MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

T a g u n g s b e r i c h t 49/1986

Komplexitätstheorie

9.11. bis 15.11.1986

The 7th Oberwolfach Conference on Complexity Theory was organized as before by C.P.Schnorr (Frankfurt), A.Schönhage (Tübingen) and V.Strassen (Zürich). The 43 participants came from 10 countries, 15 participants came from North America, USSR, and Israel.

41 lectures were given at the conference covering a large area of complexity theory.

Many lectures dealt with algebraic problems, e.g. the asymptotic complexity of matrix multiplication, complexity of algebras, complexity of rational functions and of the factors of polynomials, complexity of the permanent and of computing roots in classgroups, construction of Gröbner bases, parallel algorithms for permutation groups.

Other lectures concerned problems in logic, e.g. complexity of logical theories and of quantifier elimination, feasible constructive proofs.

Several topics have been related to cryptology, e.g. interactive proofs, interactive authentication, interactive games, zero-knowledge-proofs, communication complexity.

Many concrete computational problems have been considered, e.g. GCD-computation of polynomials, multiplication of integers, computation of eigenvalues, complex division, bin-packing, the union-find-split problem, Markov-chains, VLSI-design, problems in computational geometry, graph connectivity.

A large variety of computational models and complexity classes have been analyzed, e.g. straight-line-programs, depth bounded Boolean networks, PRAMs and WRAMs, decision trees, pushdown automata, bounded width branching programs, distributed computations and various probabilistic and parallel complexity classes.

Participants:

H. Alt, Berlin
Th. Beth, Erlangen
D. Bini, Pisa
M. Clausen, Zürich
G. Collins, Ohio
St. Cook, Toronto
D. Coppersmith, Yorktown Heights
M. Fürer, Zürich
M. Furst, Pittsburgh
Z. Galil, New York
J. von zur Gathen, Toronto
E. Grädel, Basel
D. Grigoryew, Leningrad
H. F. de Groote, Frankfurt
J. Heintz, Frankfurt
M. Jerrum, Edinburgh
B. Just, Frankfurt
E. Kaltofen, New York
M. Karpinski, Bonn
J. van Leeuwen, Utrecht
Th. Lenguaer, Paderborn,
Th. Lickteig, Zürich
E. Luks, Eugene
E. Mayr, Stanford
K. Mehlhorn, Saarbrücken
F. Meyer auf der Heide, Dortmund
S. Micali, Cambridge
A. Möbus, Düsseldorf
B. Monien, Paderborn
M. Paterson, Coventry
W. Paul, San Jose
Ch. Rackoff, Toronto
R. Reischuk, Darmstadt
L. Ronyai, Budapest
C.P. Schnorr, Frankfurt
A. Schönhage, Tübingen
U. Schöning, Koblenz
A. Shamir, Revohot
H.J. Stoss, Konstanz
V. Strassen, Zürich
K. Wagner, Augsburg
I. Wegener, Frankfurt
A. Widgerson, Jerusalem

Abstracts

H. Alt Congruence, similarity, and symmetries of geometrical objects

(joint work with K. Mehlhorn, H. Wagener, E. Welzl)

The following problems from computational geometry are investigated:

- Given two sets A, B of n points each in $\mathbb{R}^d$, decide if they are congruent or similar.
- Given one set of n points, find all its symmetries, i.e. its symmetry group.

For $d \leq 3$, we find O(n log n)-algorithms for these problems, provided that real numbers can be presented exactly and we have exact real arithmetic. If this is not the case, the problem becomes considerably more complicated. For "approximate congruence" we obtain various algorithms depending on what type of mappings (translations, rotations) are allowed, whether the assignment of the points of B to the ones of A is known or not, whether approximate congruence for a given tolerance ε should be decided or the smallest ε found, etc..

D. Bini Efficient algorithms for the evaluation of the eigenvalues of block banded (block rational) Toeplitz matrices

New efficient algorithms are proposed for the evaluation of the characteristic polynomial $p(\lambda)=\det(A-\lambda I)$ of a matrix A, where

1 - A is a block banded Toeplitz matrix, i.e. $A \in \mathbb{F}^{mn \times mn}$, $A=[A_{ij}]_{i,j=0}^{n-1}$, $A_{ij}=A_{j-i} \in \mathbb{F}^{m \times m}$, $A_i=0$ if $i>s$ or $i<-r$, $m,n,r,s \in \mathbb{N}$, $r,s<n$,

2 - A is a block rational Toeplitz matrix, $A \in \mathbb{C}^{mn \times mn}$, $A=[A_{ij}]_{i,j=0}^{n-1}$, $A_{ij}=A_{j-i} \in \mathbb{C}^{m \times m}$, where the blocks A_i define a rational function $f:\mathbb{C} \to \mathbb{C}^{m \times m}$ by means of the Laurent series $f(z)= \sum_{i=-\infty}^{+\infty} z^i A_i$.

Matrices of this kind arise in many problems (cf. Trench, SIAM J. appl. Math 15,1976).

In case 1 (with V. Pan) we compute $p(\lambda)$ as well as $p(\lambda)/p'(\lambda)$, where $p'(\lambda)=dp(\lambda)/d\lambda$, in $O(k \log k \log n + k^3)$ block multiplications, where $k=r+s$, that is, $k+1$ is the bandwidth of A.

In case 2 (with F.D. Benedetto) we compute $p(\lambda)$ as well as $p'(\lambda)$ in $O(k \log k \log n + k^3)$ block multiplications, where k is the degree of the rational function f(z), provided that f(z) can be written as

$$f(z) = \sum_{i=-r}^{s} z^i C_i \left[\left(\sum_{j=0}^{p} z^j D_j \right) \left(\sum_{l=0}^{q} z^{-l} E_l \right) \right]^{-1}, \quad C_i, D_j, E_l \in \mathbb{C}^{m \times m},$$

where the polynomials $\det(\sum_{j=0}^{p} z^j D_j)$, $\det(\sum_{l=0}^{q} z^l E_l)$ have no common zero and the blocks

D_j, E_l commute, i.e. $D_jE_l=E_lD_j$.

We compose these algorithms with two algorithms given by W. Trench, which approximate $p(\lambda)$ in $O(k \log n + k^3)$ multiplications in case 1 and 2, provided that $\mathbb{F}=\mathbb{C}$.

G. Collins Regularity in Gröbner basis construction

Gröbner basis construction for the special case of bivariate rational polynomials with total degree ordering is studied methodically, both empirically and analytically. A theorem on Gröbner basis construction, in this context and with only two input basis polynomials, analogous to the reduced p.r.s. theorem is proved and its extension to an analogue of the fundamental theorem of p.r.s. is anticipated. Whereas previously exponential coefficient growth could not be precluded, a polynomial time algorithm is now available for a special case and is forseeable also for the general case.

St. Cook Feasible constructive proofs

(joint work with A. Urguhart)

In 1974 I introduced a quantifier-free system PV of number theory which had function symbols for all polytime computable functions, and argued that theorems of PV are "polynomially verifiable" and had "feasible constructive" proofs. I proved that every family of propositional tautologies that are provably valid in PV, have polynomially bounded extended resolution proofs (see the abstracts for this conference, 27 oct. - 2 nov. 1974).

The notion of feasibly contructive proof seems to extend to mathematics generally, with many theorems of number theory and graph theory, for example, possessing such proofs, while many other theorems appear not to. An example in the latter class is Fermat's little theorem. A feasibly constructive proof of this would probably lead to a practical method for factoring large integers.

Recently Sam Buss developed an intuitionistic formal system IS'_2 in which all polytime computable functions are provably recursive, and further, if $IS'_2 \vdash \forall x \exists y A(x,y)$ then for some polytime computable function f, $\forall x A(x,f(x))$ holds. Alasdair Urguhart and I have simplified the presentation of IS'_2 and the proofs of these results, in particular dispensing with cut-elimination arguments. We also present a "Gödel Dialectica" interpretation. We argue that IS'_2 at least approximately captures the notion of feasibly constructive proof. The main open questions are to prove that interesting theorems, such as Fermat's little theorem, are not provable in IS'_2.

D. Coppersmith Matrix multiplication via arithmetic progressions

(joint work with S. Winograd)

We present a new method for accelerating matrix multiplication asymptotically. This work builds on recent ideas of Volker Strassen, by using a basic trilinear form which is not a matrix product. We make novel use of the Salem-Spencer Theorem, which gives a fairly dense set of integers with no three-term arithmetic progression. Our resulting matrix exponent is 2.376.

M. Fürer How fast can we multiply integers ?

In 1971 Schönhage and Strassen have presented two fast integer multiplication algorithms based on FFT. The first algorithm works over $\mathbb{C}$ and reduces multiplication on N-bit integers to multiplication of (log N)-bit integers.

The second one works over Fermat-rings and reduces length N to length $\sqrt{N}$. It is the fastest known algorithm with running time O(N log N log log N), because multiplications with roots of unity 2^k are just shifts.

If the Fermat primes are not extremely rare, then they can be used to build a multiplication algorithm having the adventages of both above algorithms (reduction from N to log N, and replacement of many multiplications by shifts) improving the factor log log N to $c^{\log^* n}$. The question is whether another algebraic construction can avoid the Fermat primes.

M. Furst Constant-width branching programs

Width-5, polynomial-length branching programs have been shown by Barrington to be equivalent in computational power to log-depth, poly-size circuits. The new lower bound techniques which Razborov and then Smolensky have employed to greatly simplify the constant-depth lower bounds of mine, Saxe, Sipser, Yao and Hastad may also be used in the constant-width branching program setting. The algebraic methods may be used to show that width-3 permutation branching programs cannot compute such simple Boolean functions as $x_1 \wedge x_2 \wedge \ldots \wedge x_n$ in less than $\Omega(2^n)$ length (I believe Barrington has shown $\Omega(2^{n/2})$ by other methods). Width-5 still seems a long way off.

In 1981 I introduced a hierarchy (called the safe-storage hierarchy $SF_0 \subseteq SF_1 \subseteq \ldots$) which lies between P and PSPACE. This machine-based hierarchy corresponds to constant-width BPs in exactly the same manner that the Meyer-Stockmeyer polynomial hierarchy ($\Sigma_0 \subseteq \Sigma_1 \subseteq \ldots$) coresponds to constant-depth circuits. In the safe-storage hierarchy, $SF_0 = P$, $\Sigma_1 \cup \Pi_1 \subseteq SF_1$, $\Sigma_2 \cup \Pi_2 \subseteq SF_2$. Now we question that $SF_3 = PSPACE$. It is very unlikely that the first few levels collapse.

Z. Galil Separators in pushdown graphs and lower bounds for online computations

(Joint work with R. Kannan and E. Szemeredi)

We show that the following two open problems are equivalent:

(1) is the family of k page graphs (or 3 pushdown graphs) separable?

(2) can one-tape online nondeterministic Turing machine simulate a two-tape online nondeterministic Turing machine in less than quadratic time?

The size of separators for 3 pushdown graphs is related to the time of the simulation.

We construct k page graphs and prove an $\Omega(n/\log \ldots \log n)$ (k times log) bound on their separators. Consequently, a similar lower bound applies to some 3 pushdown graphs and we derive an $\Omega(n^2/\log \ldots \log n)$ (k times log) lower bound for simulating a two-tape machine by a one-tape machine.

J. von zur Gathen Permanent and determinant

A central question in Valiant's arithmetic analogue of the Boolean theory of P vs. NP is: for which m is the n×n-permanent a projection of the m×m-determinant? Let p(n) be the smallest such m, i.e.

$$p(n) = \min \{m: \exists f \in (F \cup \{x_{11}, x_{12}, \ldots, x_{nn}\})^{m \times m}: \operatorname{per}(x_{ij}) = \det f\}.$$

Valiants hypothesis, the arithmetic analogue of Cook's hypothesis "P≠NP", would be implied by a lower bound $p(n) = 2^{(\log n)^{\omega(1)}}$. Using methods from algebraic geometry, involving the singular locus of the permanent and determinant polynomials, the first non-trivial lower bound is derived:

$$p(n) > \sqrt{8/7} \cdot n - 1 > 1.069n - 1.$$

E. Grädel Complexity of subclasses of logical theories

We investigate the complexity of subclasses of logical theories (mainly Presburger and Skolem arithmetic). These subclasses are defined by restrictions on the quantifier prefix (bounded alternations or bounded total number of quantifiers).

For Presburger arithmetic we find, for all m≥2, formula classes defined by prefixes with m+1 alternations and m+5 quantifiers, which are Σ_m^P rsp. Π_m^P-complete. For m=1 we show that the class of $\exists\forall\forall$-formulas is NP-complete. For m=0 and for all t, the class of $\exists^t$-formulas is in P (H. Lenstra, Scarpellini).

We thus have a nice characterisation of the polynomial-time hierarchy by classes of Presburger formulas.

We further develop a general method for proving lower bounds for such problems, based on recent work by W. Henson and K. Compten, and on bounded versions of the domino problem. Applications:

- The class of $\exists\forall^5\exists^*$-formulas of Presburger arithmetic is NEXPTIME-hard.

- There exists a fixed prefix $Q_1...Q_t$ such that the class of $Q_1...Q_t$-formulas of the theory of natural numbers with multiplication (Skolem arithmetic) is NEXPTIME-hard.

A generalisation of the method for ATIME-lower bounds is obtained by introducing instead of the domino problem domino-games. In such games players $\exists$ and $\forall$ tile in alternating moves successively growing squares.

Translating the claim that player $\exists$ has a winning strategy for tiling a $T(n)\times T(n)$-square in m moves into a formula from a certain subclass, gives an ATIME($T(f(n))$, m) lower bound for this class.

D. Y. Grigoryew Complexity of quantifier elimination in the theory of ordinary differential equations

Let a formula $Q_1X_1 \dots Q_nX_n(\Omega)$ of the first-order theory of ordinary differential equations be given, here Q_i are quantifiers, Ω is a quantifier-free formula with atomic subformulas of the form (f=0) where

$f \in \mathbb{Z}[X_1,X_1^{(1)},...,X_1^{(R)},...,X_n,X_n^{(1)},...,X_n^{(R)},Y_1,Y_1^{(1)},...Y_1^{(r)},...,Y_m,Y_m^{(1)},...,Y_m^{(r)}]$

is a differential polynomial. Denote by L the bit size of the formula.

Theorem: One can produce a quantifier-free formula equivalent to the given one within time polynomial in $L^{m^n}.2^{(2^nR)}$.

Previously known method due to A. Seidenberg for quantifier elimination in the theory under discussion has a nonelementary (in Kalmar sense) complexity. To obtain an elementary complexity bound our (joint with A. Chistov) procedure of quantifier elimination in the theory of algebraically closed fields is involved.

H.F. de Groote On the complexity of Lie algebras

We give a report on recent work of Heintz, Mirwald, Möhler, Schmidt, and de Groote (all U. Frankfurt) on the complexity of Lie algebras and some related mathematical problems.

Let L(g) be the complexity, R(g) the bilinear complexity of a finite dimensional Lie algebra g over $\mathbb{C}$.

Theorem: Let g be a simple Lie algebra from one of the classical series A_l, B_l, or D_l, $\mathfrak{G}$ a Cartan subalgebra of g. Then $R(g) \geq 2\cdot\dim g - \dim \mathfrak{G}$, and equality holds iff $g \simeq sl(2,\mathbb{C})$.

The proof rests on the estimate $\dim C_g^2(X) \leq \dim \mathfrak{G}$ for the dimension of double centralizers $C_g^2(X)$ $(X \in g)$.

Conjecture: For every semisimple Lie algebra g with Cartan subalgebra $\mathfrak{G}$ and every $X \in g$ we have $\dim C_g^2(X) \leq \dim \mathfrak{G}$.

Theorem: Let $\mathfrak{B}$ be a Borel-subalgebra of a simple Lie algebra g with Cartan subalgebra

$\mathfrak{H}$. Then $L(\mathfrak{B}) \geq 2 \cdot \dim[\mathfrak{B},\mathfrak{B}] - \dim \mathfrak{H}$.

Let $\Gamma^0(g)$ be the proper isotropy group of g.

Theorem: Let g be a simple Lie algebra. Then $\Gamma^0(g) \simeq \mathrm{Aut}(g)$ if $g \neq sl(2,\mathbb{C})$, $\Gamma^0(g) \simeq Gl(sl(2,\mathbb{C}))/\mathbb{C}^\times$. The same holds for Borel subalgebras of simple Lie algebras.

Theorem: $\Gamma^0(sl(2,\mathbb{C}))$ operates transitively on the variety of all optimal bilinear algorithms for $sl(2,\mathbb{C})$.

Moreover we discuss some other structures arising from the study of isotropy groups of Lie algebras.

J. Heintz Real quantifier elimination is doubly exponential

(joint work with J.H. Davenport)

We show that quantifier elimination over real closed fields can require doubly exponential space (and hence time). This is done by explicitely constructing a sequence of expressions whose length is linear in the number of quantifiers, but whose quantifier-free expression has length doubly exponential in the number of quantifiers. The result can be applied to cylindrical algebraic decomposition, showing that this can be doubly exponential. The double exponents of our lower bounds are aboute one fifth of the double exponents of the best known upper bounds.

The same result has been obtained by V. Weispfennig using a different method. Priority is due to V. Weispfennig.

M. Jerrum Rapidly converging Markov chains - characterisations and applications

The subject of this talk is Markov chains which converge very rapidly to a stationary distribution on the states. Three applications are described:

1. (Almost) uniform random generation of combinatorial structures.
2. Approximate counting of combinatorial structures.
3. Efficiently increasing the precision of approximation algorithms for counting problems.

Techniques are presented for demonstrating rapid convergence of Markov chains. These involve coupling, or the expansion properties of the graph underlying the Markov chain.

B. Just Languages that cannot be recognized by evaluating analytic functions and the floor function

(joint work with L. Babai and F. Meyer auf der Heide)

Computation models with the power of evaluating discontinuous functions have not been analyzed very much until now. Few lower bounds or results on the decidability of

languages are known for them.

Here the computational model of an "analytic computation tree" (ACT) is presented, which is a model for all algorithms that operate on real numbers and in one step either compare two reals, or evaluate the floor function, or evaluate any analytic function. The model generalizes the "algebraic computation tree" model of Ben Or.

We show by topological arguments that by ACTs a class of languages cannot be decided, examples of which are $\mathbb{Q}^n$ or the tuples $(x_1,\ldots,x_n)\in\mathbb{R}^n$ that have components which are $\mathbb{Z}$-linearly or algebraically dependent.

E. Kaltofen Computing with polynomials given by straight-line programs

A theorem is presented that shows that any factor of polynomially bounded degree of a multivariate polynomial given by a division free straight-line program such that the co-factor is relatively prime to the factor has a straight-line computation polynomially bounded in the length of the original program. Applications of this theorem are given to the GCD problem and the problem of separately computing numerators and denominators of rational multivariate straight-line functions.

M. Karpinski Randomness, provability and the separation within Monte Carlo time and space classes

(joint work with R. Verbeek)

It is known that there is "no life" other than "finite-state" below the log log n - space (both deterministic and nondeterministic). We prove that the probabilistic computations real is quite different: for every unbounded nondecreasing (u.nd.) recursive function there is a Monte Carlo space constructible u.nd. minorant. (Note that $\log^* n$ is therefore also Monte-Carlo space constructible!). Unfortunately, unlike the deterministic or nondeterministic cases, the existence of distinct constructible bounds does not guarantee separation of the Monte Carlo complexity classes.

This is because the "Monte Carlo property" of probabilistic algorithms or uniform probabilistic circuits is Π^1_1-complete in the corresponding classes. This leads to the situation that no one knows whether Monte Carlo TIME(n) $\neq$ Monte Carlo $(2^{n^{o(1)}})$. For practical purposes, however the only interesting Monte Carlo algorithms are those, which are provable within some reasonable theory (e.g. Peano arithmetic or Zermelo-Fraenkel set theory). For this class we were able to prove the existence of distinct provable Monte Carlo space classes with arbitrary small (recursive) space bounds, as well as dense time hierarchies.

In particular we were able to separate fast (polynomial time) random log log n - space from DSPACE(log log n), and terminating Monte Carlo log log n - space from

NSPACE(o(log n)).

J. van Leeuwen Distribution of records on a ring of processors

We present some first results on the analysis of the load-distribution problem in networks of processors, viewed as a discrete algorithmic rather than analytic question. Consider the problem of distributing records on a ring such that at all times the number of records in every processor is approximately equal (thus equal to approx. p/n, where p is the current number of records and n the number of processors). In every round a new record is inserted at a random node, and some action takes place to move the record counterclockwise on the ring to a node that will store it. A typical token-based algorithm maintains k tokens on the ring. A record that is inserted is moved to the first node that has ≥ tokens. The node stores the record and transfers one of its tokens to the preceding (!) node. Using Markov chain analysis it is shown that in the long run the number of nodes a record must pass before it hits a node with a token averages out to (n-1)/2k, which shows that probabilistically the tokens remain perfectly distributed on the ring. Several other approaches are analyzed, and good techniques for handling both insertions an deletions of records are discussed.

Th. Lengauer Linear time solutions for CMOS layout problems

(joint work with R. Müller, Paderborn)

We consider layout optimization problems occuring for a certain widely accepted design style for basic functional cells in CMOS technologies. The problems take the combinatorical form of optimization problems on large sets of series-parallel graphs. Here a series parallel graph represents the circuitry in the cell that implements the Boolean function to be realized. In particular, series connections represent logical-and and parallel connections represent logical-or. The optimization takes place on sets of graphs rather than on a simple graph since due to the commutability of logical-and several graphs can represent logically equivalent Boolean formulas. Specifically, the problems we consider are:

Minimum number of duplication problem. Given a series-paralles graph G, find a logically equivalent graph G' that can be made eulerian by duplicating a minimum number of edges;

Minimum number of separations problem. Given a series parallel graph G, find a logically equivalent graph G' that has a minimum number of odd vertices.

Both problems are solved in linear time in the size of G by extending a dynamic programming method of Bern, Lawler, Wong to optimization problems on sets of series parallel graphs.

Th. Lickteig Complexity of complex division

It is shown that, for any quadratic field extension $k \subset K$, the division in K requires exactly six essential multiplications and divisions over k. In particular, complex division in real arithmetic requires six multiplications and divisions.

If additions and subtractions are counted as well, exactly nine operations are required iff $k \subset K$ is radical ($K = k(\omega)$ with $\omega^2 \in k$), otherwise ten operations are required.

E. Luks Parallel algorithms for graph isomorphism

A conceptual breakthrough in graph-isomorphism testing was Babai's demonstration (1979) of the effectiveness of reducing such problems to questions in permutation groups. This led, in particular, to polynomial time algorithms for testing isomorphism of vertex-colored graphs with bounded color classes (Babai, Furst, Hopcroft, Luks 1980) and graphs having bounded eigenvalue multiplicity (Babai, Grigoryev, Mount 1982). it also inspired a study of the computational complexity of permutation group problems, resolving in polynomial time such questions as: finding order, testing membership, finding pointwise stabilizers of subsets (FHL 1980) and finding centers, composition factors (Luks 1981). It has seemed that these algorithms have been inherently sequential, requiring a 'shifting' procedure through a linear-length group tower (Sims, FHL). Nevertheless, we now show all of the above-mentioned problems are in NC. The group problems are reduced to the primitive case. By a strong consequence of the classification of Finite Simple Groups, primitive groups are either quasi-polynomial in size ($O(2^{\log^c n})$) or are 'mainly' wreath products of alternating groups. The former case is resolvable via a direct parallization of Sims' methods augmented by a parallization of the composition factors algorithm (for these groups only). The latter case involves 'decyphering' the alternating-groups-factors and a novel way to deal with A_n in parallel, given arbitrary generators. The final resolution of NC-manageability of permutation groups is joint work with L. Babai and A. Seress.

K. Mehlhorn On the union-find-split problem

(joint work with St. Näker and H. Alt)

Consider a sequence $x_1,\ldots,x_n$ of n items some of which are marked and the following three operations on such a sequence: Find(x_i) returns x_j where $j = \min \{l: l \geq i \text{ and } x_l \text{ marked}\}$, Union($x_i$) unmarks x_i, and Split(x_i) marks x_i. We prove a $\Theta(\lg \lg n)$, i.e., matching upper and lower bound, on the worst case complexity of the Union-Find-Split problem in the pointer machine model of computation. Our lower bound holds for all pointer machine algorithms and does not require the separation assumption used in the lower bound proofs of Tarjan (1979) and Blum (1985).

E. Mayr Parallel bin-packing algorithms

We study the parallel complexity (in the PRAM model) of some well known heuristics for packing n items into bins. We show that FFD (first-fit-decreasing), formulated as a decision problem, is complete for polynomial time under log-space reductions, and therefore probably not efficiently parallelizable. We then give an algorithm running on an exclusive-read-exclusive-write PRAM with n processors in time O(log n) which constructs the FFD packing, provided all items are of size at least 1/k, for some constant k. This algorithm can then be used to construct an algorithm of the same asymptotic performance which constructs packings with a number of bins bounded by $\max \{N_{FFD}, \frac{6}{5}N_{opt}+1\}$.

F. Meyer auf der Heide Probabilistic linear search algorithms

The "component counting lower bound" known for deterministic linear search algorithms (LSAs) also holds for their probabilistic versions (PLSAs) for many problems, even if two-sided error is allowed, and if one does not charge for probabilistic choice. This implies lower bounds on PLSAs for e.g. the element distinctness problem (n log n) or the knapsack problem (n^2). These results yield the first separation result between probabilistic and non-deterministic LSAs, because the above problems are non-deterministically much easier. Previous lower bounds for PLSAs either only work for one-sided error "on the nice side", i.e. on the side where the problems are even non-deterministically hard, or only for probabilistic comparison trees. The proof of the lower bound differs fundamentally from all known lower bound proofs for LSAs or PLSAs, because it does not reduce the problem to a combinatorial one, but argues extensively about a non-disrcrete measure for similarity of sets in $\mathbb{R}^n$. This lower bound solves an open problem posed by Manber and Tompa as well as by Snir.

It is further shown that the complexities of deterministic and probabilistic LSAs (as well as algebraic computation trees) are polynomially related (if we charge for probabilistic choice).

S. Micali The completeness theorem for multi-party cryptographic protocols

We exhibit an efficient algorithm that, given the description of an n-ary Turing machine M, outputs a distributed, cryptographic algorithm for n players, each player i having a secret input x_i. The output algorithm has hostle property that if > n/2 players follow their prescribed protocols, all honest players will correctly compute $y=M(x_1,x_2,...,x_n)$ and any subset of < n/2 "dishonest" collaborating, poly-time players will only know y and their own secret inputs.

S. Micali Proofs, knowledge, and computation

We consider "interactive proof systems", a way of proving theorems to a probabilistic polynomial-time verifier, that appears more generally than NP. These proof systems are powerful enough to easily prove that two graphs are not isomorphic, a problem not yet known to be in NP. Interactive proof systems also allow us to meaningfully address the following question: "How much knowledge is necessary to prove a theorem T?" Certainly enough to see that T is true, but usually much more. For instance to prove that a graph is Hamiltonian, it suffices to exhibit an Hamiltonian tour. This however appears to contain more knowledge than the simple bit "Hamiltonian / non-Hamiltonian". We give a complexity theoretic definition of the amount of "extra" knowledge contained in a proof. We show how to prove that two graphs are isomorphic or non-isomorphic by releasing zero "extra" knowledge. We also show that, assuming secure encryption algorithm, all NP statements can be proved giving away zero extra knowledge. We provide applications to complexity theory and cryptographic protocols.

B. Monien Sperner theory and worst case bounds for the subgraph isomorphism problem

We use ideas from Sperner theory to get improved worst case bounds for the subgraph isomorphism problem. The main notion in our approach is the notion of a q-representative which is strongly related to the notion of transversal-critical hypergraphs.

Theorem: Let G, H be graphs. Let m, n be the number of nodes of G, H, resp. . Then the question whether G is a subgraph of H is decidable within time $O(c_{m-k} \cdot n^{k+1})$ where k is the vertex separation number of G and c_i is some number non depending on n.

Our construction leads to a c_i of order $(2i)^{i/2}$. In proving the theorem we have to construct representations. Only very few details about such a constructive approach can be found in the literature. We discuss two constructive methods and consider also some special cases.

M.S. Paterson On Razborov's result for bounded-depth circuits over $\{\oplus, \wedge\}$

A small improvement and simplification of Razborov's lower bound result for bounded depth circuits is presented. The bound proved for depth k+2 circuits over the basis $\{\oplus, \wedge\}$ for the majority function on n inputs is $\exp\{\Omega(n^{1/k})\}$.

C. Rackoff An overview of cryptographie - from my point of view

Definitions of private key and public cryptography should allow arbitrary interaction by the two parties, and a small probability of error by the receiving party. One should

have a very strong definition of security: a polynomial time bounded person who is listening to the communication and choosing some message bits, cannot learn anything significant about any of the other message bits. This can be formalized.

If we make certain complexity assumptions from number theory, then we obtain secure 2-pass (i.e. 2-interactive) public systems, secure pseudo-random number generators, secure 1-pass private-key cryptosystems, many interesting protocols, etc..

Without any such assumption, we know very little. To do secure public cryptography it is sufficent to send one bit securely. Does it help to have 3 or more passes? There are examples where it might. Does it help to have more passes? There are no examples, and no proofs of the contrary. To do secure private key cryptography, it is sufficient to be able to send n+1 bits securely, where n = security parameter = length of the key. Does it help to have 2 or more passes?

Can one obtain secure function generators by, for each key, composing a small (polynomial in n) number of "very simple" functions: $\{0,1\}^n \to \{0,1\}^n$? This is one assumption behind DES, the U.S. "Data Encryption Standard".

R. Reischuk Communication complexity

2 processors P_X, P_Y connected by a reliable channel want to compute a Boolean function $f=f(X,Y)$ on 2 binary vectors of length n. To do so they exchange information because the first argument X is only known to P_X and the second argument only to P_Y. The communication complexity of f, denoted by C(f), is the maximum (over all pairs of inputs) of the number of bits that have to be exchanged.

It is shown that the product of the nondeterministic communication complexity of f and its complement is an upper bound on the deterministic complexity and that this bound is sharp. We further investigate how the communication complexity increases if f is evaluated simultaneously on different pairs of inputs. Bounds on C(f) for probabilistic protocols are given. For protocols with a fixed number of rounds there is an exponential gap between k-1 round deterministic and k round probabilistic complexity. These results were obtained together with B. Halstenberg.

Finally we consider the identification problem in the classical information theoretic mode. A new double exponential bound on the number of messages due to Ahlswede and Dueck is briefly presented.

L. Ronyai Computational problems in finite dimensional algebras

We consider algorithmic problems related to finite dimensional associative algebras over finite fields and algebraic number fields.

A polynomial time algorithm is presented (Las Vegas in the finite case) to find Rad(A) and the simple components of A/Rad(A) (joint work with K. Friedl).

A more general problem is to find zero divisors in A, if A contains zero divisors. A polynomial time Las Vegas algorithm is given if the ground field is finite.

The infinite case seems more difficult. We consider the case $\dim_Q A=4$, A is central simple over Q. Under GRH there exists a polynomial time Las Vegas reduction of the decision problem to quadratic residuosity. Consequently under GRH finding zero divisors over Q is at least as difficult as factoring squarefree integers.

C.P. Schnorr The complexity of roots in class groups

For a squarefree integer Δ, let C_Δ be the group of $Sl_2(\mathbb{Z})$ equivalence classes of binary quadratic forms $ax^2+bxy+cy^2$ with discriminant $\Delta=b^2-4ac$. The following problems are equivalent by probabilistic polynomial time reductions:

(1) Factoring Δ,

(2) computing square roots in C_Δ,

(3) solving in integers the equation $u^2-\Delta v^2=az^2$ when the factorisation of a is given.

For the reduction (2)$\leq$(1) we assume the ERH.

The fastest algorithm for computing p-th roots in C_Δ, p=3,5,7,... has time bound $L(\Delta)^{1+o(1)}$, $L(\Delta) = \exp\sqrt{\log\Delta \log\log\Delta}$. This time seems to be needed even if factorisations of integers are given for free.

The class number $|C(\Delta)|$ can be computed by Seysen's method within $L(\Delta)^{1+o(1)}$ steps.

A. Schönhage GCD-computations

The following probabilistic algorithm for the gcd D(x) of primitive integer polynomials A(x), B(x) of degree $\leq n$, with $|A|, |B| \leq 2^h$, is analyzed.

(0) Try (1) - (4) with t=h+1, 2h, 4h, 8h, ... until success.

(1) choose r at random, $0 \leq r < R = n(n+1)h$, set $\xi=2^t+r$;

(2) compute $d(\xi) = \gcd(A(\xi), B(\xi))$;

(3) find $F_0\in\mathbb{Z}[x]$ with coeff. $|f_j| < 2^{t-2}$ such that $F_0(\xi)=d(\xi)$, and set F(x) = primitive part of $F_o(x)$;

(4) if $F(x)|A(x)$ and $F(x)|B(x)$ then return $D(x)=F(x)$.

Termination is guaranteed by the worst case bound in

$\exists\, U(x), V(x) \in \mathbb{Z}[x] : U(x)A(x) + V(x)B(x) = QD(x)$ with $1\leq Q<2^{2nh}$,

which implies $d(\xi)=q(\xi)D(\xi)$ with $q(\xi)|Q$. The algorithm will succed in (3) and (4) iff $q(\xi)\cdot|D|_\infty < 2^{t-2}$, thus $q(\xi)$ should be small.

Prop: The arithmetic mean g of log $q(\xi)$ over any sequence of n(n+1)h consecutive integers is bounded by $g \leq n \log(nh)\cdot(\ln h + O(1))$.

This implies that the expected running time (e.g., for pointer machines) is bounded by $E(T) \leq O(nh \log(nh) + n^2\cdot\log^2(nh) \log h)$.

U. Schöning Probabilistic algorithms, lowness, and graph isomorphism

A relatively simple proof of the recent result that the graph isomorphism problem is located in the complement of Babai's class AM (which stands for "Arthur-Merlin" games) is given. This result implies that graph isomorphism is not NP-complete unless the polynomial-time hierarchy "collapses". As a second approach, it is shown that the graph isomorphism problem is located in the low hierarchy in NP, which implies again that this problem is not NP-complete, moreover, not even in the sence of γ-completeness.

A. Shamir Zero knowledge proofs of knowledge

In this talk we discuss proofs which do not even reveal whether the theorem or its converse are true. Such "truely zero knowledge" proofs can be the basis of very efficient identification schemes which are provably secure if factoring is difficult and about two orders of magnitude faster than RSA-based schemes. In the last part of the talk we prove the security of the parallel version of the new identification schemes, which are not known to be zero knowledge.

H.J. Stoss Lower bounds on the complexity of rational functions

We describe a uniform manner for all complexity measures and independent of the characteristic of the underlying field the connection between sets of rational functions with small complexity and images of suitable mappings. As applications we prove optimal lower bounds for the complexity of polynomials with algebraic coefficients and furthermore new lower complexity bounds which hold uniformly for large classes of polynomials as, e.g., sets of polynomials with 0-1-coefficients, divisors and multiples of a given polynomial.

V. Strassen Asymptotic spectrum and matrix multiplication

We introduce an asymptotic data structure for the relative computational complexity of bilinear maps. It consists of a compact space Δ together with an interpretation of the bilinear maps under consideration as continuous real functions on Δ. Asymptotic rank becomes the maximum of the associated function. Schönhage's τ-theorem is a simple consequence. We partially compute Δ in the cases of matrix multiplication and of polynomial multiplication modulo a fixed polynomial. On the way we present a new method ("Laser") for estimating the exponent of matrix multiplication, show $\omega<2.48$ and interpret Coppersmith-Winograd's improvement $\omega<2.39$.

K.W. Wagner The influence of succinct graph description to the complexity of graph problems

The practical necessity to describe very large graphs e.g. in VLSI design has led to the design of several languages for the succinct description of graphs. These languages can compress the description of a graph at most logarithmically. Hence, the complexities of graph problems (which are measured relative to the length of the descriptions) can grow at most exponentially, using these languages. However, this exponential complexity blow-up cannot be observed for all problems and all descriptional languages, i.e.
- different problems can have different blow-ups using the same language, and
- the same problem can have different blow-ups using different languages.
In the talk an overview on related results is given.

I. Wegener Lower bound methods for bounded depth circuits, PRAMs and WRAMs

Lower bounds on the complexity of PRAMs, and WRAMs, and PRAMs of restricted communication width (due to Cook, Dwork, Reischuk and Vishkin, Widgerson) depend on the critical or sensitive complexity of the considered Boolean function. We show that the sensitive complexity is equal to the "length" of a Boolean function. We discuss relations between these complexity measures, determine the asymptotic behaviour of the complexity measures for several classes of functions, and we generalize the lower bounds for the parity function due to Hastad (bounded depth circuits) and Beame (unrestricted WRAMs) to larger classes of functions.

A. Widgerson Rubber bands, convex embeddings and graph connectivity

The main result is a new, geometric characterization of k-(vertex) connected graphs. Roughly, a graph is k-connected iff it can be embedded in $\mathbb{R}^{k-1}$ such that all but k of the vertices are mapped to the convex hull of their neighbours.

The proof of this theorem appeals to physical intuition. The desired embedding is obtained by considering a physical model for the graph, in which edges are ideal springs, glue k vertices to the extreme points of a simplex and consider this system in the state of minimum potential energy.

The algebraic properties of this system support efficient computation and lead to new (randomized) algorithms for testing the connectivity of a graph, that are faster than known algorithms for dense graphs.

Berichterstatter: Bettina Just

Adressen der Tagungsteilnehmer

Prof. Dr. H. Alt
Institut für Mathematik III
F.U. Berlin
Arnimallee 2-6
1000 B e r l i n 33

Prof. Dr. W. Baur
Fakultät für Mathematik
Universität Konstanz
Postfach 5560
7750 K o n s t a n z 1

Prof. Dr. Th. Beth
Institut für Informatik
Universität Karlsruhe
Postfach 6980
7500 K a r l s r u h e 1

Prof. Dr. D. Bini
Dipartimento di Matematica
Università di Pisa
Via Buonarroti, 2
I - 56100 P i s a
Italien

Dr. M. Clausen
Institut für Informatik I
Technologie-Fabrik
Haid-und-Neu-Str. 7
7500 K a r l s r u h e 1

Prof. Dr. G. E. Collins
Computer Sciences Department
University of Wisconsin
1210 W. Dayton Street
M a d i s o n , Wisconsin 53706
U S A

Prof. Dr. St. A. Cook
Department of Computer Science
University of Toronto
Toronto, Ontario M5S 1A4
Canada

Dr. D. Coppersmith
IBM Research 32-256
Math. Sciences Department
P.O.Box 218
Yorktown Heights, N.Y. 10598
U S A

Dr. M. Fürer
Institut für Angew. Mathematik
Universität Zürich
Rämistr. 74
CH-8001 Z ü r i c h
Schweiz

Prof. Dr. M. L. Furst
Computer Science Department
Yale University
New Haven, Connecticut 06520
U S A

Prof. Dr. Z. Galil
Computer Science Department
Columbia University
Seeley W. Mudd Bldg.
N e w Y o r k , N.Y. 10027
U S A

Prof. Dr. J. von zur Gathen
Department of Computer Science
University of Toronto
10 King's College Road
Toronto, Ontario M5S 1A4
Canada

Erich Grädel

Mathematisches Institut der
Universität
Rheinsprung 21

CH-4051 B a s e l
Schweiz

Prof. Dr. D. Yu. Grigorev

Department of Mathematics
Steklov Institute Leningrad
Fontanka 27

L e n i n g r a d 191 011
Sowjetunion

Prof. Dr. H. F. de Groote

Fachbereich Mathematik der
Universität Frankfurt/M.
Postfach 11932

6000 F r a n k f u r t / M. 1

Priv.-Doz. Dr. J. Heintz

Fachbereich Mathematik der
J. W. Goethe-Universität
Robert-Mayer-Str. 6-10

6000 F r a n k f u r t/M. 90

Prof. Dr. M. R. Jerrum

Department of Computer Science
University of Edinburgh
The King's Buildings

E d i n b u r g h EH9 3JZ
Schottland

Bettina Just

Fachbereich Mathematik der
J. W. Goethe-Universität
Robert-Mayer-Str. 6-10

6000 F r a n k f u r t/M. 90

Prof. Dr. E. Kaltofen

Department of Computer Science
Rensselaer Polytechnic Institute

T r o y , New York 12180-3590

U S A

Prof. Dr. M. Karpinski

Institut für Informatik der
Universität Bonn
Wegelerstr. 6

5300 B o n n 1

Prof. Dr. J. van Leeuwen

Department of Computer Science
University of Utrecht
P.O.Box 80.012

NL-3508 TA U t r e c h t
Niederlande

Prof. Dr. Th. Lengauer

Fachbereich 17 der Universität
GH Paderborn
Warburger Str. 100; Pf. 1621

4790 P a d e r b o r n

Dr. Th. Lickteig

Institut für Angew. Mathematik
Universität Zürich
Rämistr. 74

CH-8001 Z ü r i c h
Schweiz

Prof. Dr. R. Loos

Mathematisches Institut der
Universität Tübingen
Auf der Morgenstelle 10

7400 T ü b i n g e n 1

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

Prof. Dr. E. M. Luks

Computer & Info. Science
University of Oregon

E u g e n e , Oregon 97403

U S A

Prof. Dr. B. Monien

Universität-GH Paderborn
FB 17 - Math./Inf.
Warburger Str. 100

4790 P a d e r b o r n

Prof. Dr. E. W. Mayr

Department of Computer Science
University of Stanford

S t a n f o r d , CA 94305

U S A

Prof. Dr. M. S. Paterson

Department of Computer Scienc
University of Warwick

C o v e n t r y CV4 7AL

Grossbritannien

Prof. Dr. K. Mehlhorn

FB 10; Institut für Informatik
Universität des Saarlandes

6600 S a a r b r ü c k e n

Prof. Dr. W. J. Paul

Institut für Informatik
Universität des Saarlandes
Bau 36

6600 S a a r b r ü c k e n

Dr. F. Meyer auf der Heide

Universität Dortmund
Informatik II
Postfach 500500

4600 D o r t m u n d 50

Prof. Dr. Ch. Rackoff

Department of Computer Science
University of Toronto

Toronto, Ontario M5S 1A4

Canada

Prof. Dr. S. Micali

Lab. for Computer Sciences
Mass. Institute of Technology
545 Technology Square

C a m b r i d g e , Mass. 02139
U S A

Prof. Dr. R. Reischuk

Institut für Theoretische
Informatik, T.H. Darmstadt
Alexanderstr. 24

6100 D a r m s t a d t

Dr. A. Möbus

Universität Düsseldorf
Mathematisches Institut
Universitätsstr. 1

4000 D ü s s e l d o r f 1

Dr. L. Rónyai

Computer and Automation Inst.
Hungarian Academy of Sciences
P.O.B. 63

H-1502 B u d a p e s t
Ungarn

Prof. Dr. C. P. Schnorr

Fachbereich Mathematik
Universität Frankfurt
Postfach 11 19 32

6000 F r a n k f u r t / M.

Prof. Dr. V. Strassen

Institut für Angew. Mathematik
Universität Zürich
Rämistr. 74

CH-8001 Z ü r i c h
Schweiz

Prof. Dr. A. Schönhage

Universität Tübingen
Mathematisches Institut
Auf der Morgenstelle 10

7400 T ü b i n g e n 1

Prof. Dr. K. W. Wagner

Institut für Math./Informatik
Universität Augsburg
Memminger Str. 6

8900 A u g s b u r g

Prof. Dr. U. Schöning

E W H Koblenz
-Informatik-
Rheinau 3-4

5400 K o b l e n z

Prof. Dr. I. Wegener

FB 20 - Angewandte Informatik
Johann-Wolfgang-Goethe-Univ.
Postfach 11 19 32

6000 F r a n k f u r t/M. 11

Prof. A. Shamir

Applied Mathematics Department
The Weizmann Institute of Sc.

R e h o v o t 76100

Israel

Prof. A. Wigderson

Institute for Mathematics and
Computer Science
The Hebrew University
Givat Ram

J e r u s a l e m / Israel

Prof. Dr. H. J. Stoß

Fakultät für Mathematik
Universität Konstanz
Postfach 5560

7750 K o n s t a n z

Gefördert durch
DFG Deutsche Forschungsgemeinschaft