Advances in Complexity Theory

Stephen Cook (University of Toronto),
Arvind Gupta (Simon Fraser University),
Russell Impagliazzo (University of California, San Diego),
Valentine Kabanets (Simon Fraser University),
Madhu Sudan (M.I.T.),
Avi Wigderson (Institute for Advanced Study, Princeton)

July 4–8, 2004

Computational Complexity Theory is the field that studies the efficiency of computation. Its major goals are to find efficient algorithms for natural problems in natural computational models, or to show that no efficient solutions exist. The famed "P versus NP" problem (one of the seven open problems of the Clay Institute) is the central problem of this field.

In the last two decades, our understanding of efficient computation has improved significantly through a number of concepts, techniques and results, including:

- Discovery of efficient ways of converting computational hardness into computational randomness (hardness-randomness tradeoffs), and other techniques for eliminating or reducing randomness use in probabilistic algorithms.
- Classification of hardness of approximation algorithms for a number of optimization problems, using the concept of Probabilistically Checkable Proofs (PCP).
- Connections of both items above to old and new problems in coding and information theory, which fertilized both fields.
- Investigations of the complexity of proofs, and their connections to limits on circuit lower bounds on the one hand, and to the complexity of search heuristics on the other.
- Use of quantum computation to get efficient algorithms for classically difficult problems (such as factoring), as well as using quantum arguments to obtain complexity results in the classical model of computation.

Many new developments in these areas were presented by the participants of the workshop. These new results will be described in the following sections of this report, grouped by topic. For each topic, we give a brief summary of the presented results, followed by the abstracts of the talks.

1 Probabilistically Checkable Proofs

The area of Probabilistically Checkable Proofs (PCPs) and Hardness of Approximation continues to be one of the most active research directions in complexity. The talk by Irit Dinur discussed how to make the original algebraic proof of the PCP Theorem [AS98, ALM+98] more combinatorial (and

hence, maybe simpler). Eli Ben-Sasson presented a new construction of shorter PCPs. Finally, Guy Kindler showed optimal conditional in-approximability for the problem MAX-CUT.

Irit Dinur, **Assignment testers: Towards a combinatorial proof of the PCP Theorem** (joint work with Omer Reingold)

In this talk we look back into the proof of the PCP Theorem, with the goal of finding new proofs that are "more combinatorial" and arguably simpler. For that we introduce the notion of an assignment tester, which is a strengthening of the standard PCP verifier, in the following sense. Given a statement and an alleged proof for it, while the PCP verifier checks correctness of the *statement* the assignment-tester checks correctness of the statement *and the proof*. This notion enables simpler composition that is truly modular, i.e., one can compose two assignment-testers without any assumptions on how they are constructed. A related notion was independently introduced in [Ben-Sasson et al., *STOC'04*]. Based on this notion, we present two main results: 1. The first is a new proof of the PCP Theorem. This proof relies on a rather weak PCP given as a "black box". From this, we construct combinatorially the full PCP, relying on composition and a new combinatorial aggregation technique. 2. Our second construction is a "standalone" combinatorial construction showing "NP $\subset$ PCP [polylog 1]". This implies, for example, that approximating max-SAT is quasi-NP-hard.

Eli Ben-Sasson, **Simple PCPs with poly-log rate and query complexity** (joint work with Madhu Sudan)

We give constructions of PCPs of length $n \cdot \mathrm{poly}(\log n)$ (with respect to circuits of size n) that can be verified by making $\mathrm{poly}(\log n)$ queries to bits of the proof. These PCPs are not only shorter than previous ones, but also simpler. Our (only) building blocks are Reed-Solomon codes and the Bivariate Low Degree Test of Polischuk and Spielman. First, we present a novel reduction of SAT to the following problem. Given oracle access to a string of length $n' = n \cdot \mathrm{poly}(\log n)$, verify whether it is close to being an evaluation of a univariate polynomial of degree $n'/10$. While somewhat similar reductions have been extensively used in previous PCP constructions, our new reduction favors over them in its simplicity. Notice the degree of the polynomial is larger than the size of the original SAT problem. Thus, testing low degree of this string seems to cost more queries than required for reading the original satisfying assignment in its entirety! To overcome this, we present a short PCP of Proximity for certain Reed-Solomon codes. For these codes, verifying that a string of length n' is close to an evaluation of a degree $n'/10$ polynomial can be done with $\mathrm{poly}(\log n')$ queries into the string and into an additional proof of length $n' \cdot \mathrm{poly}(\log n')$. Such PCPs of proximity also gives rise to locally testable codes with poly-logarithmic rate and query complexity.

Guy Kindler, **Conditional optimal in-approximability results for MAX-CUT** (joint work with Subhash Khot, Elchanan Mossel, and Ryan O'Donnell)

In this talk we give evidence that it is hard to approximate the maximal cut in a given graph to within a factor of $\alpha + \epsilon$, for all $\epsilon > 0$. Here $\alpha = .878567..$ denotes the approximation ratio achieved by the Goemans-Williamson algorithm [GW95], which means that we achieve an essentially optimal factor. Our result relies on two conjectures: (1) A widely-believed conjecture we fondly call "Majority is Stablest"; this conjecture leads to a long-code test that queries two bits, and whose soundness/completeness factor is exactly α. (2) The Unique Games conjecture of Khot [Khot02]. Our results suggest (even for non-believers in the above conjectures) that the geometric structure imposed on the MAX-CUT problem by the Goemans-Williamson algorithm may in fact be intrinsic to it. They also raise several interesting questions of both complexity-theoretic and geometric nature.

2 Pseudorandomness

Pseudorandomness is the area concerned with explicit constructions of various "random-like" combinatorial objects. New constructions of one type of such objects, *randomness extractors*, have been reported by Ronen Shaltiel, Russell Impagliazzo, and Guy Kindler. The work described in the talk by Impagliazzo relied on some tools from Combinatorial Number Theory. A tutorial on Combinatorial Number Theory was given by Avi Wigderson. Finally, Pavel Pudlak described a new explicit

construction of Ramsey graphs with better parameters than previously known; interestingly, the (yet unpublished) results on extractors described in the talk by Kindler actually yield the construction of Ramsey graphs with even better parameters.

Ronen Shaltiel, **Deterministic extractors for bit-fixing sources by obtaining an independent seed** (joint work with Ariel Gabizon and Ran Raz) [GRS04]

An (n, k)-bit-fixing source is a distribution X over n bit strings such that there is a subset of k variables in $X_1, ..., X_n$ which are uniformly distributed and independent of each other, and the remaining $n - k$ indices are fixed. A deterministic bit-fixing source extractor is a function E which given an arbitrary (n, k)-bit-fixing source outputs m bits which are statistically-close to uniform. Recently, Kamp and Zuckerman gave a construction of deterministic bit-fixing source extractor which extracts $\Omega(k^2/n)$ bits, and requires $k > \sqrt{n}$. In this paper we give constructions of deterministic-bit-fixing source extractors that extract $(1 - o(1))k$ bits whenever $k > (\log n)^c$ for some constant $c > 0$. Thus, our constructions extract almost all the randomness from bit-fixing sources and work even when k is small. For $k >> \sqrt{n}$ the extracted bits have statistical distance $2^{-n^{\Omega(1)}}$ from uniform, and for $k < \sqrt{n}$ the extracted bits have statistical distance $k^{-\Omega(1)}$ from uniform. Our technique gives a general method to transform deterministic bit-fixing source extractors that extract few bits into extractors which extract almost all the bits.

Avi Wigderson, **Gems of Combinatorial Number Theory**

We describe three theorems from Combinatorial Number Theory, and give their proofs. These theorems are related to the recent extractors obtained by Barak, Impagliazzo and Wigderson [Barak et al., *FOCS'04*](described in another talk of this workshop).

The extensive research area of Combinatorial Number Theory often deals with the structure of sets of (commutative) groups, and its evolution under the group operation. The theorems below are prime examples, not only being basic and powerful, but also due to their ingenious proofs that utilize ideas and tools from seemingly unrelated areas.

Let A, B be subsets of size m in an Abelian group. We use the notation $A+B = \{a+ba \in A, b \in B\}$ (here $+$ is the group operation; later we'll use both addition and multiplication over the Reals). Further if $G = (A, B; E)$ is a bipartite graph on A, B, we let $A+_G B = \{a+ba \in A, b \in B, (a, b) \in E\}$.

The theorems below will hold for all choices of m and sets A, B (and C) of this size.

Theorem [Ruzsa, Plunneke]: For every k, if $|A + B| = km$, then $|A + A| \leq k^2 m$.

Theorem [Gowers]: For every k and graph $G = (A, B; E)$ with $|E| \geq m^2/k$, if $|A +_G B| \leq km$, then there exist subsets $A' \subseteq A$ and $B' \subseteq B$ such that $|A' + B'| \leq k^8 m$

Theorem [Erdos-Szemeredi, Elekes]: Let A, B, C be subsets of size m of the real numbers. Then $|AB + C| \geq m^{3/2}$

Russell Impagliazzo, **Extracting randomness using few independent sources** (joint work with Boaz Barak and Avi Wigderson) [BIW04]

Randomness is prevalent in computer science, and is widely used in algorithms, distributed computing, and cryptography. Perhaps the main motivation and justification for the use of randomness in computation is that randomness does exist in nature, and thus it is possible to sample natural phenomena (such as radioactive decay) in order to make random choices in computation. However, there is a discrepancy between the type of random input that we expect when designing randomized algorithms and protocols, and the type of random data that can be found in nature. While randomized algorithms and protocols expect a stream of independent uniformly distributed random bits, in many cases, the sampled natural data is not distributed according to the uniform distribution.

We consider the problem of extracting truly random bits from several independent weak random sources. Previous constructions either required a large number of sources (polynomial in the input length), or required the entropy of each source to be large. Specifically, the best previous explicit construction using a constant number of n-bit sources required that at least one of the sources contains more than $n/2$ bits of (min-)entropy. In contrast, the optimal, non-explicit construction only requires the min-entropy to be more than $\log n$.

In this work, we manage to go beyond this $n/2$ "barrier" and give an explicit construction for extracting randomness from distributions with any constant entropy rate. The number of samples we

require is a constant (depending polynomially on the rate). Our main tools are results from additive number theory and in particular a recent result by Bourgain, Katz and Tao and an improvement by Konyagin.

Guy Kindler, **Breaking the 1/2-barrier for bipartite Ramsey constructions and for linear source dispersers** (joint work with Boaz Barak, Ronen Shaltiel, Benny Sudakov, and Avi Wigderson)

The k-partite Ramsey construction problem with parameter δ, is to find explicit functions f, $f : [N]^k \to \{0,1\}$, such that for every choice of k subsets $A_1, \ldots, A_k \subseteq [N]$ of size at least $[N]^\delta$ each, the restriction of f to $A_1 \times \cdots \times A_k$ is non-constant. An alternative formalization would be to find a function $f : (\{0,1\}^n)^k \to \{0,1\}$, such that for every k sources $X_1, \ldots, X_k$ of size n-bits each and with min-entropy at least δn each, $f(X_1, \ldots, X_k)$ yields both 0 and 1 with positive probability.

So far, no bipartite Ramsey constructions were known for parameters $\delta < 1/2$. In this talk we present explicit constructions of Bipartite Ramsey graphs for all positive constant parameters δ (this trivially solves the k-partite problem for the same parameters for every $k > 2$). We also show 4-source extractors, that extract bits from four n-bit independent sources with min-entropy at least δn each. This answers a question of Barak, Impagliazzo, and Wigderson [Barak et al., *FOCS'04*].

Similar ideas lead also to explicit constructions of seedless condensers for Linear sources, namely explicit functions $f : \{0,1\}^n \to \{0,1\}$, which are non-constant on every affine linear subspace of $\{0,1\}^n$ of dimension at least δn. While no such construction was known for any $\delta < 1/2$, we can construct such functions for every positive constant δ.

Pavel Pudlak, **Pseudorandom sets and explicit constructions of Ramsey graphs** (joint work with Vojtech Rödl)

We shall show a polynomial time construction of a graph G on N vertices such that neither G nor $\overline{G}$ contains $K_{r,r}$, for $r = \sqrt{N}/2^{\sqrt{\log N}} = o(\sqrt{N})$. To this end we construct a subset $X \subset \mathbb{F}^m$ which has small intersections with all subspaces of dimension $m/2$.

3 Bounded Arithmetic and Proof Complexity

The framework of Bounded Arithmetic can be used to give machine-independent characterization of various complexity classes. Thus, complexity classes may be studied through the properties of logical theories of bounded arithmetic that "capture" these complexity classes. The overview of this approach was given in the talk by Stephen Cook. The logical theories for the classes NL and $PSPACE$ were presented by Antonina Kolokolova and Alan Skelley. Sam Buss and Tsuyoshi Morioka discussed the connections between systems of bounded arithmetic and propositional proof systems, and proved witnessing theorems for certain theories of bounded arithmetic.

Stephen Cook, **Making Sense of Bounded Arithmetic**

We present a unified treatment of logical theories for each of the major complexity classes between AC^0 and P, and give simple translations into the quantified propositional calculus.

Sam Buss, **Bounded Arithmetic and Constant Depth Propositional Proofs**

We discuss the Paris-Wilkie translation from bounded arithmetic proofs to bounded depth propositional proofs. We describe normal forms for proofs in bounded arithmetic, and a definition of Σ'-depth for PK-proofs that makes the translation from bounded arithmetic to propositional logic particularly transparent. Using this, we give new proofs of the witnessing theorems for S^1_2 and T^1_2; namely, new proofs that the Σ^b_1-definable functions of S^1_2 are polynomial time computable and that those of T^1_2 are in Polynomial Local Search (PLS). Both proofs generalize to Σ^b_i-definable functions of S^i_2 and T^i_2.

Antonina Kolokolova, **A second-order theory for NL** (joint work with Stephen Cook)

We introduce a second-order theory V-Krom of bounded arithmetic for nondeterministic log space. This system is based on Grädel's characterization of NL by second-order Krom formulae with only universal first-order quantifiers, which in turn is motivated by the result that the decision problem for 2-CNF satisfiability is complete for $coNL$ (and hence for NL). This theory has the style

of the authors' theory V_1-Horn [*APAL 124 (2003)*] for polynomial time. Both theories use Zambella's elegant second-order syntax, and are axiomatized by a set 2-BASIC of simple formulae, together with a comprehension scheme for either second-order Horn formulae (in the case of V_1-Horn), or second-order Krom (2-CNF) formulae (in the case of V-Krom). Our main result for V-Krom is a formalization of the Immerman-Szelepcenyi theorem that NL is closed under complementation. This formalization is necessary to show that the NL functions are Σ_1^B-definable in V-Krom. The only other theory for NL in the literature relies on the Immerman-Szelepcenyi's result rather than proving it.

Tsuyoshi Morioka, **The witnessing problems for Quantified Propositional Calculus** (joint work with Stephen Cook)

Let H be a proof system for the quantified propositional calculus (QPC). We define the Σ_j^q-witnessing problem for H to be: given a prenex Σ_j^q-formula A, an H-proof of A, and a truth assignment to the free variables in A, find a witness for the outermost existential quantifiers in A. We point out that the Σ_1^q witnessing problems for the systems G_1^* and G_1 are complete for polynomial time and PLS (polynomial local search), respectively. We introduce and study the systems G_0^* and G_0, in which cuts are restricted to quantifier-free formulas, and prove that the Σ_1^q-witnessing problem for each is complete for NC^1. Our proof involves proving a polynomial time version of Gentzen's midsequent theorem for G_0^* and proving that G_0-proofs are TC^0-recognizable. We also introduce QPC systems for TC^0 and prove witnessing theorems for them.

Alan Skelley, **Theories and proof systems for PSPACE and beyond**

We present a new third-order theory W_1^1 for $PSPACE$ and discuss how Σ_1 theorems of it can be translated into polynomial-sized proofs in $BPLK$. $BPLK$ is a propositional proof system polynomially equivalent to G but using Boolean programs instead of quantified Boolean formulas. We then speculate as to how W_1^1 could be extended to obtain theories for the levels of the exponential-time hierarchy but, more interestingly, how $BPLK$ is uniquely amenable (unlike G) also to be extended in this direction.

4 Circuit Complexity, Probabilistic and Real Computation

Complexity theory studies the power of nonuniform (circuit-based) and uniform (Turing machine-based) models of computation. The talks by Ran Raz and Eric Allender discussed the computational power of restricted arithmetic and Boolean circuit models. Lance Fortnow presented the Probabilistic Time Hierarchy Theorem for Turing machines with constant amount of nonuniform advice. Finally, Mark Braverman discussed his results in the field of Real Computation.

Ran Raz, **Multilinear formulas for Permanent and Determinant are of superpolynomial size** [Raz04]

An arithmetic formula is multilinear if the polynomial computed by each of its subformulas is multilinear. We prove that any multilinear arithmetic formula for the permanent or the determinant of an $n \times n$ matrix is of size superpolynomial in n. Previously, superpolynomial lower bounds were not known (for any explicit function) even for the special case of multilinear formulas of constant depth.

Eric Allender, **Toward a topology for NC^1** (joint work with Samir Datta and Sambuddha Roy)

Hansen recently provided a characterization of ACC^0 as precisely the class of problems computable by constant-width PLANAR circuits of polynomial size (with AND and OR gates, with negation available at the inputs.) Barrington's theorem shows that, without the restriction of planarity, constant-width circuits characterize NC^1. We consider possible generalizations of Hansen's theorem, by considering circuits with small genus and thickness. Every problem in NC^1 is computed by a constant-width circuit of thickness two, and thus thickness does not seem to be a useful parameter for investigating the structure of NC^1. In contrast, we show that restricting constant-width circuits to have genus $O(1)$ again yields a characterization of ACC^0. It remains an intriguing

open question if there are problems that are not believed to lie in ACC^0 that can be computed by constant-width, polynomial-size circuits of small (say, logarithmic) genus.

Lance Fortnow, **A hierarchy theorem for probabilistic polynomial time with one bit of advice** (joint work with Rahul Santhanam)

We show a hierarchy for probabilistic time with one bit of advice, specifically we show that for all real numbers $1 \leq \alpha < \beta$, $BPTIME(n^\alpha)/1 \subset BPTIME(n^\beta)/1$. This result builds on and improves an earlier hierarchy by Barak using $O(\log \log n)$ bits of advice. We build on Barak's idea by a careful application of the fact that there is a PSPACE-complete problem L such that worst case probabilistic algorithms for L take only slightly more time than average case algorithms.

Mark Braverman, **On the computability of Julia sets**

While the computer is a discrete device, it is often used to solve problems of a continuous nature. The field of Real Computation addresses the issues of computability in the continuous setting. We will discuss different models of computation for subsets of $\mathbb{R}^n$. The main definition we use has a computer graphics interpretation (in the case $n = 2$), as well as a deeper mathematical meaning. The Julia sets are particularly well studied sets arising from complex dynamics. In the talk we will present the basic facts about Julia sets and some computability results for them. Our computability results come in contrast to the Julia sets noncomputability results presented by Blum/Cucker/Shub/Smale. This discrepancy follows from the fact that we are using a different computability model.

5 Matrix Multiplication, Search Heuristics, Learning, and Quantum Computation

Determining the complexity of matrix multiplication is one of the most important questions in computer science. A very interesting new approach to this problem was described in the talk by Chris Umans. Josh Buresh-Oppenheim presented a formal model for the class of backtracking algorithms, and showed lower bounds on the power of algorithms in that model. Several new (both positive and negative) results on learnability were presented by Toniann Pitassi; some of these results exploited a connection between proof complexity and learning theory. Mario Szegedy showed a very general result on "speeding up" classical algorithms by quantum algorithms; he described the conditions on classical Markov-chain based algorithms that yield quadratic speedup in the quantum model of computation. Finally, Oded Regev presented an efficient lattice-based cryptographic system, whose security relies on the assumption of quantum (rather than classical) hardness of certain lattice problems.

Chris Umans, **A group-theoretic approach to fast matrix multiplication** (joint work with Henry Cohn) [CU03]

How many operations are required to multiply two $n \times n$ matrices? The standard algorithm requires n^3 operations, but in 1969 Strassen showed that $O(n^{2.81})$ operations suffice. Over the next twenty years, a sequence of increasingly complex algorithms were devised, but since 1990 no one has been able to improve on the current best algorithm of Coppersmith and Winograd, that runs in time $O(n^{2.39})$. I'll describe work that develops a new (and self-contained) approach to the problem. In the new framework, one devises algorithms for matrix multiplication by constructing non-abelian groups with certain properties. The algorithms themselves are easy to describe, and they make critical use of the Discrete Fourier Transform over non-abelian groups. I'll outline some progress toward an improved algorithm using this new approach.

Josh Buresh-Oppenheim, **Toward a model for Backtracking** (joint work with Allan Borodin, Russell Impagliazzo, Avner Magen, and Toniann Pitassi)

In this paper, we develop a hierarchy of models for backtracking algorithms (BT). Our model generalizes both the priority model of Borodin, Neilson and Rackoff, as well as the simple dynamic programming model due to Wögenger. We demonstrate the strength of our models by showing how well-known algorithms and algorithmic techniques can be simulated within our model, both those that are usually considered back-tracking as well as a large family of greedy algorithms and dynamic

programming algorithms. Finally we prove strong lower bounds on the capabilities of algorithms in this model, often essentially proving that the known algorithms are the best possible in the model.

After defining and discussing the BT family of models, we consider the following fundamental problems: interval scheduling with proportional profit, the knapsack problem, 2SAT, 3SAT, and vertex cover. Our main results are as follows: (1) For interval scheduling of n intervals on m machines with proportional profits, the optimal width of an adaptive BT algorithm is $\Theta(n^m)$. Further, for fixed-ordering BT, we obtain similar upper and lower bounds for approximating interval scheduling. (2) For knapsack, we prove an exponential lower bound in the adaptive BT model. (3) We prove that 2SAT has a linear size adaptive BT algorithm, but that any fixed-ordering BT algorithm requires exponential size. Further the lower also extends to show that neither 2SAT nor vertex cover can be approximated by subexponential size fixed-ordering BT programs. (4) For 3SAT we prove that any adaptive BT algorithm requires exponential size.

Toniann Pitassi, **Learnability and automatizability** (joint work with Misha Alekhnovich, Mark Braverman, Vitaly Feldman, and Adam Klivans)

In this talk we prove new upper and lower bounds on the proper PAC learnability of decision trees, DNF formulas, and intersections of halfspaces. Several of our results were obtained by exploring a new connection between automatizability in proof complexity and learnability. After explaining this basic connection, we will prove the following new results: (1) We give new upper bounds for proper PAC learning of decision trees and DNF, based on similar known algorithms for automatizability of Resolution. (2) We show that it is not possible to PAC learn DNF by DNF in polynomial-time unless $NP \subseteq BPP$. We also prove the same negative result for proper PAC learning of intersections of halfspaces. (3) We show that decision trees cannot be proper PAC learned, under a different (less standard) complexity-theoretic assumption.

Mario Szegedy, **Quantum speed-up of Markov chain based algorithms**

We develop a generic method for quantizing classical algorithms based on random walks. We show that under certain conditions, the quantum version gives rise to a quadratic speed-up. This is the case, in particular, when the Markov chain is ergodic and its transition matrix is symmetric. This generalizes the celebrated result of [Grover 1996] and a number of more recent results, including [Ambainis 2003] and [Ambainis, Kempe and Rivosh, 2004]. Among the consequences is a faster search for multiple marked items. We show that the quantum escape time, just like its classical version, depends on the spectral properties of the transition matrix with the marked rows and columns deleted.

Oded Regev, **Lattice based cryptography, quantum and some learning theory**

We present strong and more efficient lattice based public key cryptographic schemes. In all previous systems, the encryption process increases the size of a message by a factor of n^2 where n is the hardness parameter. This is considered prohibitive since n has to be on the order of thousands in order to make the system secure. We reduce this blow-up to only n. This, we believe, makes our cryptographic scheme more practical. One curious feature of our construction is that it is based on the quantum hardness of lattice problems. All previous constructions were based on the classical hardness of lattice problems. The reason for this difference is the following: we present a quantum algorithm for a problem that we do not know how to solve classically.

References

[ALM+98] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy. Proof verification and the hardness of approximation problems. *Journal of the Association for Computing Machinery*, 45(3):501–555, 1998. (preliminary version in FOCS'92).

[AS98] S. Arora and S. Safra. Probabilistic checking of proofs: A new characterization of NP. *Journal of the Association for Computing Machinery*, 45(1):70–122, 1998. (preliminary version in FOCS'92).

[BIW04] B. Barak, R. Impagliazzo, and A. Wigderson. Extracting randomness using few independent sources. In *Proceedings of the Forty-Fifth Annual IEEE Symposium on Foundations of Computer Science*, 2004 (to appear).

[CU03] H. Cohn and C. Umans. A group-theoretic approach to fast matrix multiplication. In *Proceedings of the Forty-Forth Annual IEEE Symposium on Foundations of Computer Science*, 2003.

[GRS04] A. Gabizon, R. Raz, and R. Shaltiel. Deterministic extractors for bit-fixing sources by obtaining an independent seed. In *Proceedings of the Forty-Fifth Annual IEEE Symposium on Foundations of Computer Science*, 2004 (to appear).

[Raz04] R. Raz. Multi-linear formulas for Permanent and Determinant are of super-polynomial size. In *Proceedings of the Thirty-Sixth Annual ACM Symposium on Theory of Computing*, pages 633–641, 2004.