus Reinhardt was able to show that the evaluation problem of these cicuits is inherently sequential: if there is any polynomial speed-up over the best sequential running time of these problems, then every problem in P has polynomial spee-up.

Reversible Space = Deterministic Space

Pierre McKenzie
Universite de Montreal, Canada

We prove that a deterministic Turing machine operating in space $S(n)$ can be simulated by a reversible Turing machine operating in the same amount of space. This answers a question posed by Bennett in 1989 and settles in the negative a conjecture, made by Li and Vitanyi in 1996, that any reversible simulation of an irreversible computation must obey Bennett's reversible pebble game rules.

Joint work with Klaus-Jörn Lange and Alain Tapp.

P=BPP unless E has Sub-Exponential Circuits: Derandomizing the XOR Lemma

Avi Wigderson
The Hebrew University, Israel

Yao showed that the XOR of independent random instances of a somewhat hard Boolean problem becomes almost completely unpredictable. In this paper we show that, in non-uniform settings, total independence is not necessary for this result to hold. We give a pseudo-random generator which produces n instances of a problem for which the analog of the XOR lemma holds. Combining this generator with the results of [NiWi94,BFNW93] gives substantially improved results for hardness vs randomness trade-offs. In particular, we show that if any problem in $E = DTIME(2^{O(n)})$ has circuit complexity $2^{\Omega(n)}$, then $P = BPP$. Our generator is a combination of two known ones - the random walks on expander graphs of [AjKS87, CoWi89, ImZu89] and the nearly disjoint subsets generator of [Nisa91, NiWi94]. The quality of the generator is proved via a new proof of the XOR lemma which may be useful for other direct product results.

Joint work with Russell Impagliazzo.

[AjKS87] M. Ajtai, J. Komlos and E. Szemeredi, "Deterministic simulation in LOGSPACE", Proc. of *19th ACM STOC*, 132-140, 1987.

[BFNW93] L. Babai, L. Fortnow, N. Nisan and A. Wigderson, "BPP has Subexponential Time Simulations unless EXPTIME has Publishable Proofs", *Complexity Theory*, Vol 3, pp. 307–318, 1993.

[CoWi89] A. Cohen and A. Wigderson, "Dispensers, Deterministic Amplification, and Weak Random Sources", *30th FOCS*, pp. 14–19, 1989.

[ImZu89] R. Impagliazzo and D. Zuckerman, "How to Recycle Random Bits", *30th FOCS*, pp. 248-253, 1989.

[Nisa91] N. Nisan, "Pseudo-random bits for constant depth circuits", *Combinatorica 11* (1), pp. 63-70, 1991.

[NiWi94] N. Nisan, and A. Wigderson, "Hardness vs Randomness", *J. Comput. System Sci.* 49, 149-167, 1994

On the Power of Restricted Nondeterministic Branching Programs

Ingo Wegener
Univ. Dortmund, Germany

Branching programs are compact representations of Boolean functions but the equivalence test and the satisfiability test are hard problems. Hence, general branching programs (also called binary decision diagrams) cannot be used in applications like circuit verification as representations of Boolean functions. Ordered binary decision diagrams (oblivious read-once BPs) allow efficient algorithms for all important operations but the class of functions with polynomial-size OBDDs is too restricted. There are mainly three ways to generalize OBDDs: allowing more variable orderings, allowing repeated tests, and allowing some type of nondeterminism. The most important models, namely read-once BPs (free BDDs), k-OBDDs, k-IBDDs, $\oplus$-OBDDs, and partitioned OBDDs, are compared with respect to the classes of functions with polynomial-size representations. Moreover, a tight hierarchy for the classes of polynomial-size partitioned OBDDs with k parts is proved.

Joint work with B. Bollig.