Mathematisches Forschungsinstitut Oberwolfach

Report No. 44 / 2000

Complexity Theory

November 19th – November 25th, 2000

Complexity theory is concerned with the study of the intrinsic difficulty of computational tasks. It is a central field of theoretical computer science. The 14^{th} Oberwolfach Conference on Complexity Theory was organized by Joachim von zur Gathen (Paderborn), Oded Goldreich (Rehovot), and Claus Peter Schnorr (Frankfurt).

The meeting consisted of five general sessions, and in addition special sessions on the following topics:

- Algebraic Complexity
- Cryptography
- Lattices
- Pseudorandomness

Another event that took place in the meeting was the awarding of the Oberwolfach prize to Luca Trevisan, who was one of the participants.

Abstracts of General Session Talks

A Few Facts about Division

Eric Allender

Chiu, Davida, and Litow recently solved a decades-old problem, by showing that there are logspace-uniform, constant-depth threshold circuits for division. It remains open if the uniformity condition can be improved, to obtain Dlogtime-uniform circuits.

We precisely characterize the uniformity requirements, by showing that Division is complete (under first-order reductions) for the class FOM+POW (where FOM is an equivalent formalization of Dlogtime-uniform TC^0, and POW is the predicate "$a^i = b \bmod p$" for primes p of $O(\log n)$ bits). We also show that FOM and FOM+POW coincide, if a well-known conjecture about smooth primes holds.

In the talk, I also mention a recent lower bound (joint work with Koucky, Ronneburger, Roy, and Vinay) showing that the lower bound techniques of Fortnow can be extended to the probabilistic model, if division has uniform TC^0 circuits.

Other consequences of the new division algorithm include a new translational lemma for very small space-bounded complexity classes.

Joint work with David Mix Barrington, and William Hesse.

Super-linear time-space tradeoff lower bounds for randomized computation

Paul Beame

We prove the first time-space lower bound tradeoffs for randomized computation of decision problems. The bounds hold even in the case that the computation is allowed to have arbitrary probability of error on a small fraction of inputs. Our techniques are an extension of those used by Ajtai in his time-space tradeoffs for deterministic RAM algorithms computing element distinctness and for deterministic Boolean branching programs computing an explicit function based on quadratic forms over $GF(2)$.

Our results also give a quantitative improvement over those given by Ajtai. Ajtai shows, for certain specific functions, that any branching program using space $S = o(n)$ requires time T that is superlinear. The functional form of the superlinear bound is not given in his paper, but optimizing the parameters in his arguments gives $T = \Omega(n \log\log n / \log\log\log n)$ for $S = O(n^{1-\epsilon})$. For the same functions considered by Ajtai, we prove a time-space tradeoff of the form $T = \Omega(n\sqrt{\log(n/S)/\log\log(n/S)})$. In particular, for space $O(n^{1-\epsilon})$, this improves the lower bound on time to $\Omega(n\sqrt{\log n/\log\log n})$.

Joint work with Mike Saks, Xiadong Sun, and Erik Vee.

Expansion in Propositional Proof Complexity

Eli Ben-Sasson

In this survey talk, we describe the main technique used in recent years to prove lower bounds in proof complexity, for simple proof systems such as resolution and the polynomial calculus.

We define a certain form of expansion (Boundary Expansion) on bipartite graphs. We define a reduction of CNF formulas to bipartite graphs, and claim the following:

For F an unsatisfiable CNF formula, and $G(F)$ its corresponding bipartite graph, if $G(F)$ is an expander, then:

1. The minimal width of refuting F in resolution is large (linear).

2. The minimal size of refuting F in resolution is large (exponential).

3. The minimal space needed to refute F in resolution is large (linear).

Similar lower bounds hold for degree of refutation in the Polynomial Calculus.

This basic idea allows us to show non-trivial (and often optimal) lower bounds for the Pigeonhole Principles, Tseitin Graph formulas, random k-CNFs, Pseudorandom-Generator based formulas, and many others.

Based on works by Alekhnovich, Beame, Ben-Sasson, Clegg, Edmonds, Grigoriev, Impagliazzo, Pitassi, Pudlak, Razborov, Sgall, and Wigderson.

Lower bounds for the complexity of associative algebras

Markus Bläser

Let $C(A)$ resp. $R(A)$ denote the multiplicative resp. bilinear complexity of a finite dimensional associative algebra A.

We prove that $R(A) \geq \frac{5}{2} \dim A - 3(n_1 + \cdots + n_t)$ if the decomposition of $A/\operatorname{rad} A \cong A_1 \times \cdots \times A_t$ into simple algebras $A_\tau \cong {D_\tau}^{n_\tau \times n_\tau}$ contains only noncommutative factors, that is, the division algebra D_τ is noncommutative or $n_\tau \geq 2$. If A is in addition semisimple, then the same bound holds for the multiplicative complexity, i.e., $C(A) \geq \frac{5}{2} \dim A - 3(n_1 + \cdots + n_t)$. In particular, $n \times n$–matrix multiplication requires at least $\frac{5}{2}n^2 - 3n$ essential multiplications.

Approximating the Minimum Bisection

Uriel Feige

A Bisection of a graph with n vertices is a partition of its vertices into two sets, each of size $n/2$. The bisection cost is the number of edges connecting the two sets. Finding the minimum bisection cost is NP-hard. We present several approximation algorithms for bisection, the best of which finds a bisection whose cost is within a ratio of $O(\log^2 n)$ from optimal. The previously known approximation ratio for bisection was $n/2$.

Joint work with Robert Krauthgamer and in part with Kobbi Nissim.

In search of an easy witness: Applications to Exponential Time

Valentine Kabanets

Using the hardness-randomness tradeoffs as well as the idea of "easy witnesses", we show several complexity-theoretic results involving exponential-time complexity classes. First, we prove that NEXP$\subset$ P/poly iff NEXP=MA. This can be interpreted as saying that one cannot derandomize MA without proving superpolynomial circuit lower bounds for NEXP.

We also establish several downward closure results for the probabilistic complexity classes ZPP, RP, BPP, and MA. In particular, we prove that EXP=BPP iff EE=BPE, where EE is double exponential time and BPE is the $2^{O(n)}$-time analog of the class BPP.

Joint work with Russell Impagliazzo and Avi Wigderson.

On Rounds in Quantum Communication

Hartmut Klauck

We investigate the power of interaction in two player quantum communication protocols. Our main result is a rounds-communication hierarchy for the pointer jumping function f_k . We show that f_k needs quantum communication $\Omega(n)$ if Bob starts the communication and the number of rounds is limited to k (for any constant k). Trivially, if Alice starts, $O(k \log n)$ communication in k rounds suffices. The lower bound employs a result relating the relative von Neumann entropy between density matrices to their trace distance and uses a new measure of information.

We also describe a classical probabilistic k round protocol for f_k with communication $O((n/k + k) \log k)$, in which Bob starts the communication, for k at least $2 \log^* n$.

Furthermore as a consequence of the lower bound for pointer jumping we show that any k round quantum protocol for the disjointness problem needs communication $\Omega(n^{1/k})$ for $k = O(1)$.

A linear space algorithm for computing the Hermite Normal Form of an integer lattice

Daniele Micciancio

Computing the Hermite Normal Form of an $n \times n$ matrix using the best current algorithms typically requires $O(n^3 \log M)$ space, where M is a bound on the length of the columns of the input matrix. Although polynomial in the input size (which is $O(n^2 \log M)$), this space blow-up can easily become a serious issue in practice when working on big integer matrices. In this talk we present a new algorithm for computing the Hermite Normal Form which uses only $O(n^2 \log M)$ space (i.e., essentially the same as the input size). When implemented using standard integer arithmetic, our algorithm has the same time complexity of the asymptotically fastest (but space inefficient) algorithms. We also suggest simple heuristics that when incorporated in our algorithm result in essentially the same asymptotic running time of the theoretically fastest solutions, still maintaining our algorithm extremely practical.

Joint work with Bogdan Warinschi.

The Zig-Zag Graph Product, and Elementary Construction of Expander Graphs

Omer Reingold

Expander graphs are combinatorial objects which are fascinating and useful, but seemed hard to construct. The main result we present is an elementary way of constructing them.

The essential ingredient is a new type of graph product, which we call the

zig-zag product. Taking a product of a large graph with a small graph, the resulting graph inherits (roughly) its size from the large one, its degree from the small one, and its expansion properties from both! Iteration yields simple explicit constructions of constant-degree expanders of arbitrary size, starting from one constant-size expander.

Crucial to our intuition (and simple analysis) of the properties of this graph product is the view of expanders as functions which act as "entropy wave" propagators — they transform probability distributions in which entropy is concentrated in one area to distributions where that concentration is dissipated. In these terms, the graph product affords the constructive interference of two such waves.

No special background is assumed. Joint work with Salil Vadhan and Avi Wigderson

Variation of the Baur-Strassen Theorem for Size and Depth

Arnold Schönhage

In this talk I present a simple proof for the following

Theorem Let a rational function $f \in K(x_1, \dots, x_n)$ be computable by an arithmetical circuit D of size s and depth d, with the indeterminates $x_1, \dots, x_n$ and any constants $\in K$ as cost-free inputs of D, and operation nodes using $\{+, -, *, /\}$ at unit cost. Then there exists also a circuit D' of size s' and depth d', computing f plus its first partial derivatives $\partial_1 f, \dots, \partial_n f$, such that

$$s' \leq 7s, \quad d' \leq 7d, \qquad \text{or} \qquad s' \leq 15s, \quad d' \leq 6d, \qquad \text{or} \qquad s' \leq 18s, \quad d' \leq 5d.$$

The proof is by induction on d, first under the restriction that all nodes of D have fan-out ≤ 7 (or ≤ 3, respectively). Then the general case is reduced to this by a Lemma on how to transform any such D to an equivalent D^* with bounded fan-out.

Extracting Randomness via Repeated Condensing

Ronen Shaltiel

On an input probability distribution with some (min-)entropy an *extractor* outputs a distribution with a (near) maximum entropy rate (namely the uniform distribution). A natural weakening of this concept is a *condenser*, whose output distribution has a higher entropy rate than the input distribution (without losing much of the initial entropy).

In this paper we construct efficient explicit condensers. The condenser constructions combine (variants or more efficient versions of) ideas from several works, including the block extraction scheme of Nisan and Zuckerman, the observation made in Srinivasan and Zuckerman, and Nisan and Ta-Shma that a failure of the block extraction scheme is also useful, the recursive "win-win" case analysis of Impagliazzo Shaltiel and Wigderson, and the error correction of random sources used by Trevisan.

As a natural byproduct, (via repeated iterating of condensers), we obtain new extractor constructions. The new extractors give significant qualitative improvements over previous ones for sources of arbitrary min-entropy; they are nearly optimal *simultaneously* in the main two parameters - seed length and output length. Specifically, our extractors can make any of these two parameters optimal (up to a constant factor), only at a *poly-logarithmic* loss in the other. Previous constructions require *polynomial* loss in both cases for general sources.

We also give a simple reduction converting "standard" extractors (which are good for an average seed) to "strong" ones (which are good for most seeds), with essentially the same parameters. With it, all the above improvements apply to strong extractors as well.

Packing Unitary Matrices

Amin Shokrollahi

The design of signal constellations for mobile multiple antenna transmission can in certain cases be reduced to the following mathematical problem: given a number M of transmit antennas and a positive real number ϵ, construct a large set V of $M \times M$-matrices such that for any A,B in V, A not equal to B, the quantity $d(A, B) := |det(A - B)|^{(1/M)}/2$ is larger than ϵ. The minimum value of $d(A, B)$ is called the diversity product of V. The problem is thus to construct the largest possible subset of $U(M)$, the group of unitary $M \times M$-matrices, with diversity product larger than ϵ. In this talk, we review some of the known results about this "packing problem". One of the results discussed in detail will be the classification of all finite subgroups of $U(M)$ with nonzero diversity product. Part of this talk is joint work with Hassibi, Hochwald, and Sweldens.

Lower Bounds for Matrix Product, in Bounded Depth Circuits with Arbitrary Gates

Amir Shpilka

We prove super-linear lower bounds for the number of edges in constant depth circuits with n inputs and up to n outputs. Our lower bounds are proved for all types of constant depth circuits, e.g., constant depth arithmetic circuits and constant depth Boolean circuits with arbitrary gates. The bounds apply for several explicit functions, and, most importantly, for matrix product. In particular, we obtain the following results:

1. We show that the number of edges in any constant depth arithmetic circuit for **matrix product** (over any field) is super-linear in m^2 (where $m \times m$ is the size of each matrix). That is, the lower bound is super-linear in the number of input variables. Moreover, if the circuit is bilinear the result applies also for the case where the circuit gets for free any product of two linear functions.

2. We show that the number of edges in any constant depth arithmetic circuit for the trace of the product of 3 matrices (over fields with characteristic 0) is super-linear in m^2. (Note that the trace is a **single-output** function).

3. We give explicit examples for n Boolean functions $f_1, ..., f_n$, such that any constant depth **Boolean circuit with arbitrary gates** for $f_1, ..., f_n$ has a super-linear number of edges. The lower bound is proved also for **circuits with arbitrary gates over any finite field**. The bound applies for matrix product over finite fields as well as for several other explicit functions.

Joint work with Ran Raz.

List decoding of error-correcting codes

Madhu Sudan

Error-correcting codes are combinatorial objects designed to deal with the problem of noise in information transmission. A code describes how to judiciously add redundancy information that recovers from a small amount of (even malicious) corruption. "Recovery" here is interpreted as follows: If a small number, say d, of errors occur, then it is possible to detect that errors have occurred. For an even smaller number, classically $d/2$, one can even find which locations are in error and fix them.

Among the simplest and yet very efficient error-correcting codes are codes based on properties of low-degree polynomials, called Reed Solomon codes. We give a simple algorithm for recovering from error in Reed Solomon codes. One of the novel features of this algorithm is that it recovers from much more than the above-mentioned bound of $d/2$ that classical algorithms could tolerate. We also describe extensions and generalizations to other codes.

Joint work with Venkatesan Guruswami (MIT).

Unbalanced Expanders and Improved Extractors

Chris Umans

We give explicit constructions of unbalanced bipartite expanders and extractors. Our expanders have small (polylogarithmic) degree D and a near-optimal expansion factor of $(1-\epsilon)D$. We show that such expanders are equivalent to loss-less condensers, which use a small number of truly random bits to transform a weak random source on n bits to a source on fewer bits with the same min-entropy. Using these condensers, we can transform any extractor for large min-entropy ($k = \sqrt{n}$) into an extractor for arbitrary min-entropy; this leads to improved extractor constructions in a number of cases. For example, we obtain extractors that extract any constant fraction of the min-entropy k using only $O(\log n + \log k (\log\log k)^2)$ truly random bits. As applications, we improve known constructions of a–expanding graphs and depth two super-concentrators, and a hardness of approximation result.

Extracting Randomness from Samplable Distributions

Salil Vadhan

The standard notion of a randomness extractor is a procedure which converts any weak source of randomness into an almost uniform distribution. The conversion necessarily uses a small amount of pure randomness, which can be eliminated by complete enumeration in some, but not all, applications.

Here, we consider the problem of *deterministically* converting a weak source of randomness into an almost uniform distribution. Previously, deterministic extraction procedures were known only for sources satisfying strong independence requirements. In this paper, we look at sources which are "samplable", i.e., can be generated by an efficient sampling algorithm. We seek an efficient deterministic procedure that, given a sample from any samplable distribution of sufficiently large min-entropy, gives an almost uniformly distributed output. We explore the conditions under which such "deterministic extractors" exist.

We observe that no deterministic extractor exists if the sampler is allowed to use more computational resources than the extractor. On the other hand, if the extractor is allowed (polynomially) more resources than the sampler, we show that deterministic extraction becomes possible. This is true unconditionally in the nonuniform setting (i.e., when the extractor can be computed by a small circuit), and (necessarily) relies on complexity assumptions in the uniform setting.

One of our uniform constructions is as follows: assuming that there are problems in E=DTIME($2^{O(n)}$) that are not solvable by subexponential-size circuits with Σ_6 gates, there is an efficient extractor that transforms any samplable distribution of length n and min-entropy $(1-\gamma)n$ into an output distribution of length $(1-O(\gamma))n$, where gamma is any sufficiently small constant. The running time of the extractor is polynomial in n and the circuit complexity of the sampler. These extractors are based on a connection between deterministic extraction from samplable distributions and hardness against nondeterministic circuits, and on the use of nondeterminism to substantially speed up "list decoding" algorithms for error-correcting codes such as multivariate polynomial codes and Hadamard-like codes.

Joint work with Luca Trevisan (FOCS '00)

Extractor Codes

David Zuckerman

We define new error correcting codes based on extractors. We show that for certain choices of parameters these codes have better list decoding properties than are known for other codes, and are provably better than Reed-Solomon codes. We further show that codes with strong list decoding properties are equivalent to slice extractors, a variant of extractors. We give an application of extractor codes to extracting many hardcore bits from a one-way function, using few auxiliary random bits. Finally, we show that explicit slice extractors for certain other parameters would yield optimal bipartite Ramsey graphs.

Joint work with Amnon Ta-Shma.

Abstracts of Special Sessions Talks

On the (Im)possibility of Software Obfuscation

Boaz Barak

Informally, a software obfuscator is an algorithm $\mathcal{O}$ such that for any program P , $\mathcal{O}(P)$ is a program that has the same functionality as P, but yet is impossible to "reverse-engineer". We consider several possible definitions for obfuscators, and show that even the weakest of them is impossible to achieve.

We also investigate several "obfuscation-like" concepts, and show a connection with attempts of obtaining a complexity theory analog of Rice's Theorem.

Joint work with Oded Goldreich, Russell Impagliazzo , Steven Rudich , Amit Sahai, Salil Vadhan and Ke Yang.

Inverting bivariate power series

Markus Bläser

We consider the multiplicative complexity of inversion and division of bivariate power series modulo the "triangular" ideal generated by all monomials of total degree $n+1$. For the inversion, we obtain a lower bound of $\frac{7}{8}n^2 - O(n)$ opposed to an upper bound of $2\frac{1}{3}n^2 + O(n)$. The former bound holds for all fields with characteristic distinct from two while the latter is valid over fields of characteristic zero that contain all roots of unity (like e.g. the complex numbers). Regarding division, we prove a lower bound of $\frac{5}{4}n^2 - O(n)$ and an upper bound of $3\frac{5}{6}n^2 + O(n)$. Here, the former bound is obtained for all fields while the latter again holds for fields of characteristic zero that contain all roots of unity.

The Complexity of Factors of Multivariate Polynomials

Peter Buergisser

The existence of string functions, which are not polynomial time computable, but whose graph is checkable in polynomial time, is a basic assumption in cryptography, intimately related to the existence of one-way functions.

We basically show that in the algebraic framework of computation of polynomials over infinite fields, such functions do not exist, when assuming that the degrees of the polynomials to be computed grow at most polynomially in the number of variables. Technically, we prove that the approximative complexity of a polynomial φ is polynomially bounded by the decision complexity of the graph of φ and the degree of φ. We show this by extending a result by Kaltofen (1986), which relates the complexity of a polynomial to those of its factors. The concept of approximative complexity allows to cope with the case that a factor has an exponential multiplicity, by using a perturbation argument.

Quadratic Convergence for Scaling of Matrices

Martin Fürer

Matrix scaling is an operation on nonnegative matrices with nonzero permanent. It multiplies the rows and columns of a matrix with positive factors such that the resulting matrix is (approximately) doubly stochastic. Scaling is useful at a preprocessing stage to make certain algorithms more stable. Linial, Samorodnitsky and Wigderson have recently developed the first strongly polynomial time algorithm for scaling. They have proposed to use it to approximate permanents in deterministic polynomial time. They have noticed an intriguing possibility to attack the notorious parallel matching problem. If scaling could be done efficiently in parallel, then it would approximate the permanent sufficiently well to solve the bipartite matching problem. As a first step towards this goal, we propose a scaling algorithm that converges quadratically.

Polar varieties, efficient real solving and discussion of its optimality : universal elimination is exponential

Marc Giusti

Given a system of polynomials with rational coefficients, a basic question consists of finding efficiently one point per connected component of the real solutions. We generalize previous work done for compact smooth hypersurfaces to compact smooth complete intersections. The algorithm we exhibit runs in time linear in the evaluation complexity of the input equations, and polynomial in the degree of the successive generic polar varieties [Bank-G-Heintz-Mbakop].

Then we investigate variants of polar varieties, in order to drop the compactness assumption. This leads to algorithms of essentially the same complexity [previous authors + Pardo].

Finally, we discuss the optimality of these algorithms, all based on Kronecker's elimination theory revisited algorithmically. Actually, we show that any elimination procedure satisfying a natural universality property runs at least in exponential time. And this is the case for all elimination procedure known up to now, including ours.

Complexity lower bounds for Positivstellensatz proofs

Dima Grigoriev

Recently an approach to NP-coNP problem based on proof systems using the Nullstellensatz was developed and there were shown complexity lower bounds for the proofs in such systems. In the talk a stronger proof system which relies on the Positivstellensatz is introduced and complexity lower bounds for several problems like the knapsack or the parity principle are established.

The Hardness of the Closest Vector Problem with Preprocessing

Daniele Micciancio

In the closest vector problem (CVP) one is given a lattice L and a target vector y and the goal is to find the lattice point closest to y. We consider a variant of CVP in which L is known in advance and can be arbitrarily preprocessed before the target vector is revealed. In this talk we show that there are lattices for which CVP remains hard, regardless of the amount of preprocessing. In particular, we reduce an NP-hard problem (exact 3 cover, X3C) to CVP instances (L, y) where L depends only on the size of the X3C instance being reduced.

Calculating quivers from algebras

Michael Nüsken

Straightforward description of finite dimensional algebras are usually by giving either the multiplication tensor or by embedding it in a matrix algebra $M_n(k)$ and specifying either a basis or a generating set. E.g. the upper triangular matrices would be defined by giving E_{ii} and $E_{i,i+1}$ for all meaningful i as generators.

For representation theory usually a much more informative description is used: an algebra is defined by a quiver Q, i.e. a finite, directed graph possibly with multiple edges and loops, and a set of relations R. The quiver defines a path algebra kQ with multiplication induced by concatenation of paths in Q. Then $kQ/ < R >$ is the algebra.

We use algorithms by Eberly & Giessbrecht (1996) and Ivanyos (2000) to derive an algorithm to calculate such a description for finite algebras. In fact, the notion of quiver has to be generalized to capture the existence of proper extensions of the ground fields (though no non-commutative division algebras occur). The final algorithm runs in polynomial time. It is not clear whether a conversion in the other direction can be done in polynomial time.

Segment LLL-Reduction of Lattice bases

Claus Peter Schnorr

We improve practical algorithms for LLL-reduction of lattice bases in the sense of Lenstra, Lenstra and Lovász. We organize the LLL-algorithm individual basis vectors by segments of k consecutive vectors. Local LLL-reduction of segments is done using local coordinates of dimension k.

Segment LLL-*reduced bases*, a variant of LLL-reduced bases, saves a factor n in the running time compared to standard LLL-reduction of lattices of dimension n. The concept of *iterated segments* yields a novel reduction concept admitting a divide a conquer approach. The resulting reduction algorithm runs in $O(n^3 \log_2 n)$ arithmetic steps for integer lattices of dimenstion n with basis vectors of length 2^n.

Joint work with Henrik Koy.

Improved OBDD and FBDD lower bounds for integer multiplication via universal hashing

Ingo Wegener

Integer multiplication (in particular, the middle bit of multiplication) is one of the fundamental boolean functions. It is the simplest hardware function such that circuits for them are hard to verify (even for $n = 32$). OBDDs (oblivious read-once branching programs) and FBDDs (read-once branching programs) are representations of boolean function used in verification. Hence, we are interested in improving the known lower bounds on the OBDD and FBDD size for multiplication. We are looking for asymptotically larger bounds which are large already for reasonable n. This aim has been reached by using results on universal hashing and hash functions mainly based on integer multiplication. The new results are:

a $\frac{7}{3}2^{4n/3}$ upper bound,

a $\frac{1}{96}2^{\lfloor n/2 \rfloor}$ lower bound for OBDDs, and

a $2^{\lfloor (n-9)/4 \rfloor}$ lower bounds for FBDDs.

Results of the research group members B. Bollig and P. Wlfel.

Edited by Boaz Barak

Participants

Prof. Dr. Eric Allender
allender@cs.rutgers.edu
Department of Computer Sciences
Rutgers University
Piscataway , NJ 08855
USA

Boaz Barak
boaz@wisdom.weizmann.ac.il
Dept. of Applied Mathematics and
Computer Science
The Weizmann Institute of Science
P. O. Box 26
Rehovot 76 100
ISRAEL

Prof. Dr. Paul Beame
beame@cs.washington.edu
Department of Computer Science
& Engineering FR-35
University of Washington
Seattle WA 98195
USA

Prof. Dr. Michael Ben-Or
benor@cs.huji.ac.il
Institute of Mathematics and
Computer Science
The Hebrew University
Givat-Ram
91904 Jerusalem
ISRAEL

Dr. Eli Ben-Sasson
elli@math.ias.edu
23 Ben-Zion st.
95423 Jerusalem
ISRAEL

Markus Bläser
blaeser@tcs.mu-luebeck.de
Inst. für Theoretische Informatik
Medizinische Universität Lübeck
Wallstr. 40
23560 Lübeck

Johannes Blömer
bloemer@uni-paderborn.de
FB 17: Mathematik/Informatik
Universität Paderborn
Warburger Str. 100
33098 Paderborn

Prof. Dr. Peter Bürgisser
pbuerg@math.uni-paderborn.de
FB 17: Mathematik - Informatik
- Dekanat -
Universität Paderborn
Warburger Str. 100
33098 Paderborn

Prof. Dr. Uriel Feige
feige@wisdom.weizmann.ac.il
Dept. of Applied Mathematics and
Computer Science
The Weizmann Institute of Science
P. O. Box 26
Rehovot 76 100
ISRAEL

Prof. Dr. Martin Fürer
furer@cse.psu.edu
Dept. of Computer Science & Eng.
Pennsylvania State University
State College
University Park , PA 16802
USA

Prof. Dr. Marc Giusti
Marc.Giusti@polytechnique.fr
GAGE
Ecole Polytechnique
Plateau de Palaiseau
F-91128 Palaiseau Cedex

Prof. Dr. Oded Goldreich
oded@wisdom.weizmann.ac.il,
oded@theory.lcs.mit.edu
Dept. of Applied Mathematics and Computer Science
The Weizmann Institute of Science
P. O. Box 26
Rehovot 76 100
ISRAEL

Prof. Dr. Shafi Goldwasser
shafi@theory.lcs.mit.edu
Laboratory for Computer Science
MIT
545 Technology Square
Cambridge , MA 02139
USA

Prof. Dr. Dima A. Grigoriev
dima@maths.univ-rennes1.fr
IMR
Universite Rennes 1
Beaulieu
F-35042 Rennes

Prof. Dr. Johan Hastad
johanh@nada.kth.se
Dept. of Numerical Analysis and Computing Science
Royal Institute of Technology
Lindstedtsvägen 25
S-100 44 Stockholm

Dr. Valentine Kabanets
kabanets@ias.edu
School of Mathematics
Institute for Advanced Study
Olden Lane
Princeton , NJ 08540
USA

Prof. Dr. Marek Karpinski
marek@cs.uni-bonn.de
Institut für Informatik
Universität Bonn
Römerstraße 164
53117 Bonn

Dr. Hartmut Klauck
klauck@thi.informatik.uni-frankfurt.de
Fachbereich Informatik - FB 20
Universität Frankfurt
Postfach 111932
60054 Frankfurt

Prof. Dr. Matthias Krause
krause@th.informatik.uni-mannheim.de
Theoretische Informatik
Universität Mannheim
L 13,17
68131 Mannheim

Prof. Dr. Friedhelm Meyer auf der Heide
fmadh@uni-paderborn.de
Heinz-Nixdorf Institut &
FB Mathematik - Informatik
Universität Paderborn
Fürstenallee 11
33102 Paderborn

Daniele Micciancio
daniele@cs.ucsd.edu
Dept. of Computer Science
University of California, San Diego
La Jolla , CA 92037
USA

Michael Nüsken
nuesken@uni-paderborn.de
FB 17: Mathematik/Informatik
Universität Paderborn
33095 Paderborn

Prof. Dr. Ran Raz
ranraz@wisdom.weizmann.ac.il
Dept. of Applied Mathematics and
Computer Science
The Weizmann Institute of Science
P. O. Box 26
Rehovot 76 100
ISRAEL

Omer Reingold
omer@research.att.com
AT&T Labs-Research
Room A243
180 Park Avenue
Florham Park , NJ 07932
USA

Prof. Dr. Rüdiger Reischuk
reischuk@tcs.mu-luebeck.de
Inst. für Theoretische Informatik
Medizinische Universität Lübeck
Wallstr. 40
23560 Lübeck

Prof. Dr. Shmuel Safra
safra@math.tau.ac.il
School of Mathematics
Tel-Aviv University
69978 Tel-Aviv
ISRAEL

Amit Sahai
amits@theory.lcs.mit.edu
Laboratory for Computer Science
Massachusetts Institute of
Technology
545 Technology Square
Cambridge , Ma 02139
USA

Prof. Dr. Georg Schnitger
georg@informatik.uni-frankfurt.de
Fachbereich Informatik - FB 20
Universität Frankfurt
Postfach 111932
60054 Frankfurt

Prof. Dr. Claus-Peter Schnorr
schnorr@informatik.uni-frankfurt.de,
schnorr@cs.uni-frankfurt.de
Mathematisches Seminar
Fachbereich Mathematik
Universität Frankfurt
Postfach 111932
60054 Frankfurt

Prof. Dr. Arnold Schönhage
schoe@informatik.uni-bonn.de
Institut für Informatik II
Universität Bonn
Römerstraße 164
53117 Bonn

Dr. Uwe Schöning
schoenin@informatik.uni-ulm.de
Fakultät für Informatik
Universität Ulm
Albert-Einstein-Allee 11
89081 Ulm

Dr. Ronen Shaltiel
ronens@math.ias.edu
School of Mathematics
Institute for Advanced Study
Olden Lane
Princeton , NJ 08540
USA

Dr. Amin Shokrollahi
amin@digitalfountain.com
Digital Fountain, Inc.
600 Alabama Street
San Francisco , CA 94110
USA

Dr. Amir Shpilka
amirs@cs.huji.ac.il
Institute of Mathematics and
Computer Science
The Hebrew University
Givat-Ram
91904 Jerusalem
ISRAEL

Prof. Dr. Madhu Sudan
madhu@mit.edu
Lab. for Computer Science
MIT
NE43-332
545 Tech Square
Cambridge , MA 02139
USA

Dr. Luca Trevisan
luca@cs.columbia.edu
Dept. of Computer Science
Columbia University
450 Computer Science Building
New York , NY 10027
USA

Prof. Dr. Chris Umans
umans@cs.berkeley.edu
15606 NE 40th St. #T175
Redmond , WA 98052
USA

Salil Vadhan
salil@deas.harvard.edu
DEAS
Harward University
Maxwell Dworkin 337
33 Oxford Street
Cambridge , MA 02138
USA

Prof. Dr. Ingo Wegener
wegener@ls2.informatik.uni-dortmund.de
Institut für Informatik II
Universität Dortmund
44221 Dortmund

Prof. Dr. Avi Wigderson
avi@cs.huji.ac.il
School of Mathematics
Institute of Advanced Studies
Olden Lane
Princeton , NJ 08540
USA

Prof. Dr. David Zuckerman
diz@cs.utexas.edu
Computer Science Division
University of California
at Berkeley
387 Soda Hall
Berkeley , CA 94720
USA