MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

T a g u n g s b e r i c h t   50/1990

# Komplexitätstheorie

## 18.11. – 24.11.1990

The ninth Oberwolfach Conference on Complexity Theory was organized as before by C.-P. Schnorr (Frankfurt), A. Schönhage (Bonn) and V. Strassen (Konstanz). The 33 participants came from nine countries, twelve of them came from North and South America and from the USSR.

The 28 lectures given at the conference covered many different areas of complexity theory, with a major focus on topics related to algebraic problems, graphs, and computational number theory.

Lectures were given on the sequential resp. parallel complexity of computational problems in linear algebra, Discrete Fourier Transforms, computations in finite fields, and factoring polynomials. Computational aspects of algebraic geometry and geometric problems in semialgebraic sets were discussed.

Other lectures dealt with unit computation, principal ideal testing, factoring integers, computing discrete logarithms, and the reduction of quadratic forms. Further topics were polynomial interpolation, counting solutions of GF[2]-polynomials, computation of real numbers, and asymptotics.

Several topics on graphs have been considered, e.g. spanning trees, algorithms on dense graphs, and the analysis of random walks.

Various other topics were discussed, such as polygonal chains, circuit design, branching programs for symmetric Boolean functions, sorting, hashing, communication in parallel machines, relations between logics and complexity classes, and learning algorithms.

# Participants

H. Alt, Berlin
W. Baur, Konstanz
P. Borwein, Halifax
J. Buchmann, Saarbrücken
P. Bürgisser, Berkeley
M. Clausen, Bonn
J. von zur Gathen, Toronto
E. Grädel, Basel
D.Yu. Grigor'ev, Leningrad
J. Hastad, Stockholm
J. Heintz, Buenos Aires
E. Kaltofen, Troy
M. Karpinski, Bonn
P. Kirrinnis, Bonn
T. Lickteig, Berkeley
H. Lombardi, Besançon
W. Maass, Chicago
E. W. Mayr, Frankfurt
K. Mehlhorn, Saarbrücken
F. Meyer auf der Heide, Paderborn
R. Mirwald, Frankfurt
A.M. Odlyzko, Murray Hill
M.S. Paterson, Coventry
A.A. Razborov, Moscow
R. Reischuk, Darmstadt
C.-P. Schnorr, Frankfurt
A. Schönhage, Bonn
M.A. Shokrollahi, Bonn
H.-J. Stoß, Konstanz
V. Strassen, Konstanz
P. Tiwari, Madison
U.V. Vazirani, Berkeley
I. Wegener, Dortmund

# Abstracts

*H. Alt*

**Measuring the Distance between Polygonal Chains**

Motivated by shape- and pattern-recognition problems a distance measure between curves is introduced which is compatible with parametrizations of the curves and is called "continuous distance" $\delta_c$. It is shown, that in the case of convex curves $\delta_c$ coincides with the Hausdorff-distance.

Therefore for convex polygons $P, Q$ $\delta_c(P, Q)$ can be determined in time $O(p+q)$ ($p, q =$ numbers of edges of $P, Q$, respectively), using an algorithm by Atallah. For arbitrary polygonal chains $P, Q$ an algorithm of runtime $O(pq)$ is presented for the decision problem whether $\delta_c(P, Q) \leq \varepsilon$ for a given $\varepsilon$. This can be used to obtain an $O((p^2q + pq^2)\log(pq))$-algorithm for the problem of computing $\delta_c(P, Q)$.

*(Joint work with Michael Godau.)*

*P. Borwein*

**Strange and Fraudulent Series**

The series

$$\left(\frac{1}{10^5}\sum_{n=-\infty}^{\infty} e^{-n^2/10^{10}}\right)^2$$

approximates $\pi$ to 42 billion places (but not to 43 billion places).

The series

$$\sum_{n=1}^{\infty} \frac{\lfloor ne^{\pi\sqrt{163/9}}\rfloor}{2^n}$$

is 1280640 to 1/2 billion places (and then goes wrong). These and other strange series will be the topic of this short talk.

*J. Buchmann*

**Complexity of Unit Computation and Principal Ideal Testing in Number Fields**

Starting with the diophantine equation

$$x^2 - Dy^2 = \pm 4p$$

we discuss the complexity of unit computation and principal ideal testing in number fields and prove

**Theorem.**

a) There is an algorithm for computing a generating system for the unit group of an order of discriminant $D$ in a number field of degree $n$ in time $(n \log |D|)^{O(n)} \cdot R$ where $R$ is the regulator of the order.

b) In the situation of a) an ideal $a$ can be tested for principality in time $(n \log |D|)^{O(n)} \cdot (R + |a|)$ where $|a|$ is the input size of $a$.

*P. Bürgisser*

**Some Computational Problems in Linear Algebra as Hard as Matrix Multiplication**

Let $F$ be a field of characteristic 0. Consider the following problems:

3-COMPRESSION($n$):
data: $(A_1, A_2, A_3) \in (F^{n\times n})^3$
solution: $(B_1, B_2) \in (F^{n\times n})^2$ with $A_1A_2A_3 = B_1B_2$.

KERNEL($n$):
data: $A \in F^{n\times n}$
solution: a basis of $\ker(A)$.

ORTHOGONAL BASIS($n$):
data: $A \in F^{n\times n}$ symmetric
solution: $S \in \mathrm{GL}_n(F)$ with $SAS^T$ diagonal.

We use the model of a computation tree with operations $F \cup \{+, -, *, /\}$ and branchings according to the relation "=".

We show that there are $c, d > 0$ such that every computation tree solving one of the above problems has a complexity of at least

$$c \cdot M_n - d \cdot n^2,$$

where $M_n$ denotes the nonschalar complexity of $n \times n$ matrix multiplication.

*(Joint work with T. Lickteig and M. Karpinski.)*

*M. Clausen*

**Lower and Upper Complexity Bounds for Discrete Fourier Transforms**

Let $2 \leq c \leq \infty$. The $c$-linear complexity $L_c(A)$ of a complex matrix $A$ is the minimal number of additions, subtractions and multiplication by complex constants of absolute value $\leq c$ needed to evaluate $A$ at a generic input vector. For a finite group $G$ let DFT$(G)$ denote the set of all DFT-matrices corresponding to $G$ and call $L_c(G) := \min\{L_c(A) : A \in \mathrm{DFT}(G)\}$ the $c$-linear complexity of G.

**Theorem.** Let $G$ be a finite group, $A \in \mathrm{DFT}(G)$.

(1) $|L_\infty(A) - L_\infty(A^{-1})| \leq |G|$.

(2) $L_2(G) > \frac{1}{4} \cdot |G| \cdot \log |G|$.

(3) If $G_n := \{\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} | \alpha, \beta \in GF(2^n), \alpha \neq 0\}$ then $L_2(G_n) \leq 0.6 \cdot |G_n| \cdot \log |G_n|$ for all $n \geq 7$.

(4) $G$ abelian $\Rightarrow L_2(G) < 8 \cdot |G| \cdot \log |G|$.

((1) – (3) *is joint work with Ulrich Baum,* (4) *is joint work with U. Baum and Benno Tietz.*)

*J. von zur Gathen*

**Exponentiation in Finite Fields**

A basis of a finite field $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ ($q$ a prime power) of the form $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$ is called a *normal basis.* We show that a random $\alpha \in \mathbb{F}_{q^n}$ generates a normal basis with large probability $\Omega(1/\log_q n)$. Hensel's test (1888) then provides an efficient probabilistic method to generate a normal basis, with $O\tilde{}(n^2 \log q)$ operations in $\mathbb{F}_q$. (*This is joint work with Mark Giesbrecht.*)

The property $(\sum a_i \alpha^{q^i})^q = \sum a_{i-1}\alpha^{q^i}$, with $a_i \in \mathbb{F}_q$, shows that a $q$-th power is just a cyclic shift of coordinates. The computation of a large power, say $x^e$ with $1 \leq e < q^n$, by multiplications and divisions is appropriately modelled by *addition/subtraction chains with free multiplication by* $q$. The minimal size is $O(n/\log_q n)$, and a counting argument shows a lower bound $\Omega(n/log_q n)$ for almost all $e$. The parallel complexity is exactly $\lceil \log_2 \sigma_q(e) \rceil$ with additions, and exactly $\lceil \log_2 \sigma_q^{\pm}(e) \rceil$ with additions and subtractions. Here $\sigma_q(e)$ is the sum of the digits of the $q$-ary representation of $e$, and $\sigma_q^{\pm}(e) = \min\{\sigma_q(a) + \sigma_q(b) : a, b \in \mathbb{N}, e = a - b\}$. We give an example where Fermat's Little Theorem speeds up a computation: $\lceil \log_2 \sigma_q^{\pm}(e) \rceil > \lceil \log_2 \sigma_q^{\pm}(e + \lambda(q^n - 1)) \rceil$.

*E. Grädel*

**Descriptive Complexity via Fragments of Second Order Logic**

It is well known that NP can be characterized as the set of problems that are expressible by existential second order logic. Other complexity classes (P, NLOG, LOG, $AC^0$) are captured by increasing the expressive power of first order logic (with order) by operators for the least fixed point, transitive closure etc. Here we discuss logical descriptions of complexity classes not by increasing first order logic but by restricting second order logic. We define second order Horn logic SO-HORN, second order Krom logic SO-KROM and a symmetric fragment SO-SymKROM.

We show:

- These logics collapse to their existential fragments.
- In the presence of a successor relation, SO-HORN, SO-KROM and SO-SymKROM capture P, NLOG and CoSymLOG, respectively.
- Without successor relation, SO-HORN is strictly weaker than fixed point logic.

*D.Yu. Grigor'ev*

**Finding Connected Components of a Semialgebraic Set in Subexponential Time**

Let a semialgebraic set be given by a boolean combination of systems of polynomial inequalities in $n$ variables with degrees at most $d$ and bit-sizes of coefficients at most $M$. An algorithm is designed which finds the connected components of the semialgebraic set presenting them in a similar way with the running time $Md^{n^{O(1)}}$.

*(Joint work with N.N. Vorobjov (jr.) and J. Canny.)*

*J. Heintz*

**(Un)precise Complexity Bounds in Elementary Geometry** *

We present in this talk algorithmical results in semialgebraic geometry whose qualitative aspect is known since this can be deduced from cylindrical algebraical decomposition (involving *doubly* exponential sequential complexity bounds). The new outcome are the *single* exponential complexity bounds we present here. This improvement is due to recent progress in commutative algebra (effective Nullstellensätze).

We show a general technical theorem which can be generalized to a result on the complexity of quantifier elimination in the first order language of ordered fields (where the formulae are interpreted in the real numbers).

The dimension, topological closure, and the interior of a s.a. set can be computed in *admissible* time, i.e. with sequential complexity $s^{O(1)}d^{n^{O(1)}}$ and parallel complexity $(n \log(sd))^{O(1)}$ where $d$ is a bound on the degree of the polynomials $F_1, \ldots, F_s \in \mathbb{Z}[x_1, \ldots, x_n]$ involved in the definition of the semialgebraic set which is considered.

Applications to questions concerning connected components of s.a. sets are discussed, an *effective* Lojasiewicz Inequality is derived from the methods described, and it is shown that integer programming with quasiconvex polynomial restrictions is in NEXPTIME.

*(Joint work with Teresa Krick, Pablo Solonó (Noaï Fitchas, Buenos Aires) and Marie-Françoise Roy (Rennes).)*

* *As no sufficiently short abstract was available, an extended abstract has been summarized by the reporter.*

*E. Kaltofen*

**Effective Noether Irreducibility Forms and Applications**

We consider the problem of factoring multivariate polynomials over the algebraic closure of the coefficient field. A major instance of this is the problem of factoring rational polynomials into irreducible factors with complex coefficients. The contributions discussed are threefold: first, we derive effective irreducibility theorems applicable to this problem; second, we establish a methodology for estimating the bit complexity of an algorithm that is defined for abstract algebraic extension fields, in our case the polynomial factorization algorithm over an algebraically closed field; and third, we describe a representation model for algebraic numbers with the property that factorization of multivariate polynomials with rational coefficients into complex factors, using common polynomial representations, such as the sparse representation, is within the complexity class $\mathcal{NC}$. Our representation for the complex coefficients also yields their rational approximations to a given precision with computaional complexity in $\mathcal{NC}$.

*M. Karpinski*

**An Efficient Approximation Algorithm for the Number of Solutions of a GF[2]-Polynomial**

We construct an efficient Monte Carlo algorithm for estimating the number of solutions of a multivariate polynomial over GF[2]. This gives the first efficient method for estimating the number of points on algebraic varieties over GF[2]. For the case of counting the number of zeros of an $n$-variate, $m$-term polynomial (without constants), the $(\varepsilon, \delta)$-approximation algorithm runs in time $O(\frac{nm^2 \ln(2/\delta)}{\varepsilon^2})$. There exists also an $\mathrm{RNC}^1$-implementation of the algorithm. The method of solution involves the new (sharp) bound on the number of satisfying assignments and zeros of multivariate polynomials with $m$ terms over GF[2]. In the case of the number of zeros $|G|$ of an $n$-variate polynomial without constant terms, the following inequality is true: $2^n/|G| \leq m+1$. This bound is also sharp.

*(Joint work with M. Luby, Berkeley.)*

*T. Lickteig*

**Real Tests and Real Spectra**

A semialgebraic decision problem is a finite partition $\{S_1, \ldots, S_r\}$ of the real $n$-space $\mathbb{R}^n$ into semialgebraic subsets $S_1, \ldots, S_r$. The (multiplicative) complexity of computation trees (CT) $\mathcal{T}$ solving the decision question to which $S_i$ an arbitrary input vector $x \in \mathbb{R}^n$ belongs is discussed for various decision problems from computational linear algebra, and relative lower bounds in terms of the approximative (multiplicative) complexity AMAMU and ASOL of the two main problems, matrix multiplication and solving a linear system, are given.

Examples:

1. If $\mathcal{T}$ is a CT for $\{SL_n, \mathbb{R}^{n\times n} \setminus SL_n\}$ then almost all matrices $x \in SL_n$ follow a path in $\mathcal{T}$ of length $\gtrsim \mathrm{AMAMU}_n$.

2. If $\mathcal{T}$ is a CT for $\{P, S \setminus P\}$ ($P$ = positive symmetric matrices, $S$ = symmetric matrices) then almost all $x$ with $\det x = 0$ follow a path in $\mathcal{T}$ of length $\gtrsim \mathrm{ASOL}_n$.

3. If $\mathcal{T}$ is a CT for computing the rank of matrices from $\mathbb{R}^{n\times n}$ then almost all $x$ with rank $x = r < n$ follow a path in $\mathcal{T}$ of length $\gtrsim \mathrm{ASOL}_r$.

Language and concepts of real algebraic geometry are well suited for discussing complexity of CTs in the real case.

*H. Lombardi*

**Constructive real Nullstellensatz and Explicit Bounds for the Degrees**

We give a constructive proof of the real Nullstellensatz. So we obtain, for every ordered field $K$, a uniformly primitive recursive algorithm that computes, for the input "a sytem of generalized sign conditions (gsc) on polynomials of $K[X_1, \ldots, X_n]$ impossible to satisfy in the real closure of $K$", an algebraic identity that makes this impossibility evident.

Our proof is a translation, step by step, of the Hörmander algorithm for testing the impossibility of the system of gsc.

We can pease our constructions sufficiently to obtain an explicit bound for the degrees of the polynomials appearing in the final algebraic identity, as a function of the degrees, the number of variables and the number of polynomials in the input.

*W. Maass*

**On the Complexity of Learning from Counterexamples and Membership Queries**

We prove a lower bound for the required number of learning steps in a common learning model in computational learning theory.

In this model the "environment" fixes an arbitrary target concept $C_T \in \mathcal{C}$ from the considered concept class $\mathcal{C}$ (where $\mathcal{C} \subseteq 2^X$ for some finite domain $X$; both $X$ and $\mathcal{C}$ are known to the learner). The goal of the "learner" (= learning algorithm) is to identify $C_T$ in as few steps as possible. The allowed moves of the learner are queries of the form "$H = C_T$?" for some hypothesis $H \in \mathcal{C}$ (to which he gets the reply "yes", or the reply "no" together with a counterexample $x \in (C_T - H) \cup (H - C_T)$), and queries of the form "$x \in C_T$?" for $x \in X$.

We show that no matter which algorithm the learner uses, the worst case number of queries that he has to ask is for every concept class $\mathcal{C}$ bounded below by VC-dim($\mathcal{C}$)/7 (where VC-dim($\mathcal{C}$) $:= \max\{|S| : S \subseteq X$ and $\mathcal{C} \cap S = 2^S\}$ is the Vapnik - Chervonenkis dimension of $\mathcal{C}$).

*(Joint work with G. Turan.)*

*E. W. Mayr*

**Spanning Trees in Weighted Graphs**

Given a weighted graph, let $W_1, W_2, W_3, \ldots$ denote the increasing sequence of all possible distinct spanning tree weights. Settling a conjecture due to Kano, we prove that every spanning tree of weight $W_1$ is at most $k-1$ edge swaps away from some spanning tree of weight $W_k$. Three other conjectures posed by Kano are unified and proven for two special classes of graphs. Finally, we consider the algorithmic complexity of generating a spanning tree of weight $W_k$.

*(Joint work with C.G. Plaxton, UT Texas.)*

*K. Mehlhorn*

**Algorithms on Dense Graphs**

We show how to speed up several algorithms on dense graphs by exploiting the parallelism at the word level inherent to the RAM model of computation. In particular, DFS, BFS, and strongly and biconnected components can be computed in time $O(n^2/\log n)$, maximum bipartite matchings in time $O(n^{2.5}/\log n)$, shortest paths in time $O(n^2 \log C/\log n)$, and min cost matchings in time $O(n^{2.5} \log nC \cdot (\log\log n/\log n)^{1/4})$. For the latter two problems the weights are integers in the range $[0 \ldots C]$.

*(Joint work with J. Cherigan.)*

*F. Meyer auf der Heide*

**Dynamic Hashing**

We present a new universal class of hash functions which have many desirable features of random functions but can (probabilistically) be constructed using sublinear time and space, and can be evaluated in constant time.

These functions are used to construct a dynamic hashing scheme that performs in real time, i.e. it uses linear space and needs worst case constant time per instruction. Thus instructions can be given in fixed constant length time intervals. Answers given by the algorithm are always correct, the space bound is always satisfied, and the algorithm fails to fulfil the time bound only with probability $O(n^{-k})$ where n is the number of items currently stored. $k$ can be made an arbitrarily large constant.

We further sketch simulations of shared memory, i.e. of $p$-processor parallel random access machines ($p$-PRAMs), on networks with $p$ processors without shared memory. For restricted classes of $p$-PRAMs, we show simulations with expected constant time delay.

*(Joint work with Martin Dietzfelbinger, Paderborn.)*

*R. Mirwald*

**The Rank of a Pair of Matrices over $\mathbb{Z}_2$ and the Multiplicative Complexity of a Pair of Boolean Quadratic Forms**

**I.** Let $(A, B)$ be a pair of $m \times n$ matrices with coefficients from the field $\mathbb{Z}_2$. We characterize the rank $R(A, B)$ of $(A, B)$ — i.e. the rank of the corresponding tensor in $\mathbb{Z}_2^m \otimes \mathbb{Z}_2^n \otimes \mathbb{Z}_2^2$ — in terms of invariants related to the Kronecker canonical form of $(A, B)$.

For all pairs $(A, B)$ we prove the lower bound $R(A, B) \geq \lceil \frac{1}{2}(R(A) + R(B) + R(A + B)) \rceil$. We show that this lower bound is tight if $(A, B)$ is non exceptional in the sense that all its invariants are different from five exceptional ones (which correspond to diagonal blocks of small size in a Kronecker canonical form). We prove upper and lower bounds for arbitrary pairs $(A, B)$. The maximal rank of a pair of $n \times n$ matrices over $\mathbb{Z}_2$ is $\lceil \frac{3}{2} n \rceil$.

**II.** We compare the multiplicative complexity of a set of quadratic forms to the multiplicative complexity of the corresponding set of Boolean quadratic forms. The multiplicative complexity of a pair of Boolean quadratic forms equals half the rank of an associated pair of matrices over $\mathbb{Z}_2$ provided that this pair of matrices is non exceptional.

*(Joint work with C.-P. Schnorr, Frankfurt.)*

*A.M. Odlyzko*

**An Elementary Method in Asymptotics**

When a generating function $f(z) = \sum f_n z^n$ is analytic, there are many methods for extracting asymptotic estimates for the $f_n$ from information about the behavior of $f(z)$. When $f(z)$ is known only for real $z$, fewer methods are known, and usually they give cruder estimates than can be obtained when $f(z)$ is analytic. When $f_n \geq 0$ for all $n$, one can use a very simple elementary method that is very general, and often produces fairly good estimates. The upper bound is very well known, and says that

$$f_n \leq x^{-n} f(x)$$

for every $x > 0$. What is perhaps slightly surprising is that one can often obtain lower bounds for partial sums $\sum_{k \leq n} f_k$ by a variant of this method.

*M.S. Paterson*

**Shallow Multiplication Circuits**

Carry save adders were used by Ofman, Wallace and others to design multiplication circuits whose total delay is proportional to the logarithm of the length of the two numbers multiplied. An extension of this method was presented here. We have a general theory giving the optimal way of combining a given design of carry save adder. In addition we have detailed designs for carry save adders which yield multiplication circuits of depth $4.57 \log_2 n$.

*(Joint work with Uri Zwick (Warwick) and Nick Pippenger (UBC).)*

*A.A. Razborov*

**Nondeterministic Branching Programs for MAJORITY Require Superlinear Size**

It is shown that the size of nondeterministic branching programs (known also as switching-and-rectifier networks) computing MAJORITY and several other symmetric Boolean functions must be superlinear. The proof uses a reduction to a particular instance of the "Minimum Cover" problem. Another essential ingredient in the proof is Ramsey theory.

*R. Reischuk*

**Degree Bounds for Communication by Exclusive Write Shared Memory**

We consider parallel machines in which the processors communicate via a shared memory with exclusive write access (CREW PRAM). The time complexity of Boolean functions is estimated improving results of Cook, Dwork, Reischuk [SIAM J. Computing, 1986]. We set up a full information model in which states of processors and memory cells correspond to partitions of the input domain $\{0,1\}^n$. The notion of degree for such partitions is defined by associating elements of the $\mathbb{R}$-Algebra of functions $g : \{0,1\}^n \longrightarrow \mathbb{R}$ to the characteristic functions of a partition. We show that the growth rate of the degrees is upper bounded by the Fibonacci sequence. That way the time complexity of functions like $\mathrm{OR}_n$, $\mathrm{AND}_n$, $\mathrm{PARITY}_n$ and many others can be determined exactly or up to a small additive constant. Generalizations to nondeterministic and probabilistic computations are obtained. We finally mention new upper time bounds achieved by processor efficient algorithms.

*(Joint work with M. Kutylowski and M. Dietzfelbinger.)*

*C.-P. Schnorr*

**Factoring Integers and Computing Discrete Logarithms via Diophantine Approximation**

Let $N$ be an integer with at least two distinct prime factors. We reduce the problem of factoring $N$ to the task of finding random integer solutions $(e_1, \ldots, e_t) \in \mathbb{Z}^t$ of the inequalities

$$\Big|\sum_{i=1}^{t} e_i \log p_i - \log N\Big| \leq N^{-c}$$

and

$$\sum_{i=1}^{t} |e_i \log p_i| \leq (2c-1)\log N + o(\log p_t),$$

where $c > 1$ is fixed and $p_1, \ldots, p_t$ are the first $t$ primes. We show, under the assumption that the smooth integers distribute "uniformly", that there are $N^{\varepsilon + o(1)}$ many solutions $(e_1, \ldots, e_t)$ if $c > 1$ and if $\varepsilon := c - 1 - (2c - 1)\log\log N / \log p_t > 0$. We associate with the primes $p_1, \ldots, p_t$ a lattice $L \subset \mathbb{R}^{t+1}$ of dimension $t$ and we associate with N a point $\mathbf{N} \in \mathbb{R}^{t+1}$. We reduce the problem of factoring $N$ to the task of finding random lattice vectors $\mathbf{z}$

that are sufficiently close to $n$ in both the $\infty$-norm and the 1-Norm. The dimension $t$ of the lattice $L$ is polynomial in $\log N$. For $N \approx 2^{512}$ it is about 6300. We also reduce the problem of computing, for a prime $N$, discrete logarithms of the units in $\mathbb{Z}_{/N\mathbb{Z}}$ to a similar diophantine approximation problem.

*A. Schönhage*

**Fast Reduction and Composition of Binary Quadratic Forms**

Similar to the fast computation of integer gcd's, the reduction of binary quadratic forms $ax^2 + bxy + cy^2$ with integral coefficients $a, b, c$ bounded by $2^n$ is possible in time $O(\mu(n)\log n)$, where $\mu(n)$ denotes a time bound for $n$-bit integer multiplication. This result is obtained by a corresponding algorithm for the *monotone reduction of positive forms* (after which the final reduction of definite and indefinite forms can easily be done in a few steps).

Given integers $x, y > 0$, reduction of the form $[m^2x^2+1, 2m^2xy, m^2y^2]$ with sufficiently large $m$, like $m = 2y$, admits to find $u, v$ for $ux + vy = \gcd(x, y)$, whence mere reduction of forms has at least the complexity of *extended* gcd.

The *composition* in the special case $[a_1, b, a_2c]$ with $[a_2, b, a_1c]$ gives simply $[a_1a_2, b, c]$. Fast transformation of the general case to this relies on the following

**Lemma.** Given $a, m > 2^n$, decomposing $a = u \cdot v$ such that $p|a \wedge p|m \Leftrightarrow p|u$ and $p|a \wedge p \not| m \Leftrightarrow p|v$ for any prime $p$ is possible in time $O(\mu(n)\log n)$.

*M.A. Shokrollahi*

**On the Rank of Certain Finite Fields**

Using results of D.V. Chudnovsky and G.V. Chudnovsky and W.C. Waterhouse we prove that the rank (= bilinear complexity of multiplication) of the finite field $\mathbb{F}_{q^n}$ regarded as an $\mathbb{F}_q$-algebra is $2n$ if $n$ satisfies $\frac{1}{2}q + 1 < n < \frac{1}{2}(q + 1 + \varepsilon(q))$. Here $\varepsilon(q)$ is the greatest integer $\leq 2\sqrt{q}$ which is prime to $q$ if $q$ is not a perfect square and $\varepsilon(q) = 2\sqrt{q}$ if $q$ is a perfect square. For the case $q = 4, n = 4$ a machine constructed bilinear algorithm is presented *(joint work with U.Baum)*.

*P. Tiwari*

**On the Decidability of Sparse Univariate Polynomial Interpolation**

We consider the problem of whether or not there exists a sparse univariate polynomial $p(x)$ that interpolates a given set $S = \{(x_i, y_i)\}$ of points. Several cases are resolved, e.g. the case when the $x_i$'s are all positive. But the general problem remains open.

*(Joint work with Allan Borodin, University of Toronto.)*

*U.V. Vazirani*

**Rapidly Mixing Markov Chains**

The conductance of a graph is a measure of the connectedness of the graph. It has been established via eigenvalue arguments by Jerrum and Sinclair, and by direct combinatorial arguments by Mihail that the mixing rate of the random walk on a graph is determined by its conductance.

We extend the latter approach to analyze mixing in graphs where all but $K$ vertices of the graph are well-connected. We prove that the conductance of all but $K$ vertices in a graph determines the mixing rate when the random walk is started with uniform probability on any subset of vertices of size $\gg K$. Similar results have been proved independently by Lovasz and Simonovitz by completely different arguments.

*I. Wegener*

**On Some Variants of HEAP SORT**

BOTTOM-UP HEAP SORT is a fast HEAP SORT variant where the reheap procedure consists of three modules. With procedure leaf-search we look for the so-called special leaf. Starting at the root we always look for the smaller son. Then we search bottom-up for the new position of the root object and, finally, we perform the data transport. The worst case number of comparisons is bounded by $1.5n \log n$. The average case number is $n \log n + a(n)n$ where $a(n) \in [0.35, 0.39]$ depends on $n$. This result can be proved only under some realistic assumptions and is supported by simulations. MDR HEAP SORT is a variant of BOTTOM-UP HEAP SORT using $n$ extra bits to store information about smaller sons. Its worst case complexity can be computed. It equals $n \log n$, if $n = 2^k$.

Berichterstatter: Peter Kirrinnis

# Addresses

Prof.Dr. Helmut Alt
Institut für Informatik (WE3)
Freie Universität Berlin
Nestorstr. 8-9

1000 Berlin 31

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

5300 Bonn 1

Prof.Dr. Walter Baur
Fakultät für Mathematik
Universität Konstanz
Postfach 5560

7750 Konstanz 1

Prof.Dr. Joachim von zur Gathen
Department of Computer Science
University of Toronto
10 Kings College Road

Toronto, Ontario , M5S 1A4
CANADA

Prof.Dr. Peter Borwein
Department of Mathematics
Dalhousie University

Halifax , N.S. B3H 3J5
CANADA

Erich Grädel
Mathematisches Institut
Universität Basel
Rheinsprung 21

CH-4051 Basel

Prof.Dr. Johannes Buchmann
Fachbereich Informatik
Universität des Saarlandes
Im Stadtwald 15

6600 Saarbrücken 11

Prof.Dr. Dimitrii Yu. Grigor'ev
Steklov Inst. of the Academy of
Sciences of the USSR
Leningrad Br.
Nab. Fontanka 27

Leningrad 191011
USSR

Peter Bürgisser
International Computer Science
Institute
1974 Center Street,Suite 600

Berkeley , CA 94704 -1105
USA

Prof.Dr. Johan Hastad
Dept. of Numerical Analysis and
Computing Science
Royal Institute of Technology
Lindstedtsvägen 25

S-100 44 Stockholm

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

1055 Buenos Aires
ARGENTINA

Dr. Henri Lombardi
Laboratoire de Mathematiques
Universite de Franche-Comte
16, Route de Gray

F-25030 Besancon Cedex

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

Troy , NY 12180-3590
USA

Prof.Dr. Wolfgang Maass
Dept. of Mathematics (mk 249)
University of Illinois at Chicago
Box 4348

Chicago , IL 60680
USA

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

5300 Bonn 1

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

6000 Frankfurt 11

Peter Kirrinnis
Institut für Informatik
Universität Bonn
Römerstraße 164

5300 Bonn 1

Prof. Ph.D. Kurt Mehlhorn
Fachbereich Informatik
Universität des Saarlandes
Im Stadtwald 15

6600 Saarbrücken 11

Dr. Thomas Lickteig
International Computer Science
Institute
Suite 600
1947 Center Street

Berkeley , CA 94704-1105
USA

Prof.Dr. Friedhelm Meyer auf der Heide
Fachbereich Mathematik/Informatik
Universität Paderborn
Postfach 1621
Warburger Str. 100

4790 Paderborn

Roland Mirwald
Fachbereich Mathematik
Universität Frankfurt
Postfach 11 19 32
Robert-Mayer-Str. 6-10

6000 Frankfurt 1

Prof.Dr. Claus-Peter Schnorr
Mathematisches Seminar
Fachbereich Mathematik
Universität Frankfurt
Postfach 11 19 32

6000 Frankfurt 1

Prof.Dr. Andrew M. Odlyzko
AT & T
Bell Laboratories
600 Mountain Avenue

Murray Hill , NJ 07974-2070
USA

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

5300 Bonn 1

Prof. Michael Paterson
Department of Computer Science
University of Warwick

GB- Coventry CV4 7AL

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

5300 Bonn 1

Prof.Dr. Alexander Razborov
Steklov Mathematical Institute
Academy of Sciences of the USSR
42, Vavilova str.

Moscow 117 966 GSP-1
USSR

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

7750 Konstanz 1

Dr. Rüdiger Reischuk
Institut für Theoretische
Informatik
Technische Hochschule Darmstadt
Alexanderstr. 10

6100 Darmstadt

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

7750 Konstanz 1

Dr. Prasoon Tiwari
Computer Science Department
University of Wisconsin-Madison
1210 W. Dayton St.

Madison , WI 53706
USA

Prof.Dr. Umesh 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
Postfach 50 05 00

4600 Dortmund 50

# E-Mail Addresses

| | |
|---|---|
| P. Borwein : | pborwein@cs.dal.ca |
| P. Bürgisser : | buerg@icsi.berkeley.edu |
| J. Buchmann : | buchmann@cs.uni-sb.de |
| M. Clausen : | clausen@leon.informatik.uni-bonn.de |
| J. von zur Gathen : | gathen@theory.toronto.edu |
| E. Grädel : | graedel@urz.unibas.ch |
| J. Hastad : | johanh@nada.kth.se |
| E. Kaltofen : | kaltofen@cs.rpi.edu |
| M. Karpinski : | marek@theory.cs.uni-bonn.de |
| T. Lickteig : | lickteig@icsi.berkeley.edu |
| W. Maass : | U45381@UIVCM.BITNET |
| E. W. Mayr : | mayr@vax1.rz.uni-frankfurt.dbp.de |
| K. Mehlhorn : | mehlhorn@cs.uni-sb.de |
| F. Meyer auf der Heide : | fmadh@uni-paderborn.de |
| R. Mirwald : | rbiffm!mirwald |
| A.M. Odlyzko : | amo@research.att.com |
| M.S. Paterson : | paterson@cs.warwick.ac.uk |
| A.A. Razborov : | razb@log.mian.su |
| R. Reischuk : | xitirrei@ddathd21.bitnet |
| C.-P. Schnorr : | rbiffm!schnorr |
| M.A. Shokrollahi : | amin@leon.informatik.uni-bonn.de |
| P. Tiwari : | tiwari@cs.wisc.edu |
| U.V. Vazirani : | vazirani@ernie.berkeley.edu |