MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

T a g u n g s b e r i c h t 44/1979

Complexity Theory

October 21-28, 1979

The fourth Oberwolfach conference on complexity theory has been guided as before by C.P. Schnorr (Frankfurt), A. Schönhage (Tübingen) and V. Strassen (Zürich). The 40 participants came from 9 countries, 10 participants came from North-America.

There were given 34 lectures covering a large area of complexity theory. 17 of them dealt with subjects of algebraic nature including fast matrix multiplication; multiplicative complexity of bilinear forms, of multiplication in algebras and of the Fourier transform; complexity of evaluation, factorization and of testing polynomials. Some more results about solvability of systems of polynomial equations, testing primality of polynomial ideals, optimality of algorithms solving linear equation systems were presented.

Other lectures concerned various general computational models and complexity measures such as Kolmogorov complexity, Crypto-complexity, Boolean complexity, decision trees, iterative arrays, Petri nets, and in particular Turing machine complexity, where time, space (both in the deterministic, nondeterministic and probabilistic model) alternations and tapes have been counted. The specific problems of the lectures dealt with e.g. context-free languages, sorting, searching, text edition, encryption systems, tree layout, graph threadability.

C.P. Schnorr

Participants

M. Atkinson, Cardiff
W. Baur, Zürich
P. van Emde Boas, Amsterdam
E. Börger, Dortmund
A. Borodin Toronto
G.E. Collins, Madison (USA)
S.A. Cook, Toronto
S. Even, Haifa
M.J. Fischer, Seattle (USA)
M. Fürer, Edinburgh
J. von zur Gathen, Zürich
H.F. de Groote, Frankfurt/M.
J. Heintz, Frankfurt/M.
G. Hotz, Saarbrücken
L. Hyafil, Paris
R.E. Ladner, Seattle
J.C. Lafon, Strasbourg
D. Lazard, Poitiers (France)
K. Leeb, Erlangen
R. Loos, Karlsruhe
E.W. Mayr, München
K. Mehlhorn, Saarbrücken
M. Mignotte, Strasbourg
B. Monien, Paderborn
J. Morgenstern, Nice (France)
H. Noltmeier, Aachen
V. Pan, Sunya, Albany (USA)
M.S. Paterson, Coventry
W. Paul, Bielefeld
Ch. Rackoff, Toronto
R. Reischuk, Bielefeld
F. Romani, Pisa
A. Schönhage, Tübingen
C.P. Schnorr, Frankfurt/M.
P. Schuster, Tübingen
H.J. Stoß, Konstanz
V. Strassen, Zürich
I. Hal Sudborough, Paderborn
J.F. Traub, Columbia, N.Y. (USA)
S. Winograd, Yorktown Heights, N.Y. (USA)

Vortragsauszüge

EXACT AND APPROXIMATE COMPUTATION OF BILINEAR FORMS AND APPLICATION TO THE MATRIX MULTIPLICATION PROBLEM

F. Romani, Pisa

An alternative approach to the computation of bilinear forms is presented. A new class of algorithms (APA-algorithms) is introduced.

APA-algorithms allow a reduction of the number of non-scalar multiplications in exchange for an arbitrarily small error in the result and they can be converted into exact ones with small increase of complexity (Bini). The application of this technique to matrix multiplication allowed reducing the upper bounds of the problem (Bini et al., Pan, Schönhage).

Two complexity measures are introduced for matrix multiplication algorithms which take into account the stability properties of algorithms. Namely fixed precision complexity is the number of bit operations needed to get a given accuracy in the result; asymptotic complexity is a finite measure for the "infinite precision" complexity of matrix multiplication.

TRILINEAR AGGREGATING, UNITING AND CANCELLING REVISITED

V. Pan, Albany

At first the problems of matrix multiplication and inversion are reduced to a special decomposition of a certain trilinear form. This generalizes recent analogous reductions done by D. Bini, M. Capavani, G. Lotti, F. Romani, A. Schönhage.

Then the techniques of trilinear aggregating, uniting and cancelling (introduced earlier by the author) are applied to derive an appropriate decomposition of the trilinear form. Although the resulting exponent of the complexity of matrix multiplication and inversion is inferior comparing with one derived very recently by A. Schönhage 1979 (2.6054 vs 2.548) the techniques applied by the author and by A. Schönhage seem to be different and may complement each other to derive better exponents in the future.

PARTIAL AND TOTAL MATRIX MULTIPLICATION

A. Schönhage, Tübingen

By using the notion of approximate rank and observing the fact that favourable patterns of partial matrix multiplication $A \cdot B$ - some of the a's and b's may be zero - can efficiently be utilized to speed up multiplication of large total matrices I recently have found new bounds on the exponent ω for matrix multiplication (Preprint, University of Tübingen, June 1979), for instance $\omega < 2.609$.

Now a further improvement is presented: Multiplying a $(k,1)$-matrix A (i.e. a column vector) with a $(1,n)$-matrix B and, in addition, evaluating a scalar product $U \cdot V$ of length $m=(k-1)(n-1)$ in variables disjoint from those in A and B can be done by an approximate algorithm of length $kn+1$ (which, for $m \geq 2$, is better than the obvious bound $kn+m$). Based upon this the bound $\omega \leq 3\tau$ is derived, where τ is determined as the solution of $(kn)^{\tau}+m^{\tau}=kn+1$. The best value is obtained by $k=n=4$, $m=9$, namely $\omega < 2.548$.

THE EVALUATION OF SEVERAL BILINEAR FORMS

M.D. Atkinson, Cardiff

Methods of computing the rank of an arbitrary $m \times n \times p$ tensor are currently known only for $p=1,2$ and require the theory of canonical forms of matrices. Such a theory does not exist for $p=3,4,\ldots$ and so we concentrate on evaluating $r(m,n,p)$ = highest rank of any $m \times n \times p$ tensor over C. It is possible to prove

$$r(m,n,p) \leq \begin{cases} m + \left\lfloor \frac{1}{2}p \right\rfloor n & \text{if } m < n \\ (\frac{1}{2}p+1)n & \text{if } m \geq n \end{cases}$$

For large values of p rather more precise results can be proved. In particular, if $p=mn-1$, $mn-2$ and a tensor is described by p linearly independent matrices $A_1,\ldots,A_p$, then its exact rank

can be found. For small values of m,n,p one can show the following

$$r(3,3,3) = 5, \quad r(4,4,4) = 8 \text{ or } 9, \quad r(5,5,5) \leq 13$$

together with similar results.

MULTIPLICATIVE COMPLEXITY OF A BILINEAR FORM OVER A COMMUTATIVE RING *)

D.Ju. Grigor'ev, Leningrad

The complexity of a bilinear form with parameters reduces to the complexity of a bilinear form over some commutative ring. Multiplicative complexity $Rg_K A$ of a bilinear form A over a commutative ring K is no less than its rank rgA.

Theorem 1 For every bilinear form A (over a noetherian commutative ring K) the equality $Rg_K A = rgA$ is fulfilled iff $K = K_1 \oplus \ldots \oplus K_n$ where K_i $(1 \leq i \leq n)$ is an integer domain such that
1) global homological dimension of K_i is no greater than 2;
2) every K_i-projective module is free.

A bilinear form A over a polynomial ring $K = F[x_1,..,x_n]$ (F is a field) is free of squares if every coefficient of A is a F-linear form over $x_1,..,x_n$ (note that $F[x_1,x_2]$ satisfies the conditions of theorem 1).

Theorem 2 For free of squares bilinear forms A $(Rg_K A/rgA) < 2$ and $\sup(Rg_K A/rgA) = 2$ (for $n=3$ $\max(Rg_K A/rgA) = 3/2$).

THE MULTIPLICATIVE COMPLEXITY OF A PAIR OF BILINEAR FORMS

P. Schuster, Tübingen

A formula for the rank of a $2 \times m \times n$ tensor is exhibited. It holds over any field that is large enough. This result contains the results of Grigor'ev and Ja'Ja' as special cases. Given the coefficients of the tensor over R, this formula can be evaluated by a number of arithmetic operations growing polynomially in n+m.

*) This lecture was not given at the conference

COMPLEXITY OF ALGEBRAS

V. Strassen, Zürich

A joint result with A. Alder: Let A be a finite dimensional associative algebra of dimension n, L(A) its multiplicative complexity. Then:
$L(A) \geq 2n$-number of maximal ideals of A. This implies almost all known lower bounds for algebras.

MULTIPLICATIVE COMPLEXITY OF FOURIER TRANSFORM

S. Winograd, Yorktown Heights

Let G and $F \supseteq G$ be two fields. Let $P(u) \in G[u]$ be irreducible, and let Π_P be its companion matrix. For every vector $f = (f_o, f_1, .., f_{n-1}) \in F^n$ we assign the matrix $\Pi_{P;f} = \Sigma_{i=o}^{n-1} f_i \Pi_P^i$ where $n = \deg P(u)$. Let $D = D(f_1, f_2, .., f_k; P_1, P_2, .., P_k)$ denote the block diagonal matrix whose i^{th} block is $\Pi_{P_i;f_i}$, $1 \leq i \leq k$. D is an $m \times m$ matrix where $m = \Sigma_{i=1}^k n_i = \Sigma_{i=1}^k \deg P_i(u)$. We are interested in the multiplicative complexity of $DM\underline{y}$, where M is an $m \times 1$ matrix over G and $\underline{y}$ is the vector $\underline{y} = (y_1, y_2, .., y_1)^t$ of 1 indeterminates. Let $\rho: F \to F/G$ be the natural vector space homomorphism. We denote by $\rho(\underline{f})$ the vector $(\rho(f_o), \rho(f_1), .., \rho(f_{n-1}))$ and by $L_G(\rho(\underline{f}))$ the G linear space of the elements of $\rho(\underline{f})$. A special case of the result (which is sufficient for applications to Fourier transform) is:

<u>Theorem:</u> If $|G| \geq \max_i \{2(n_i - 1)\}$ and

1) for each $1 \leq i \leq k$ $\dim L_G(\rho(f_i)) = n_i$

2) for $i \neq j$ either $L_G(\rho(f_i)) \cap L_G(\rho(f_j)) = \{0\}$ or else $\rho(f_i) = \rho(f_j)$ and $P_i = P_j$

then $M_G(D_{\underline{y}}) = 2mk$

Let $\underline{A} = W\underline{a}$ be the Fourier transform over the group $\mathbb{Z}/N_1 \times \mathbb{Z}/N_2 \times \ldots \times \mathbb{Z}/N_s$. There exist two invertible matrices

(over $\mathbb{Q}$) R and S such that W = RDS, where D is a block diagonal matrix with each block a $\Pi_{P;f}$. Whenever $N_1, N_2, .., N_s$ satisfy: "If for a prime number p, $p^2 | N_i$ then $p \nmid N_j$ for every $j \neq i$" the matrix D satisfies the assumptions of the theorem. Therefore one can determine the multiplicative complexity of these Fourier transforms. For example, a corollary of the theorem is that $\mu_Q(FT(2^n)) = 2^{n+1} - n^2 - 3$.

TESTS ON POLYNOMIALS

M. Mignotte, Strasbourg

Given a polynomial $P \in \mathbb{Z}[x_1, .., x_n]$ such that one can compute $P(x_1, .., x_n)$, $(x_1, .., x_n) \in \mathbb{Z}^n$, and which satisfies $\deg(P) \leq d$, $\text{Height}(P) \leq H$, we consider the question <<P = 0?>>.

We show that a suitable choice of $(x_1, .., x_n)$ leads to the answer. We compare this method with "probabilistic" ones and show that the second may fail even on small examples.

SOME APPLICATIONS OF BEZOUT'S THEOREM TO THE COMPLEXITY OF POLYNOMIALS

C.P. Schnorr, Frankfurt

Let $E_i \subset \mathbb{K}^n$ $i = 1, .., r$ be (Zariski)-closed (affine) sets definable over the field $\mathbb{K}_o \subset \mathbb{K}$. Then Bezout's inequality for the degree of affine closed sets implies

Lemma $\deg \bigcap_{i \leq r} E_i \leq \deg E_1 \cdot (\max_{i>1} \deg E_i)^{\dim E_1}$

The following consequence yields a random polynomial decision procedure for deciding whether a given polynomial is 0:

Cor. 1 Let $P \in \mathbb{K}[x_1, .., x_n]$ and let $B \subset \mathbb{K}^n$ be finite and the intersection of hypersurfaces of degree $\leq m$, then

$\#\{x \in B \mid P(x) = 0\} \leq \deg P \cdot m^{n-1}$, provided $P \not\equiv 0$.

Cor. 2 (common with Heintz) There is a closed set $W(v,n) \subset \mathbb{K}^n$ which contains all $(a_1, .., a_n) \in \mathbb{K}^n$ such that $\Sigma_{i=1}^n a_i x^i$ can be

computed with $\leq v$ nonscalar steps and

(1) $\deg W(v,n) \leq (2vn)^{(v+1)(v+2)}$, (2) $\dim W(v,n) \leq (v+1)(v+2)$

Cor. 3 $\max\{L_{ns}(\Sigma_{i=1}^{n} a_i x^i) \mid a_i \in \{0,1\}\} \geq \sqrt{\frac{2}{3} n/\log n}$ and for most $(a_1,..,a_n) \in \{0,1\}^n$ this bound is achieved.

We also establish lower bounds on the minimal number of nonscalar operations which are necessary to evaluate some specific multivariate polynomials with 0,1-coefficients; e.g.: $L_{ns}(\Sigma_{i=1}^{k} y^i x_i^n) \geq \frac{1}{2} k \log n$ provided $k < n^{1/4}$.

SOME POLYNOMIALS THAT ARE HARD TO COMPUTE

J. von zur Gathen, Zürich

The nonscalar complexity $L(f)$ of a polynomial $f \in \mathbb{C}(X)$ is the minimal number of nonscalar multiplications/divisions sufficient to evaluate f by a straight-line program. "Nonscalar" means that multiplication by a complex number which may depend on the coefficients of f, but not on the value of X, is free. Paterson and Stockmeyer have proved that for all f, $L(f) \leq O(\sqrt{n})$, and for almost all f, $L(f) \geq \sqrt{n-2}$ where $n = \deg f$. Strassen, Schnorr, and Heintz and Sieveking have given specific polynomials which are hard to compute. Using a theorem by the latter two authors, Strassen & von zur Gathen showed that for

$z \in \mathbb{Q}-\mathbb{Z}$: $L(\Sigma_{1 \leq j \leq n} z^j x^j) \geq \sqrt{\frac{n}{\log n}}$ and for $z \in \mathbb{C}$ not zero or a root of unity $L(\Sigma_{1 \leq j \leq n} z^{1/j} x^j) \geq \sqrt{\frac{n}{\log n}}$

The bounds make use of the fact that the coefficient sequences generate algebraic field extensions of high degree.

Analogous results hold in the case where all operations are counted.

POLYNOMIALS WITH SIMPLE COEFFICIENTS WHICH ARE HARD TO COMPUTE

H.J. Stoss, Konstanz

We are interested on the complexity of polynomials of degree n over the complex field using computations in the field $\mathbb{C}(x)$. The main result is the following:

Definition: A polynomial $p(x) = p(0)+\sum_{i=1}^{n} a_i x^i \in \mathbb{C}[x]$ is of type $\mathcal{M}$, where $\mathcal{M} \subset \{1,2,\ldots,n\}$ iff $a_i \neq 0 \iff i \in \mathcal{M}$ $(i=1,2,..,n)$. Then we get

Theorem: Given ε, $0<\varepsilon<1$, there exists $n_0(\varepsilon)$ such that for all $n>n_0$ and all $g: \frac{n}{2} \geq g \geq (\lg n)^2$ at least $(1-\varepsilon)\binom{n}{g}$ sets $\mathcal{M} \subset \{1,2,..,n\}$ with $\#\mathcal{M} = g$ have the property that all polynomials p of type $\mathcal{M}$ have complexity

$$L_*(p) > 0.8 \sqrt{\frac{g}{\lg n}}$$

$$L_{tot}(p) > 0.19 \frac{g}{\lg n}$$

From this theorem we get some further results, e.g. that almost all 0-1 polynomials are hard to compute.

It is also possible to derive lower bounds for specific polynomials with algebraic coefficients.

FACTORIZATION OF UNIVARIATE INTEGRAL POLYNOMIALS

G.E. Collins

Let A be a primitive squarefree univariate integral polynomial of degree n. An irreducible factor of A can be found by forming products of lifted modulo p factors of A for a suitable small prime p. One can either form first the products consisting of the smallest numbers of lifted factors (cardinality procedure) or form first the products with smallest degrees (degree procedure). Let π be the partition of n consisting of the degrees of the irreducible factors of A. The average number of products formed before finding an irreducible factor of A is a function of π, $C(\pi)$ or $D(\pi)$ respectively.

Let $C^*(n)$ (resp. $D^*(n)$) be the maximum of $C(\pi)$ (resp. $D(\pi)$) for all partitions π of n. It is proved that $D^*(n)$ is an exponential function of n whereas, subject to a conjecture for which there is considerable evidence, $C^*(n)$ is dominated by n^2. If the conjecture is indeed true then the cardinality procedure provides a complete factorization algorithm whose "maximum average" computing time is dominated by a polynomial function of its degree n.

TOWARDS A DECISION PROCEDURE FOR PRIME IDEALS IN POLYNOMIALS RINGS

J. Heintz, Frankfurt

Let k be an algebraically closed field, $X_1,..,X_n$ indeterminates over k and $F_1,..,F_r \in k[X_1,..,X_n]$.

Goal: decide if $(F_1,..,F_r) \subset k[X_1,..,X_n]$ is prime when the elementary theory of k is given.

A partial solution of the problem is given by the following

Theorem: Let $d = (\deg F_1+...+\deg F_r)^n$
$(F_1,..,F_r)$ is prime and $\{F_1 = 0,..,F_r = 0\}$ is smooth iff

(i) for all polynomials $H,L \in k[X_1,..,X_n]$ with $\deg H + \deg L \leq d$ there is: $H \cdot L \in (F_1,..,F_r) \Rightarrow H \in (F_1,..,F_r)$ or $L \in (F_1,..,F_r)$

(ii) for all $x \in \{F_1 = 0,..,F_r = 0\}$ holds:

$$\operatorname{rank}\left(\frac{\partial F_j}{\partial X_i}(x)\right)_{\substack{j=1,..,r \\ i=1,..,n}} = n-s$$

where $s = \min\{k: (\exists\, u_1^1,..,u_{n+1}^1,..,u_1^k,..,u_{n+1}^k)$

$$0 < \#\{F_1 = 0,..,F_r = 0 \ , \ u_1^1X_1+...+u_n^1X_n-u_{n+1}^1 = 0,..,$$
$$u_1^kX_1+...+u_n^kX_n - u_{n+1}^k = 0\} \leq d$$

By the theorem we can decide if $(F_1,..,F_r)$ is prime and $\{F_1 = 0,..,F_r = 0\}$ is smooth. However, this decision procedure is not polynomial in $\deg F_1+..+\deg F_r$.

COMPLEXITY OF SYSTEMS OF ALGEBRAIC EQUATIONS

D. Lazard, Poitiers

Let $f_1,..,f_n$ be n homogeneous polynomials in n indeterminates which have a finite number of common zeros in the algebraic closure of the ground field, counting the zeros at infinity. An algorithm is described which computes all those zeros. If d is the highest degree of the polynomials, the computations needed by this algorithm consist in the resolution of one univariate polynomial whose degree is the number of solutions and a number of operations of the ground field which is polynomial in $(ed)^n$ where e bounds the number of solutions.

OPTIMALITY OF SOME ALGORITHMS USING ELEMENTARY MATRICES

J. Lafon, Strasbourg

Let k be an infinite field. M(k) denote the space of m×n matrices over k. An elementary matrix $E_{ij}(a)$ has all its elements null except element i,j equal to a and diagonal elements equal to 1.

1) Linear system resolution
   To a general linear system AX = B we associate the n×(n+1) matrix A' = (AB). We define $\mathcal{A}_R$ (resp. $\mathcal{A}_P$) as the set of algorithms which compute the triangular matrices $R = \begin{pmatrix} \ddots & * \\ 0 & \ddots \end{pmatrix}$ resp. the diagonal $D = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ from A' by using only left products by elementary matrices and rational operations on k. We prove the following fact:
   - Gauss is the unique optimal algorithm in $\mathcal{A}_R$ (with respect to the number of mult. div. (or add.) used)
   - Gauss is also optimal in $\mathcal{A}_P$ but it is not unique. There exist optimal algorithms which don't make first the triangularisation.

2) Transformation of a matrix in a Hessenberg tridiagonal or Frobenius form.

We consider only algorithms which use transmutation by elementary matrices and rational operations on k. The results are the following:

- The classical algorithm is optimal to obtain the Hessenberg form - The minimum cost (number of mult./divisions) is:

$$\frac{5n^3}{6} - 2n^2 + \frac{n}{6} + 1.$$

- The optimal algorithms are different from the classical one both for the computation of the tridiagonal and the Frobenius forms. The minimum costs are:

$$n^3 - \frac{n}{2} - 11n + 5 - \begin{cases} p^2-2 & \text{if } n=2p \\ p^2+p-2 & \text{if } n=2p+1 \\ 2 & \text{if } n=3 \end{cases} \quad \text{for the tridiagonal form}$$

$n^3 - n^2 + 9n - 4$ for the Frobenius form.

HORN COMPLEXITY FOR BOOLEAN FUNCTIONS

E. Börger, Dortmund
(joint work with S.O. Aanderaa)

We measure the complexity of Boolean fcts in terms of the complexity of the logical structure defining them. The hope is that one may become able to derive impossibility results (lower bounds) for particular Boolean fcts if the logical structure of the formulae defining them is "simple" but at the same time "comprehensive enough" to express interesting facts.

The Horn complexity $C_H(f)$ is defined as minimal length of any formula defining f which is Horn in its working variables. Here α defines f iff for all q $(f(q))=1$ iff $\alpha(x|q,y)$ is satisfiable; x are the input variables, y the output variables; $\alpha(x,y)$ is Horn in y iff it is a Horn formula when the occurrences of the input variables are disregarded.

Theorem: $C_H(f) \leq O(C_N(f))$, $C_N(f) \leq O(C_H(f)^2 \cdot (\lg C_H(f))^3)$ where $C_N(f)$ denotes the network complexity of f.

Interesting connexions to the P=NP-problem are discussed.

GENERALIZED NONDETERMINISTIC ITERATIVE ARRAYS

M. Fürer, Edinburgh

A d-dimensional iterative array consists of identical finite automata in all points of $\mathbb{Z}^d - (0,0,\ldots,0)$. The automaton at $(0,0,\ldots,0)$ has in addition an input device and an accepting state. The new state of each automaton depends not only on its old state but also on the old states of all automata with distance 1.

Another simple and highly regular interconnection pattern which is a combination of array and tree structure yields a very powerful machine (generalized iterative array) if the automata are nondeterministic. Linear time of this machine corresponds exactly to exponential nondeterministic Turing machine time. If there are not so many interconnections (e.g. with a tree structure), polynomial time of the generalized iterative array corresponds only to polynomial Turing machine space (as in the deterministic case). Generalized iterative arrays are therefore a helpful object to study the time versus space and determinism versus nondeterminism problems, and to investigate the influence of the structure of memory on the computational complexity.

The linear time bounded alternating version of the above parallel machine with array-tree structure is exactly as powerful as an exponential time bounded alternating Turing machine with a linear number of alternations. The languages accepted by such machines form a very natural class. E.g. the first order theory of real numbers with addition $TH(\mathbb{R},+)$ is complete in this class.

NEW ALGORITHM AND COUNTERALGORITHM FOR SELECTION

L. Hyafil, Paris

In this paper we present a new algorithm for selecting the first k elements of an ordered set of size n, which improves, for asymptotic values of n, over all previously known algorithms; it improves also over algorithms restricted to the search for the k-th element. A counteralgorithm (adversary strategy) is also given which reduces the gap between the lower and the upper bound to a few comparisons.

A TIME-SPACE TRADEOFF FOR SORTING ON A GENERAL SEQUENTIAL MODEL OF COMPUTATION

A. Borodin, Toronto

On a general model of computation, no restriction is placed on the way in which the computation may proceed, even though the inputs and outputs come from a specific mathematical structure. For example, a "bucket sort" does not restrict itself to the structure of a totally ordered set. We define a "most general" sequential model of computation and then prove that for sorting N distinct integers, each in $[1,N^2]$, we must have $T \cdot S = \Omega(N^2/\log N)$ where T is the time and S the space used in the computation. This result is due to A.Borodin and S.Cook.

EVERY DETERMINISTIC CFL IS ACCEPTED SIMULTANEOUSLY IN POLYNOMIAL TIME AND LOG SQUARED SPACE

S.A. Cook, Toronto

We prove the theorem in the title by showing how to simulate a deterministic pushdown automaton in small time and space. The simulating machine remembers enough about the pushdown stack (and past history of the computation) so that recomputations are not frequently necessary, but remembers little enough that the $O(\log^2 n)$ space bound is not exceeded. The paper provides the first examples in the literature of a language L and a proof that L can be recognized simultaneously in small time and space, such that no proof is known that L is in DSPACE(log n).

PEBBLING MOUNTAIN RANGES

K. Mehlhorn, Saarbrücken

Recently, S.A. Cook showed that DCFL's can be recognized in $O((\log n)^2)$ space and polynomial time simultaneously. We show that $O((\log n)^2/\log \log n)$ space suffices under the assumption that the height of the pushdownstore as a function of time is given as an additional input.

TIME VERSUS SPACE

R. Reischuk, Bielefeld

The pebble-game is generalized and a generalized pebble-lemma is proved. With the help of this it can be shown that $t(n)$-time bounded tree-tape Turing machines and logarithmically $t(n)$-time bounded RAM's can be simulated by a $t(n)/\log t(n)$-tape bounded Turing machine. For an extended model of Turing machines with ps-admissible storage structure (this includes multidimensional Turing machines) an analogous space bound $t(n) \log \log t(n)/\log t(n)$ can be obtained. With the help of a fast simulation of time bounded multidimensional Turing machines by tree-tape Turing machines the space-bound for multidimensional Turing machines can be improved to "nearly" $t(n)/\log t(n)$.

KOLMOGOROV COMPLEXITY AND ON-LINE COMPUTATIONS

W.J. Paul, Bielefeld

If $d \geq 2$, then for d-dimensional on-line Turing machines $k+1$ tapes are better than k. The proof uses the concept of Kolmogorov complexity.

COMPLETE PROBLEMS FOR NONDETERMINISTIC COMPLEXITY CLASSES DEFINED BY SUBLINEAR SPACE BOUNDS AND POLYNOMIAL TIME

B. Monien, Paderborn

In this talk we consider a class of pseudopolynomial problems. A problem $L \subset X^*$, $L \in NP$, is called pseudopolynomial if to each $u \in X^*$ there is associated a number $m = m_u \in \mathbb{N}$ such that (u,m) is accepted by a det. TM within a time bound which is polynomial in m. We use reductions which guarantee that for every pair (u,m) the number m grows at most polynomial. Let $Pair_2$ be the class of all sets R such that $(u,m) \in R$ can be tested by a nondet. TM within the time bound $pol(|u|, \log m)$ and the space bound $\max(\log|u|, \log m)$. We present a problem which is complete for $Pair_2$ with respect to our reductions.

If R is complete for $Pair_2$ then for every easily computable function f the class $L_R(f) = \{u\#v \mid (u,v) \in R \text{ and } |v| \leq f(|u|)\}$ is complete for $\bigcup_d NPTIMESPACE(f(n^d))$.

PATH SYSTEM PROBLEMS

I.H. Sudborough, Paderborn

Path systems with bounded bandwidth are considered. It is shown that the family of solvable path systems with bandwidth $2^{cf(n)}$, denoted by $\{SPS(2^{cf(n)})\}_{c \geq 1}$, is complete for the set of languages recognized by alternating Turing machines within space f(n), denoted by ASPACE(f(n)), with respect to log space reductions, when $f \in O(\log n)$ is constructible. It is also shown that SPS(f(n)) can be solved deterministically within space $f(n) \log n$. Thus, it follows that, for constructible functions $f \in O(\log n)$, $ASPACE(f(n)) \subseteq \bigcup_{k \geq 1} DSPACE(2^{kf(n)} \log n)$. In particular, $ASPACE(\log \log n) \subseteq \bigcup_{k \geq 1} DSPACE((\log n)^k)$.

NP-HARDNESS AND CRYPTOCOMPLEXITY

S. Even, Haifa

A family of encryption systems which are NP-hard to break is shown. One such highly "linear" system is shown to be almost always easy to crack, but others are believed to be hard to break in most cases, although this remains to be proven.

The Public-Key-Crypto-System (PKCS) model is formulated and it is shown that such a system is unlikely to be NP-hard to break. This differs from the result of Brassard, Fortune and Hopcroft in two respects. First, the one-way functions they analyse cannot have trapdoors (and therefore are not suitable for PKCS); this allows the possibility of existence of a one-way trapdoor function, since the cracking algorithm must solve for all encryption keys, which may change with the input. Second, we do not require that the function is onto.

A NON PRIMITIVE RECURSIVE DECISION PROBLEM FOR PETRI NETS

E.W. Mayr, München

Finite reachability sets of Petri nets or vector addition systems can effectively be constructed. The complexity of the inclusion and equality problem for finite reachability sets can, however, be shown to be very hard as the time or space complexity of each decision procedure for these problems exceeds any primitive recursive function i.o. For the proof of this lower bound a bounded version of Hilbert's Tenth Problem concerning integer solutions of diophantine equations is reduced to the finite inclusion problem using the concept of weak computation of a function by a Petri net. The finite inclusion and equality problem are thus first uncontrived decidable problems which are not primitive recursive.

LOCAL OPTIMIZATION OF QUAD TREES

P. van Emde Boas, Amsterdam

In their 1974 paper Finkel and Bentley write that they have obtained a 10% reduction of the total path length of randomly created QUAD trees by application of local transformations. It is not clear from their paper which transformations were used and how they were applied. Our empirical investigation tries to answer these questions. We also look for new tricks which might increase the reduction of path length obtained. Our results suggest that Finkel and Bentley have used dynamic optimisation (optimising after each insertion) without Guards. We present two patterns which give a small increase over the one obtained by Finkel and Bentley. Combination of Patterns seems not to be helpful.

One of our patterns can be used to solve the deletion problem for QUAD trees. Nodes are not really deleted but tagged as being virtual for not being present, keeping this way their role in guiding searches in the tree. Our transformations allow to eliminate virtual nodes with only one son, whereas subtrees consisting of virtual nodes only may be deleted right away. Therefore the virtual nodes will never form the majority of nodes in a tree.

OPTIMAL TREE LAYOUT

M.S. Paterson, Warwick
(joint work with M.J. Fischer)

Given i) a planted tree T with leaves $x_1,..,x_n$, root z, and with a weight w_e associated with each edge e, and
ii) fixed positions for $\underset{\sim}{x},z$, in $\mathbb{R}^k$

We seek positions $y_1,y_2,...$ for the internal nodes of T so as to minimize $\sum_{e\in T} w_e \cdot \text{length}(e)$. Denote minimum by $\text{COST}_T(\underset{\sim}{x},z)$

Theorem

If we consider planar embeddings in $\mathbb{R}^2$, i.e. with no edges crossing, then the recognition problem

$$\{\langle T, \underset{\sim}{x}, z, k\rangle \mid \text{cost}_T^{(\text{planar})}(\underset{\sim}{x}, z) < k\}$$

is NP-complete.

If edges must be made from line segments parallel to the co-ordinate axes, length(e) becomes the L_1 norm and

Observation:

Each L_1-optimal layout problem in $\mathbb{R}^k$ decomposes into k independent layout problems in $\mathbb{R}^1$.

We have linear time algorithms for the one-dimensional problem in the following cases:

i) unit weights

ii) leaf positions are in "natural" tree order.

Otherwise we have an algorithm with complexity O(n log n).

The following characterization, used in deriving the algorithms, describes the dependence of cost_T on $\underset{\sim}{x}$ and z.

Theorem

For any fixed ordering of the leaves, say $x_1 \leq x_2 \leq \ldots \leq x_n$,

$$\text{cost}_T(\underset{\sim}{x}, z) = \int_{-\infty}^{z} a(\underset{\sim}{x}, t)\,dt + \int_{z}^{+\infty} b(\underset{\sim}{x}, t)\,dt$$

where a-b is non-decreasing function of t and
where a and b are step-functions defined by

$$\left.\begin{array}{lll} a(\underset{\sim}{x},t) = 0 & b(\underset{\sim}{x},t) = b_0 & \text{if } t \in (-\infty, x_1) \\ = a_i & = b_i & \text{if } t \in [x_i, x_{i+1}) \\ = a_n & = 0 & \text{if } t \in [x_n, \infty) \end{array}\right\} \text{and } \underset{\sim}{a}, \underset{\sim}{b} \text{ depend only on w's and ordering of x's}$$

CONCURRENT GRAPH SEARCHING

M.J. Fischer, Seattle
(joint work with M.O. Rabin)

We present concurrent algorithms for searching a list-structured memory. The memory is a finite labelled directed graph augmented by a fixed number of pointer- and integer-valued storage registers at each node. A process has a finite state control and a fixed number of such storage registers. In one step, a process can access any single node to which it holds a pointer. We say such a node is visited. A process is placed on a node by initializing all its registers with pointers to that node. A sequence $\{P_i\}_{i\geq 1}$ of processes solves the graph-searching problem if for all n and all memories of suitable type but arbitrarily many nodes, if $P_1,..,P_n$ are placed arbitrarily on the graph, then every non-failing P_i eventually visits every node accessible from its starting places. (A process fails if it ceases execution).

Theorem There exists a sequence of processes, each having the same number of registers, which solves the graph-searching problem. Moreover, on any run of the first n processes, all integer-valued registers are bounded by O(n). If one assumes pointers are totally ordered and can be compared, then the processes can be chosen to be identical, and the bound on the register size becomes constant.

A PROBABILISTIC LOG SPACE ALGORITHM FOR UNDIRECTED GRAPH THREADABILITY

Ch. Rackoff, Toronto
(joint work with Aleliunas, Karp, Lipton, Lovász)

Let $T = \{(G,a,b) \mid$ G is an undirected graph containing nodes a and b, and there is a path from a to b $\}$

Theorem 1: There is a polynomial time, log space coin-tossing algorithm for T: if the input $\notin$ T, the algorithm says NO; if the input $\in$ T, the algorithm says YES with probability >1/2.

Theorem 2: There is a log space, non-uniform algorithm for T. That is, for each n there is a finite state machine M with a polynomial (in n) number of states, such that M accepts precisely the members of T of size n.

EFFICIENT IMPLEMENTATION OF STICKY POINTERS IN TEXT EDITORS

R.E. Ladner, Seattle
(joint work with M.J. Fischer)

Efficient algorithms for insertion and deletion of text which supports sticky pointers in the base text is presented. The cost of n edit operations is O(n) for the insertions and deletions and O(n log n) for locating the pointers in the text. The algorithm uses balanced trees in a new and unusual way.

NOTWENDIGE BEDINGUNGEN FÜR DIE ÄQUIVALENZ KONTEXTFREIER SPRACHEN

G. Hotz, Saarbrücken

Sei $G = (X,T,P,S)$ eine kontextfreie Grammatik und $L(G)$ die durch G erzeugte Sprache. Wir bilden die freie Gruppe $F(X)$, die durch X erzeugt wird und den Gruppenring $\mathbb{Z}(F(X))$. $\mathbb{Z}(A(X))$ ist der Gruppenring der freien abelschen Gruppe, die X erzeugt. $e,c:F(X) \to A(X)$ sind Gruppenhomomorphismen, die wir zu Gruppenringhomomorphismen fortsetzen. Wir bilden $\overline{P}=\{u-v \mid (u,v)\in P\}$ und $a(\overline{P}) = e(\overline{P}) \cup c(\overline{P})$ und das durch $a(\overline{P})$ in $\mathbb{Z}(A(X))$ erzeugte Ideal $(a(\overline{P}))$. Es sei $R = \mathbb{Z}(A(X))/(a(\overline{P}))$ und $\overline{c},\overline{e}$ die kanonischen Verlängerungen von c,e zu Homomorphismen in R. Wir bilden nun den $\mathbb{Z}(A(X))$-Modul $\mathfrak{M} = \bigoplus_{x\in X} Rdx$, worin dx eine freie Variable ist. Eine freie Differentiation ist eine Abbildung d von $Z(F(X))$ in $\mathfrak{M}$ mit folgenden Eigenschaften:

$$1)\ d(f+g) = d(f) + d(g)$$
$$2)\ d(f\cdot g) = d(f)\cdot\overline{e}(g) + \overline{c}(f)\cdot d(f).$$

Setzen wir fest, daß dx für $x \in X$ eine freie Variable ist, dann ist d durch e und c eindeutig bestimmt. Wir bilden den

durch $d(\bar{P})$ erzeugten $\mathbb{Z}(A(X))$-Modul $(d(\bar{P}))$ und faktorisieren $\mathfrak{M}$ nach $(d(\bar{P}))$. Das Resultat bezeichnen wir mit $\mathfrak{M}(P,e,c)$. Es wurde der Beweis des folgenden Satzes skizziert.

Satz: Sind G und G' kontextfreie Grammatiken ohne überflüssige Variablen, und ist $L(G) = L(G')$, dann ist $\mathfrak{M}(P,e,c)$ isomorph zu $\mathfrak{M}(P',e,c)$ und zwar unter den folgenden Voraussetzungen:

1) $c(x) = e(x) = \pm x$; $c(x) = 1$ und $e(x) = \pm x$, $c(x) = \pm x$ und $e(x) = 1$.

Modifiziert man die Definition von $\mathfrak{M}(P,e,c)$ für $e(x) = c(x) = 1$ in naheliegender Weise, dann erhält man auch hierfür das gleiche Resultat.

A GENERAL THEORY OF OPTIMAL ALGORITHMS

J.F. Traub, Columbia (N.Y.)
(joint work with H. Wozniakowski)

Assume we are given N(f) where $f \in G$. We wish to compute or approximate S(f). The information operator N and the solution operator S can be linear or nonlinear. The basic concepts of optimal error algorithm, optimal complexity algorithm, optimal information, and problem complexity are defined. Instances are given of general theorems which can be established in this framework. One example: If S and N are linear operators then adaptive information is no better than nonadaptive information. Kiefer's famous result on optimal search for unimodal functions show this result is false if S is nonlinear.

Applications illustrate that very tight bounds can often be obtained for problem complexity.

Berichterstatter: J. Heintz

List of the participants of the Complexity Theory Symposium

Michael Atkinson
Department of Computing
Mathematics
University College
Cardiff, G.B.

Walter Baur
Seminar für Angewandte
Mathematik
Universität Zürich
Freiestraße 36
CH 8032 Zürich

P. van Emde Boas
ITW/VPW Universität
von Amsterdam
Roetersstraat 15
1018 WB Amsterdam
Niederlande

E. Börger
Lehrstuhl für Informatik II
Universität Dortmund
4600 Dortmund

A. Borodin
Department of Computer
Science
University of Toronto
Toronto, Canada

George E. Collins
Computer Science Department
University of Wisconsin
1210 W. Dayton St.
Madison, Wis. 53706, USA

Stephen A. Cook
Department of Computer Science
University of Toronto
Toronto, Canada

Shimon Even
Department of Computer Science
TECHNICON
Haifa, Israel

Michael J. Fischer
Department of Computer Science
FR-35
University of Washington
Seattle, Wa. 98195, USA

Martin Fürer
Department of Computer Science
University of Edinburgh
King's Buildings
Edinburgh, G.B.

Joachim v. zur Gathen
Seminar für
Angewandte Mathematik
Universität Zürich
Freiestraße 36
CH 8032 Zürich

H.F. de Groote
FB Mathematik
Universität Frankfurt
Robert Mayer-Str. 10
6000 Frankfurt am Main

Joos Heintz
FB Mathematik
Universität Frankfurt
Robert Mayer-Str. 10
6000 Frankfurt am Main

G. Hotz
FB Mathematik-Informatik
Universität Saarbrücken
6600 Saarbrücken

L. Hyafil
Centre Scientifique
IBM France
36 Ave. R.Poincaré
75116 Paris, France

R.E. Ladner
Department of Computer Science
University of Washington
Seattle, Wa. 98195, USA

J.C. Lafon
Université Louis Pasteur
Centre de Calcul Esplanade
6784 Strasbourg, France

Daniel Lazard
Mathématiques
Université de Poitiers
86022 Poitiers Cedex
France

K. Leeb
Informatik I
Universität Erlangen
Martensstr. 3
8520 Erlangen

R. Loos
Universität Karlsruhe
Informatik I
Zirkel 2
7500 Karlsruhe

Ernst W. Mayr
Institut für Informatik
TU München
Postfach 2o242o
8000 München

K. Mehlhorn
FB 10
Universität d. Saarlandes
6600 Saarbrücken

M. Mignotte
Université Louis Pasteur
Centre de Calcul
67o34 Strasbourg, France

B. Monien
GH Paderborn FB 17
Warburger Str. 100
4790 Paderborn

J. Morgenstern
Département de Mathematiques
Université de Nice
Parc Valrose
o6o34 Nice, France

H. Noltmeier
Informatik III
RWTH Aachen
Büchel 29
5100 Aachen

Victor Pan
Computer Science Department
Sunya, Albany, N.Y. 12222, USA

M.S. Paterson
Department of Computer Science
University of Warwick
Coventry CV4 7AL, G.B.

W. Paul
FB Mathematik
Universität Bielefeld
4800 Bielefeld

Ch. Rackoff
Department of Computer Science
University of Toronto
Toronto, Canada

R. Reischuk
Fakultät Mathematik
Universität Bielefeld
4800 Bielefeld

Francesco Romani
IEI - CNR
Via S. Maria 4631
56100 Pisa, Italy

A. Schönhage
Mathematisches Institut
Universität Tübingen
Auf der Morgenstelle 10
7400 Tübingen

C.P. Schnorr
FB Mathematik
Universität Frankfurt
Robert Mayer-Str. 10
6000 Frankfurt

P. Schuster
Mathematisches Institut
Universität Tübingen

H.J. Stoß
Mathematik
Universität Konstanz
7750 Konstanz

Volker Strassen
Seminar für Angewandte Mathematik
Universität Zürich
Freiestraße 36
CH 8032 Zürich

I. Hal Sudborough
FB 17 GH Paderborn
4790 Paderborn

J.F. Traub
Department of Computer Science
Columbia University
Seeley W. Mudd Building
New York 10027, USA

S. Winograd
IBM T.J. Watson Research Center
P.O.Box 218
Yorktown Heights
New York 10598, USA