06111 Abstracts Collection
Complexity of Boolean Functions
— Dagstuhl Seminar —

Matthias Krause[1], Pavel Pudlak[2], Rüdiger Reischuk[3] and Dieter van Melkebeek[4]

[1] Univ. Mannheim, DE
krause@informatik.uni-mannheim.de
[2] Czech Academy of Sciences, Prague, CZ
pudlak@math.cas.cz
[3] Univ. Lübeck, DE
reischuk@tcs.uni-luebeck.de
[4] Univ. Wisconsin - Madison, US
dieter@cs.wisc.edu

Abstract. From 12.03.06 to 17.03.06, the Dagstuhl Seminar 06111 "Complexity of Boolean Functions" was held in the International Conference and Research Center (IBFI), Schloss Dagstuhl. During the seminar, several participants presented their current research, and ongoing work and open problems were discussed. Abstracts of the presentations given during the seminar as well as abstracts of seminar results and ideas are put together in this paper. The first section describes the seminar topics and goals in general. Links to extended abstracts or full papers are provided, if available.

Keywords. Complexity of Boolean functions, Boolean circuits, binary decision diagrams, lower bound proof techniques, combinatorics of Boolean functions, communication complexity, propositional proof complexity, algorithmic learning, cryptography, derandomization

06111 Executive Summary – Complexity of Boolean Functions

We briefly describe the state of the art concerning the complexity of discrete functions. Computational models and analytical techniques are summarized. After describing the formal organization of the Dagstuhl seminar "Complexity of Boolean Functions" held in March 2006, we introduce the different topics that have been discussed there and mention some of the major achievements. The summary closes with an outlook on the development of discrete computational complexity in the future.

Keywords: Boolean and quantum circuits, discrete problems, computational complexity, lower bounds, communication complexity, proof and query complexity, randomization, pseudo-randomness, derandomization, approximation, cryptography, computational learning

Dagstuhl Seminar Proceedings 06111
Complexity of Boolean Functions
http://drops.dagstuhl.de/opus/volltexte/2006/759

Joint work of: Krause, Matthias; van Melkebeek, Dieter, Pudlák, Pavel; Reischuk, Rüdiger

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/840

The optimal sequence compression

Alexander E. Andreev (LSI Logic Corp. - Milpitas, USA)

This paper presents the optimal compression for sequences with undefined values.

Let we have $(N-m)$ undefined and m defined positions in the boolean sequence V of length N. The sequence code length can't be less then m in general case, otherwise at least two sequences will have the same code. We present the coding algorithm which generates codes of almost m length, i.e. almost equal to the lower bound. The paper presents the decoding circuit too. The circuit has low complexity which depends from the inverse density of defined values $D(V)=\frac{N}{m}$. The decoding circuit includes RAM and random logic. It performs sequential decoding. The total RAM size is proportional to the

$$\log\left(D(V)\right) \ ,$$

the number of random logic cells is proportional to

$$\log\log\left(D(V)\right) * \left(\log\log\log\left(D(V)\right)\right)^2 \ .$$

So the decoding circuit will be small enough even for the very low density sequences. The decoder complexity doesn't depend of the sequence length at all.

Keywords: Compression, partial boolean function

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/602

Approximability of Minimum AND-Circuits

Jan Arpe (Universität Lübeck, D)

Given a set of monomials, the MINIMUM AND-CIRCUIT problem asks for a circuit that computes these monomials using AND-gates of fan-in two and being of minimum size.

We prove that the problem is not polynomial time approximable within a factor of less than 1.0051 unless $\mathbf{P}=\mathbf{NP}$, even if the monomials are restricted to be of degree at most three. For the latter case, we devise several efficient approximation algorithms, yielding an approximation ratio of 1.278. For the general problem, we achieve an approximation ratio of $d-3/2$, where d is the degree of the largest monomial.

In addition, we prove that the problem is fixed parameter tractable with the number of monomials as parameter. Finally, we reveal connections between the MINIMUM AND-CIRCUIT problem and several problems from different areas.

Keywords: Optimization problems, approximability, automated circuit design

Joint work of: Arpe, Jan; Manthey, Bodo

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/603

Teaching Boolean Functions

Frank Balbach (Universität Lübeck, D)

Algorithmic learning of Boolean functions is a widely investigated field, whereas models for the dual notion of teaching are much less developed. We give an introduction to a common teaching model for Boolean concept classes based on a concept's teaching dimension. The teaching dimension is the minimum number of examples needed to uniquely specify the concept with respect to a given concept class. We present several basic results for this model and some of its variants.

Finally we argue that the teaching dimension model yields implausible results when applied to memory-limited learning algorithms or to learners providing feedback.

Keywords: Algorithmic learning theory, teaching dimension

Grid Graph Reachability Problems

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

We study the complexity of restricted versions of st-connectivity, which is the standard complete problem for **NL**. Grid graphs are a useful tool in this regard, since reachability on grid graphs is logspace equivalent to reachability in general planar digraphs, and reachability on certain classes of grid graphs gives natural examples of problems that are hard for $\mathbf{NC^1}$ under $\mathbf{AC^0}$ reductions but are not known to be hard for **L**.

In addition to explicating the structure of **L**, another of our goals is tho expand the class of digraphs for which connectivity can be solved in logspace, by building on the work of Jakoby *et al.* who showed that reachability in series-parallel digraphs is solvable in **L**.

We show that many of the natural restrictions on grid-graph reachability (GGR) are equivalent under $\mathbf{AC^0}$ reductions. For instance, undirected GGR, out-degree-one GGR, and indegree-one-outdegree-one GGR are all equivalent. These problems are also equivalent to the problem of determining whether a game position in HEX is a winning position, and to the maze reachability problem studied by Blum and Kozen.

Series-Parallel graphs are a special case of single-source single-sink planar dags. We show that reachability for such graphs logspace reduces to single-source single-sink acyclic grid graphs. We then show that reachability on such grid graphs $\mathbf{AC^0}$ reduces to undirected GGR.

Finally, we build on this to show that reachability for single-source multiple-sink planar dags is solvable in **L**.

Keywords: Graph reachability, **NL**, logspace, first-order reductions, $\mathbf{NC^1}$

Joint work of: Allender, Eric; Barrington, David A. Mix; Chakraborty, Tanmoy; Datta, Samir; Roy, Sambuddha

Parity

Jehoshua Bruck (CalTech - Pasadena, USA)

We review the notion of RAID (Reliable Array of Independent Disks) storage system and address the topic of creating redundancy to tolerate multiple disk failures. We present the concept of array codes: those are optimal (MDS) error correcting codes that are based on simple parity calculations. The array codes introduced are: EVENODD and B-CODE. We also discuss the Perfect-1-Factorization conjecture and its connection to constructing optimal array codes. Finally, we discuss the circuit complexity of parity and pose some open problems.

Keywords: RAID, array codes, parity, circuit complexity

Full Paper:
http://www.paradise.caltech.edu/papers/etr075.pdf

See also: V. Bohossian and J. Bruck, Shortening Array Codes and the Perfect 1-Factorization Conjecture, IEEE International Symposium on Information Theory, Seattle, WA, July 2006.

The complexity of Boolean functions from cryptographic viewpoint

Claude Carlet (Université de Paris VIII, F)

Cryptographic Boolean functions must be complex to satisfy Shannon's principle of confusion. But the cryptographic viewpoint on complexity is not the same as in circuit complexity.

The two main criteria evaluating the cryptographic complexity of Boolean functions on F_2^n are the nonlinearity (and more generally the r-th order nonlinearity, for every positive $r < n$) and the algebraic degree. Two other criteria have also been considered: the algebraic thickness and the non-normality. After recalling the definitions of these criteria and why, asymptotically, almost all Boolean functions are deeply non-normal and have high algebraic degrees, high (r-th order) nonlinearities and high algebraic thicknesses, we study the relationship between the r-th order nonlinearity and a recent cryptographic criterion called the algebraic immunity. This relationship strengthens the reasons why the algebraic immunity can be considered as a further cryptographic complexity criterion.

Keywords: Symmetric cryptography, Boolean functions, nonlinearity, algebraic degree, Reed-Muller code

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/604

Some Remarks on Combining McEliece's Cryptosystem with List-Decoding

Carsten Damm (Universität Göttingen, D)

In 1978 McEliece proposed a knapsack-like public key cryptostem that is based on error-correcting codes, in particular Goppa-Codes. So far no serious attack against the key is known, but the system is vulnerable to message resend attacks. The attack relies on the bad (designed) distance to length ratio that Goppa-Codes have. Replacing Goppa-Codes by generalized Reed-Solomon-Codes (GRS) that offer better performance turned out to be no solution, since being MDS they have too much exploitable structure. In a 2005 paper Berger and Loidreau demonstrated that by using subcodes of GRS the single known key recovering attack cannot be mounted anymore. We observed that the security of the system based on Berger/Loidreau's codes against all known decryption attacks can be improved by the use of list-decoding. The idea generalizes to all efficiently list-decodable codes that have small average lengh of decoding lists.

Joint work of: Damm, Carsten; Rühaak, Jan

Time-Space Lower Bounds for the Polynomial-Time Hierarchy on Randomized Machines

Scott Diehl (University of Wisconsin - Madison, USA)

In this talk, we establish lower bounds for the running time of randomized machines with two-sided error which use a small amount of workspace to solve complete problems in the polynomial-time hierarchy. In particular, we show that for integers $l > 1$, a randomized machine with two-sided error using subpolynomial space requires time $n^{l-o(1)}$ to solve QSATl, where QSATl denotes the problem of deciding the validity of a Boolean first-order formula with at most $l - 1$ quantifier alternations. This represents the first time-space lower bounds for complete problems in the polynomial-time hierarchy on randomized machines with two-sided error.

Corresponding to $l = 1$, we show that a randomized machine with one-sided error using subpolynomial space requires time $n^{1.759}$ to decide the set of Boolean tautologies. As a corollary, this gives the same lower bound for satisfiability on deterministic machines, improving on the previously best known such result.

Keywords: Time-space lower bounds, lower bounds, randomness, polynomial-time hierarchy

Joint work of: Diehl, Scott; van Melkebeek, Dieter

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/605

Full Paper:
http://www.cs.wisc.edu/~sfdiehl/060517.pdf

A characterization of average case communication complexity

Martin Dietzfelbinger (TU Ilmenau, D)

We consider the average case deterministic communication complexity $D^0_\mu(f)$ of functions f with respect to error-free protocols and arbitrary input distributions μ.

It is well known that $E(|\Pi(X,Y)|)$ (the expected number of bits transmitted when carrying out protocol Π) is bounded below by the entropy H_Π of the distribution induced on the leaves of the protocol. Thus, the quantity $IC_\mu(f) = \min\{H_\Pi \mid \Pi \text{ computes } f\}$, which could be called the *deterministic information complexity* of f, satisfies $D^0_\mu(f) \geq IC_\mu(f)$. We show that this bound is tight up to a constant factor.

Further, using H_Π we improve known lower bounds for the public coin Las Vegas communication complexity by a constant factor and for some functions obtain tight lower bounds not noted before.

Keywords: Communication complexity, information cost, zero-error protocols

Joint work of: Dietzfelbinger, Martin; Wunderlich, Henning

Regularity and robustness of graph partitions

Eldar Fischer (Technion - Haifa, IL)

Szemeredi's Regularity Lemma states that the vertices of any graph can be partitioned in a way that for most pairs of the partition sets, the edges between them satisfy a strong uniformity property. This lemma from the late seventies has seen many uses in combinatorics and theoretical computer science (unfortunately, the full version of the lemma does not allow for practical uses because of the constants involved).

Property testing deals with algorithms that read only a small portion of the input, and distinguish between the case that the input satisfies a given property and the case that it is far from satisfying it. Motivated by applications to property testing of graphs, stronger versions of the lemma had to be formulated and used.

The search for stronger notions of regularity has leads to the definition of robust partitions. This framework allows to unify and generalize previous notions. On the other hand, it also shows how the regular partitions of a graph can be analyzed based only on a small sample of the graph.

In this talk I will give a short survey on the Regularity Lemma and its use in property testing, and then present the framework of robust partitions and its applications.

The talk is mainly based on a joint work with Ilan Newman.

Worst-Case Running Times for Average-Case Algorithms

Lance Fortnow (University of Chicago, USA)

Under a standard hardness assumption we exactly characterize the worst-case running time of languages that are in average polynomial-time over all polynomial-time sampleable distributions.

More precisely we show that if exponential time does not have subexponential-size circuits with Σ_2 gates, then the following are equivalent for any algorithm A:

- For all **P**-sampleable distributions u, A runs in time polynomial on u-average.
- For some polynomial p, the running time for A is bounded by
$$2^{O(K^p(x)-K(x)+\log(|x|)}$$
for *all* inputs x.

To prove this result we explore the time-bounded Kolmogorov distribution, $m^t(x) = 2^{-K^t(x)}$ where $K^t(x)$ is the Kolmogorov complexity (smallest program size to generate x) with programs limited to run in time $t(|x|)$ and show that under the hardness assumption, the time-bounded Kolmogorov distribution is a universal sampleable distribution.

Joint work of: Antunes, Luis; Fortnow, Lance

Full Paper:
http://eccc.hpi-web.de/eccc-reports/2005/TR05-144/Paper.pdf

Hadamard Tensors and Lower Bounds on Multiparty Communication Complexity

Anna Gál (Univ. of Texas at Austin, USA)

We develop a new method for estimating the discrepancy of tensors associated with multiparty communication problems in the "Number on the Forehead" model of Chandra, Furst and Lipton.

We define an analogue of the Hadamard property of matrices for tensors in multiple dimensions and show that any k-party communication problem represented by a Hadamard tensor must have $\Omega(n/2^k)$ multiparty communication complexity.

We also exhibit constructions of Hadamard tensors, giving $\Omega(n/2^k)$ lower bounds on multiparty communication complexity for a new class of explicitly defined Boolean functions.

Keywords: Multiparty communication complexity, lower bounds

Joint work of: Ford, Jeff; Gál, Anna

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/607

The Cell Probe Complexity of Succinct Data Structures

Anna Gál (Univ. of Texas at Austin, USA)

In the cell probe model with word size 1 (the bit probe model), a static data structure problem is given by a map $f : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}$, where $\{0,1\}^n$ is a set of possible data to be stored, $\{0,1\}^m$ is a set of possible queries (for natural problems, we have $m \ll n$) and $f(x,y)$ is the answer to question y about data x.

A solution is given by a representation $\phi : \{0,1\}^n \to \{0,1\}^s$ and a query algorithm q so that $q(\phi(x),y) = f(x,y)$. The time t of the query algorithm is the number of bits it reads in $\phi(x)$.

In this paper, we consider the case of *succinct* representations where $s = n+r$ for some *redundancy* $r \ll n$. For a boolean version of the problem of polynomial evaluation with preprocessing of coefficients, we show a lower bound on the redundancy-query time tradeoff of the form

$$(r+1)t \geq \Omega(n/\log n).$$

In particular, for very small redundancies r, we get an almost optimal lower bound stating that the query algorithm has to inspect almost the entire data structure (up to a logarithmic factor). We show similar lower bounds for problems satisfying a certain combinatorial property of a coding theoretic flavor. Previously, no $\omega(m)$ lower bounds were known on t in the general model for explicit functions, even for very small redundancies.

By restricting our attention to *systematic* or *index* structures ϕ satisfying $\phi(x) = x \cdot \phi^*(x)$ for some map ϕ^* (where $\cdot$ denotes concatenation) we show similar lower bounds on the redundancy-query time tradeoff for the natural data structuring problems of Prefix Sum and Substring Search.

Keywords: Cell probe model, data structures, lower bounds, time-space tradeoffs

Joint work of: Gál, Anna; Miltersen, Peter Bro

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/606

On the Correlation Between Mod_q and Log-degree Polynomials mod m

Frederic Green (Clark University - Worcester, USA)

We prove that the correlation between the Mod_q function and polynomials mod m is exponentially small, provided $q, m \in \mathbf{Z}^+$ are relatively prime and the degree of the polynomials is $O(\log n)$, where the constant depends on q and m.

This in turn implies that in order to compute the Mod_q function, circuits consisting of a threshold at the top, Mod_m gates in the middle layer, and $O(\log n)$ fan-in AND gates at the inputs must have exponential size.

The result follows from a study of exponential sums of the form

$$S = 2^{-n} \sum_{x \in \{0,1\}^n} e^{2\pi i h(x)/q} e^{2\pi i p(x)/m},$$

where p is a polynomial with coefficients in $\mathbf{Z}_m$, and $h(x) = a(x_1 + \cdots + x_n)$ for some $1 \leq a < q$. We prove an upper bound of the form $2^{-\Omega(n)}$ on $|S|$. Upper bounds of the form 2^{-n^ϵ} hold if one allows the degree of the polynomial to be $O(\log n)$. This generalizes a result of J. Bourgain, who establishes this bound in the case where m is odd.

Keywords: Circuit complexity, lower bounds, number theory

Joint work of: Green, Frederic; Roy, Amitabha; Straubing, Howard

See also: C. R. Acad. Sci. Paris, Ser. I 340 (2005)

Minimization of DNF Formulas Given a Truth Table

Lisa Hellerstein (Polytechnic Univ. - New York, USA)

A classical problem in logic minimization is to find the smallest DNF formula consistent with a given truth table. We call this problem minDNF. It is well-known that minDNF is a special case of Set Cover, and that the standard greedy set cover heuristic can be used to obtain an approximate solution to minDNF that is within a factor $O(n)$ of optimal, where n is the number of variables on which the function is defined.

In the 1970's, Masek showed that minDNF is **NP**-complete. However, few people have taken the time to understand his proof, which consists of a gadget-based reduction from Circuit-SAT. We begin by presenting a new and simpler proof that minDNF is **NP**-complete, by reduction from 3-Partite Set Cover. We then show that unless **NP** is contained in quasipolynomial time, there is an absolute constant $\delta < 1$ such that minDNF cannot be approximated to within a factor $O(n^\delta)$ of optimal.

We also construct an instance of minDNF on which the greedy set cover heuristic produces a solution that is $\Omega(n)$ larger than optimal.

The material in this talk is contained in a paper coauthored with Eric Allender, Paul McCabe, Toni Pitassi, and Michael Saks.

An algorithm for a generalized maximum subsequence problem.

Thomas Hofmeister (Universität Dortmund, D)

We consider a generalization of the maximum subsequence problem. Given an array $a_1, \ldots, a_n$ of real numbers, the generalized problem consists in finding an interval $[i, j]$ such that the length and the sum of the subsequence $a_i, \ldots, a_j$ maximize a given quasiconvex function f.

Problems of this type occur, e.g., in bioinformatics. We show that the generalized problem can be solved in time $O(n \log n)$.

As an example, we show how the so-called multiresolution criteria problem can be solved in time $O(n \log n)$.

Joint work of: Hofmeister, Thomas; Bernholt, Thorsten

See also: Thorsten Bernholt, Thomas Hofmeister: An algorithm for a generalized maximum subsequence problem, 7th Latin American Theoretical Informatics Symposium (LATIN), 2006, pages 178-189.

Quantum Network Coding

Kazuo Iwama (Kyoto University, J)

Since quantum information is continuous, its handling is sometimes surprisingly harder than the classical counterpart. A typical example is cloning; making a copy of digital information is straightforward but it is not possible exactly for quantum information. The question in this paper is whether or not *quantum* network coding is possible. Its classical counterpart is another good example to show that digital information flow can be done much more efficiently than conventional (say, liquid) flow.

Our answer to the question is similar to the case of cloning, namely, it is shown that quantum network coding is possible if approximation is allowed, by using a simple network model called Butterfly. In this network, there are two flow paths, s_1 to t_1 and s_2 to t_2, which shares a single bottleneck channel of capacity one. In the classical case, we can send two bits simultaneously, one for each path, in spite of the bottleneck. Our results for quantum network coding include: (i) We can send any quantum state $|\psi_1\rangle$ from s_1 to t_1 and $|\psi_2\rangle$ from s_2 to t_2 simultaneously with a fidelity strictly greater than 1/2. (ii) If one of $|\psi_1\rangle$ and $|\psi_2\rangle$ is classical, then the fidelity can be improved to 2/3. (iii) Similar improvement is also possible if $|\psi_1\rangle$ and $|\psi_2\rangle$ are restricted to only a finite number of (previously known) states. (iv) Several impossibility results including the general upper bound of the fidelity are also given.

Keywords: Network coding, quantum computation, quantum information

Joint work of: Hayashi, Masahito; Iwama, Kazuo; Nishimura, Harumichi; Raymond, Rudy; Yamashita, Shigeru

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/608

Revealing Additional Information in Two-Party Computations

Andreas Jakoby (Universität Frankfurt, D)

A two-argument function is computed privately by two parties if after the computation, no party should know anything about the other inputs except for what he is able to deduce from his own input and the function value. 1993 Bar-Yehuda, Chor, Kushilevitz, and Orlitsky give a complete characterisation of two-argument functions which can be computed privately (in the information-theoretical sense) in the Honest-But-Curious model and study protocols for "non-private" functions revealing as little information about the inputs as possible. The authors define a measure which determines for any function f the additional information $\mathcal{E}(f)$ required for computing f and claim that f is privately-computable if and only if $\mathcal{E}(f) = 0$. In our paper we show that the characterisation is false: we give a privately-computable function f with $\mathcal{E}(f) \neq 0$ and another function g with $\mathcal{E}(g) = 0$ that is *not* privately-computable. Moreover, we show some rather unexpected and strange properties of the measure for additional information given by Bar-Yehuda et al. and we introduce an alternative measure. We show that for this new measure the minimal leakage of information of randomized and deterministic protocols are equal. Finally, we present some general relations between the information gain of an optimal protocol and the communication complexity of a function.

Joint work of: Jakoby, Andreas; Liśkiewicz, Maciej

Disproving the Single Level Conjecture for Quadratic Functions and Graphs

Stasys Jukna (Universität Frankfurt, D)

We consider the size of monotone circuits for quadratic boolean functions, that is, for disjunctions of length-2 monomials: $f(x_1, \ldots, x_n) = \bigvee_{ij \in E} x_i x_j$. Such functions are related to the circuit complexity of graphs.

Our motivation is that a good (linear in the number n of variables) lower bound on the monotone circuit size for graphs as well as for a certain type of quadratic function would imply a good (even exponential) lower bound on the general non-monotone(!) circuit size. In particular, a lower bound of the form n^c for an arbitrary small constant $c > 0$ in the class of depth-3 circuits would imply a superlinear lower bound for $\mathbf{NC^1}$ circuits (non-monotone log-depth circuits).

We first consider monotone circuits with fanin-2 gates. Razborov's method (and its derivatives) cannot yield lower bounds larger than n. To get more insight into the structure of monotone circuits for quadratic functions we consider the so-called "single level conjecture". A *single level circuit* is a circuit which has only one level of AND gates. For example, every quadratic function can be computed by a single level circuit $f = \bigvee_{i=1}^{n} x_i \wedge \left(\bigvee_{j:ij\in E} x_j\right)$ with only n AND gates.

Single Level Conjecture: *Monotone single level circuits for quadratic functions are almost optimal.*

A strong support for the conjecture was given by Mirwald and Schnorr in 1987: if we consider circuits over $\{\oplus, \wedge, 1\}$ for quadratic functions $f = \sum_{ij} a_{ij} x_i x_j$ over GF(2) and count only AND gates, then every optimal circuit is a single level circuit! Thus, the *algebraic* version of the conjecture is true in a very strong sense.

Motivated by this result, the *boolean* version of the conjecture for circuits over $\{\vee, \wedge, 0, 1\}$ was then considered by several authors, but no (even constant) gap $Gap(n) > 1$ between the single level and general circuit complexities was known.

In this talk we disprove the boolean version of the conjecture by showing an almost maximal gap: $Gap(n) = \Omega(n/\log^3 n)$. Similar gaps are established for the multiplicative complexity as well as for formulas. For this purpose we use the quadratic functions of Kneser and Sylvester graphs.

We then consider the single level conjecture for *unbouded fanin* circuits. Single level circuits are then precisely the depth-3 circuits. We show that depth-3 circuits for quadratic functions may be by a factor $\sqrt{\log n}$ worse than general (monotone) circuits. The same gap is also shown for graphs. This gives a partial answer to a question raised by Pudlak, Rodl and Savicky in 1986.

We conclude with an open problem. Let $f(x, y)$ be a boolean function in $2n$ variables. Say that f is *ϵ-good* if its communication matrix has at least $2^{(1+\epsilon)n}$ zeroes and contains no 2×2 all-0 submatrix.

Let $NCC(f)$ be the nondeterministic communication complexity of f.

Problem $P(\epsilon)$**:** *Does $NCC(f) = \Omega(n)$ for every ϵ-good function f?*

If true for some constant $\epsilon < 1/2$ this would imply a super-linear lower bound for $\mathbf{NC^1}$-circuits. (For $\epsilon = 1/2$ the answer is *yes*.)

Keywords: Quadratic functions, boolean sums, graph complexity, clique covering number, Kneser graph, Sylvester graph

Very Large Cliques are Easy to Detect

Stasys Jukna (Universität Frankfurt, D)

It is known that, for every constant $k \geq 3$, the presence of a k-clique (a complete subgraph on k vertices) in an n-vertex graph cannot be detected by a monotone boolean circuit using fewer than $\Omega((n/\log n)^k)$ gates. We show that, for every constant k, the presence of an $(n-k)$-clique in an n-vertex graph can be detected by a monotone circuit using only $O(n^2 \log n)$ gates.

Moreover, if we allow unbounded fanin, then $O(\log n)$ gates are enough.

Keywords: Clique function, monotone circuits, perfect hashing

Joint work of: Andreev, Alexander; Jukna, Stasys

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/609

Graphs and Circuits: Some Further Remarks

Stasys Jukna (Universität Frankfurt, D)

We consider the power of single level circuits in the context of graph complexity. We first prove that the single level conjecture fails for fanin-2 circuits over the basis $\{\oplus, \wedge, 1\}$.

This shows that the (surpisingly tight) phenomenon, established by Mirwald and Schnorr (1992) for quadratic functions, has no analogon for graphs. We then show that the single level conjecture fails for unbounded fanin circuits over $\{\vee, \wedge, 1\}$. This partially answers the question of Pudlák, Rödl and Savický (1986). We also prove that $\Sigma_2 \neq \Pi_2$ in a restricted version of the hierarhy of communication complexity classes introduced by Babai, Frankl and Simon (1986). Further, we show that even depth-2 circuits are surprisingly powerful: every bipartite $n \times n$ graph of maximum degree Δ can be represented by a monotone CNF with $O(\Delta \log n)$ clauses. We also discuss a relation between graphs and **ACC**-circuits.

Keywords: Graph complexity, single level conjecture, Sylvester graphs, communication complexity, **ACC**-circuits

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/621

Approximate list-decoding and hardness amplification

Valentine Kabanets (Simon Fraser University, CA)

Error-correcting codes have found many applications in complexity theory. For example, codes are used for amplifying computational hardness of hard functions, which in turn are useful as the building blocks of pseudorandom generators that allow to convert any randomized polytime algorithm into a deterministic polytime algorithm.

On the other hand, complexity theory has hardness amplification tools which (a priori) do not seem to be based on error-correcting codes. One such tool is the classical XOR Lemma of Yao that says, roughly, that if a Boolean function f is hard to compute, then computing f on k independent inputs is exponentially in k harder. This lemma can be interpreted in terms of error-correcting codes, giving rise to codes which are approximately list-decodable. That is, given a corrupted codeword corresponding to a message msg where the fraction of corrupted bits is at most $1/2-\epsilon$, it is possible to construct a small list of words that contains at

least one word that agrees with msg in many bit positions. The known proofs of Yao's XOR Lemma give approximate list-decoding algorithms with the list size that is exponential in $(1/\epsilon)$, whereas the optimal list size should be polynomial in $(1/\epsilon)$.

Our main result is the list-decoding algorithm that achieves the list-size polynomial in $(1/\epsilon)$, but works only for "large" ϵ. Our proof uses a somewhat counter-intuitive reduction to a generalization of the classical approximate list-decoding algorithm by Impagliazzo and Wigderson. We also give an application of our list-decoding algorithm to the problem of hardness amplification within polynomial hierarchy.

Keywords: Error-correcting codes, list-decoding, hardness amplification

Joint work of: Impagliazzo, Russell; Jaiswal, Ragesh (UCSD)

Secure Two-party Computation of Matrix Singularity with Low Communication and Round Complexity

Eike Kiltz (CWI - Amsterdam, NL)

In this work we present secure two-party protocols for various core problems in linear algebra. Our main building block is a protocol to obliviously decide singularity of an encrypted matrix:

Bob holds an $n \times n$ matrix M, encrypted with Alice's secret key, and wants to learn whether the matrix is singular or not (and nothing beyond that). We give an interactive protocol between Alice and Bob that solves the above problem with optimal communication complexity while at the same time achieving low round complexity.

More precisely, the number of communication rounds in our protocol is polylog(n) and the overall communication is roughly $O(n^2)$ (note that the input size is n^2). At the core of our protocol we exploit some nice mathematical properties of linearly recurrent sequences and their relation to the characteristic polynomial of the matrix M, following [Wiedemann, 1986]. With our new techniques we are able to improve the round complexity of the communication efficient solution of [Nissim and Weinreb, 2006] from $n^{0.275}$ to polylog(n).

Based on our singularity protocol we further extend our result to the problems of securely computing the rank of an encrypted matrix and solving systems of linear equations.

Keywords: Secure Linear Algebra, Linearly Recurrent Sequences, Wiedemann's Algorithm

Joint work of: Kiltz, Eike; Weinreb, Enav

Secure Linear Algebra Using Linearly Recurrent Sequences

Eike Kiltz (CWI - Amsterdam, NL)

In this work we present secure two-party protocols for various core problems in linear algebra.

Our main building block is a protocol to obliviously decide singularity of an encrypted matrix: Bob holds an $n \times n$ matrix M, encrypted with Alice's secret key, and wants to learn whether the matrix is singular or not (and nothing beyond that). We give an interactive protocol between Alice and Bob that solves the above problem with optimal communication complexity while at the same time achieving low round complexity. More precisely, the number of communication rounds in our protocol is polylog(n) and the overall communication is roughly $O(n^2)$ (note that the input size is n^2). At the core of our protocol we exploit some nice mathematical properties of linearly recurrent sequences and their relation to the characteristic polynomial of the matrix M, following [Wiedemann, 1986]. With our new techniques we are able to improve the round complexity of the communication efficient solution of [Nissim and Weinreb, 2006] from $n^{0.275}$ to polylog(n).

Based on our singularity protocol we further extend our result to the problems of securely computing the rank of an encrypted matrix and solving systems of linear equations.

Keywords: Secure Linear Algebra, Linearly Recurrent Sequences, Wiedemann's Algorithm

Joint work of: Kiltz, Eike; Weinreb, Enav

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/610

High-entropy random selection protocols

Michal Koucký (Academy of Sciences - Prague, CZ)

We consider the problem of generating a random string by mutually distrusting parties. We present a protocol for two parties that guarantees the entropy of the outcome to be at least $n - O(1)$ even if one of the parties deviates from the protocol. This protocol runs in $\log^* n$ rounds and communicates $O(n^2)$ bits. Furthemore, we present a three-round protocol that guarantees the output entropy to be at least $3n/4$ and that communicates $O(n)$ bits. We present a connection of our protocol to Kakeya problem.

Keywords: Random string selection, leader election

Joint work of: Buhrman, Harry; Vereshchagin, Kolia; Lotker, Zvi; Patt-Shamir, Boaz; Christandl, Matthias; Lee, Troy; Tromp, John; Koucký, Michal

Pseudorandom generators and fault cryptanalysis

Miroslaw Kutylowski (Institute of Mathematics & Informatics/TU Wroclaw, PL)

We present fault attacks on pseudorandom bit generators such as A5/1 and Krawczyk's shrinking generator.

The attacks turn out to be very efficient, provided that one can insert a fault in a hardware bit generator. This shows that either one has to pay a lot of attention to hardware design or to take into acount that the secret key stored in a device may be retreived even if the device is tamper resistant.

Keywords: Pseudorandom bit generator, shrinking generator, A5/1, fault cryptanalysis

Full Paper:
http://kutylowski.im.pwr.wroc.pl/bib-html.html#hardwarecrypto

Fault Jumping Attacks against Shrinking Generator

Miroslaw Kutylowski (Institute of Mathematics & Informatics/TU Wroclaw, PL)

In this paper we outline two new cryptoanalytic attacks against hardware implementation of the shrinking generator by Coppersmith et al., a classic design in low-cost, simple-design pseudorandom bitstream generator.

This is a report on work on progress, since implementation and careful adjusting the attack strategy in order to optimize the atatck is still not completed.

Keywords: Pseudorandom generator, shrinking generator, fault cryptanalysis

Joint work of: Gomulkiewicz, Marcin; Kutylowski, Miroslaw; Wlaz, Pawel

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/611

Using Quantum Oblivious Transfer to Cheat Sensitive Quantum Bit Commitment

Maciej Liśkiewicz (Universität Lübeck, D)

We define (ε, δ)-secure quantum computations between two parties that can play dishonestly to maximise advantage δ, however keeping small the probability ε that the computation fails in evaluating correct value.

We present a simple quantum protocol for computing one-out-of-two oblivious transfer that is $(O(\sqrt{\varepsilon}), \varepsilon)$-secure.

Using the protocol as a black box we construct a scheme for cheat sensitive quantum bit commitment which guarantee that a mistrustful party has a nonzero probability of detecting a cheating.

Keywords: Two-Party Computations, Quantum Protocols, Bit Commitment, Oblivious Transfer

Joint work of: Jakoby, Andreas; Liśkiewicz, Maciej; Madry, Aleksander

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/622

Incremental branching programs

Pierre McKenzie (Université de Montréal, CA)

We propose a new model of restricted branching programs which we call *incremental branching programs*.

We show that *syntactic* incremental branching programs capture previously studied structured models of computation for the problem GEN, namely marking machines [Cook74]. and Poon's extension [Poon93] of jumping automata on graphs [CookRackoff80]. We then prove exponential size lower bounds for our syntactic incremental model, and for some other restricted branching program models as well. We further show that nondeterministic syntactic incremental branching programs are provably stronger than their deterministic counterpart when solving a natural **NL**-complete GEN subproblem.

It remains open if syntactic incremental branching programs are as powerful as unrestricted branching programs for GEN problems.

Keywords: Complexity theory, branching programs, logarithmic space, marking machines

Joint work of: Gál, Anna; McKenzie, Pierre; Koucký, Michal

The Complexity of Numerical Analysis

Peter Bro Miltersen (Univ. of Aarhus, DK)

We study two quite different approaches to understanding the complexity of fundamental problems in numerical analysis. We show that both hinge on the question of understanding the complexity of the following problem, which we call PosSlp: Given a division-free straight-line program producing an integer N, decide whether $N > 0$. We show that OrdSlp lies in the counting hierarchy, and combining our results with work of Tiwari, we show that the Euclidean Traveling Salesman Problem lies in the counting hierarchy – the previous best upper bound for this important problem (in terms of classical complexity classes) being **PSPACE**.

Keywords: Blum-Shub-Smale Model, Euclidean Traveling Salesman Problem, Counting Hierarchy

Joint work of: Allender, Eric; Bürgisser, Peter; Kjeldgaard-Pedersen, Johan; Miltersen, Peter Bro

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/613

A non-trivial $(1-\epsilon)$ approximation for max sat.

Ilan Newman (Haifa University, IL)

We give an algorithm that given ϵ and a general CNF formula over n variables, it approximate the number of clauses that are simultaneously satisfiable up to a factor of $1-\epsilon$ in expected time that is c^n where $c = c(\epsilon) < 2$.

Hirsch (2000) such an algorithm that approximates max-sat but for k-CNF where $k = O(1)$. Previously to this, there was no algorithm for approximating max-sat in the general case, of running time c^n for $c < 2$.

Keywords: Max sat, non trivial algorithm

Joint work of: Newman, Ilan; Wolfovich, Guy

Narrow Proofs May Be Spacious: Separating Space and Width in Resolution

Jakob Nordström (KTH Stockholm, S)

The width of a resolution proof is the maximal number of literals in any clause of the proof. The space of a proof is the maximal number of memory cells used if the proof is only allowed to resolve on clauses kept in memory. Both of these measures have previously been studied and related to the refutation size of unsatisfiable CNF formulas. Also, the resolution refutation space of a formula has been proven to be at least as large as the refutation width, but it has remained unknown whether space can be separated from width or the two measures coincide asymptotically. We prove that there is a family of k-CNF formulas for which the refutation width in resolution is constant but the refutation space is non-constant, thus solving an open problem mentioned in several previous papers.

Keywords: Proof complexity, resolution, width, space, separation, lower bound, pebble game, pebbling contradiction

Full Paper:
http://eccc.hpi-web.de/eccc-reports/2005/TR05-066/Paper.pdf

See also: Jakob Nordström. Narrow proofs may be spacious: Separating space and width in resolution. Technical Report TR05-066, Revision 02, Electronic Colloquium on Computational Complexity (ECCC), Nov. 2005. Extended abstract to appear in STOC '06.

A Generic Time Hierarchy for Semantic Models With One Bit of Advice

Konstantin Pervyshev (Steklov Inst. - St. Petersburg, RUS)

We show that for any reasonable semantic model of computation and for any positive integer a and rationals $1 \leq c < d$, there exists a language computable in time n^d with a bits of advice but not in time n^c with a bits of advice. A semantic model is one for which there exists a computable enumeration that contains all machines in the model but may also contain others. We call such a model reasonable if it has an efficient universal machine that can be complemented within the model in exponential time and if it is efficiently closed under deterministic transducers. Our result implies the first such hierarchy theorem for randomized machines with zero-sided error, quantum machines with one- or zero-sided error, unambiguous machines, symmetric alternation, Arthur-Merlin games of any signature, etc. Our argument yields considerably simpler proofs of known hierarchy theorems with one bit of advice for randomized and quantum machines with two-sided error. Our paradigm also allows us to derive stronger separation results in a unified way. For models that have an efficient universal machine that can be simulated deterministically in exponential time and that are efficiently closed under randomized reductions with two-sided error, we establish the following: For any constants a and c, there exists a language computable in polynomial time with one bit of advice but not in time n^c with $a \log n$ bits of advice. In particular, we obtain such separation for randomized and quantum machines with two-sided error. For randomized machines with one-sided error, we get that for any constants a and c there exists a language computable in polynomial time with one bit of advice but not in time n^c with $a(\log n)^{1/c}$ bits of advice.

Keywords: Time hierarchy; non-uniformity; one bit of advice; probabilistic algorithms

Joint work of: van Melkebeek, Dieter; Pervyshev, Konstantin

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/615

Classical vs. Quantum Read-Once BPs

Martin Sauerhoff (Universität Dortmund, D)

A simple, explicit boolean function on $2n$ input bits is presented that is computable by errorfree quantum read-once branching programs of size $O(n^3)$, while each classical randomized read-once branching program and each quantum OBDD for this function with bounded two-sided error requires size $2^{\Omega(n)}$.

Keywords: Quantum branching program, randomized branching program, read-once
Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/616

2-source dispersers for $n^{o(1)}$-entropy and Ramsey graphs beating the Frankl-Wilson construction

Ronen Shaltiel (Haifa University, IL)

The main result of this talk is an explicit disperser for two independent sources on n bits, each of entropy $k = n^{o(1)}$. Put differently, setting $N = 2^n$ and $K = 2^k$, we construct explicit $N \times N$ Boolean matrices for which no $K \times K$ submatrix is monochromatic. Viewed as adjacency matrices of bipartite graphs, this gives an explicit construction of K-Ramsey bipartite graphs of size N.

This greatly improves the previous the previous bound of $k = o(n)$ of Barak, Kindler, Shaltiel, Sudakov and Wigderson. It also significantly improves the 25-year record of $k = \tilde{O}(\sqrt{n})$ on the very special case of Ramsey graphs, due to Frankl and Wilson.

The construction uses (besides "classical" extractor ideas) almost all of the machinery developed in the last couple of years for extraction from independent sources.

The main novelty comes in a bootstrap procedure which allows the Challenge-Response mechanism of Barak, Kindler, Sudakov, Shaltiel and Wigderson to be used with sources of less and less entropy, using recursive calls to itself. Subtleties arise since the success of this mechanism depends on restricting the given sources, and so recursion constantly changes the original sources. These are resolved via a new construct, in between a disperser and an extractor, which behaves like an extractor on sufficiently large subsources of the given ones.

Keywords: Ramsey graphs, Randomness extractors, Dispersers

Joint work of: Barak, Boaz; Rao, Anup; Wigderson, Avi

Bounds on the Fourier Coefficients of the Weighted Sum Function

Igor Shparlinski (Macquarie Univ. - Sydney, AU)

We estimate Fourier coefficients of a Boolean function which has recently been introduced in the study of read-once branching programs. Our bound implies that this function has an asymptotically "flat" Fourier spectrum and thus implies several lower bounds of its various complexity measures.

Keywords: Fourier coefficients, congruences, average sensitivity, decision tree

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/617

Computing Shortest Paths in Series-Parallel Graphs in Logarithmic Space

Till Tantau (Universität Lübeck, D)

Series-parallel graphs, which are built by repeatedly applying series or parallel composition operations to paths, play an important role in computer science as they model the flow of information in many types of programs. For directed series-parallel graphs, we study the problem of finding a shortest path between two given vertices. Our main result is that we can find such a path in logarithmic space, which shows that the distance problem for series-parallel graphs is **L**-complete. Previously, it was known that one can compute some path in logarithmic space; but for other graph types, like undirected graphs or tournament graphs, constructing some path between given vertices is possible in logarithmic space while constructing a shortest path is **NL**-complete.

Keywords: Series-parallel graphs, shortest path, logspace

Joint work of: Jakoby, Andreas; Tantau, Till

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/618

On the perfect matching problem

Thomas Thierauf (FH Aalen, D)

The perfect matching problem is known to be in **P**, and in randomized **NC**. Wheteher the perfect matching problem is in **NC** is one of the most prominent open questions in complexity theory regarding parallel computations. Grigoriev and Karpinski studied the perfect matching problem for bipartite graphs with polynomially bounded permanent. They showed that the problem of counting the number of perfect matchings in such bipartite graphs is in $\mathbf{NC^3}$. We improve this upper bound to $\mathbf{NC^2}$.

Keywords: Perfect matching, polynomially bounded permanent

Joint work of: Hoang, Minh Thanh; Thierauf, Thomas

Group-theoretic Algorithms for Matrix Multiplication

Chris Umans (CalTech - Pasadena, USA)

We present a group-theoretic approach to producing fast algorithms for matrix multiplication. In this framework, one devises algorithms by constructing non-abelian groups with certain properties. The algorithms themselves are natural and are based on taking the discrete Fourier transform over these groups.

We construct several families of groups that achieve matrix multiplication exponent significantly less than 3 (but not better than the current best bound, 2.376 . . .). This leads to two appealing conjectures, one combinatorial and the other algebraic. Either one would imply that the exponent of matrix multiplication is 2.

Joint work of: Cohn, Henry; Kleinberg, Bobby; Szegedy, Balazs; Umans, Chris

Full Paper:
http://www.cs.caltech.edu/∼umans/papers/CKSU05.pdf

On Probabilistic Time versus Alternating Time

Emanuele Viola (Harvard University, USA)

Sipser and Gács, and independently Lautemann, proved in '83 that probabilistic polynomial time is contained in the second level of the polynomial-time hierarchy, i.e. BPP is in $\Sigma_2 P$. This is essentially the only non-trivial upper bound that we have on the power of probabilistic computation. More precisely, the Sipser-Gács-Lautemann simulation shows that probabilistic time can be simulated deterministically, using two quantifiers, *with a quadratic blow-up in the running time*. That is, BPTime(t) is contained in Σ_2Time(t^2).

In this talk we discuss whether this quadratic blow-up in the running time is necessary. We show that the quadratic blow-up is indeed necessary for black-box simulations that use two quantifiers, such as those of Sipser, Gï£¡s, and Lautemann. To obtain this result, we prove a new circuit lower bound for computing *approximate majority*, i.e. computing the majority of a given bit-string whose fraction of 1's is bounded away from 1/2 (by a constant): We show that small depth-3 circuits for approximate majority must have bottom fan-in $\Omega(\log n)$.

On the positive side, we obtain that probabilistic time can be simulated deterministically, using three quantifiers, in quasilinear time. That is, BPTime(t) is contained in Σ_3Time$(t \operatorname{polylog} t)$. Along the way, we show that approximate majority can be computed by uniform polynomial-size depth-3 circuits. This is a uniform version of a striking result by Ajtai that gives *non-uniform* polynomial-size depth-3 circuits for approximate majority.

If time permits, we will discuss some applications of our results to proving lower bounds on randomized Turing machines.

Keywords: Probabilistic time, alternating time, polynomial-time hierarchy, approximate majority, constant-depth circuit

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/619

Parity-BDDs : Repeated Tests und Approximation

Stephan Waack (Universität Göttingen, D)

The following two observations on $\oplus$OBDDs are presented:

- In contrast to the deterministic case, nondeterministic polynomial-size k-OBDDs obeying the existential, parity or majority acceptance mode are not more powerful than the corresponding OBDDs of polynomial size.
- Quasipolynomial $\vee$OBDDs can be approximated with quasipolynomial error rate by quasipolynomial $\oplus$OBDDs.

Keywords: Parity-BDDs, repeated tests, approximation

Nechiporuk Bounds for the Middle Bit of Multiplication

Ingo Wegener (Universität Dortmund, D)

Our construction of a polynomial-size randomized syntactial read-$O(\log n)$ branching program for the middle bit of multiplication MM_n with two-sided error probability at most n^{-c} (for a given constant c) has led to many insights about the subfunction structure of MM_n. This leads to the question whether non trivial lower bounds can be obtained by the classical methods due to Nechiporuk. Lower bounds of size $n^{3/2}/\log n$ for the branching program size and of size $n^{3/2}$ for the formula size are proved. Moreover it is shown that bounds of larger order than $n^{5/3}/\log n$ and $n^{5/3}$, resp., cannot be obtained by this method.

Joint work of: Woelfel, Philipp; Wegener, Ingo

On the Teachability of Randomized Learners

Thomas Zeugmann (Hokkaido Univ. - Sapporo, J)

The present paper introduces a new model for teaching *randomized learners*.

Our new model, though based on the classical teaching dimension model, allows to study the influence of various parameters such as the learner's memory size, its ability to provide or to not provide feedback, and the influence of the order in which examples are presented.

Furthermore, within the new model it is possible to investigate new aspects of teaching like teaching from positive data only or teaching with inconsistent teachers.

Furthermore, we provide characterization theorems for teachability from positive data for both ordinary teachers and inconsistent teachers with and without feedback.

Keywords: Algorithmic Teaching, Complexity of teaching

Joint work of: Zeugmann, Thomas; Balbach, Frank J.

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/620

Full Paper:
http://www-alg.ist.hokudai.ac.jp/~thomas/TCSTR/tcstr_06_13/tcstr_06_13.pdf

Bounded-Error Quantum State Identification and Exponential Separations in Communication Complexity

Ronald de Wolf (CWI - Amsterdam, NL)

We consider the problem of bounded-error quantum state identification: given either state α_0 or state α_1, we are required to output '0', '1' or '?' ("don't know"), such that conditioned on outputting '0' or '1', our guess is correct with high probability. The goal is to maximize the probability of not outputting '?'. We prove a direct product theorem: if we're given two such problems, with optimal probabilities a and b, respectively, and the states in the first problem are pure, then the optimal probability for the joint bounded-error state identification problem is $O(ab)$. Our proof is based on semidefinite programming duality and may be of wider interest.

Using this result, we present two exponential separations in the simultaneous message passing model of communication complexity. Both are shown in the strongest possible sense. First, we describe a relation that can be computed with $O(\log n)$ classical bits of communication in the presence of shared randomness, but needs $\Omega(n^{1/3})$ communication if the parties don't share randomness, even if communication is quantum.

This shows the optimality of Yao's recent exponential simulation of shared-randomness protocols by quantum protocols without shared randomness. Second, we describe a relation that can be computed with $O(\log n)$ classical bits of communication in the presence of shared entanglement, but needs $\Omega((n/\log n)^{1/3})$ communication if the parties share randomness but no entanglement, even if communication is quantum. This is the first example in communication complexity of a situation where entanglement buys you much more than quantum communication does.

Keywords: Quantum computing, communication complexity, state identification, shared randomness, entanglement

Joint work of: Gavinsky, Dmitry; Kempe, Julia; Regev, Oded; de Wolf, Ronald

Full Paper:
http://arxiv.org/abs/quant-ph/0511013

See also: Accepted for STOC 06