MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

Tagungsbericht 48/1988

Komplexitätstheorie

13.11. - 19.11.1988

The 8th Oberwolfach Conference on Complexity Theory was organized as before by C.P. Schnorr (Frankfurt), A. Schönhage (Tübingen) and V. Strassen (Konstanz). The 42 participants came from 9 countries, 17 participants came from North and South America, USSR and Israel.

34 lectures were given at the conference covering various areas of complexity theory. Most of them dealt with topics related to algebraic problems, quantifier elimination and decision problems, graphs, communication processes and cryptography.

Lectures were given on sequential resp. parallel complexity of iterations, spectral transforms, computations in finite fields, derivatives, tests, boolean functions, computing the order of finite abelian groups and multidimensional continued fraction algorithms. Others dealt with questions on polynomial ideals, differential fields, quantifier elimination and feasible functionals. Several topics on graphs have been considered, e.g. planarity, graph isomorphy, chromatic numbers, universal traversal sequences, perfect matchings, expander graphs and decomposition of graphs. Beside new algorithms for concrete problems such as hashing, routing, computing n! and the subset-sum problem further lectures were concerned with complexity classes, robust oracle machines, P-NP analogues, communication, Byzantine agreement and complexity of justice.

Participants:

H. Alt, Berlin
W. Baur, Konstanz
A. Borodin, Toronto
P. Bürgisser, Konstanz
M. Clausen, Karlsruhe
S.A. Cook, Toronto
D. Coppersmith, Yorktown Heights
U. Faigle, Enschede
M.J. Fischer, New Haven
M. Fürer, University Park, PA
M. Furst, Pittsburgh
Z. Galil, New York
J. von zur Gathen, Toronto
D.J. Grigor'ev, Leningrad
J. Heintz, Buenos Aires
B. Just, Frankfurt
E. Kaltofen, Troy
M. Karpinski, Bonn
J.C. Lagarias, Murray Hill
Th. Lickteig, Tübingen
R. Loos, Tübingen

W. Maass, Chicago
E.W. Mayr, Frankfurt
K. Mehlhorn, Saarbrücken
F. Meyer auf der Heide, Dortmund
S. Micali, Cambridge
R. Mirwald, Frankfurt
N.T. Müller, Trier
M. Paterson, Coventry
R. Reischuk, Darmstadt
C.P. Schnorr, Frankfurt
A. Schönhage, Tübingen
U. Schöning, Koblenz
A. Shamir, Rehovot
H.-J. Stoß, Konstanz
V. Strassen, Konstanz
E. Szemeredi, Budapest
V. Tobler, Konstanz
E. Upfal, San Jose
U.V. Vazirani, Berkeley
I. Wegener, Dortmund
v. Weispfenning, Passau

Abstracts

H. Alt On the Complexity of Analytic Functions

Beame, Cook and Hoover showed that integer division can be performed by log-depth Boolean circuits using an expansion of $1/x$ into a power series. With the same approach we show that the same bound can be obtained for any meromorphic function whose domain is a closed subset of $\hat{\mathbb{C}}$. Naturally, these circuit families are in general highly nonuniform or even noncomputable. Some standard elementary functions like exp, ln, sin, cos,..., however, can be shown to be NC^1-reducible to integer division and thus can be evaluated polynomial-time uniformly in logarithmic depth.

W. Baur On the algebraic complexity of iteration procedures

Let $\alpha \varepsilon \mathbb{C}$ be algebraic over some subfield k of $\mathbb{C}$. An n-point iteration procedure (I.P.) for α is a rational function $f(X_0,\ldots,X_{n-1})$ with coefficients from k such that for all starting values $x_0,\ldots,x_{n-1}$ sufficiently close to α the sequence $x_i := f(x_{i-n},\ldots,x_{i-1})$ $(i \geq n)$ converges to α. It is shown that any multipoint I.P. for α whose power series expansion at α has a unique term that determines its order of convergence can be replaced by a onepoint I.P. of the same efficiency (with respect to the nonscalar algebraic model of computation).

A. Borodin Lower Bounds for Universal Traversal Sequences

Let $\tilde{G}(d,n)$ be the set of all connected, d-regular, n-node, edge labelled, undirected graphs. For every edge (u,v) there are two labels $l_{u,v}$ and $l_{v,u}$ with the property that for every $u \varepsilon V$, $\{l_{u,v} | v \varepsilon V\} = \{0,1,2,\ldots,d-1\}$. A sequence $\alpha \varepsilon \{0,1,\ldots,d-1\}^*$ can be thought of as a sequence of edge traversal commands. That is, given a starting node $v_0 \varepsilon V$, a sequence $\alpha = \alpha_1\alpha_2\ldots\alpha_k$ determines a unique node sequence $v_0v_1 \ldots v_k$ such that $l_{v_{i-1},v_i} = \alpha_i$. The sequence α is said to traverse G starting at v_0 if and only if every node in G appears at least once in the induced sequence $v_0v_1 \ldots v_k$. Finally, α is a universal traversal sequence for $\tilde{G}(d,n)$ iff for all $G \varepsilon \tilde{G}(d,n)$ and $v_0 \varepsilon V$, α traverses $\tilde{G}$ starting at v_0. $U(d,n)$ denotes the length of the shortest universal traversal sequence for $\tilde{G}(d,n)$. (Since $\tilde{G}(d,n) \neq \emptyset$ iff dn even, we only consider $U(d,n)$ when dn is even). At present the best known upper bound for $U(d,n)$ is $O(dn^3 \log n)$ (Kahn, Linial, Nison and Saks). We prove the following lower bounds:

1) for $3 \le d \le n/4-1$ (and for infinitely many n satisfying $3 \le d \le n/3-1$), $U(d,n) = \Omega(d^2n^2)$. Then for $d = \Omega(n)$ and $d \le n/4-1$, the lower bound is within a factor of $\log n$ of optimality.

2) for small $d \ge 3$, $U(d,n) = \Omega(dn^2 \log n/d))$

(Joint work with Larry Ruzzo and Martin Tompa)

M. Clausen <u>Fast spectral transforms</u>

According to Wedderburn's Theorem the group algebra $\mathbb{C}G$ of a finite group G of order n is isomorphic to a suitable algebra of block-diagonal matrices. Every such isomorphism $W : \mathbb{C}G \to \oplus_i \mathbb{C}^{d_i x d_i}$ is called a <u>spectral</u> <u>transform</u> for $\mathbb{C}G$. W.r.t. natural $\mathbb{C}$-bases, W can be viewed as an n-square matrix. The linear complexity of W is the minimal number $L_s(W)$ of $\mathbb{C}$-operations sufficient to compute $W \cdot x$, for a generic input vector x. The <u>linear</u> <u>complexity</u> of G is defined by $L_s(G) :=$ $\min\{\max(L_s(W),L_s(W^{-1}))|W$ a spectral transform for $\mathbb{C}G\}$. The classical FFT-algorithms show that $L_s(G) = O(|G|\log|G|)$, for cyclic groups G.

<u>Theorem 1</u> If G is metabelian $(G''=1)$ then $L_s(G) = O(|G|\log|G|)$.

<u>Theorem 2</u> For arbitrary G : $L_s(G) = O(|G|^{3/2})$.

<u>Theorem 3</u> For symmetric groups: $L_s(S_n) = \mathcal{O}(|S_n|\cdot\log^3|S_n|)$.

The proofs of these results "nearly automatically" translate into highly regular VLSI-Designs.

S.A. Cook <u>Feasible Functionals</u>

(joint with Alasdair Urquhart and Bruce Kapron)

The type 1 functionals take tuples of natural numbers to natural numbers, and in general functionals of type $k+1$ take functionals of type k together possibly with functionals of type less than k and numbers, to numbers. We say that a functional is <u>feasible</u> if it is defined by some term of typed the λ-calculus using function symbols for the type 1 polynomial time computable functions and a type 2 function symbol for a recursor R which represents higher type limited recursion on notation. The type 1 feasible functionals provably coincide with the polynomial time computable functions.

We give two characterizations of the feasible functionals, both in terms of programming languages which allow procedure declarations for functionals. First, F is feasible iff it is computable by a kind of bounded loop program, and second, F is feasible iff it is computed by a kind of typed white programm in time bounded by $|G|$, for some feasible G.

D. Coppersmith Polynomials whose Powers are sparse

We produce polynomials all of whose jth powers, $j=2,3,\dots,k$, are simultaneously sparse. That is, for each integer $k \geq 2$, we find reals $c > 0$, $d < 1$, and a family of dense real univariate polynomials

$$p_n(x) = \Sigma_{i=0}^{n} p_i x^i , \quad p_i \neq 0$$

with degree n going to infinity, such that for all $j=2,3,\dots,k$, the number of nonzero terms in

$$(p_n(x))^j$$

is bounded by cn^d.
This is joint work with James Davenport (Bath).

U. Faigle Communication Complexity

Interpreting (0,1)-matrices as (reduced) incidence matrices of (partially) ordered sets, the following general problem is considered: Given an ordered set P via its incidence matrix, player I chooses an element x and player II chooses an element y. How many bits of information must the two players exchange in order to settle the question "? $x < y$?". In this context, the communication complexity of binary relations may be viewed as a parameter which is closely related to "classical" order parameters such as width, setup number, dimension. The communication complexity may be explicitly determined for special classes of orders, e.g., N-free orders and interval orders (The results are obtained jointly with Gy. Turán).

M.J. Fischer Communicating a Secret Bit without Cryptography

We consider the problem of transmitting a secret bit s from player A to player B in a situation where all communication is public and the only common information comes from a random deal of a deck of n cards. In a (p, q, r) protocol, A receives p cards, B receives q cards, and the remaining $r = n - p - q$ cards go to the opponents. For example, one simple protocol may allow A and B to find a pair of cards such that each holds exactly one card of the pair, but the opponent does not know who holds which. A then transmits s by naming the card of the pair held by A if $s=1$ and the card held by B if $s=0$. This works whenever $p,q \geq 1$ and $p+q \geq r+2$.

We then investigate whether or not a secret bit transmission protocol exists for particular triples (p, q, r) and show for example that for all $a > 0$ and all sufficiently large r, there is a (p, q, r) protocol for $p = ar$.

Theorem (Rackhoff) Let m be the probability that randomly dealt hands u and v of sizes p and q respectively have a non-empty intersection when dealt from different n-card decks. No secret bit transmission protocol for (p, q, r) exists if $m < 1/2$.

This shows for example that no $(1, 1, 1)$ protocol exists.

Finally, we investigate deterministic protocols. In a full disclosure protocol, A's first message lets B deduce the opponent's hand, but at least two hands are possible (and equiprobable) from the opponent's point of view. We exhibit full disclosure protocols for $(2, 3, 1)$ and $(3, 3, 1)$. The case $(3, 2, 1)$ is possible, but not by any full disclosure protocol.
(Joint work with Michael Paterson and Charles Rackoff)

M. Fürer A Counterexample In Graph Isomorphism Testing

Vertex classification by coloring k-simplices or ordered k-tuples for bounded k has been conjectured to solve all or many of the known tractable subclasses of the graph isomorphism problem. For $k=2$, the vertex classification by edge coloring has a fast parallel implementation, and it is so simple that most of the practical isomorphism tests should start with this algorithm. However, coloring k-tuples for bounded k is not sufficient for most of the known feasible subclasses of the graph isomorphism problem including the bounded valence case. A counterexample of valence 3 requiring valence $k = \Omega(n)$ is presented.

Z. Galil The Subset-Sum Problem and Analytic Number Theory, an Interplay

We consider the dense version of the subset-sum problem in which the number of elements (m) is longer than some power of the bound (ℓ) on the size of the elements. We describe a new approach due to G. Freman which uses theorems proved by analytic number theoretical means to characterize the set of subset sums as a collection of arithmetic progressions with the same difference. The theorems lead to algorithms for the subset-sum problem which are better than the dynamic programming approach. Recently, new algorithms which use only elementary methods have been designed (with O. Margalit). They can be used to give a proof for a theorem which is stronger than the theorems mentioned above. These algorithms are linear $(O(m))$ in some cases and are $O(\ell \log \ell)$ in all cases; thus are two orders of magnitude faster than dynamic programming. The talk discussed the limitation as well as the potential of this approach.

J. von zur Gathen Inversion in Finite Fields

Inverses in $GF(p^n)$ can be computed by (P-uniform) arithmetic circuits over $\mathbb{Z}_p$ $(\subseteq GF(p^n))$ of optimal depth $O(\log n)$. This algorithm is based on a numerical method proposed by Litow and Davida, and extends the corresponding result by Fich and Tompa, valid for small p (say, $p \leq n$).

D. Yu. Grigor'ev Complexity of factorizing and GC(R)D calculating for linear ordinary differential operators

An algorithm is designed which for a linear ordinary differential operator $L = \Sigma_{o \leq i \leq n}\, a_i(X)d/dX \varepsilon \mathbb{Q}(X)[d/dX]$ with the order n factorizes $L = L_1 \ldots L_s$, where the operators $L_1,\ldots,L_s \varepsilon \mathbb{C}(X)[d/dX]$ are irreducible. Assume that for any operators $Q_1,Q_2,Q_3 \varepsilon \mathbb{C}(X)[d/dX]$ such that $L = Q_1Q_2Q_3$ and Q_2,Q_3 are monic, $\deg_X(Q_2) \leq N$ holds. The designed factorizing algorithm has a time-bound polynomial in $(N\, \mathrm{size}(L))^{n^4}$. Besides, the bound $N \leq \exp(\mathrm{size}(L)^{2^n})$ is proved.

Also a polynomial time algorithm is produced which for a family of operators $L_1,\ldots,L_k \varepsilon \mathbb{Q}(X)[d/dX]$ yields their greatest common (right) divisor $L_o = GC(R)D(L_1,\ldots,L_k) \varepsilon\ \mathbb{Q}(X)[d/dX]$ such that $L_1 = \tilde{L}_1L_o,\ldots,$ $L_K = \tilde{L}_KL_o$ for some $\tilde{L}_1,\ldots,\tilde{L}_K \varepsilon \mathbb{Q}(X)[d/dX]$ the order of L_o is the largest possible (or in other words $\forall v\, (L_1v = \ldots = L_kv = 0 \Leftrightarrow L_ov = 0)$ holds).

J. Heintz New complexity results in computational geometry

Effective Nullstellensätze which appeared in the last time (Brownawell 1986 for characteristic 0 fields, Caniglia-Galligo-Heintz 1987, Kollár 1988, Fitchas-Galligo 1988 for arbitrary fields) allowed to consider basic algorithmic problems in Computer Algebra from the complexity point of view. In some cases satisfactory sequential complexity bounds were already known, due to previous work of Chistov-Grigor'ev and Grigor'ev-Vorobjov jr., in other cases problems became for the first time accessible to complexity analysis. However, all parallel results are new and algorithms became essentially simpler, since polynomial factorization is avoided. Linear Algebra (parallelizable) is used (Berkowitz, Chistov and Mulmuley). We now list some of the results:

Let be given an arbitrary field k, $X_1,\ldots,X_n$ indeterminates over k and $F,F_1,\ldots,F_s \ \varepsilon\ k[X_1,\ldots,X_n]$ with $d := \max_{1 \leq i \leq s} \deg F_i$. Let $\bar{k}$ be the algebraic closure of k and $V_i = \{x \in \bar{k}^n;\ F_1(x) = 0,\dots,F_s(x) = 0\}$. Write also $\mathfrak{a} := (F_1,\dots,F_s) \subset k[X_1,\dots,X_n]$.

Theorem 1: The following problems/functions can be decided/computed in sequential time $s^4 d^{O(n^2)}$ and parallel time $O(n^4 \log^2 sd)$ simultaneously:

(i) $V = \emptyset$?

(ii) $\dim V = ?$

(iii) $\deg V = ?$ (if all irreducible components of V are of the same dimension)

(iv) F zero on V ? (if $\deg F \le d$).

Theorem 2: Suppose $\dim V \le 0$ (i.e. $\# V < \infty$). Then a Gröbner (standard)-basis of $\mathfrak{a}$ can be computed in sequential time $s^4 d^{O(n^2)}$ and parallel time $O(n^4 \log^2 sd)$.

Theorem 3: (Effective and quantitative version of Suslin's Theorem) Let k be infinite and $R := k[X_1,\dots,X_n]$. Let $F = (F_{ij}) \in R^{r\times s}$ a polynomial $r\times s$-matrix with $d := \deg F := \max\limits_{i,j} \deg F_{ij}$. Suppose that F is unimodular (i.e. the $r\times r$-minors of F generate the trivial ideal R). Then there exists an unimodular matrix $M \in R^{s\times s}$ such that

(i) $F \cdot M = (1_r | 0)$ ($r\times s$ Matrix)

(ii) $\deg M = (rd)^{O(n)}$

(iii) M is computable in sequential time $r^{O(n^2)} s^{O(r^2)} d^{O(n^2+r^2)}$ and parallel time $O(n^6 r^4 \log^4 rd \log^2 sd)$.

Theorem 4: Let L be the first order language with the following nonlogical symbols: constants corresponding to the elements of k, $+,-,*,=$. We consider the first order theory of $\bar{k}$. Let $\Phi(X_1,\dots,X_r) \in L$ a formula involving $F_1,\dots,F_s \in k[X_1,\dots X_n]$. Suppose that Φ is prenex with m quantifier blocks. Then quantifiers can be eliminated from Φ in sequential time $(sd)^{n^{O(m)}}$ and parallel time $n^{O(m)}(\log sd)^{O(1)}$. (The doubly exponential sequential and the simply exponential parallel bound are intrinsic by the existence of corresponding lower bounds.) As a consequence one obtains for $k = \mathbb{Q}$ and n fixed an NC-algorithm deciding the satisfiability of quantifier free formulas in $\mathbb{R}^n$. In particular, this algorithm "solves" polynomial inequality systems (compare corresponding sequential results of Grigor'ev-Vorobjov jr. and Grigor'ev 1988).

(joint work of the Noai Fitchas working group, Instituto Argentino de Mathemática COMICET - Buenos Aires, André Galligo, Jacques Morgenstern, Nice, Marie-Françoise Roy, Rennes.)

B. Just Generalisation of the continued fraction algorithm to arbitrary dimensions

It is well known that the continued fraction algorithm (CFA) applied to a real number x constructs a sequence of bases of $\mathbb{Z}^2$ that is finite iff $x \in \mathbb{Q}$, and moreover the basisvectors are best diophantine approximations for x. We present for the first time an algorithm that generalises these properties. Given real numbers $x_1,\dots,x_{n-1}$, it

1.) constructs by elementary transformations a sequence of bases of approximating $(x_1,\dots,x_{n-1})R$,

2.) stops iff $x_1,\dots,x_{n-1},1$ are $\mathbb{Z}$-linearly dependent,

3.) produces diophantine approximations of more than linear goodness: if $(p_1,\dots,p_n)$ is the first vector of a basis, then

$$\max_{1 \le i \le n-1} \left|x_i - \frac{p_i}{p_n}\right| \le \frac{\text{const}}{p_n^{1+1/2n(n-1)}} .$$

E. Kaltofen Efficient Parallel Algebraic Circuits for Partial Derivatives

Given be a straight-line program P of length ℓ that computes a rational function $f \in K(x_1,\dots,x_n)$, K an arbitrary field. The depth d of P is the length of the longest chain of variables, the values of the next depending on the preceeding ones. We construct two straight-line programs Q_1 and Q_2, Q_1, computing $\partial_{x_1}(f), \partial_{x_1}^2(f),\dots,\partial_{x_1}^K(f)$, and Q_2, computing $\partial_{x_1}(f), \partial_{x_2}(f),\dots,\partial_{x_n}(f)$, where $\partial_{x_i}(f)$ is the partial derivitive of f with respect to the variable x_i and $\partial_{x_i}^j(f) = \partial_{x_i}(\dots(\partial_{x_i}(f)))$, the j-th fold iteration of ∂_{x_i}.

Our constructions satisfy

$$\text{length}(Q_1)=O(K\log(K)\log(\log K)\ell),\ \text{length}(Q_2) = 4\ell ,$$

$$\text{depth}(Q_1)=O(\log(K)(d+\log(K))),\ \text{depth}\ (Q_2) = O(d).$$

Q_1 is constructed using the Taylor series expansion of $f(x_1+y,x_2,\dots,x_n)$ with respect to y, carried out in P. Q_2 is a variant of a construction by Baur and Strassen, that preserves asymptotically the depth by using a fan-out reduction in circuits due to Hoover, Klawe and Pippenger.

M. Karpinski The Parallel Complexity of Perfect Matching and algebraic Interpolation

We construct a fast parallel algorithm for enumerating all the perfect matchings in bipartite graphs with polynomially bounded permanents. Some implications towards the general maximum matching and counting problems are formulated as well as some surprising applications towards efficient deterministic interpolation schemes for polynomials over arbitrary fields. These results imply in particular the existence of efficient deterministic sparse conversion algorithms working over arbitrary fields. As another application we display a deterministic polynomial time (boolean NC) RSE-conversion algorithm for the (GF[2]-) sparse boolean circuits.

J.C. Lagarias More on Multidimensional Continued Fractions

Multidimensional continued fraction algorithms are desired to find simultaneous Diophantine approximations to $(\Theta_1,\ldots,\Theta_d) \in \mathbb{R}^d$, to find small values of a linear form $\Theta_1 x_1+\ldots+\Theta_d x_d$, and integer relations $\Theta_1 x_1+\ldots+\Theta_d x_d = 0$ if they exist. We describe a new class of such algorithms, parametric multidimensional continued fractions, or geodesic continued fractions, having these properties. One takes a parametrized family B_t of bases of lattices, where

$$B_t = \begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ \Theta_1 & \cdots & \Theta_d & t \end{bmatrix}$$

is a (row) basis of a lattice Λ_t. We vary t from $1 \geq t > 0$, decreasing t. Let $P_t \in GL(d+1,\mathbb{Z})$ be chosen so that $P_t B_t$ is Minkowski-reduced where

$$P_t = \begin{bmatrix} p_{11} & \cdots & p_{1d} & q_1 \\ & & & \\ p_{d+1,1} & \cdots & p_{d+1,d} & q_d \end{bmatrix},$$

$P_1 = I$. There is a sequence of critical values $1 \geq t_1 > t_2 > t_3\ldots$ decreasing to 0 at which P_t changes value. Define $P^{(i)} \equiv P_t$ for $t_i > t > t_{i+1}$, and define A_{i+1} by $P^{(i+1)} = A_{i+1}P^{(i)}$. The A_i are partial quotient matrices of algorithm, $P^{(i)}$ are convergent. The A_i are drawn from a finite set Σ_{d+1} in 1-1 correspondence with walls of Minkowski fundamental domain (MCF algorithm in the sense of Brentjes). There is a way to calculate t_{i+1} and A_{i+1} directly from t_i and $P^{(i)}$: one solves a set of quadratic equations in 1-1 correspondence with elements of Σ_{d+1}. The algorithm has a geometric interpretation in that $M = B_t B_t^T$ follows a geodesic in the cone P_{d+1}^{+} of positive definite symmetric matrices $(P_{d+1}^{+} = GL(d+1,\mathbb{R}/O(d+1,\mathbb{R}))$ with respect to the usual invariant Riemannian metric. This algorithm has the property that $(p_{11}^{(i)}/q_1^{(i)},\ldots,p_{d1}^{(i)}/q_1^{(i)})$ gives good simultaneous approximation $\|\Theta_j - p_{j1}^{(i)}/q_1^{(i)}\| \leq c(d)/(q_1^{(i)})^{1+1/d+1}$, and infinitely often in a best Euclidean norm approximation. The linear form problem is solved using $((P^{(i)})^{T})^{-1}$. This algorithm generalizes to solve several linear forms problems; one can also use different reduction theories (e.g. Korkine-Zolotarev reduction) instead; one can do it on other symmetric spaces modulo discrete subgroups.

Th. Lickteig Lower bounds on testing vanishing of polynomials

We present new lower bounds on testing polynomials for zero. Non-trivial lower bounds have recently been given by Ben-Or based on real algebraic geometry. The computational model is that of computation trees. The main differences between Ben-Or's method and the present one are:
a) the lower bounds hold for the purely arithmetic costs (i.e. comparisons are free of charge), b) additions and subtractions can be treated as well, c) the bcunds hold for the "thick path" in computation trees. The concept of approximative complexity, which has been introduced by Strassen in 1974, comes in in a natural way. The proofs employ Strassen's degree method, the Baur-Strassen derivation theorem and Strassen's local reduction method, thus showing the power of these methods.
Examples: 1. Testing the Lagrangian interpolation polynomial for a certain value has multiplicative complexity $\geq$ const. n log n.
2. Testing the determinant for 1 has multiplicative (additive) complexity $\geq$ const. $\underline{R}\langle n,n,n\rangle$ (border rank of matix multiplication).

W. Maass The Complexity Types of Computable Sets
(joint work with Theodore A. Slaman)

We analyze the fine structure of time complexity classes for RAM's, in particular the equivalence relation $A =_c B$ ("A and B have the same time complexity") $\Leftrightarrow$ (for all time constructible f : $A \in \mathrm{DTIME}_{RAM}(f) \Leftrightarrow B \in \mathrm{DTIME}_{RAM}(f)$). The $=_c$-equivalence class of A is called its complexity type. We prove that every set X can be partitioned into two sets A and B such that $X =_c A =_c B$, that a complexity type C contains sets A,B which are incomparable with respect to polynomial time reductions if and only if $C \not\subseteq P$, and that there is a complexity type C that contains a minimal pair with respect to polynomial time reductions. Furthermore we analyze the fine structure of P with respect to linear time reductions: we show that each complexity type $C \not\subseteq \mathrm{DTIME}(n)$ contains a rich structure of linear time degrees, and that these degree structures are not all isomorphic (in particular we characterize those C that have a maximal linear time degree). Finally we show that every complexity type contains a sparse set. Our proofs employ finite injury priority arguments, together with a new technique for constructing sets of a given time complexity type.

E.W. Mayr Membership in Polynomial Ideals over $\mathbb{Q}$ Is Exponential Space Complete

A polynomial ideal membership problem is an (n+1)-tuple $P = \langle p,p_1,p_2,\ldots,p_n\rangle$ where p and the p_i are multivariate polynomials over some ring, and the problem is to determine whether p is in the ideal generated by the p_i . For polynomials over the integers or rationals, it is known that this problem is exponential space hard.
We show that the problem for multivariate polynomials over the rationals is solvable in exponential space, establishing its exponential space completeness.

K. Mehlhorn Dynamic Perfect Hashing: Upper and Lower bounds
(joint work with M. Dietzfelbinger, A. Karlin, F. Meyer auf der Heide, H. Rohnert, and R.E. Tarjan)

We give a randomized algorithm for the dictionary problem with O(1) worst case time for lookup and O(1) amortized expected time for insertion and deletion. We also prove an $\Omega(\log n)$ lower bound on the amortized worst case time complexity of any deterministic algorithm in a class of algorithms encompassing realistic hashing-based schemes. Furthermore, if the worst case lookup time is restricted to k, then the lower bound for insertion becomes $\Omega(k\cdot n^{1/k})$.

F. Meyer auf der Heide On Genuinely Polynomial Computations

We consider random access machines with fixed set $S \subseteq \{+,-,*,DIV,\ldots\}$ of arithmetic operations. They read the input integer by integer, not bit by bit. We use the uniform cost criterion and measure the runtime $T(n)$ to be the worst case runtime taken over all inputs consisting of n integers. Algorithms that are polynomial in this sense are called genuinely (or strongly) polynomial over S . We define complexity classes relative to the set S of arithmetic operations using this notion of complexity.
In this context we are able to prove separations between complexity classes. E.g., the genuine classes P and NP, for operation set $\{+,-,DIV\}$ are different.
(joint work with M. Karpinski)

S. Micali Fast Byzantine agreement

Consider a communication network in which messages are exchanged in pulses between pairs of processors. A Byzantine agreement protocol (BAP) allows the good (properly computing) processor to coordinate themselves. Namely, if each processor holds an initial value, for any set of initial values a BAP guarantees the following properties:

1) All good processors adopt a common value.
2) If all good processors start with the same value then they will adopt that value.

We present a probabilistic BAP that runs in expected constant time and tolerates 1/3 of the processors to be bad, have arbitrary computational power, and coordinate their strategies for trying to disrupt the protocol.
(joint with Paul Feldman)

M. Paterson Planar Acyclic Computation

Restricting acyclic Boolean circuits to two dimensions is a severe limitation. Although for most bases we may design 'crossovers', i.e., planar subcircuits simulating the crossing of a pair of wires, such a simulation is deficient in one important respect: acyclicity may be violated.

Thus the computations of some functions may become more expensive using planar circuits, while for some sets of functions with input and output locations specified the computation may become impossible.

In this joint work with Bill McColl (Oxford) we characterise those input/output specifications which are realisable with planar acyclic circuits.

R. Reischuk Decomposition of Graphs - A Uniform Approach for the Design of Fast Sequential and Parallel Algorithms on Graphs
(joint work with W. Hohberg)

For general $k \in \mathbb{N}$ we develop the graphtheoretic notion how an arbitrary (hyper)-graph can be decomposed into k-connected components and describe a sequential algorithm for this task. An independence relation for separating sets is defined; based on this notion the work can be extended to derive also a fast parallel algorithm. Consider the class of graphs for which an arbitrary decomposition into k-connected components generates components of small size. It turns out that the families of graphs for which the known NP-complete graph problems can be solved in polynomial time are all subsets of this class. Decomposing a graph into k-connected components is the basis for a uniform method to derive fast polynomial algorithms for all those problems restricted to this class - decision as well as construction. This approach can also be parallelized such that we get NC-algorithms in all these cases. We can even handle problems above NP and illustrate the method by solving the #P-complete problem of network reliability.

C.P. Schnorr Computing the Order of Finite, Abelian Groups via Random Relations
(joint work with A.K. Lenstra)

Let G be a finite, abelian group with generators $s_1,\dots,s_n$. We present two efficient methods that compute with high probability the group order $|G|$ using random relations with respect to these generators. If the relations $z_1,\dots,z_{n+1}$ are uniformly distributed over all relations in the cube $\{0,\dots,B-1\}^n$ then the order of G equals, with probability at least $0.2-o(1)$, the gcd of $\det(z_1,\dots,z_{n-1},z)$ for $z = z_n, z_{n+1}$ where $o(1)$ is arbitrarily small for sufficiently large B. Our second method for computing $|G|$ uses an arbitrary set of n linearly independent relations in $\{0,\dots,B-1\}^n$ and in addition $O(\log n)$ random relations. Based on this method we present and analyse a probabilistic algorithm for computing the class number h_Δ of quadratic field extensions with negative discriminant Δ, i.e. for computing the order of the group of $SL_2(\mathbb{Z})$-equivalence classes of binary quadratic forms with negative discriminant Δ. Under the sole assumption of the GRH we prove that this algorithm computes h_Δ with probability $1/2 + o(1)$ in an expected number of $L(|\Delta|)^{3/\sqrt{8}+o(1)}$ bit operations, where $L(n) = \exp\sqrt{\log n \log \log n}$.

A. Schönhage How to compute n!

The obvious divide-and-conquer approach to compute n! by $\log n$ passes of multiplying "neighbored" factors has a time bound of order $M(n.\log n).\log n$, where $M(N)$ is a time bound for N-bit integer multiplication, but there is a better method based on the prime factor decomposition of n! with time bound $O(M(n.\log n))$ - see also P.B. Borwein, J. of Algorithms 6, 376-380 (1985), who obtained a bound of order $M(n.\log n).\log\log n$. -

The basic idea is best explained by an example. For $n=38$, we have

$$38! = 2^{35}.3^{17}.5^{8}.7^{5}.11^{3}.13^{2}.17^{2}.19^{2}.23.29.31.37$$

$$= (2^{17}.3^{8}.5^{4}.7^{2}.11.13.17.19)^{2}.(2.3.7.11.23.29.31.37) = y^{2}.P,$$

similarly $y = (2^{8}.3^{4}.5^{2}.7)^{2}.(2.11.13.17.19)$, etc.
The time for the nested squarings can be estimated by a geometric series, and a similar argument applies to the length bounds for the products P of single primes. Moreover, a sufficiently fast implementation for the sieve of Erathostenes is required, e.g. on a multitape Turing machine or for a pointer machine.

U. Schöning Robust Oracle Machines

The notion of a robust oracle machine and an oracle set "helping" a robust oracle machine has been introduced for better understanding the nondeterministic "witness searching" process in NP problems. It is shown that straightforward modifications of the original notion are closely related with other concepts in structural complexity theory, such as "self-reducibility", "lowness", and "interactive proof systems".

A. Shamir The Complexity of Justice

In this talk we consider a model in which one resource bounded verifier interacts with two infinitely powerful provers. Unlike the multi prover model of Ben-Or, Goldwasser, Kilian and Wigderson, we assume that one prover is trustworthy and the other prover acts maliciously, but the verifier does not know who is who. The problem we consider is which languages L can be decided correctly with overwhelming probability by the verifier. The main two results are that polynomial time verifiers can accept exactly PSPACE languages, while log space verifiers can accept all the elementary recursive languages and some non-elementary recursive languages.
(Joint work with Uri Feige)

E. Szemerédi Construction of a thin set with small Fourier coefficients
(Joint work with M. Astai, H. Iwaniec, J. Komlós, S. Pintz)

Let m be a positive integer. Given a set $T = \{t_1,t_2,\ldots,t_n\}$ $\{0,1,\ldots,m-1\}$ the sequence

$$f_T(k) = \Sigma_{j=1}^{n}\, e\,(z_j\ k/m)$$

$$k = 0,\ldots,m-1 \quad \text{where} \quad e(x) = e^{2\pi ix}$$

is called the (discrete) Fourier Transform of T .

We construct a set $T = T_m$ for every m such that

$$|T_m| = g(m) \cdot \log m \qquad g(m) \ll \log m$$

and $\|f_{T_m}\| = o|T_m|$

where $\|f\| = \max\limits_{1 \le k \le m-1} |f(k)|$

Such a construction has applications in graph theory, computer science and in combinatorial number theory.

E. Upfal An $O(\log N)$ Deterministic Packet Routing Scheme

We present a deterministic $O(\log N)$ time algorithm for the problem of routing an arbitrary permutation on an N-processor bounded-degree network with bounded buffers.

Unlike all previous deterministic solutions to this problem our routing scheme does not reduce the routing problem to sorting and does not use the Ajtai, Komlós and Szemerédi sorting network [AKS]. Consequently, the constant in the run time of our routing scheme is substantially smaller, and the network topology is significantly simpler.

U. Vazirani $\chi(G^2)$ and approximations for chromatic numbers

The square of a graph $G(V,E)$ is a graph $G^2(V\times V, E)$ where (x,y) and (x',y') are adjacent if $(x,x') \in E$ or $(y,y') \in E$. We show that the chromatic number of G^2 is bounded between:

$$\chi(G)^2 \ge \chi(G^2) \ge \frac{\chi(G)^2}{\ln n} \qquad \text{where } n = |V|.$$

The bounds are tight: the lower bound is achieved by the squares of directed line graphs. In fact, we show that $\chi(DL(G)^2) \le c\chi(DL(G))$ for some constant c.

The bounds stated above imply that any approximation algorithm for chromatic numbers that guarantees an answer within an $f(n)$ multiplicative factor on n vertex graphs, where $\log^{1+\alpha} n \le f(n) \le n^{\varepsilon}$ for every $\varepsilon > 0$ and some $\alpha > 0$, can be improved to one that achieves an asymptotically better approximation ratio. In view of this result and the fact that the best known approximation algorithms guarantee only an $n^{1-c/K-1}$ coloring for K chromatic graphs of size n (Wigderson 1983, Blum 1988), we speculate that no polynomial time algorithm approximates chromatic numbers better than n^{ε} ratio for every $\varepsilon > 0$.

(joint work with Nati Linial)

I. Wegener How to compute the parity functions

The circuit complexity of the parity function is well studied for fan-in 2 circuits. For unbounded fan-in circuits over $(\wedge, \vee, 1)$ Hastad has proved that depth $\Omega(\log n/\log\log n)$ is necessary for polynomial size. Here we consider the exact complexity over various bases with unbounded fan-in. Optimal NOR-circuits have size $3n-2$ and $8(n-1)$ wires. Over the basis of all AND-type gates the minimal number of gates is in the interval $[2n-1, \lceil 5/2(n-1)\rceil]$ and the minimal number of wires is $6(n-1)$, but circuits with $6(n-1)$ wires need $3(n-1)$ gates. Optimal synchronous threshold circuits have size $n+1$ while optimal asynchronous threshold circuits have only $\lceil \log(n+1)\rceil$ gates, this gives an exponential gap between synchronous and asynchronous threshold complexity.

V. Weispfenning Complexity of quantifier elimination

The talk presents 3 uniform methods to obtain good upper and lower complexity bounds for quantifier elimination (QE) in various classes of algebraic structures:

1. Skolem terms.
2. Isomorphism type extensions.
3. Topological boundaries of definable sets.

Applications concern eg. linear formulas in fields, ordered and valued fields; Presburger arithmetic, Boolean algebras and Stone algebras, semilattices, linear and partial orders, graphs, trees. Most of the results appear in the author's papers in Proc. AAECC-3, Grenoble 1985, Proc. ISSAC-88, Rome, Journal Symb. Comput. 5 (1988). New results include:

- a triple exponential upper and lower bound for QE in Presburger arithmetic.
- a double exponential lower bound for QE in atomless Boolean algebras and existentially closed Stone algebras.
- an exponential lower bound for QE in existentially closed semilattices, linear and partial orders, graphs and abelian m-groups.

Berichterstatter: Thomas Lickteig

Tagungsteilnehmer

Prof. Dr. H. Alt
Institut für Mathematik III
der Freien Universität Berlin
Arnimallee 2-6

1000 Berlin 33

Prof. Dr. W. Baur
Fakultät für Mathematik
der Universität Konstanz
Postfach 5560

7750 Konstanz 1

Prof. Dr. A. Borodin
Department of Computer Science
University of Toronto

Toronto , M5S 1A4
CANADA

P. Bürgisser
Fakultät für Mathematik
der Universität Konstanz
Postfach 5560

7750 Konstanz 1

Dr. M. Clausen
Institut für Algorithmen und
Kognitive Systeme
Universität Karlsruhe
Haid-und-Neu-Str. 7

7500 Karlsruhe

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

Toronto , M5S 1A4
CANADA

Prof. Dr. D. Coppersmith
IBM Corporation
Thomas J. Watson Research Center
P. O. Box 218

Yorktown Heights , NY 10598
USA

Prof. Dr. U. Faigle
Department of Applied Mathematics
Twente University
P.O.Box 217

NL-7500 AE Enschede

Prof. Dr. M. J. Fischer
Department of Computer Science
Yale University
P.O. Box 2158, Yale Station

New Haven , CT 06520
USA

Prof. Dr. M. Fürer
Computer Science Dept.
Whitmore Lab.
Pennsylvania State University

University Park , PA 16 802
USA

Prof. Dr. M. L. Furst
Department of Computer Science
Carnegie Mellon University
Schenley Park

Pittsburgh , PA 15213
USA

Prof. Dr. Z. Galil
Department of Computer Sciences
Columbia University
Seeley W. Mudd Building

New York , NY 10027
USA

Prof. Dr. J. von zur Gathen
Department of Computer Science
University of Toronto

Toronto , M5S 1A4
CANADA

Prof. Dr. D. J. Grigor'ev
Leningrad Branch of Steklov
Mathematical Institute - LOMI
USSR Academy of Science
Fontanka 27

Leningrad 191011
USSR

Prof. Dr. J. Heintz
Instituto Argentino de
Matematica
Viamonte 1636, 2 A

1055 Buenos Aires
ARGENTINA

B. Just
Fachbereich Mathematik
der Universität Frankfurt
Robert-Mayer-Str. 6-10

6000 Frankfurt 1

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

Troy , NY 12180-3590
USA

Prof. Dr. M. Karpinski
Institut für Informatik III
Universität Bonn
Römerstraße 164

5300 Bonn 1

Prof. Dr. J. C. Lagarias
AT & T
Bell Laboratories
600 Mountain Avenue

Murray Hill , NJ 07974-2070
USA

Dr. T. Lickteig
Mathematisches Institut
der Universität Tübingen
Auf der Morgenstelle 10

7400 Tübingen 1

Prof. Dr. R. Loos
Wilhelm-Schickard-Institut für
Informatik
Universität Tübingen
Auf der Morgenstelle 10

7400 Tübingen 1

Prof. Dr. W. Maass
Dept. of Mathematics
University of Illinois at Chicago
Box 4348

Chicago , IL 60680
USA

Prof. Dr. E. W. Mayr
Fachbereich 20 Informatik
Universität
Postfach 11 19 32

6000 Frankfurt 11

Prof. Ph.D. K. Mehlhorn
Fachbereich 10 - Informatik
Universität des Saarlandes
Im Stadtwald 15

6600 Saarbrücken 11

Prof. Dr. F. Meyer auf der Heide
Institut für Informatik II
Universität Dortmund
Postfach 50 05 00

4600 Dortmund 50

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

Cambridge, MA 02139
USA

R. Mirwald
Fachbereich Mathematik
der Universität Frankfurt
Robert-Mayer-Str. 6-10

6000 Frankfurt 1

Dr. N. T. Müller
Fachbereich IV
Mathematik/Informatik
der Universität Trier
Postfach 3825

5500 Trier

Prof. M. S. Paterson
Department of Computer Science
University of Warwick

GB- Coventry CV4 7AL

Dr. R. Reischuk
Institut für Theoretische
Informatik
Technische Hochschule Darmstadt
Alexanderstr. 24

6100 Darmstadt

Prof. Dr. C.P. Schnorr
Mathematisches Seminar
Fachbereich Mathematik
der Universität Frankfurt
Postfach 11 19 32

6000 Frankfurt 1

Prof. Dr. A. Schönhage
Mathematisches Institut
der Universität Tübingen
Auf der Morgenstelle 10

7400 Tübingen 1

Dr. U. Schöning
Institut für Informatik
EWH Koblenz
Rheinau 3 - 4

5400 Koblenz

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

Rehovot 76 100
ISRAEL

Prof. Dr. H.-J. Stoß
Fakultät für Mathematik
der Universität Konstanz
Postfach 5560

7750 Konstanz 1

Prof. Dr. V. Strassen
Fakultät für Mathematik
der Universität Konstanz
Postfach 5560

7750 Konstanz 1

Prof. Dr. E. Szemeredi
Mathematical Institute of the
Hungarian Academy of Sciences
Realtanoda u. 13 - 15
P. O. Box 127

H-1053 Budapest

V. Tobler
Fakultät für Mathematik
der Universität Konstanz
Postfach 5560

7750 Konstanz 1

Dr. E. Upfal
Dept. of Mathematics
The Weizmann Institute of Science
P. O. Box 26

Rehovot 76 100
ISRAEL

Prof. Dr. U. V. Vazirani
Computer Science Division
University of California
at Berkeley

Berkeley , CA 94720
USA

Prof. Dr. I. Wegener
Institut für Informatik III
der Universität Dortmund
Postfach 50 05 00

4600 Dortmund 50

Prof. Dr. V. Weispfenning
Fakultät für Mathematik
und Informatik
Universität Passau
Innstr. 27, PF 2540

8390 Passau