Tagungsbericht 48/1994

Komplexitätstheorie

13. bis 19.11.1994

The 11th Oberwolfach Conference on Complexity Theory was organized by Joachim von zur Gathen (Paderborn/Toronto), Claus-Peter Schnorr (Frankfurt) and Volker Strassen (Konstanz). There were 35 participants coming from nine countries.
The 30 lectures covered a broad range of current research in complexity theory. Several talks dealt with the new theories of approximability and probabilistically checkable proofs. Another major area was the complexity of algebraic, arithmetic, geometric, and combinatorial problems. Further topics included (visual) cryptography, parallel computation, anticipating software, and quantum computation. It was an active and stimulating meeting.

Vortragsauszüge

M. Bellare:

Free bits in PCP – How low can you go?

The best known approximation algorithm for Max Clique approximates within a factor of $N^{1-o(1)}$ (Boppana-Haldorsen), scarcely better than trivial. The past few years have seen much progress towards establishing matching "lower bounds", based on the use of probabilistically checkable proofs (the current record is that Max Clique cannot be approximated within $N^{\frac{1}{4}}$ unless $NP \subseteq coRP$). In application of proof checking it turns out that a particular measure of proof verification complexity is crucial – the number of *amortized, free bits* used (if a verifier uses f of these the Max Clique is hard within $N^{\frac{1}{1+f}}$).
The work described here continues to further the free bit approach, strengthening and deepening the free bit to approximation connection. The talk described two main results:

- $NP \subseteq FPCP(\log, 2)$ – NP can be recognized with logarithmic randomness and 2 amortized free bits. This implies that Clique is hard within $N^{\frac{1}{3}}$ (the techniques also imply Max 3SAT hard within $\frac{38}{39}$ and Max 2SAT hard within $\frac{95}{96}$).
- More interesting, from the point of view of the authors, is a result saying that to prove Clique is hard within $N^{\frac{1}{1+\hat{f}}}$ it is *necessary* to first provide a non-trivial $FPCP(\log, \hat{f})$ proof system. Free bits and proofs are intrinsically connected to approximation.

(Joint work with O. Goldreich and M. Sudan)

A. Björner:

Topological and combinatorial methods for decision trees

In the first part of the talk an overview was given of the recent Betti number lower bounds for various decision trees and computation networks, due to Björner–Lovász, Yao and Montaña–Morais–Pardo. In the second part examples were given showing that these theoretical lower bounds can actually be computed for realistic problems in some cases, using a mixture of topological and combinatorial techniques.

S. Cook:

The Relative Complexity of NP Search Problems

Papadimitriou introduced classes of search problems based on combinatorial principles which guarantee the existence of solutions. For example, the class PPA is based on the lemma that every undirected graph with an odd degree node must have another odd degree node, and PPP is based on the pigeonhole principle. The class PPAD is a directed version of PPA. Whereas Papadimitriou used Turing machines to present the graphs in question, we treat each problem as a second-order search problem in which the graph is presented by an oracle. We close each class under polynomial-time Turing reducibility.

Some inclusions among these classes are easy to prove; for example PPAD can be seen to be a subclass of PPA by ignoring the direction information on the edges. To show that the reverse inclusion fails is more difficult, and involves a combinatorial lemma of interest in its own right. In fact, we (with Edmonds and Impagliazzo) have been able to give an almost complete picture of inclusions and separations among the classes that we consider. We also show that these problems are not polynomial-time equivalent to decision problems (in contrast to search problems based on NP complete languages).

This work grew out of my collaborators' study of the propositional proof complexity of the combinatorial principles in question. They have developed powerful techniques to bear on both areas, involving for example Hilbert's Nullstellensatz.

(Joint work with P. Beame and T. Pitassi)

U. Feige:

Towards subexponential algorithms for NP

An approach is presented that may lead to subexponential algorithms for NP. The approach involves designing algorithms that moderately improve over exhaustive search for finding small cliques in graphs. In particular, if cliques of size $\log n$ can be found in polynomial time, then nondeterministic circuits of size s can be simulated by deterministic circuits of size slightly above $2^{\sqrt{s}}$.

(Joint work with J. Kilian)

M. Fürer:

Lower Bounds on the Performance of Approximate Coloring Algorithms

Graph coloring has long been conjectured to be hard to approximate. No polynomial time algorithm is known to color every graph G with $\chi(G)n^{1-\delta}$ colors where n is the number of vertices, $\chi(G)$ is the chromatic number, and δ is any positive constant. The recent hardness results based on interactive proof systems have partially explained this situation by enabling lower bounds of n^{ϵ} on the performance ratio of any polynomial time coloring algorithm (based on complexity assumptions).

A simplified geometric proof is presented for just this result without trying to maximize ϵ. More sophisticated techniques are required to improve ϵ. A randomized twisting method allows us to completely pack a certain space with copies of a graph without much affecting the independence number. This implies improvements under widely believed complexity assumptions. Unless $NP \subseteq ZPP$, we get a lower bound of $n^{1/5-o(1)}$, based on new results of Bellare, Goldreich and Sudan on the number of free bits ($f = 2 + o(1)$). We also get polynomial lower bounds in terms of $\chi(G)$.

M. Furst:

Anticipating Software

While computers are getting faster and faster, humans are not. At present machine speeds, computers are able to ask themselves the question "has he hit a key yet?" more than a million times before a person manages to make the next stroke. The way current systems are built, essentially all of these million cycles go to waste.

In anticipating software, during idle cycles the computer considers what command the person typing means to issue. For example, after typing "L", the computer might guess that the person is planning to type "latex my-latest-paper.tex". Based on its guess, anticipating software carries out that part of the command which can be done in anticipation of the actual request. In the event that the computer guesses correctly, a great deal of computational work will already be finished before the user is done saying the command. In the event the computer guesses incorrectly, the computational work is thrown away and

the user is unaware that anything went on.
We have done some work developing systems designs which can accomplish these kinds of anticipatory behaviors.
An interesting on-line mathematical model is the following: Servers will be asked to process a series of requests $R_1, R_2, \ldots, R_n$. Before each request the servers will be presented with a probability distribution on the R_i's such that $p(R_i)$ is the probability the next request will be R_i. Before seeing the next request the servers may carry out any single request for free. Then when the actual request arrives they are charged for the time it takes them to process it.
We have results describing what happens when the requests are requests to Move-To-Front, Splay-Tree, and the Double-Coverage k-server algorithm.

J. von zur Gathen:

Permutation functions

A polynomial $f \in \mathbb{F}_q[x]$ over a finite field $\mathbb{F}_q$ is called a permutation polynomial iff the associated mapping $\mathbb{F}_q \longrightarrow \mathbb{F}_q$ is bijective. We discuss various aspects: fast tests for this property, generalizations to rational functions, behaviour under composition, and counting the number of points on a curve or on its projection.
This topic brings together several areas: algebra, geometry, number theory, combinatorics, algorithmics.

M. Giusti:

Duality and straight-line programs

This talk is devoted to upper bounds on the complexity of elimination theory for polynomials with integer coefficients.
First are presented results of Krick–Pardo based on previous work by Fitchas–Giusti–Smietanski: the membership to a complete intersection and the Nullstellensatz (decision and representation of some non-zero integer constant) are in the BPP-class of bounded error probabilistic polynomial machines.
More precisely, let $f_1, \ldots, f_s$ be polynomials in $\mathbb{Z}[x_1, \ldots, x_n]$ of degree and absolute height bounded by $d \geq n$ and η respectively, which don't share any zero in $\mathbb{C}^n$. Then there exists a non-scalar straight-line program of size $d^{O(n)}$, depth $O(n \log_2 d)$ and integer parameters of absolute height $\max(d^{O(n)}, \eta)$ which evaluates an integer $a \in \mathbb{Z} - \{0\}$ and polynomials in $\mathbb{Z}[x_1, \ldots, x_n]$ such that $a = g_1 f_1 + \ldots + g_s f_s$ holds.
As a corollary is obtained a bound for the height of any isolated point of an algebraic variety defined over $\mathbb{Z}$: with the same notations as above, this height is at most $d^{O(n)}(\log_2 s + \log_2 \eta)$.
This bound is similar to the one obtained by Bost–Gillet–Soulé using arithmetic intersection theory.
Eventually, work in progress by Giusti–Heintz–Morais–Pardo is presented in comparison

of the results of Shub–Smale: solving 0-dimensional systems in sequential time polynomial in the affine degree and the maximal length of straight-line programs encoding the input polynomial. This needs a slight modification of the models used before.

O. Goldreich:

Knowledge Complexity

Zero-knowledge is the lowest level of a knowledge-complexity hierarchy which quantifies the "knowledge revealed in an interaction". Knowledge complexity may be defined as the minimum number of oracle-queries required in order to (efficiently) simulate an interaction with the prover. This natural definition is shown to be almost equivalent to another natural definition. Preliminary results concerning knowledge complexity assert that languages which have interactive proofs of logarithmic knowledge complexity can be recognized by a probabilistic polynomial-time machine with access to an NP oracle.
(Based on joint works with E. Petrank and R. Ostrovsky)

E. Grädel:

The power of syntactic criteria for approximability

There exist a number of logically defined classes of numerical invariants of finite structures, which provide syntactic criteria for approximability: MAX SNP, MAX NP, MIN $F^+\Pi_1$, $\#\Sigma_1$, ...

The relationship to computational approximation classes was discussed, in connection to the general problem of computing complexity classes on unordered finite structures. A probabilistic analysis of the syntactic classes $\#\Sigma_1$, MAX Σ_1^{FP}, ... was presented, using limit laws from finite model theory. As a consequence it was shown that a number of simple (i.e. PTIME) problems are not in these classes.

We also proved that there are general limits for the power of logical counting classes $\#L$ (for arbitrary logics L). On the other side, logical classes contain functions that coincide with computational classes almost everywhere.
(Joint work with K. Compton)

D. Grigoriev:

Complexity lower bounds for extended classes of computation trees

This is a survey of recent results on lower bounds for different computational models. A lower bound log N was obtained for complexity of the membership problem to a polyhedron with N facets by means of an algebraic decision tree. This generalizes the result of A. Yao, R. Rivest ascertained for linear decision trees. If we add to the arithmetic operations in a tree the gate functions like exp, log (on the positive half line), sin (on the interval $(-\pi, \pi)$), or any other Pfaffian function, the complexity lower bound $(\log N)^{\frac{1}{2}}$ for this problem was proved.

For a circuit using exp, log in addition to the arithmetic operations and computing an algebraic function, a lower bound $\log \|G\|$ was proved, where G is the Galois group of the algebraic function. This generalizes the result of J. Ja'Ja' obtained for the circuits with root extractions.

A step towards the open problem of computability of the additive complexity was made: we proved that the additive complexity is computable for the circuits with root extractions.

J. Heintz:

Much ado about $\emptyset$

The subject of the talk is the conjectured unfeasibility of geometric elimination with respect to sequential time. Main examples come from consistency testing and (0-dimensional) equation solving of polynomial systems. The assumption of a polynomial complexity character of elimination is incompatible with a series of generally accepted conjectures in Computer Science (Cook's thesis, Valiant's thesis, existence of one-way functions etc.). On the other hand slight modifications of the mentioned elimination problems (e.g. through conditions imposed on the form of the output) lead immediately to exponential lower bounds.

(Joint work with J. Morgenstern)

E. Kaltofen:

Subquadratic-Time Factoring of Polynomials over Finite Fields

A new probabilistic algorithm is presented for factoring univariate polynomials over finite fields. The algorithm factors a polynomial of degree n over a field of constant cardinality in time $O(n^{1.815})$ arithmetic operations. The new algorithm relies on fast matrix multiplication techniques. The baby step/giant step techniques employed also yield new practical implementations with $O(n^{2.5})$ running time.

(Joint work with V. Shoup)

M. Karpinski:

Lower bounds for randomized computation trees

We introduce a new method for proving lower bounds for algebraic computation trees. We prove, for the first time, that the minimum depth for any randomised computation tree for the problem of testing membership to a polygon with N nodes is $\Omega(\log N)$(the method also yields the first $\Omega(\log N)$ lower bound for the deterministic computation trees). Moreover,

we prove that the corresponding lower bound for the algebraic exp-log computation trees is $\Omega(\sqrt{\log N})$.
(Joint work with D. Grigoriev)

F. Meyer auf der Heide:
Hashing Strategies for Simulating Shared Memory
The talk surveys joint work with R. Karp, M. Luby, M. Dietzfelbinger, C. Scheideler, A. Csumaj and V. Stemann on Simulations of PRAMs on Distributed Memory Machines, DMMs.
We introduce methods to map the shared memory cells to the memory modules of the DMM, that are defined by a hash functions $h_1, \ldots, h_a$, randomly chosen from some high performance universal class of hash functions: $h_i : U \longrightarrow [U]$ maps the shared memory cells $u \in U$ to modules $M_{h_i(u)}$, for $i = 1, \ldots, a$. For $a = 1$, and given access requests $u_1, \ldots, u_n \in U$, it is well known that time $\Theta(\frac{\log(n)}{\log\log(n)})$ is best possible for satisfying all requests.
We show that such an inherent lower bound does not hold, if we apply $a \geq 2$, and only require $b < a$ of the copies of each u_j to be accessed. For this case, we present and analyse an access protocoll that needs time $O(\log\log(n))$, with high probability. A more sophisticated protocol, that does explorations of the access graph, can be designed with delay $O(\log\log\log(n)\log^*(n))$, with high probability. This is the fastest known simulation of shared memory on DMMs.

S. Micali:
CS Proofs
We introduce the new model of a Computationally Sound Proof. CS Proofs are short strings, vouching the correctness of a given statement, satisfying the following conditions: for any statement, if the statement is true a CS proof for it is easily found (i.e. not harder to find than *deciding* the statement), while if the statement is wrong then a CS proof for it is impossibly hard to find. CS Proofs are polylogarithmically long in the time necessary to decide their corresponding statements, and can be inspected in polynomial time. They have important applications to computational correctness. We can construct CS Proofs (for any theorem and without any unproven assumptions) given a random oracle.

N. Nisan:
Symmetric Logspace is Closed Under Complement
We present a Logspace, many-one reduction from the undirected *st*-connectivity problem

to its complement. This shows that SL=co-SL.
(Joint work with A. Ta-Shma)

T. Recio:

Complexity of semialgebraic sets

The complexity of a semialgebraic set S is defined as the complexity of solving the "membership" problem to this set. In the talk we review several recent results of the team of the University of Cantabria (Montaña, Morais, Pardo, Recio) to finding *lower bounds* for this compexity: estimation of the complexity of arithmetic networks (parallel RAMs) in terms of the number of connected components and sum of Betti numbers; estimation by means of "intersection" with auxiliar sets; estimation by means of the concept of "width" of a semialgebraic set and "corner" points.

R. Reischuk:

Asymptotics of Average Circuit Complexity

A distribution μ is *malign* for a class of computational problems if for each problem in that class the average time complexity with respect to μ is almost as large as the worst case complexity (no more than a constant factor smaller). It has been shown that uniform complexity classes have malign distributions. In this talk the nonuniform Boolean circuit model is considered and the minimal depth (delay) to compute Boolean functions by such devices. For the worst case, it has been well known that almost all n-ary Boolean functions require circuit depth $n - \log\log n + O(1)$.
We show that circuits do not have malign distributions. For any distribution μ on $\{0,1\}^n$ one can find a Boolean function f_μ over that domain with a huge gap between its worst case delay, which is $n - \log n - \log\log n$, and its average delay, which is constant.
For the asymptotic case, however, it proved that almost all n-ary Boolean functions have average complexity at least $n - \log n - \log\log n$. Finally we show that for any Boolean function f of worst case complexity t one can construct a distribution μ_f such that the average complexity of f with respect to μ_f is at least $t - \log n - \log t$.
(Joint work with A. Jacoby and C. Schindelhauer)

H. Ritter:

Construction of a shortest lattice vector in any $\|.\|_p$-norm

Several NP-complete problems can efficiently be reduced to the problem of finding shortest lattice vectors with respect to $\|.\|_p$-norms ($\|.\|_\infty$-norm for subset sum, 3-SAT, $\|.\|_1$ for integer factorization). We use the equivalence of all norms on $\mathbb{R}^n$ to extend the enumeration algorithm with respect to the Euclidean norm to get short vectors in the $\|.\|_p$-norm. Using

Hölder's inequality we achieve a deterministic pruning rule which cuts down the size of the enumeration tree by an exponential factor. With these techniques it is possible to solve *all* subset sum problems up to dimension 66 with a deterministic algorithm in average time less than 2 hours on a 132 MFLOPS workstation. We also succeed in attacking a toy example of the Chor-Rivest cryptosystem in dimension 103.

C. Schnorr:

Black Box Cryptanalysis of Hash Networks

Black box cryptanalysis applies to hash algorithms consisting of many small boxes, connected by a known graph structure, so that the boxes can be evaluated forward and backwards by given oracles. We study attacks that work for arbitrary boxes that perform a multipermutation with two inputs and two outputs. Multipermutations correspond to pairs of orthogonal lattice squares. We present optimal black box inversions of FFT-compression functions along with matching upper and lower complexity bounds. The lower bound uses a degree concept where the multipermutation boxes have degree of freedom 2. Then the lower bound follows from a lower bound on the local expansion rate of the FFT-graph. We determine this expansion rate by a combinatorial argument.
(Joint work with S. Vaudenay)

A. Schönhage:

Speed-ups for algorithms with exact division

First we show how to speed up exact division $\frac{f}{g} = q$ of integers or polynomials over some finite field or $\mathbb{Z}$ (where the remainder is known to be zero) by a factor of about 4 as compared to the classical standard algorithm for full division. This is done by combining 2-adic division for the lower half of the quotient and approximate (real) division for its upper half.
Then we apply this technique for speeding up Barreiss' method for exact Gaussian elimination and Collins' subresultant algorithm by similar factors. Moreover, with regard to large problem size, we demonstrate an asymptotical method based on exact divisions in rings $\mathbb{Z}$ mod $(2^N + 1)$.
(Joint work with E. Vetter)

A. Shamir:

Visual cryptography

In this talk I consider a new type of cryptographic scheme, which can decode concealed images without any cryptographic computations. The scheme is perfectly secure and very easy to implement. I extend it into a visual variant of the k out of n secret sharing problem,

in which a dealer provides a transparency to each of the n users; any k of them can see the image by stacking their transparencies, but any $k-1$ of them gain no information about it.
(Joint work with M. Naor)

A. Shokrollahi:

Computation of irregular indices

A pair $(p, 2i)$ is called irregular if $p \in \mathbb{P}, 2 \leq 2i \leq p-3$, and $p|B_{2i}$, where B_n is the nth Bernoulli number. We propose a new method for computing irregular pairs. This method is based on the zeores of a certain polynomial of degree $\frac{p+1}{2}$ over $\mathbb{F}_p$.

A. Sinclair:

Monte Carlo algorithms in physics

Many quantities in statistical physics are computed using so-called "Monte Carlo experiments". The algorithms involve simulating a Markov chain whose states are the configurations of a physical system, and which converges to some carefully chosen stationary distribution. In most cases, the time to convergence has not been precisely analyzed, so the results obtained from such algorithms must be taken on good faith. This talk describes three examples in which a precise analysis is possible: the monomer-dimer model, the ferromagnetic Ising model, and the self-avoiding walk model for linear polymers. As a result, one can prove the existence of Monte Carlo algorithms for each of these systems that provide statistically rigorous outputs in polynomial time.

J. Stern:

k-transitivity of random graphs and an application to cryptography

Let τ_0, τ_1 be two independent random permutations of $\{1, \ldots, n\}$. We consider the directed graph $G_k(\tau_0, \tau_1)$ whose vertices consist of k-tuples of distinct integers in $\{1, \ldots, n\}$ and whose edges are the pairs

$$\{(a_1, \ldots, a_k), (\tau_i(a_1), \ldots, \tau_i(a_k)\} \quad i = 0, 1.$$

We show that, with high probability, $G_k(\tau_0, \tau_1)$ is a good expander hence has small diameter.

The problem comes from a suggestion in cryptography: it has been thought that secret key identification could be achieved by sending a query of N bits, w, and requesting the final vertex reached by a walk starting at some fixed integer in $\{1, \ldots, n\}$ and following edges of $G_1(\tau_0, \tau_1)$ according to w. Our result shows that such a scheme is secure (slightly

more elaborate proposals might be safe).
(Joint work with J. Friedmann, A. Joux, Y. Roichman and J.-P. Tillich)

M. Sudan:

Linearity Testing

Given finite groups G and H and f mapping G to H, define

$$\epsilon_f \triangleq \min_{g \in \mathrm{Hom}(G,H)} \{\Pr_x[f(x) \neq g(x)]\}, \text{ and } \delta_f \triangleq \Pr_{x,y}[f(x)+f(y) \neq f(x+y)].$$

Both ϵ_f and δ_f study the "proximity" of f to the space of homomorphisms among groups. In particular $\epsilon_f = 0 \Leftrightarrow \delta_f = 0 \Leftrightarrow f$ is a homomorphism. "Linearity Testing" studies the relationship between ϵ and δ.
Tight analysis of this picture was undertaken by Blum, Luby and Rubinfeld, and later by Coppersmith – for the case of general graphs. A tight analysis for the case where $G = \mathbb{Z}_2^n$ and $H = \mathbb{Z}_2$ is presented here yielding the relationship

$$\delta_f < \frac{45}{128} \Longrightarrow \epsilon_f < \frac{1}{4}.$$

(Joint work with M. Bellare and D. Coppersmith)

U. Vazirani:

Quantum Computation

An exciting sequence of recent results have established that computers based on quantum physics can perform tasks that appear inherently intractible on classical computers. These results rely on the exponential growth of the dimension of the Hilbert space associated with a system of several 2-state units. All the known algorithms for quantum computers rely on their ability to efficiently sample from the Fourier power spectrum even in exponentially high dimensional spaces. This talk will survey the model and its capabilities and explain the workings of the recent algorithm by Shor for factoring integers in polynomial time on a quantum computer.

I. Wegener:

Hierarchy results for restricted branching programs

Branching programs are a well-known computation model in complexity theory. Restricted models like read k times or oblivious branching programs have been investigated intensively. Similar models are considered in applications like formal verification. For such models of polynomial size, tight hierarchy results are proved. The models are read once branching programs, where on each path k variables may be tested arbitrarily often, and ordered and indexed binary decision diagrams with k layers. The results are proved with methods from combinatorics, linear algebra and communication complexity.

V. Weispfenning:

On the complexity of parametric optimization problems

We consider optimization problems

$$A\underline{x} \geq \underline{b}, \quad q = \min!$$

where the constraints are linear and the objective function q is linear, fractional linear or quadratic. Parameters may enter either additively (i.e. $\underline{b} = \underline{b}(\underline{u})$) or more generally in all coefficients of the problem.

We describe an elimination algorithm that outputs a list of polynomial (or rational function) data that provide a solution uniformly in the parameters. The algorithm runs in EXPTIME, and for non-parametric input in PSPACE. For linear objective function q and/or band matrices A the upper bounds can be improved further.

Conerning lower bounds, we show that the linear optimization problem with additive parameters is inherently exponential. Moreover the classical Fourier–Motzkin elimination method for this problem has a doubly exponential worst-case lower bound.

Examples with up to 50 variables computed in a REDUCE implementation confirm the practical applicability of the algorithm.

Berichterstatterin: S. Hartlieb

Monday, 14.11.

Chair: A. Shamir

9:30-9:40	Opening	
9:40-10:40	S. Micali	CS proofs and program correctness
11:00-11:40	D. Grigoriev	Complexity lower bounds for extended classes of computation trees
11:45-12:25	E. Grädel	The power of syntactic criteria for approximability

Chair: M. Furst

15:30-16:10	O. Goldreich	Knowledge Complexity
16:15-16:45	M. Bellare	Free bits in PCP
17:05-17:45	M. Fürer	On the hardness of approximating the chromatic number
17:50-18:30	M. Karpinski	Lower bounds for randomized computation trees

Tuesday, 15.11.

Chair: S. Micali

9:00-9:50	S. Cook	The relative complexity of NP search problems
9:55-10:30	I. Wegener	Hierarchy results for restricted branching programs
10:50-11:40	M. Sudan	Linearity Testing
11:45-12:15	R. Reischuk	Asymptotics of average circuit complexity

Chair: M. Giusti

15:30-16:00	A. Schönhage	Speed-ups for algorithms with exact division
16:05-16:35	J. von zur Gathen	Permutation Functions
16:55-17:25	A. Shokrollahi	Computation of indices of irregularity
17:30-17:55	T. Recio	Complexity of semialgebraic sets

Wednesday, 16.11.

Chair: A. Schönhage

9:15-9:45	A. Shamir	Visual cryptography
9:50-10:30	U. Feige	Towards subexponential algorithms for NP
10:50-11:10	A. Björner	Topological and combinatorial methods for linear decision trees
11:15-11:55	U. Vazirani	Quantum computation

Thursday, 17.11.

Chair: S. Cook

9:15-9:55	A. Sinclair	Monte Carlo algorithms in physics
10:05-10:50	M. Giusti	Duality and straight line programs
11:10-11:40	J. Heintz	The intrinsic complexity of geometric eliminaton

Chair: E. Kaltofen

16:00-16:30	C. P. Schnorr	Black box cryptanalysis
16:35-17:05	M. Furst	Anticipating Software
17:25-17:55	N. Nisan	Symmetric log space is closed under complement
18:00-18:30	H. Ritter	Construction of a shortest lattice vector in the $\|.\|_p$-norm

Friday, 18.11.

Chair: O. Goldreich

9:30-10:00	E. Kaltofen	Subquadratic-time factoring of polynomials
10:10-10:45	V. Weispfenning	On the complexity of parametric optimization problems
11:05-11:45	F. Meyer auf der Heide	Hashing Strategies for Simulating Shared Memory
11:50-12:20	J. Stern	k-transitivity of random graphs and an application to cryptography

Bellare, M.	mihir@watson.ibm.com
Bjőrner, A.	bjorner@math.kth.se
Bürgisser, P.	buerg@amath.unizh.ch
Clausen, M.	clausen@cs.uni-bonn.de
Cook, S.	sacook@cs.toronto.edu
Feige, U.	feige@wisdom.weizmann.ac.il
Fürer, M.	furer@cse.psu.edu
Furst, M.	furst@cs.cmu.edu
von zur Gathen, J.	gathen@uni-paderborn.de
Giusti, M.	giusti@polytechnique.fr
Goldreich, O.	oded@wisdom.weizmann.ac.il
Grädel, E.	graedel@informatik.rwth-aachen.de
Grigoriev, D.	dima@cse.psu.edu
Hartlieb, S.	hartlieb@uni-paderborn.de
Heintz, J.	heintz@ccucvx.unican.es
	joos@mate.dm.uba.ar
Kaltofen, E.	kaltofen@cs.rpi.edu
Karpinski, M.	marek@cs.uni-bonn.de
Meyer auf der Heide, F.	fmadh@uni-paderborn.de
Micali, S.	silvio@lcs.mit.edu
Nisan, N.	noam@cs.huji.ac.il
Recio, T.	recio@matsun1.unican.es
Reischuk, R.	reischuk@informatik.mu-luebeck.de
Ritter, H.	ritter@mi.informatik.uni-frankfurt.de
Safra, S.	safra@cs.huji.ac.il
Schnorr, C.	schnorr@cs.uni-frankfurt.de
Shamir, A.	shamir@wisdom.weizmann.ac.il
Shokrollahi, A.	amin@cs.uni-bonn.de
Sinclair, A.	sinclair@cs.berkeley.edu
Stern, J.	stern@dmi.ens.fr
Sudan, M.	madhu@watson.ibm.com
Vazirani, U.	vazirani@cs.berkeley.edu
Wegener, I.	wegener@ls2.informatik.uni-dortmund.de
Weispfenning, V.	weispfen@alice.fmi.uni-passau.de

Tagungsteilnehmer

Dr. Mihir Bellare
IBM Corporation
Thomas J. Watson Research Center
P.O. Box 704

Yorktown Heights , NY 10598
USA

Prof.Dr. Anders Björner
Dept. of Mathematics
Royal Institute of Technology

S-100 44 Stockholm

Peter Bürgisser
Institut für Angewandte Mathematik
Universität Zürich
UZI
Winterthurer Str. 190

CH-8057 Zürich

Prof.Dr. Michael Clausen
Institut für Informatik V
Universität Bonn
Römerstr. 164

53117 Bonn

Prof.Dr. Stephen A. Cook
Department of Computer Science
University of Toronto

Toronto, Ontario , M5S 1A4
CANADA

Prof.Dr. Uriel Feige
Dept. of Applied Mathematics and
Computer Science
The Weizmann Institute of Science
P. O. Box 26

Rehovot 76 100
ISRAEL

Prof.Dr. Martin Fürer
Dept. of Computer Science & Eng.
Pennsylvania State University
State College

University Park , PA 16802
USA

Prof.Dr. Merrick L. Furst
School of Computer Science
Carnegie Mellon University
Schenley Park

Pittsburgh , PA 15213-3890
USA

Prof.Dr. Joachim von zur Gathen
FB 17: Mathematik/Informatik
Universität Paderborn
Warburger Str. 100

33098 Paderborn

Prof.Dr. Marc Giusti
Centre de Mathematiques
Ecole Polytechnique
Plateau de Palaiseau

F-91128 Palaiseau Cedex

Prof.Dr. Oded Goldreich
Dept. of Applied Mathematics and
Computer Science
The Weizmann Institute of Science
P. O. Box 26

Rehovot 76 100
ISRAEL

Erich Grädel
Lehr- u. Forschungsgebiet
Mathem. Grundlagen der Informatik
RWTH Aachen
Ahornstr. 55

52074 Aachen

Prof.Dr. Dima A. Grigoriev
Dept. of Computer Science & Eng.
Pennsylvania State University
State College

University Park , PA 16802
USA

Silke Hartlieb
FB 17: Mathematik/Informatik
Universität Paderborn
Warburger Str. 100

33098 Paderborn

Prof.Dr. Joos Heintz
Departamento de Matematicas
Fac. Ciencias
Universidad de Cantabria
Avenida de los Castros s/w

E-39071 Santander

Prof.Dr. Erich Kaltofen
Department of Computer Science
Rensselaer Polytechnic Institute

Troy , NY 12180-3590
USA

Prof.Dr. Marek Karpinski
Institut für Informatik
Universität Bonn
Römerstraße 164

53117 Bonn

Prof.Dr. Friedhelm Meyer auf der Heide
FB 17: Mathematik/Informatik
Universität Paderborn
Warburger Str. 100

33098 Paderborn

Prof.Dr. Silvio Micali
Laboratory for Computer Science
Massachusetts Institute of
Technology
545 Technology Square

Cambridge , Ma 02139
USA

Prof.Dr. Noam Nisan
Institute of Computer Science
Hebrew University of Jerusalem
Givat-Ram

91904 Jerusalem

Prof.Dr. Tomas Recio
Departamento de Matematicas,
Estadistica y Computacion
Universidad de Cantabria

E-39071 Santander

Prof.Dr. Rüdiger Reischuk
Institut für Techn. Informatik
Medizinische Universität Lübeck
Wallstr. 40

23560 Lübeck

Harald Ritter
Fachbereich Mathematik
Universität Frankfurt
Robert-Mayer-Str. 6-10

60325 Frankfurt

Prof.Dr. Shmuel Safra
Institute of Computer Science
Hebrew University of Jerusalem
Givat-Ram

91904 Jerusalem

Prof.Dr. Claus-Peter Schnorr
Mathematisches Seminar
Fachbereich Mathematik
Universität Frankfurt
Postfach 111932

60054 Frankfurt

Prof.Dr. Arnold Schönhage
Institut für Informatik II
Universität Bonn
Römerstraße 164

53117 Bonn

Prof.Dr. Adi Shamir
Dept. of Mathematics
The Weizmann Institute of Science
P. O. Box 26

Rehovot 76 100
ISRAEL

Dr. Mohammad Amin Shokrollahi
Institut für Informatik V
Universität Bonn
Römerstr. 164

53117 Bonn

Prof.Dr. Alistair J. Sinclair
Dept. of Computer Science
University of California
587 Evans Hall

Berkeley , CA 94720
USA

Prof.Dr. Jacques Stern
Departement de Mathematiques et
Informatiques
Ecole Normale Superieure
45, rue d'Ulm

F-75230 Paris Cedex 05

Prof.Dr. Hanns-Jörg Stoß
Fakultät für Mathematik
Universität Konstanz
D 201
Postfach 5560

78434 Konstanz

Prof.Dr. Volker Strassen
Fakultät für Mathematik
Universität Konstanz
D 201
Postfach 5560

78434 Konstanz

Dr. Madhu Sudan
IBM Corporation
Thomas J. Watson Research Center
P. O. Box 218

Yorktown Heights , NY 10598
USA

Prof.Dr. Umesh V. Vazirani
Computer Science Division
University of California
at Berkeley
591 Evans Hall

Berkeley , CA 94720
USA

Prof.Dr. Ingo Wegener
Institut für Informatik II
Universität Dortmund

44221 Dortmund

Prof.Dr. Volker Weispfenning
Fakultät für Mathematik
und Informatik
Universität Passau

94030 Passau