MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

T a g u n g s b e r i c h t 47/1981

Complexity Theory

1.11. bis 7.11.1981

The 5th Oberwolfach Conference on Complexity Theory was organized as before by C.P. Schnorr (Frankfurt), A. Schönhage (Tübingen), and V. Straßen (Zürich). The 42 participants came from 9 countries, 13 participants came from North America, USSR, and Israel.

37 lectures were given at the conference covering a large area of complexity theory. They dealt with subjects of algebraical, numerical, number theoretical and geometrical nature such as complexity of evaluation and multiplication of polynomials, complexity of different bilinear problems, approximative and exact tensorrank, tensorrank of finite dimensional algebras, fast matrix multiplication, complexity of gcd-computations in sequential and parallel models, complexity of algebraic decision problems in polynomial rings and group theory, fast algorithms constructing generators of permutation groups, primality testing, fast Fourier transformation, and quadratic reciprocity law, decomposition of real n-space in semi-algebraical sets, complexity of sets of homographies and affine linear transformations in the complex plane. Other lectures were given on complexity of Boolean functions, Turing complexity (from the point of view of time and space), general parallel computing and programming, VLSI computing and programming, complexity of graph theoretical decision problems and graph matching, cryptology, and skillful use of memories and information exchange.

C. P. Schnorr

Participants

Atkinson, M.,Cardiff
Auslander, L., New York
Bini, D., Pisa
Blum, N., Saarbrücken
Van Emde Boas, P., Amsterdam
Borodin, A., Toronto
Collins, E., Madison
Cook, St., Toronto
Fürer, M., Tübingen
Galil, Z., Tel-Aviv
Gathen von zur, J., Toronto
Groote de, H.F., Frankfurt
Heintz, J., Frankfurt
Hotz, G., Saarbrücken
Knuth, D., Stanford
Koller, A., München
Ladner, R., Seattle
Lautemann, C., Berlin
Leeuwen van, J., Utrecht
Lengauer, Th., Saarbrücken
Lenstra Jr., H.W., Amsterdam
Loos, R., Karlsruhe
Lickteig, Th., Konstanz
Luks, E.M., Lewisbury
Mayr, E., Stanford
Mehlhorn, K., Saarbrücken
Monien, B., Paderborn
Pan, V., Albany
Paterson, M., Coventry
Paul, W., Bielefeld
Scarpellini, B., Basel
Schnorr, C.P., Frankfurt
Schönhage, A., Tübingen
Shamir, A., Rehovot
Slisenko, A., Leningrad
Specker, E., Zürich
Stoß, H.J., Konstanz
Straßen, V., Zürich
Valiant, L., Edinburgh
Volger, H., Tübingen
Wegener, I., Frankfurt
Winograd, S., Yorktown Heights

Vortragsauszüge

A. ALDER : Border rank

The border rank $\underline{R}(t)$ of a tensor $t \in k^n \otimes k^n \otimes k^n$ is the minimum r such that there exists a decomposition
$\sum_{\rho=1}^{r} u_\rho(\varepsilon) \otimes v_\rho(\varepsilon) \otimes w_\rho(\varepsilon) = \varepsilon^h \cdot t + O(\varepsilon^{h+1})$, where $h \geq 0$, and
$u_\rho(\varepsilon) = u_{\rho 0} + u_{\rho 1} \cdot \varepsilon + \ldots + u_{\rho h} \cdot \varepsilon^h$, $u_{\rho\alpha} \in k^n$, etc.

If k is algebraically closed, there is another possible definition of border rank : The topological border rank $R_{top}(t)$ of a tensor t is the minimum r such that t is in the closure of the set of tensors of rank $\leq r$. The following theorem holds :
Let k be algebraically closed. Then $\underline{R} = R_{top}$.

M.D. ATKINSON : Affine and projective equivalence of sets of complex numbers

Let S and T be two sets of complex numbers each of size n. An algorithm is given for finding, in time $n \log n$, all the mappings $z \mapsto az + b$ which map S onto T. The algorithm extends to finding, in time $n^2 \log n$, all the mappings $z \mapsto (az+b)/(cz+d)$ which map S onto T. The methods use geometrical properties of the Argand diagram and reduce the problem to one of finding a "pattern" of length n within a "text" of length $2n-1$. Finally some preliminary work is described on a similar problem involving rigid movements in real 3-dimensional space.

L. AUSLANDER : Fourier transforms and Gauss sums

Using ideas motivated from fast algorithms for the finite Fourier transforms in p points, p a prime, $F(p)$, we introduce a matrix A such that $A\,F(p)\,A^{-1}$ has entries that are linear Gauss sums. The properties of $A\,F(p)\,A^{-1}$ can be used to establish many results centering about quadratic reciprocity.

D. BINI : A note on commutativity and approximation

The action of commutativity and approximation is investigated for certain problems in Computational Complexity. Some lower bound criteria are formulated in terms of border rank (brk) and commutative border rank (cbrk) of a tensor. Some applications are shown. We obtain in particular $cbrk\langle nm1\rangle \geq (nm+m)/2$, $cbrk\langle 222\rangle \geq 5$, $brk\langle 222\rangle \geq 6$, where $\langle nmp\rangle$ denotes the tensor associated to $(n\times m)\times(m\times p)$ matrix multiplication. For what concerns upper bounds we have $cbrk\langle 222\rangle \leq 6$, $cbrk\langle nm1\rangle \leq (nm+m)/2$ (even m), that is $(nm+m)/2$ non-scalar multiplications are needed and suffice to approximate the $n\times m$ matrix - vector product. As an immediate consequence we obtain that $n/2+2$ non-scalar multiplications and $2n$ additions (or alternatively $n/2+3$ multiplications and $2n+(n+10n)k/8$ additions, where the error is proportional to 2^{-k}) suffice to approximate any polynomial of degree n at a point. The function $f_{cb}(nmp) = 3(\log cbrk\langle nmp\rangle)/\log nmp$, which allows to compare algorithms for different size matrix multiplications, is considered. We have $\theta = \inf f_{cb}(nmp) \leq \lim f_{cb}(nnn) = \omega$ and $\theta \leq 2.32..$ Conditions under which $\theta = \omega$ are examinated.

N. BLUM : On the power of chain rules in context free grammars

It is well known that for each context free grammar G there exists a context free grammar G' with :

(1) $L(G) = L(G')$

(2) G' is chain rule free .

This is done constructively by an algorithm. This algorithm works squaring the size of the grammar. But it is not clear whether chain rules really help. We prove this. More exactly, we construct for all $n \in \mathbb{N}$ a context free language L_n with :

(1) there exists a context free grammar G_n (with chain rules) with $L(G_n) = L_n$ and $|G_n| = O(n)$

(2) for all chain rule free context free grammars G'_n with $L(G'_n) = L_n$ holds : $|G'_n| = \Omega(n \log\log n)$.

A. BORODIN : Merging, sorting, and routing on parallel models of computation

We give an overview of several models of parallel computation, distinguishing two major classes - fixed connection machines (e.g. n-dim cube, cube connected cycles, shuffle exchange) and shared memory models (e.g. PRAC, PRAM, WRAM). The paradigm problem for fixed connection machines is the rooting problem which is important in a variety of contexts including the complexity relating the shared memory models with fixed connection machines. For all known (small degree) fixed connection machines the best known strategy (det.) is $O(\log^2 n)$ based on Batcher's sort. Even though simple strategies are asymptotically optimal (i.e. $O(\log^2 n)$) when we consider "average case" or Monte Carlo analysis, we show that $\sqrt{n/d^{3/2}}$ is a worst case lower bound for any "oblivious" strategy (i.e. where the route is determined by the origin and destination pairs). With regard to shared memory models, we show that $\log\log n - \log\log r$ is asymptotically optimal for merging two sorted n-lists using rn processors, by implementing Valiant's algorithm and deriving a corresponding lower bound.

(Work done jointly with J. Hopcroft.)

B. BUCHBERGER : An upper bound for constructing Groebner-bases (bivariate case)

Groebner-bases are a special kind of bases for polynomial ideals. Many constructive problems in polynomial ideal theory are easy for Groebner-bases whereas they are extremely complex in general. We present an algorithm for computing Groebner-bases and analyze its complexity for the bivariate case. Roughly, the bound for the time complexity is $2\cdot(L+27D^2)^4$, where L is the number of polynomials in the given basis and D is the maximum degree of these polynomials. The maximum degree of polynomials in the resulting Groebner-basis is $M+W$, where M is the maximum degree of lcm of the leading monoms in the given polynomials, and W is the "width" of the polynomials.

G.E. COLLINS : Recent advances in cylindrical algebraic decompositions

Cylindrical Algebraic Decomposition (CAD) is the essential ingredient of the quantifier elimination method for real closed fields presented in the 1975 paper of Collins. CADs also have other applications, including solution of polynomial equation and inequality systems. Arnon, Collins and McCallum (1981) have, at least for r (the number of variables) $\leqq 3$, augmented CAD calculation with adjacency calculations to "cluster" CADs and obtain geometric descriptions of semi-algebraic sets. Such clustering furthermore economizes CAD calculations by reducing the number of calls and avoiding some difficult algebraic number calculations. Collins and McCallum are currently investigating the possibilities to reduce the CAD projections by omitting some subresultants, and have already obtained such a result for $r = 3$.

P. VAN EMDE BOAS : The weakness of two cryptosystems based upon polynomial interpolation

Contemporary complexity based cryptosystems involve encryption algorithms with the property that both encryption and decryption are easy, provided the necessary keys are known. Knowledge of only the algorithm involved, or even, in case of a public key system, the encryption key, does not prevent the decryption problem to be intractable.
Since we have very little methods for proving some (non-artificial) problem to be complex, it is no wonder that systems proposed in the literature are only made plausible by incomplete arguments: "The authors see no way to do it." As a consequence these systems may be shown to be breakable afterwards. In our talk we show that the systems recently proposed by Luccio & Mazzone (IPL 10 (80) 180-183) and Denning & Schneider (IPL 12 (81) 23-25) can be broken. For the first system this had been shown before by H. Meijer (IPL 12(81) 179-181) and M. Hellman (IPL 12(81) 182-183) , but the system is actually even weaker than is indicated by these published attacks.

(The report is based upon joint work with A.E. Brouwer and P. Hogendoorn.)

M. FÜRER : The tight deterministic time hierarchy

Let k be a constant ≥ 2, and let us consider only deterministic k-tape Turing machines.
We assume $t_2(n) > n$ and $t_2(n)$ is computable in time $O(t_2(n))$. Then there is a language which is accepted in time $t_2(n)$, but not accepted in any time $t_1(n)$ with $t_1(n) = o(t_2(n))$. This improves Paul's result ($t_1(n) \log^* t_1(n) = o(t_2(n))$ is sufficient).
Furthermore, a set of functions δ_q, $q \in \mathbb{Q}$ (η hierarchy) is defined with the properties :

(1) $\delta_p(n) = o(\delta_q(n))$ for $p < q$ and
(2) there is a language accepted in space $s(n)$ and time $s(n)\delta_q(n)$, but not in space $s(n)$ and time $s(n)\delta_p(n)$ for any $p < q$.

Z. GALIL : An $O(EV \log V)$ algorithm for finding maximal weighted matching in general graphs

The problem of max-weighted-matching is the following: Given a (not necessarily bipartite) graph with weights on the edges, find a matching (a subset of the edges no two of which share a vertex) of maximal weight.
We show a way to implement Edmonds algorithm for solving the problem in time $O(EV \log V)$. Previous implementations yielded an $O(V^4)$ algorithm (by Edmonds) and $O(V^3)$ algorithms (by Lawler and by Gabow).

(The research reported was done together with S. Micali.)

J. v.z. GATHEN : Fast parallel gcd algorithms

We give algorithms for computing the determinant, characteristic polynomial, and inverse (if existing) of an $n \times n$-matrix in parallel time $O(\log^2 n)$, using a polynomial number of processors (model PRAM with usual arithmetic). These algorithms work over any field, in particular finite ones, in contrast to Csanky's previous result requiring characteristic zero. Ibarra-Moran-Rosher have an algorithm for the rank of real matrices of the same cost as above. From this one gets a fast parallel algorithm to compute the gcd of two real polynomials.

(Work done jointly with A. Borodin and J. Hopcroft.)

H.F. DE GROOTE : Algebras of minimal rank

All algebras considered here are finite-dimensional over a field k. The rank of a k-algebra A, denoted by rk(A), is the minimal R such that there exist $u_1,..,u_R, v_1,..,v_R \in A^*$ and $w_1,..,w_R \in A$ such that for all $x,y \in A$

$$xy = \sum_{\rho=1}^{R} u_\rho(x)\, v_\rho(y)\, w_\rho$$

holds. In the 1979 complexity meeting V. Strassen presented a general lower bound for the rank of algebras (actually for the complexity):

Theorem (A. Alder and V. Strassen, TCS 1980)
Let A be a k-algebra, then $rk(A) \geq 2 \dim A - \sharp M(A)$, where M(A) denotes the set of maximal ideals of A.

Definition A is an algebra of minimal rank, if $rk(A) = 2\dim A - \sharp M(A)$.

We determine the structure of algebras of minimal rank for two classes of algebras

(1) Division algebras

Theorem 1 Every division algebra A over k of minimal rank is a simple field extension of k.

Corollary If A is a non-commutative division algebra, then $rk(A) \geq 2 \dim A$.

(2) Commutative algebras (joint work with J. Heintz Univ. Frankfurt)

Theorem 2 Let A be a local k-algebra with maximal ideal m such that $A/m \cong k$ and $\sharp k \geq 2 \dim A - 2$. Then A is of minimal rank if and only if m is a sum of pairwise orthogonal principal ideals.

Corollary Let A be a commutative algebra over an algebraically closed field k. Then A is of minimal rank if and only if the radical of A is a sum of pairwise orthogonal principal ideals.

Remark If k is any perfect field, then the condition for m in Theorem 2 is still necessary, but no longer sufficient :
Let $N(\omega_1,\omega_2)$ the null-algebra of dimension 3 over $\mathbb{Q}$. Then the maximal ideal of $A = \mathbb{Q}(i) \otimes_{\mathbb{Q}} N(\omega_1,\omega_2)$ still satisfies the condition of Theorem 2, but $rk(A) > 2 \dim A - 1$.

Note (11. 11. 81) Meanwhile we could prove the following

Theorem Let k be a perfect field and A a local k-algebra with maximal ideal m and residue class field K:= A/m. If $\sharp k \geq 2\dim_k A - 2$ and $\dim_k K > 1$, then A is of minimal rank if and only if m is a principal ideal.

Therefore for perfect groundfields the classification problem of commutative algebras of minimal rank is completely solved.

J. HEINTZ : Upper bounds to decide absolute irreducibility of polynomials

Let k_o be a field, k an algebraical closed extension of k_o. Let $X_1,\dots,X_n$ be indeterminates over k. Absolute irreducibility (i.e. irreducibility over k) of a polynomial $F \in k_o[X_1,\dots,X_n]$ with $\deg F = d$ is decidable in time

$$C\, n^d\, 2^{c\, d^5} \qquad \text{randomly}$$

and

$$C\, 2^{c(d^6 + n^2 d^3)} \qquad \text{deterministically},$$

where arithmetic operations in k_o are counted ($C, c > 0$ suitable constants).

Consequences : Let $F_1,\dots,F_s \in k_o[X_1,\dots,X_n]$, $d = \sum_{i=1}^{s} \deg F_i$.

(1) Irreducibility of $C = \{x \in k^n;\ F_1(x) = 0, \dots, F_s(x) = 0\}$ is decidable in time $\leq 2^{d^{c n^2}}$.

(2) The property "$(F_1,\dots,F_s) \subset k[X_1,\dots,X_n]$ is prime and C is smooth" is decidable in time $d^{2^{2^{c n^2}}} + 2^{d^{c n^2}}$.

These bounds, although unsatisfactory for practical purposes, are some exponentiations better than those obtained in a straight forward manner by quantifier elimination.

(Work jointly done with M. Sieveking.)

G. HOTZ : Ein Darstellungssatz von Algebren

Seien X_l und X_r nicht leere Mengen, $X = X_l \cup X_r$, $X_l \cap X_r \neq \emptyset$. Eine Multiplikationstafel δ :

$$x \cdot y = \sum_{z \in X} \alpha^{z}_{x,y} \cdot z \quad \text{für } x \in X_l,\ y \in X_r,\ \alpha^{z}_{x,y} \in R,\ R \text{ Semiring}$$

definiert eine assoziative Algebra unendlicher Dimension über R. Für diese Algebra $A_R(\delta)$ wird eine nicht triviale Darstellung im Semiring $R\langle\langle \{x_1,x_2\}^{(*)} \rangle\rangle$ angegeben. Hierin ist $\{x_1,x_2\}^{(*)}$ das Monoid, das sich aus dem freien Monoid $\{x_1^{\pm 1}, x_2^{\pm 1}\}^*$ durch Faktorisieren nach den Relationen $x_1 x_1^{-1} = x_2 x_2^{-1} = 1$, $x_1 x_2^{-1} = x_2 x_1^{-1} = 0$ ergibt. Dieser Semiring ist auch in dem Sinne universell, daß er für jede endlich dimensionale Algebra über R mit 1-Element eine treue Darstellung zuläßt.

Nun kann man jeder kontext freien Grammatik G in einfacher Weise eine solche Algebra $A_R(G)$ zuordnen. Der Darstellungssatz liefert in sehr einfacher Weise die Sätze von Chomsky - Schützenberger, Shamir und den Satz über die schwerste kontext freie Sprache von Greibach. Weiter erlaubt $A_R(G)$ eine einfache Charakterisierung der LR(k) Grammatiken und einen Zusammenhang mit unserer Darstellung der Konstruktion eines Akzeptors für die zugehörigen Sprachen. Die Darstellung liefert unmittelbar eine Grammatik $\tilde{G}$ in Greibach Normalform mit $L(G) = L(\tilde{G})$ und

$$|\tilde{G}| = 32\,|P_N| \cdot |P_T| \cdot |Y|$$

mit P_N nonterminalen Produkten, P_T terminalen Produkten, Y Alphabet von G (nonterminal).

D. KNUTH : Permutation groups with generators

An algorithm is presented for determining the group generated by permutations $\Pi_1,\ldots,\Pi_m$ of $\{1,\ldots,n\}$. By formulating this algorithm properly the proof of correctness becomes quite simple, and it is shown that the running time in the worst case is $O(n^5 \log\log n + mn^2)$,

R.E. LADNER : Parallel algorithms for linear recurrences

The computation of $\{x_i ; 1 \leq i \leq N\}$ for the recurrence $x_i = \sum_{j=1}^{m} a_{ij} x_{i-j} + b_i$ can be done in parallel time $O(\log m \log N)$ using $O(m^2 N)$ operations in a semiring and $O(m^{d-1} N)$ in a ring (where matrix multiplication of $m \times m$-matrices can be done in time $O(m^\alpha)$). The proof is an application of the parallel prefix problem together with some valuable suggestions of Z. Galil and M. Paterson.
(joint work with A.G. Greenberg)

J. VAN LEEUWEN : VLSI layouts for perfect binary trees

Use Thompson's model of a chip surface. Let T_k $(k \geq 0)$ be the perfect (complete) binary tree of depth k, with $n = 2^k$ leaves. It is wellknown that T_k (having $2n-1$ nodes) has an embedding requiring only $O(n)$ area. The H-pattern construction due to Mead and Rem actually achieves a bound of $4n$. Our presentation aims at finding best possible embeddings.

Let $A_{opt}(k)$ be the smallest number of grid-cells required for an embedding of T_k.

Theorem. $A_{opt}(k)/2k$ converges for $k \to \infty$.

Let the limit be γ. We prove that $2.03 < \gamma < 2.743055$.

The upper bound derives from (i) an embedding of T_{12} in a 105×106 rectangle that has a free cell in every corner and (ii) the use of an "efficient" induction pattern (less wasteful than the H-pattern) to construct embeddings for T_k's with $k > 12$.

There exist area $O(n)$ embeddings of T_k with short side (of the bounding rectangle) as small as $O(\log n)$. But the following can be shown. Let the aspect ratio of an embedding be defined as

length short side / length long side.

Theorem. There exists a layout of the T_k that is asymptotically optimal and has aspect ratio converging to 1, for $k \to \infty$.

(Work done jointly with M.H. Overmars and D. Wood.)

T. LENGAUER: On the complexity of VLSI computations

We present four results on the complexity of VLSI computations:

(1) We justify the Boolean circuit model by showing that it is able to model multi-directional VLSI devices (e.g. pass transistors, pre-charged bus-drivers).

(2) We prove a general cut theorem for compact regions in $\mathbb{R}^d$ ($d \geq 2$) that allows us to drop the convexity assumption in lower bound proofs based on the crossing sequence argument.

(3) We exhibit an $\Omega(n^{1/3})$ asymptotically tight lower bound on the area of strongly where-oblivious chips for transitive functions.

(4) We prove a lower bound on the switching energy needed for computing transitive functions.

H.W. LENSTRA, JR.: Recent advances in primality testing

We discuss the primality testing algorithm that was recently proposed by Adleman and Rumely; its relation to older tests; and its theoretical implications.

T. LICKTEIG : On typical tensor rank

The typical rank R of tensors in a tensor product space $U \otimes V \otimes W$ over algebraically closed fields is studied. R is equal to the common rank of tensors in some nonempty Zariski - open subset of $U \otimes V \otimes W$ or the maximum border rank respectively. In order to get a deeper insight in the set V_r of tensors with rank $\leq r$, it is necessary to know its dimension, determined in some important cases of tensor product spaces. The presented results are the following :

(1) A quite sharp upper bound on the typical rank R is obtained: If $\dim U = n$, $\dim V = m$, and $\dim W = \ell$ $(2 \leq n \leq m \leq \ell)$, then

$$\left\lceil \frac{n \cdot m \cdot \ell}{n+m+\ell-2} \right\rceil \leq R \leq \left\lceil \frac{n \cdot m \cdot \ell}{n+m+\ell-2} \right\rceil_{\ell/2}$$

(For $k \in \mathbb{Z}$: $\lceil x \rceil_k = \min \{ y \in k\mathbb{Z} : y \geq x \}$).

(2) In the case $\dim U = \dim V = \dim W = n \in \mathbb{N}$:

For $n \neq 3$: $\dim V_r = \min \{ r(3n-2), n^3 \}$, $R = \left\lceil \frac{n^3}{3n-2} \right\rceil$.

For $n = 3$: $\dim V_r = 7r$ $(r \leq 3)$, $\operatorname{codim} V_4 = 1$, $R = 5$.

R. LOOS : Subresultant chains

Based on theorems of Habicht we derive an $O(n^2 M(L(nd)))$ algorithm for computing the subresultant chain of two polynomials of maximal degree n and maximal seminorm d, where $M(b)$ is the time to compute two b-bit numbers and $L(a)$ is the number of bits of a. The algorithm can be specialized to the Brown - Collins subresultant gcd algorithm (Knuth 4.6.1,2^{nd}). We suggest to replace in the Lehmer - Knuth - Schönhage gcd algorithm the remainder operation over a field k by the exact division operations over an integral domain of Habicht's Theorem. Both, modular and non - modular polynomial remainder algorithms can be improved in this way.

E.M. LUKS : The complexity of permutation group computations

The algebraic nature of recent breakthroughs in graph isomorphism testing motivates a study of the computational complexity of various permutation group problems. In particular, the isomorphism problem is polynomial - time reducible to the problem of finding generators for the subgroup of a given permutation group (itself specified only by generators) which stabilizes a specified subset.

Although apparently efficient algorithms are known for the latter problem, none has been shown to be subexponential in the worst case. We observe that the subset stabilizer problem is actually polynomial-time equivalent to a large number of other classical problems of computational group theory; among these are finding generators for the intersection of two given permutation groups, testing conjugacy within a given group, and finding the centralizer of a subgroup. We describe some special cases where polynomial - time solutions are known. Some 'slight' variations of these problems are NP - complete.

E. MAYR : Well structured parallel programs are not easier to schedule

The scheduling problem for unit time task systems with arbitrary precedence constraints is known to be NP - complete. We show that the same is true even if the precedence constraints are restricted to certain subclasses which make the corresponding parallel programs more structured. Among these classes are those derived from hierarchic cobegin - coend programming constructs, level graph forests, and the parallel or serial composition of an out-tree and an in-tree. In each case, the completeness proof depends heavily on the number of processors being part of the problem instances.

K. MEHLHORN : On the complexity of distributive computing, with an application to VLSI

Let X and Y be sets, and let $f : X \times Y \to \{0,1\}$ be a boolean function. Let $x \in X$ and $y \in Y$ be known to persons P_1 and P_2 respectively. For P_1 and P_2 to determine cooperatively the value $f(x,y)$, they send information to each other. We will prove the following lower bound on the number of bits exchanged in any deterministic algorithm. $C_{det}(f) \geq \log \operatorname{rank}_k f$, for all fields k, where $\operatorname{rank}_k f$ is the rank of the $|X|$ by $|Y|$ 0-1 - matrix $(f(x,y))_{x \in X, y \in Y}$ over the field k. The method is strong enough to distinguish nondeterministic and deterministic algorithms, more precisely we exhibit an f such that $C_{ndet}(f)$, $C_{ndet}(\bar{f}) \ll C_{det}(f)$.
The method can be used to obtain lower bounds on the complexity of deterministic VLSI computations.

(Joint work with E.M. Schmidt, Aarhus)

V. PAN : The arithmetic and logical complexity of some arithmetic computational problems

The time - complexity of algorithms for arithmetic computational problems such as DFT, convolution of vectors (CV), matrix multiplication (MM) can be measured by the numbers A and B of respectively arithmetic operations and bit - operations involved in the algorithms. B/A characterizes the stability of the algorithms. It is proved that any algorithm for MM can be stabilized so that asymptotically A and B have roughly the same order of their growth. The efficiency of algorithms can be also characterized by the simplicity (or by the complexity) of their structure. A new quantity, S, is introduced in order to measure the synchronicity (asynchronicity) of linear and bilinear computational schemes. S is defined in terms of the properties of the digraph associated with the scheme. It is proved that

$S \geq n \log_2 n - C(\pm)$ for any algorithm for DFT and CV ,

$S \geq n^2 \log_2 n - C(\pm)$ for any algorithm for MM, where $C(\pm)$ is the number of additions/subtractions used in the algorithm.

M. PATERSON : Dealing and bidding for secret messages

In a formal analogue of "bidding", as in the game of Bridge, a set of distinct cards is distributed randomly among several players. Next, a sequence of bids, i.e. statements about their own heads, is made by the players according to a given protocol or convention. Circumstances are demonstrated in which any two of the players may exchange information, provably secret from even a coalition of all the other players, by means of a sequence of open bids according to the fixed convention.

In formulating bids it is helpful for players to have access to a randomizing device such as dice. Such a convention is a probabilistic protocol. It is shown that at least one bit of secret information can always be exchanged provided the numbers a,b,c of cards of the two partners and their opposition respectively, satisfy

either I) $a + b \geq c + 2$, $a \geq 1$, $b \geq 1$ (with an easy protocol)

or II) $a = b = n/p$, $c = (1 - 2/p)n$, where $n \geq p^{O(\log p)}$ (with a more involved recursive protocol).

An OPEN PROBLEM is to show that $\forall a,b\ \exists c$ such that no secret information can be guaranteed to be exchanged. Even for $a = b = 2$, this is open.
A deterministic protocol is one without probabilistic bids. It seems much harder to exchange secrets in this case. We have one successful protocol for $a = b = 3$, $c = 1$, but as yet nothing even for the case $c = 2$.

W. PAUL : On heads versus tapes

2-dimensional 2-tape Turing machines cannot simulate 2-dimensional 2-head machines in real time.

C.P. SCHNORR : Constructing the automorphism group $Aut_e(X)$ for trivalent graphs in time $O(n^3 \log n)$

We consider the following group theoretic algorithmic problem which lies at the bottom of the recent polynomial time algorithms for constructing the automorphism group of graphs with bounded valence by Luks. Given a group $G \subset Sym(A)$, A a colored set, $\sigma \in Sym(A)$, construct $C_A(G) := \{\sigma \in G ; \sigma \text{ color preserving}\}$. We introduce some efficiencies into the previous solution for this problem which are particularly valuable in the case that only a few elements of A are colored. The new method is exemplified in the Luks algorithm for constructing the group $Aut_e(X)$ of automorphisms of a trivalent graph X which keep the edge e fixed. The improved algorithm constructs $Aut_e(X)$ for trivalent graphs with n edges in time $O(n^3 \log n)$. The obvious way to apply this to testing graph isomorphisms of trivalent graphs and to constructing the full automorphism group Aut(X) of trivalent graphs yield $O(n^4 \log n)$ - time algorithms.

(Joint work with A. Weber, Frankfurt)

A. SCHÖNHAGE : How to multiply polynomials numerically

In the algebraic model multiplication of polynomials of degree $\leq n$ is possible in $O(n \log n)$ arithmetic operations. For numbers of length ℓ - or with relative accuracy $2^{-\ell}$, respectively - each arithmetic step is possible in $O(\ell)$, at least for pointer machines (= successor RAM = SMM); otherwise an extra factor of $\log \ell \cdot \log\log \ell$ comes in. Here a new method is presented for multiplying n-th degree polynomials with complex coefficients of binary length $\ell \geq \log n$ (and bounded by 1) which requires only linear time $O(n\ell)$, or $O(n\ell \cdot \log(n\ell) \cdot \log\log(n\ell))$, respectively. Similarly, Fourier transform of size N with accuracy $2^{-\ell}$ is possible in $O(N\ell)$, division of polynomials in $O(n\ell + n^2)$, interpolation etc. in $O(n\ell \cdot \log(n\ell))$.

A. SHAMIR : Efficient codes for write-once memories

Many storage media, such as video discs, PROMs, or paper tapes, are "write-once" in the sense that each of its memory positions is initially fabricated in a "0" state that may be irreversibly transformed into a "1" state when written. Nonetheless, we shall demonstrate that such storage media are capable of being "updated" to a surprising degree. For example, only 3 bits of memory are needed to represent any 2-bit value in such a way that we can later "update" the memory to represent any other 2-bit value.

A.O. SLISENKO : The complexity of the Hamiltonian circuit problem for context free graphs

We consider context free graph grammars (CFGG) with rules which preserve boundaries, i.e. a rule permits to replace a node with all the incident edges by a graph with the same amount of boundary edges. For any CFGG Γ there is a polynomial-time algorithm for recognizing the language $L(\Gamma)$ generated by Γ and for parsing graphs in $L(\Gamma)$.

Theorem. For any CFGG Γ the Hamiltonian circuit problem for graphs in $L(\Gamma)$ has polynomial-time complexity.

H.J. STOSS : Simulation of multihead Turing machines by multitape machines

W. Paul showed that it is impossible for $d \geq 2$ to simulate a Turing machine with k heads on one d-dimensional tape by a Turing machine with several d-dimensional tapes one head each in real-time without increasing the number of heads. It's also known that all Turing machines with k heads on 1-dimensional tapes can be simulated by each other in linear time.

We have the following results :

Theorem 1 Turing machines with a fixed number k of heads on 2-dimensional tapes can be simulated by each other in linear time.

Theorem 2 A Turing machine with k heads on one d-dimensional tape with $d \geq 3$ can be simulated

- by a machine with k d-dimensional tapes one head each in time $O(d \lg^* k)$
- by a machine with k d-dimensional tapes one head each and one additional 1-dimensional tape with 1 head in linear time.

(Joint work with W. Schnitzlein)

V. STRASSEN : Computing derivatives

Let k be an infinite field, $f \in k(x_1, \ldots, x_n)$. For the nonscalar complexity L we prove

$$L(f, \frac{\partial}{\partial x_1} f, \ldots, \frac{\partial}{\partial x_n} f) \leq 3\, L(f) .$$

In combination with the degree method this yields nonlinear bounds for single functions.

(Joint work with W. Baur, Zürich)

L.G. VALIANT : Computing polynomials in parallel using few processors

Consider any homogeneous straight line program of complexity C with operations from $\{+,-,\cdot\}$ that computes a polynomial of degree d in i indeterminates. We show that there is another program that computes the same polynomial in parallel time $O((\log C)(\log d))$ and performs only $O(C^3)$ operations in total. The result can be applied to monotone arithmetic programs and hence monotone Boolean circuits. Ruzzo's simultaneous resource bound for context free recognition follows as a corollary.

(Work done jointly with S. Skynm, S. Berkowitz, C. Rackoff.)

I. WEGENER : The monotone complexity of Boolean functions

For a monotone Boolean function f the monotone complexity is the minimal number of gates in each network for f consisting only of $\wedge$ - and $\vee$ - gates. We discuss the known methods for the proof of lower bounds on this complexity measure: graph theoretical methods, elimination method (together with the pigeon-hole - principle), replacement method and the assumption that certain functions are given for free. Then we introduce the method of defining value functions to measure the value of each gate for each part of the function we like to compute. This method yields an $n^2/\log n$ - lower bound which is the largest known bound for explicitly defined monotone Boolean functions. Afterwards we discuss how to use this new method to obtain partial results on the problem of determining the monotone complexity of the disjunction of f and g if f and g have no variable in common.

S. WINOGRAD : On the asymptotic complexity of matrix multiplication

The main result reported in this talk is that for every algorithm for computing (or λ - computing) the product of matrices there exists another algorithm which yields a better bound for the exponent of matrix multiplication. In other words, the exponent is a limit point. Using the proof of this result, which is constructive, one obtains that the exponent is smaller than 2.4956 .

Berichterstatter: J. Heintz

Adressen der Tagungsteilnehmer

Dr. M. Atkinson
Department of Comp. Mathemati cs
University College
C
Cardiff, Wales, G.B.

Dr. St. Cook
Department of Computer Science
Universität v. Toronto

Toronto M5S 1A7
CANADA

Dr. L Auslander
Department of Mathematics
U.U. N.Y.
33 W 42 St
N.Y. 10036 USA

Dr. Martin Fürer
Universität Tübingen
FB Mathematik

7400 Tübingen
Auf der Morgenstelle

Dr. Dario Bini
Istituto Matematico
Universita

IT 56100 Pisa, Italen

Dr. Zvi Galil
School of Mathematical Sciences
Tel-Aviv University
Tel - Aviv, Israel

Prof. Dr. Norbert Blum
FB 10
Universität des Saarlandes
6600 Saarbrücken

Dr. Joachim von zur Gathen
Department of Computer Science
University of Toronto

Toronto MS5 1A7
CANADA

Dr. Peter Van Emde Boas
ITW/VPW
Universität Amsterdam

Roeterstraat 15
NL 1018 WB Amsterdam
Niederlande

Herrn Prof. Dr. H.F. de Groote
FB Mathematik
Universität Frankfurt
6000 Frankfurt
Postf. 11 19 32

Dr. Allan Borodin
Department of Computer Science
University of Toronto
Toronto M5S 1A7
CANADA

Herrn Joos Heintz
FB Mathematik
Universität Frankfurt a.M.
Postfach 11 19 32
6000 Frankfurt

Dr. E. George Collins
Computer Science Department
University of Wisconsin
Madison, Wisconsin 537o6
USA

Prof. Dr. G. Hotz
Angew. Math. u. Informatik
Universität

6600 Saarbrücken

Dr. D. Knuth
Computer Science Department
Stanford University

Stanford, CA 94305
USA

Herrn Thomas Lickteig
Fakultät f. Mathematik
Universität Konstanz
7750 Konstanz

Dr. Alois Koller
Siemens AG, ZT - ZTI

Otto Hahn-Ring 6
8000 München 83

Herrn Prof. Dr. R. Loos
Fachbereich Informatik
Universität Karlsruhe

7500 Karlsruhe

Dr. Richard Ladner
Department of Computer Science
University of Washington

Seattle, Wa. 98195
USA

Dr. Eugene M. Luks
Dept. of Mathematics
Bucknell University
Lewisbury, PA. 17837 USA

Dr. Clemens Lautemann
Inst. f. Software u. Theor.Inf.
TU Berlin FB 20

1000 Berlin 10

Dr. Ernst Mayr
Department of Computer Science
Stanford University

Stanford, CA 94305
USA

Dr. Jan van Leeuwen
Dept. of Computer Science
Universität von Utrecht
P.O.B. 80.002
NL 3508 TA UTRECHT

Prof. Dr. K. Mehlhorn
FB 10
Universität

6600 Saarbrücken

Dr. Thomas Lengauer
Fachbereich 10
Universität des Saarlandes

6600 Saarbrücken

Prof. Dr. B. Monien
FB Mathematik / Informatik
Universität

4790 Paderborn

Dr. H.W. Lenstra, Jr.
Mathematisch Instituut
Universiteit van Amsterdam

Roetersstraat 15
NL 1018 WB AMSTERDAM

Dr. V. Pan
Computer Science Department
SUNY
Albany, N.Y. 12222
USA

Prof. Mike Paterson
Department of Computer Science
University of Warwick
Coventry CV4 7 AL
G.B.

Prof. Dr. E. Specker
ETH HG g. 16

Leonhardstr. 33
CH 8006 Zürich

Prof. Dr. W. Paul
Fakultät für Mathematik
Universität Bielefeld

4800 Bielefeld

Dr. H.J. Stoß
Fakultät f. Mathematik
Universität Konstanz
7750 Konstanz

Dr. Bruno Scarpellini
Mathemat. Institut
Universität Basel

Basel, Schweiz

Prof. Dr. V. Straßen
Universität Zürich (Mathematik)

Freie Straße 36
CH Zürich 8032

Herrn Prof. Dr. C.P. Schnorr
FB Mathematik
Universität Frankfurt a.M.
6000 Frankfurt
Postf. 11 19 32

Prof. L. Valiant
Computer Science Department
Edinburgh University
Kings Buildings

Edinburgh, G.B.

Prof. Dr. A. Schönhage
Mathemat. Institut
Universität Tübingen

7400 Tübingen
Auf der Morgenstelle 10

Dr. Hugo Volger
Math. Institut Tübingen
Universität
7400 Tübingen
Auf der Morgenstelle 10

Prof. A. Shamir
Department of Mathematics
The Weizman Institut of Science

Rehovot, Israel

Herrn Ingo Wegener
FB Informatik
J.W.G. Universität Frankfurt
6000 Frankfurt
Postf. 11 19 32

Dr. Anatol Slisenko
LOMI, Fontanka 27,

Leningrad 191011
USSR

Prof. Shmuel Winograd
IBM Research Center

P.O.B. 218
Yorktown Heights,
N.Y. 10598
USA