MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

T a g u n g s b e r i c h t 50/1992

Komplexitätstheorie

15.-21.11.1992

The 10-th Oberwolfach conference on Complexity Theory was organized by Joachim von zur Gathen (Toronto), Claus-Peter Schnorr (Frankfurt) and Volker Strassen (Konstanz). There were 38 participants coming from nine countries.
The 32 lectures covered a broad range of actual resarch in complexity theory as well as in classical subjects. Some talks were given about various aspects of cryptography. The new theory of probabilistically checkable proofs was addressed. A group of talks dealt with combinatorical optimization. Others investigated general models for parallel computing and average–case complexity. A big topic was the complexity of algebraical and arithmetical problems. It was a quite active and stimulating conference.

Abstracts

ERIC BACH

Statistical Evidence for Small Generating Sets

Joint work with LORENZ HUELSBERGEN

For an integer n, let $G(n)$ denote the smallest x such that the primes $\leq x$ generate the multiplicative group modulo n. We offer heuristic arguments and numerical data supporting the idea that $G(n) \leq (\log 2)^{-1} \log n \log\log n$ asymptotically. We believe that the coefficient $1/\log 2$ is optimal. Finally, we show the average value of $G(n)$ for $n \leq N$ is at least $(1 + o(1)) \log\log N \log\log\log N$, and give a heuristic argument that this is also an upper bound. This work gives additional evidence, independent of the ERH, that primality testing can be done in deterministic polynomial time; if our bound on $G(n)$ is correct, there is a deterministic primality test using $O(\log n)^2$ multiplications modulo n.

ULRICH BAUM

Computing Irreducible Representations of Supersolvable Groups

Joint work with MICHAEL CLAUSEN

We present an algorithm that, given a power–commutator presentation of a supersolvable group G, computes a full set of inequivalent irreducible and *monomial* ordinary matrix representations of G in time $O(|G| \log |G|)$. The algorithm is based on Clifford theory and adapting the representations to a chief series of G. The algorithm only requires *symbolic* calculations in a suitable group of roots of unity; no field arithmetic is needed at all. The result is valid over every field containing a suitable (e.g. $exp(G)$-th) primitive root of unity.

INGRID BIEHL

Models for Average–Case Complexity

In 1984 L. Levin developed a definition of "a function $f : \Sigma^* \to N$ is polynomial on average with respect to a distribution $\mu : \Sigma^* \to [0, 1]$". We study the question, of how Levin's definition can be generalized and whether this definition is the only reasonable one. We characterize properties which seem to be "natural" for a reasonable average–case model. This leads to the definitions of *strong average–case models* and *weak average–case models*. We show that basic results, well–known from worst–case complexity theory e.g. relations between time and space complexity classes ..., hold in all weak average–case models. Moreover we show that for a special class of weak average–case models completeness results similar to known completeness results in Levin's theory hold.

PETER BÜRGISSER

Decision Complexity of Generic Complete Intersections

We study the complexity of algebraic decision trees that decide membership in a semi-algebraic subset $X \subseteq R^m$, where R is a real (or algebraically) closed field. We prove a general lower bound on the verification complexity of the vanishing ideal of an irreducible algebraic subset $X \subseteq R^m$ in terms of the degree of transcendency of its minimal field of definition. As an application, we determine exactly the number of additions, subtractions and comparisons that are needed to test membership in a generic complete intersection $X = Z(f_1, \ldots, f_r) \subseteq R^m$; for the number of multiplications, divisions and comparisons needed, we obtain an asymptotically optimal lower bound as $max_i deg f_i \to \infty$. A

further application is given to test problems related to partial or continued fractions.

MARTIN FÜRER

Minimum Degree Steiner Tree Approximation

Joint work with BALAJI RAGHAVACHARI

There is a polynomial time deterministic algorithm to compute a spanning tree of degree at most $\Delta + 1$ for every graph for which a spanning tree of degree Δ exists. The same result holds for Steiner trees, whereas the directed version of the minimum degree spanning tree problem can be approximated by a spanning tree of degree $O(\Delta + \log n)$. To compute the minimum degree is well known to be NP-hard in all of these three cases.

MERRICK FURST

Are Relevant Bits Hard to Find?

Since the first seminal paper of Valiant on learning we have known if certain cryptographic systems are secure, then certain families of circuits are unlearnable. He pointed that if one-way functions exist, then there are methods to show that general polynomial size circuits are not even weakly learnable.

We show that if certain cryptographic systems do *not* exist, then certain classes of circuits are learnable. We show that if we assume that a certain cryptographic assumption is false, then we can weakly learn polynomial size DNF in polynomial-time in the query model. Under a similar assumption we partially solve another learning problem due to Avrim Blum.

The importance of these results is two-fold. First, they show a potential approach to resolving these open questions. Perhaps it will be possible to prove that these assumptions are true. Of course many may believe that our assumptions are false; however, all the more reason to study the consequences of assuming that certain crypto-systems do not exist. Second, they show an interesting link between two important areas of complexity theory.

We study two questions about learning. The first is whether or not we can weakly learn a family of circuits given the ability to ask arbitrary queries. The first problem, more precisely, is the following. Suppose that C is a family of boolean circuits. We can ***weakly learn*** the family provided there is a polynomial-time procedure that given an oracle for any circuit C from the family with one output, can construct a new circuit D so that

$$Pr[D(x) = C(x)] \geq 1/2 + 1/n^{O(1)}.$$

Thus, we can weakly learn circuits from a family provided we can build a new circuit that "predicts" the given circuits output. We are allowed only a polynomial number of questions. It is currently open whether or not we can weakly learn many families of circuits. In particular, this is true for the important family of DNF that are of size at most $n^{O(1)}$ and of AC^0 circuits.

The second problem is due to A. Blum. It really is a spectrum of questions which we will denote by $AB(s(n), S)$ where $s(n)$ is integer valued function between 1 and $\log(n)$. The set S is a class of boolean functions. A problem instance consists of a function f from the class S with $s(n) = m$ inputs and a set of indices $i_1 < i_2 < \ldots < i_m$. A learner gets to "see" the value $f(x_{i_1}, \ldots, x_{i_m})$ where $x_1, \ldots, x_n$ are randomly selected from the uniform distribution. The learner is to both exactly determine the function f and the indices. As usual the key open question is whether or not the learner can do this with a polynomial time procedure. The question appears to be open even if S is restricted to the class of symmetric functions. Here are the main results.

Theorem 1: If a family of circuits $\mathcal{C}$ does not contain a pseudo-random generator, then $\mathcal{C}$ is weakly learnable.

Corollary 1: If depth 2 and size $n^{O(1)}$ circuits do not contain a pseudo-random number generator, then polynomial size DNF is weakly learnable.
Corollary 2: If AC^0 circuits do not contain a pseudo-random number generator, then AC^0 is weakly learnable.
The class of all boolean functions is denote by ALL.
Theorem 2: If depth $O(1)$ and size $n^{O(1)}$ circuits do not contain a pseudo-random number generator, then $AB(\log\log(n), ALL)$ is exactly learnable in polynomial time.

MARC GIUSTI

Complexity of Effective Nullstellensätze

Joint work with JOOS HEINTZ
Let k be an infinite and perfect field, and $f_1, \ldots, f_s$ polynomials in $k[x_1, \ldots, x_n]$, of degree at most $d \geq n$, given by the array of their coefficients in dense representation.
Then there exists an arithmetic network over k of size $L = s^{O(1)}d^{O(n)}$ and depth $\ell = O(n^{12}\log^9 sd)$ which decides if the ideal $(f_1, \ldots, f_s)$ is trivial (i.e. contains 1).
If so, the network constructs a straight–line program in $k[x_1, \ldots, x_n]$ without divisions, of size and depth of the same order as L and ℓ, which represents polynomials $p_1, \ldots, p_s$ of degree $d^{O(n)}$ such that the Bézout identity $1 = p_1 f_1 + \cdots + p_s f_s$ holds.
Eventually, this network can be constructed by a probabilistic (random) algorithm in sequential and parallel time of the same order as L and ℓ.

ODED GOLDREICH

Towards a Theory of Statistical Tests

Joint work with MANUEL BLUM (UC–BERKELEY)
We initiate a computational theory of statistical tests. Loosely speaking, we say that an algorithm is a *statistical test* if it rejects a "negligible" fraction of strings. We say that a statistical test is *universal* for a class of algorithms if it rejects all (but finitely many) of the strings rejected by each algorithm in the class.
We consider the existence and efficiency of universal statistical tests for various classes of statistical tests. We also consider the relation between ensembles passing statistical tests of particular complexity and ensembles which are indistinguishable from uniform by algorithms of the same complexity.
Some of our results refer to relatively simple statistical tests (e.g., those implemented by counter machines). In addition to their own merit, we hope that these results will stimulate investigations directed towards results that refer to more complex statistical tests (e.g., those implemented in log–space).

SHAFI GOLDWASSER

Probabilicsticaly Checkable Proofs and Approximation Problems

We address the question of how hard is it to approximate the solution of several optimization problems such as maximum–clique in a graph, minimum–coloring in a graph, minimum–set cover, and maximum-3-satisfiability. The corresponding decision problems of clique, coloring, set cover, and satisfiability are well known to be NP complete.
We surveyed work of the last few years on classifying the complexity of the above approximation problems. This work relies on new characterization of NP as languages which have "compact"

probabilistically checkable proofs(pcp). A language L is in $pcp(r, a, \epsilon)$ if there exists a probabilistic polynomial time verifier V which has access to an oracle Π such that

1. if $x \in L$, then there exists Π. $Pr(V^{\Pi}(x) = 1) = 1$.
2. if $x \notin L$, then for all Π, $Pr(V^{\Pi}(x) = 1) < 1 - \epsilon$
3. the verifier V uses at most r coins, and gets from oracle total of at most a answer bits.

Through a sequence of results originating with Feige–Goldwasser–Lovasz–Safra , followed by Szegedi, Arora–Safra, and Arora–Lund–Motwani–Sudan–Szegedi it has been shown that NP is in $pcp(O(logn), O(1), O(1))$.
In the talk we proved a theorem by FGLS90 as follows: if approximating max–clique within a constant c is in polynomial time, then NP is contained in $DTIME(2^{r+a})$ where r and a are the number of coins (and respectively number of answer bits) used by a verifier accepting NP languages with probability $\epsilon = \frac{1}{c^2}$. Since $NP \subseteq pcp(O(logn), O(1), O(1))$, it follows that there exists an ϵ such that approximating max–clique within n^{ϵ} is NP–complete.
We announced some new results concerning the results of minimum set–cover. In joint work with Bellare and Russel we showed (again improving the best bounds known on the compactness of pcp proofs with small ϵ) that (1) approximating set–cover within an constant c in polynomial time is NP–complete, and (2) there exists a c such that approximating set–cover within $c \log n$ factor, implies that NP is in $U_d DTIME(n^d)$.

Johan Håstad

The Shrinkage Constant is 2

Given a Boolean formula of size L and suppose we hit it with a random restriction from R_p, i.e. for each variable x_i independently we keep it as a variable with probability p and otherwise we set it with equal probability to 0 or 1. After this we do the following simplifications at each V-gate.

1. If one input is 1 replace the gate by the constant 1.
2. If both inputs are 0 replace the gate by the constant 0.
3. If one input is 0 replace the output by the other input.
4. If one input reduces to a single variable x_i ($\bar{x}_i$), substitute $x_i = 0$ ($x_i = 1$) in the subformula giving the other input.

We have similar simplification rules at the $\wedge$-gates.
We prove that the expected size of the reduced formula is bounded by $O(p^2(\log p^{-1})^{3/2}L + p\sqrt{L})$. This is optimal except for the factor $(\log p^{-1})^{3/2}$. As a corollary we obtain a formula size lower bound $\Omega(n^{3-o(1)})$ for a simple explicit function.

Michael Kaib

A Sharp Worst–Case–Analysis of the Gauß Lattice Basis Reduction Algorithm for any Norm

Joint work with Claus Schnorr
We study the reduction of 2–dimensional lattices in a real vector space with arbitrary norm. We prove for any norm that the Gauß reduction algorithm terminates after at most $\log_{1+\sqrt{2}}(2\sqrt{2}B/\lambda_2) + o(1)$ many iterations, where B is the maximum of the norms of the two input vectors and λ_2 is the second

successive minimum of the lattice with respect to the given norm. This bound is sharp for all norms and all lattices.

ERICH KALTOFEN

Parallel Sparse Linear System Solving

In our algorithms, a sparse matrix is a matrix that has an efficient algorithm for multiplying it by a vector. D. Wiedemann in 1986 invented an algorithm that can find the solution of a non-singular linear system with a sparse coefficient matrix in $O(N)$ matrix times vector operations and additionally $O(N^2)$ arithmetic operations in the coefficient field; here N is the dimension of the (square) matrix. D. Coppersmith in 1992 showed how this approach could be parallelized. With n processors the parallel time is then $O(N/n)$ matrix times vector operations, and an additional $O(nN^2)$ sequential field operation. Both algorithms are randomized.

We show that if the matrix has the property that the degree of the minimum polynomial is equal to the rank plus 1, the parallel algorithm has a high probability of finding such a solution. This condition can be also enforced by pre- and postmultiplying by random triangular Toeplitz matrices and then post-multiplying by a random diagonal matrix. We have also implemented the method on a network of 8 Sun Sparc workstations. A system of dimension 10.000 with 300.000 non-zero entries over $GF(2^{15}-19)$ can be solved in two days.

MAREK KARPINSKI

An Approximation Algorithm for Counting the Number of Zeros of Polynomials over $GF(q)$

Joint work with D. GRIGORIEV

We design the first polynomial time (for an arbitrary and fixed field $GF(q)$) (ε,δ)-approximation algorithm for the number of zeros of an arbitrary polynomial $f(x_1,\ldots,x_n)$ over $GF(q)$. This extends the recent approximation algorithms over $GF(2)$ [Karpinski, Luby, 1991], and gives the first efficient method for estimating the number of zeros and nonzeros of multivariate polynomials over small fields other than $GF(2)$.

The algorithm is based on the tight upper bounds proved on the sampling ratios for the number of nonzeros of certain polynomials over $GF(q)$ in the function of the number m of terms only. The bound is proven to be $m^{\log q}$, sharply.

PETER KIRRINNIS

Fast Computation of Numerical Partial Fraction Decompositions and Contour Integrals of Rational Functions

The problem of computing the numerical value of the integral $\int_\Gamma q(z)/p(z)dz$, where q and p are polynomials, given by their coefficients, and Γ is a curve in the complex plane, is investigated from the point of view of (serial) *bit complexity*.

Two algorithms are presented: The first one computes the integral in the special case that the zeros of p lie in a small circle not intersected by Γ. The second algorithm computes a special type of partial fraction decomposition especially well suited for this application, but also of interest by itself. Combining these algorithms yields an algorithm for the computation of contour integrals of rational functions in the general case.

It turns out that under reasonable norming conditions, the integral can be computed up to an error of 2^{-s} with $\tilde{O}(n^3(1+r)+n^2s)$ bit operations ($\tilde{O}$ indicates that logarithmic factors are neglected) if for every zero z of p and every point y on Γ the estimates $|z|\le 1$ and $|z-y|\ge 2^{-r}$ hold.

JAN KRAJICEK

Complexity of Propositional Logic

The following is a combinatorical situation encountered in lower bounds to the size of constant-depth propositional proofs. Let $\varepsilon > 0$, n large and $k \sim n^{\varepsilon}$. M is a set of partial partitions of $2n+1 = \{0, \ldots, 2n\}$ into 2-element classes. For $k_1, k_2 \in M$, k_1 and k_2 are compatible if $k_1 \cup k_2 \in M$. A *k-complete system* is any $\emptyset \neq S \subseteq M$ such that

1. $\forall h \in S \longrightarrow |h| \leq k$,
2. $\forall h_1, h_2 \in S$, $h_1 \neq h_2 \longrightarrow h_1$ and h_2 are incompatible,
3. $\forall f \in M$, $|f| + k \leq 2n \longrightarrow \exists h \in S, h$ and f are compatible.

Let φ be arbitrary formula built from atoms p_{ij}, $0 \leq i, j < 2n+1$, with connections $0, 1, \neg, \bigvee$. A *k-evaluation* of φ is a pair of maps H, S assigning to any subformula ψ of φ a k-complete system S_ψ and $H_\psi \subseteq S_\psi$ such that

1. $S_0 = S_1 = S_{p_{..}} = \{\emptyset\}$, $\quad H_0 = \emptyset, H_1 = H_{p_{ij}} = \{\emptyset\}$.
2. $S_{p_{i_0 j_0}} = \{p_{i_0 j}\} \cup \{p_{i_0 j} p_{i j_0} | \text{all } i, j, i_0, j_0 \text{different}\}$ and $H_{p_{i_0 j_0}} = \{p_{i_0 j_0}\}$.
3. $S_{\psi\varphi} = S_\psi$, $\quad H_{\psi\varphi} = S_\psi - H_\psi$.
4. If $\psi = \bigvee_n \psi_n$, none of ψ_n starts with $\bigvee$, then
   (a) $\forall h \in S_\psi$, either h is compatible with all $f \in \bigcup_n H\psi_n$, or h contains some $f \in \bigcup_n H\psi_n$.
   (b) $H_\psi = \{h \in S_\psi | h \text{ contains some } f \in \bigcup_n H\psi_n\}$.

Lemma. *If $H_\varphi \neq \emptyset$ is any k-evaluation of φ then the parity principle requires exponential-size constant-depth proofs from φ.*

Parity principle says that the relation $\{(i,j) | p_{ij} = 1\}$ is not a total partition of $2n+1$ into 2-element classes. It is open wheter the hypothesis of the lemma is satisfied when φ is an instance of MOD_3-principle (saying that $3l+1$ cannot be partitioned into 3-element classes) for formulas built from atoms p_{ij}.

THOMAS LICKTEIG

On Randomized Algebraic Decision Complexity

The impact of randomization on the complexity of deciding membership in a semi-algebraic subset of the real n-space is investigated. Examples are exhibited where allowing for a certain error probability in the answer of the algorithm the complexity of decision problems decreases. A general lower bound is given which on the other hand shows that in many cases randomization does not help much. This lower bound on randomized complexity is based on previous lower bound results on decision complexity by [Lickteig 90], and [Buergisser & Lickteig 92].

MICHAEL LUBY

Efficient construction of a small hitting set for combinatorial rectangles in high dimension

Joint work with NATI LINIAL

Given d, m and ϵ, we deterministically produce a sequence of points S that hits every combinatorial rectangle in $\{0, \ldots, m-1\}^d$ of volume at least ϵ. Both the running time of the algorithm and $|S|$

are polynomial in d, m and $1/\epsilon$. This algorithm has applications to deterministic constructions of small sample spaces for general multivalued random variables.

O. B. LUPANOV

On the Realization Complexity of Iterations of Boolean Maps

Let $\mathcal{M} = \{\sigma_1, \ldots, \sigma_M\}$ be a set of binary strings of length n; let $\mathcal{S}_\mathcal{M}$ be the set of all one–to–one maps $\mathcal{M} \longrightarrow \mathcal{M}$. For any F from $\mathcal{S}_\mathcal{M}$ let $A_F(\tilde{x}, \tilde{y})$ be the following function:

$$A_F(\tilde{\sigma}, \tilde{\tau}) = \underbrace{F(F(\ldots F(\tilde{\sigma})\ldots))}_{|\tilde{\tau}| \text{ times}}$$

($|\tilde{\tau}|$ denotes the number, the binary notation of which is $\tilde{\tau}$.) Let us consider all possible extensions of F and A_F to the outside of $\mathcal{M}$. The complexity of a function f is defined to equal the minimal number of elements which is sufficient for the realization of f by a scheme of functional elements over the basis $\{\&, \vee, -\}$. Let $L^*(F)$ denote the complexity of the simplest extension of A_F to the outside of $\mathcal{M}$, and let

$$L^*(\mathcal{M}) = \max_{F \in \mathcal{S}_\mathcal{M}} L^*(F), \quad L^*(n, M) = \max_{\mathcal{M}} L^*(\mathcal{M}) .$$

Theorem. If $\frac{M}{\log n} \longrightarrow \infty$ then $L^*(n, M) \sim \frac{Mn}{\log_2(Mn)}$.

The proof of the Theorem is based on the principle of local coding of the author, along with certain version of the result of D. Uhlig on the simultaneous realization of a function on several strings (mass–production), some modifications of certain theorems on the complexity of partial functions (E.I. Nechiporuk, N.P. Redkin, A.E. Andreev) and some bounds of formula depth of certain functions (V.M. Khrapchenko); there is also a certain amount of "programming" in terms of circuits.

WOLFGANG MAASS

Bounds for the Computational Power and Learning Complexity of Analog Neural Nets

It is shown that high order feedforward neural nets of constant depth with piecewise polynomial activation functions and arbitrary real weights can be simulated for boolean inputs and outputs by neural nets of a somewhat larger size and depth with heaviside gates and weights from $\{0, 1\}$. This provides the first known upper bound for the computational power and VC–dimension of such neural nets. It is also shown that in the case of first order nets with piecewise linear activation functions one can replace arbitrary real weights by rational numbers with polynomially many bits, without changing the boolean function that is computed by the neural net. In order to prove these results we introduce two new methods for reducing nonlinear problems about weights in multi–layer neural nets to linear problems for a transformed set of parameters.

In addition we improve the best known lower bound for the VC–dimension of a neural net with w weights and gates that use the heaviside function (or other common activation functions such as σ) from $\Omega(w)$ to $\Omega(w \log w)$. This implies the somewhat surprising fact that the Baum–Haussler upper bound for the VC–dimension of a neural net with heaviside gates is asymptotically optimal.

Finally it is shown that neural nets with piecewise polynomial activation functions and a constant number of analog inputs are probably approximately learnable (in Valiant's model for PAC–learning)

KURT MEHLHORN

Variation on the Dictionary Problem

Joint work with PAUL DIETZ, RAJEEV RAMAN AND CHRISTIAN UHRIG

We consider the following *set intersection reporting* problem. We have a collection of initially empty sets and would like to process an intermixed sequence of n updates (insertions into and deletions from individual sets) and q queries (reporting the intersection of two sets). We cast this problem in the *arithmetic* model of computation of Fredman [JACM '82] and Yao [SIAM, J. on Comp. 85] and show that any algorithm that fits in this model must take time $\Omega(q + n\sqrt{q})$ to process a sequence of n updates and q queries, ignoring factors that are polynomial in $\log n$. We also show that this bound is tight in this model of computation, again to within a polynomial in $\log n$ factor, improving upon a result of Yellin [SODA '92]. Furthermore we consider the case $q = O(n)$ with an additional space restriction. We only allow to use m memory locations, where $m \leq n^{3/2}$. We show a tight bound of $\Theta(n^2/m^{1/3})$ for a sequence of $O(n)$ operations, again ignoring polynomial in $\log n$ factors.

Furthermore we present a data structure for maintaining a dynamic family of sequences under equality-tests. We allow to create new sequences by concatenating or splitting existing sequences without destroying them. The data structure supports equality-tests in $O(1)$ time and concatenates and splits in time $O(\log n(\log m \log^* m + \log n))$ where n is the length of the sequence and m is the number of the operations performed so far. The solution is deterministic and almost achieves the time bound of Sundar's randomized solution [FSTTCS '92].

FRIEDHELM MEYER AUF DER HEIDE

Computation with Integer Division

Joint work with KATHARINA LÜRWER-BRÜGGEMEIER

Computation trees with integer inputs and operations from $S \subseteq \{+, -, *, DIV, DIV_c\}$ are considered; DIV denotes integer division, DIV_c integer division by constants. It is shown that the expressive powers of different such operation sets are also different, if languages from $\mathbb{Z}^n$, $n > 1$, are considered. It was shown earlier by Just, Wigderson and the author that the expressive power of a set S is only dependent on whether DIV or DIV_c is in S or not, for $n = 1$.

We characterize the expressive powers of different operation sets.

Further we prove lower bounds, including the first lower bound for the powerful operation set $S = \{+, -, *, DIV\}$.

SILVIO MICALI

Fair Cryptosystems

We show that the secret decryption key of a public-key cryptosystem can be shared among several trustees so that no university of the trustees can reconstruct the secret key, while any majority of the trustees can easily compute it. Furthermore, upon receiving his own piece of the secret key, each trustee can verify (without any interaction with other trustees or with the owner of the public/secret key pair) that he indeed has a concret piece of the secret key. That is, each trustee can verify that, given any majority of shares that have satisfied a check similar to his own, the secret key of the given public key can be recomputed. This scheme can be used to achieve private (encrypted) communication among citizens of a democratic country while permitting court-authorized line tapping under the circumstances envisaged by the law.

PAVEL PUDLAK

Communication Complexity, Circuits and Tensor Rank

Joint work with V. RÖDL

For $i, j \in [0, n-1]$, $\bar{x} \in \{0,1\}^n$ let f be the function

$$f(i, j, \bar{x}) = x_{i+j} (\mathrm{mod} n) .$$

Suppose f should be computed by three players where

Player 0 knows i, j
Player 1 knows $j, \bar{x}$
Player 2 knows $i, \bar{x}$.

Players 1 and 2 send independently messages to Player 0 and he gives the value of $f(i, j, \bar{x})$.

Theorem. They need only $O(n \log\log n / \log n)$ to communicate.

RÜDIGER REISCHUK

Average Case Analysis

Joint work with CHRISTIAN SCHINDELHAUER

To measure the complexity in the average case Levin has proposed a modification of the classical measure, which is obtained by taking the expectation. His motivation was to overcome problems with the expectation when trying to set up a theory of average case complexity classes. But this new measure basically can only differenciate between polynomial and superpolynomial complexity. We define and analyse a new measure obtained from monotone transformations of the probability distributions. It is shown that in this case only the ranking of the inputs by decreasing probabilities matters. As a main result we obtain tight time hierarchy results for average case complexity classes comparable to those for worst case classes. Thus, this measure turns out to be very precise. Also, a tight separation with respect to the complexity of the distributions involved – their rankability – can be established. Finally, we consider reductions and completeness in this new approach and propose a classification of NP-problems with respect to their average case behaviour.

ADI SHAMIR

On the Generation of Multivariate Polynomials

In this talk we consider the difficulty of factoring multivariate polynomials $F(x, y, z, \ldots)$ modulo n. We consider in particular the case in which F is a product of two randomly chosen polynomials P and Q with algebraically specified coefficients, and n is the product of two randomly chosen primes p and q. The general problem of factoring F is known to be at least as hard as the factorization of n, but in many restricted cases (when P or Q are known to have a particular form) the problem can be much easier. The main result of this paper is that (with one trivial exception), the problem of factoring F is at least as hard as the factorization of n whenever P and Q are randomly chosen from the same sample space, regardless of what may be known about its form.

ALISTAIR SINCLAIR

Quadratic Dynamical Systems

Joint work with YURI RABINOVICH AND AVI WIGDERSON

Quadratic dynamical systems are widely used to model phenomena in the natural sciences, and serve as the basis for many computer simulations of these phenomena. Examples include population genetics and the kinetic theory of ideal gases. Less classically, they also provide an appropriate framework for the study of genetic algorithms for combinatorial optimization. In contrast to linear systems, which are well understood, there is little general theory available for the quantitative analysis of quadratic systems.

In this talk, we present several fundamental properties of the large class of symmetric quadratic systems acting on populations over a fixed set of types. We go on to give a complete analysis of one particular system, defined on populations over the set of matchings in a tree. In particular, it will turn out that convergence to the limit in this system requires only polynomial time. This demonstrates that such systems, though non-linear, are sometimes amenable to analysis.

ARNOLD SCHÖNHAGE

Power Sums mod p and a generalized Padé Approximation Problem

Over fields of characteristic zero parallel computation of matrix inverse A^{-1} or $\det A = \sigma_n$ (in the eigenvalues α_i of a) is easily done by computing $s_j = tr(A^j)$ for $1 \le j \le n$ and then using Newton identities. Here this approach is adopted to fields of characteristic $p \le n$. One computes some extra power sums s_j for $j \in J(p,n)$ = first n elements of $\mathbb{N} \setminus p\mathbb{N}$; from these sufficiently many coefficients $q_{k,i}$ in

$$\frac{a_k + a_{k+p}z + a_{k+2p}z^2 + \cdots}{1 + a_p z + a_{2p}z^2 + \cdots} = \sum_{i=0}^{\infty} q_{k,i} z^i \quad (1 \le k \le p-1)$$

are obtained; then the coefficients of the characteristic polynomial $f(t) = 1 + a_1 t + a_2 t^2 + \cdots + a_n t^n$ are determined by solving this Padé approximation problem.

Leslie Valiant

Models in Parallel Computation

Two aspects of the bulk-synchonous parallel (BSP) models of computation are described. First it is argued that this is an appropriate pragmatic model for expressing the parallel complexity of algorithms in a machine-independant manner. For problems such as sorting and Gauss-Jordan elimination, such transportable algorithms can be developed that are efficient to within a factor of 1 (asyptotically as the problem size increases), when compared with a corresponding sequential algorithm, for wide ranges of the parameters of the model. (Joint work with A. Gerbessiotis)
Second, an algorithm for performing combining for arbitrary concurrent access patterns is described. The algorithm requires no combining within the router. It recirculates the requests through the router a small number, m, of times and performs the neccessary combining at the processor nodes. For any $\epsilon > 0$, if there are at most p^ϵ requests from each of the p nodes, and if the requests are to an approximately hashed address space, then the algorithm takes time $(1 + o(1))mgp^\epsilon$ where $m = 1 + \lfloor \epsilon^{-1} \rfloor$ and g is time per message is charged. This is a factor of about m more than would be required on this model for access patterns requiring no combining.

Brigitte Vallée

On the average–case time complexity of the three algorithms: Euclid, Gauss, LLL

The aim of these algorithms is to build short bases for integer lattices; when dimension n is increasing, this is, first, the Euclid algorithm ($n = 1$), then the Gauss algorithm ($n = 2$), and finally the LLL algorithm ($n \geq 3$). We consider here the number L_M of iterations of these algorithms on integer inputs less than M. The average number $E(L_M)$ of iterations is a $O(\log M)$ for the Euclid algorithm [Heilbronn, Dixon, 1980], it is asymptotically constant for the Gauss algorithm [Vallée, Flajolet, 90]. It was shown [Daudé, Vallée, 91] that, for the LLL algorithm in n dimensions, the expectation $E(L_M)$ is upper-bounded by $O(n^2 \log n)$. We present here a variant of the LLL algorithm, called the Gram algorithm. This variant is very close to the original one, and we can show, under a very natural hypothesis, that the expectation $E(L_M)$ is bounded by $O(n)$.

Umesh Vazirani

Quantum Complexity Theory

Joint work with Ethan Bernstein

In its modern form, the Church-Turing thesis asserts that any reasonable (i.e. physically realizable) computing device can be simulated with at most a polynomial slowdown by a probabilistic Turing Machine. About a decade ago, Feynman pointed out that no straightforward simulation of a quantum physical system appeared possible without an exponential slowdown. A precise model of a quantum physical computer was formulated by Deutsch. His 'quantum Turing Machine' is the quantum mechanical analog of a probabilistic Turing Machine.
Our first result is the existence of a universal quantum TM. The first difficulty in designing a universal quantum TM is that even though a quantum TM is a finitely specified by its state transition diagram, it is a valid quantum TM only if it is time-reversible, or equivalently the corresponding time evolution operator (which is an infinite object) is unitary. We start by giving a completely local criterion for checking whether a quantum TM is well formed. The second interesting feature that distinguishes the construction of a universal quantum TM from the classical case is the conflicting requirement to preserve both the reversibility and the quantum interference. In full generality, on any given input a quantum TM produces a random sample from a probability distribution. We say that quantum TM

T simulates T' with accuracy ϵ, if on every input x T' outputs a sample from a distribution which is within total variation distance ϵ of the corresponding distribution for T. We prove that there is a universal quantum TM, which takes as input the description of a quantum TM T, and input x, and outputs an ϵ approximation to T(x). The slowdown is polynomial in $1/\epsilon$.
Our second result explores the computational power of the quantum Turing machine. Given any boolean function on n bits (specified by a program), we show how to sample from the Fourier spectrum of the function in polynomial time on a quantum computer. This problem is not known to be polynomially solvable on a classical computer. By specifying the function by an oracle, and building on the sampling problem using recursion, we show that there is an oracle relative to which quantum polyomial time is not contained in two–sided error $o(n^{\log n})$ time. This result gives the first evidence that quantum TMs might be more powerful than classical probabilistic TMs. A more careful analysis shows that relative to the same oracle, quantum polynomial time is not even contained in one round Arthur-Merlin in which the verifier has $o(n^{\log n})$ time.

Ingo Wegener

Graph Driven BDD's — A New Data Structure for Boolean Functions

Joint work with Detlef Sieling

(Ordered) binary decision diagrams (OBDD's) are used as data structure for Boolean functions in the logical synthesis process, for verification and test pattern generation, and as part of CAD tools. For several important functions like arithmetical and logical units with quite different functions, the indirect storage access function or the hidden weighted bit function OBDD's have exponential size for any ordering of the variables. Since an ordering of the variables may be stored as a list, ordered binary decision diagrams may be called also list driven BDD's. Two new generalized models of graph driven BDD's are presented. The above mentioned and many other functions can be represented in small polynomial size in this model and the usual operations on OBDD's can be performed efficiently also for graph driven BDD's.

Avi Wigderson

Undirected Connectivity in $O(\log^{1.5} n)$ Space

Joint work with Noam Nisan and Endre Szemeredi

We present a deterministic algorithm for the connectivity problem on undirected graphs that runs in $O(\log^{1.5} n)$ space. Thus, the recursive doubling technique of Savich which requres $O(\log^2 n)$ space is not optimal for this problem.

Berichterstatter: Michael Kaib

Tagungsteilnehmer

Prof.Dr. Helmut Alt
Institut für Informatik (WE3)
Freie Universität Berlin
Arnimallee 2-6

W-1000 Berlin 33
GERMANY

Dr. Eric Bach
Computer Science Department
University of Wisconsin-Madison
1210 West Dayton St.

Madison , WI 53706
USA

Dr. Ulrich Baum
Institut für Informatik V
Universität Bonn
Römerstr. 164

W-5300 Bonn 1
GERMANY

Ingrid Biehl
Fachbereich Informatik
Universität des Saarlandes
Im Stadtwald 15

W-6600 Saarbrücken 11
GERMANY

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

W-6600 Saarbrücken 11
GERMANY

Peter Bürgisser
Institut für Informatik
Universität Bonn
Römerstraße 164

W-5300 Bonn 1
GERMANY

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

W-5300 Bonn 1
GERMANY

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

University Park , PA 16 802
USA

Prof.Dr. Merrick L. Furst
School of Computer Science
Carnegie Mellon University
Schenley Park

Pittsburgh , PA 15213
USA

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

Toronto, Ontario , M5S 1A4
CANADA

Prof.Dr. Marc Giusti
Centre de Mathematiques
Ecole Polytechnique
Plateau de Palaiseau

F-91128 Palaiseau Cedex

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

Troy , NY 12180-3590
USA

Prof.Dr. Oded Goldreich
Computer Science Department
TECHNION
Israel Institute of Technology

Haifa 32000
ISRAEL

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

W-5300 Bonn 1
GERMANY

Prof.Dr. Shafi Goldwasser
Laboratory for Computer Science
MIT
545 Technology Square

Cambridge , MA 02139
USA

Peter Kirrinnis
Institut für Informatik II
Universität Bonn
Römerstraße 164

W-5300 Bonn 1
GERMANY

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

S-100 44 Stockholm

Dr. Jan Krajicek
Institute of Mathematics of the
CSAV
Zitna 25

115 67 Praha 1
CZECHOSLOVAKIA

Michael Kaib
Mathematisches Seminar
Fachbereich Mathematik
Universität Frankfurt
Grafstr. 38 u.39, Pf 11 19 32

W-6000 Frankfurt 1
GERMANY

Dr. Thomas Lickteig
Institut für Informatik V
Universität Bonn
Römerstr. 164

W-5300 Bonn 1
GERMANY

Prof.Dr. Michael Luby
International Computer Science
Institute
1947 Center Street
Suite 600

Berkeley , CA 94704-1105
USA

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

Cambridge , Ma 02139
USA

Prof.Dr. Oleg B. Lupanov
Moscow State University
Depart.of Mechanics & Mathematics
Chair of Algebra
Leninskie Gori

119899 Moscow
RUSSIA

Prof.Dr. Pavel Pudlak
Institute of Mathematics of the
CSAV
Zitna 25

115 67 Praha 1
CZECHOSLOVAKIA

Prof.Dr. Wolfgang Maass
Institut für Grundlagen der
Informationsverarbeitung
Technische Universität Graz
Klosterwiesgasse 32/II

A-8010 Graz

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

W-6100 Darmstadt
GERMANY

Prof.Dr. Kurt Mehlhorn
Max-Planck-Institut für Informatik
Im Stadtwald

W-6600 Saarbrücken
GERMANY

Prof.Dr. Claus-Peter Schnorr
Mathematisches Seminar
Fachbereich Mathematik
Universität Frankfurt
Gräfstr. 38 u.39, Pf 11 19 32

W-6000 Frankfurt 1
GERMANY

Prof.Dr. Friedhelm Meyer auf der Heide
FB 17: Mathematik - Informatik
Universität Paderborn-GH
Warburger Str. 100

W-4790 Paderborn
GERMANY

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

W-5300 Bonn 1
GERMANY

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

Rehovot 76 100
ISRAEL

Prof.Dr. Leslie G. Valiant
Aiken Computation Laboratory
Computer Science Division of
Applied Sciences
Harvard University

Cambridge , MA 02138
USA

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

W-5300 Bonn 1
GERMANY

Prof.Dr. Brigitte Vallée
Dépt. de Mathématiques
Université de Caen

F-14032 Caen Cedex

Prof.Dr. Alistair J. Sinclair
International Computer Science
Institute
1947 Center Street- Suite 600

Berkeley , CA 94704-1105
USA

Prof.Dr. Umesh V. Vazirani
Computer Science Division
University of California
at Berkeley
591 Evans Hall

Berkeley , CA 94720
USA

Prof.Dr. Hans-Jörg Stoss
Fakultät für Mathematik
Universität Konstanz
Postfach 5560

W-7750 Konstanz 1
GERMANY

Prof.Dr. Ingo Wegener
Institut für Informatik II
Universität Dortmund
Postfach 50 05 00

W-4600 Dortmund 50
GERMANY

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

W-7750 Konstanz 1
GERMANY

Prof.Dr. Avi Wigderson
Institute of Mathematics and
Computer Science
The Hebrew University
Givat-Ram

91904 Jerusalem
ISRAEL

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

e-mail addresses

BACH, ERIC (Madison)	bach@cs.wisc.edu
BAUM, ULRICH (Bonn)	uli@leon.informatik.uni-bonn.de
BIEHL, INGRID (Saarbrücken)	ingi@cs.uni-sb.de
BUCHMANN, JOHANNES (Saarbrücken)	buchmann@cs.uni-sb.de
BÜRGISSER, PETER (Bonn)	buerg@leon.cs.uni-bonn.de
CLAUSEN, MICHAEL (Bonn)	
FÜRER, MARTIN (University Park)	furer@cs.psu.edu
FURST, MERRICK (Pittsburgh)	mxf@cs.cmu.edu
v.z.GATHEN, JOACHIM (Toronto)	gathen@cs.toronto.edu
GIUSTI, MARC (CNRS)	
GOLDREICH, ODED (Haifa)	oded@cs.technion.ac.il
GOLDWASSER, SHAFI (Cambridge)	shafi@theory.lcs.mit.edu
HÅSTAD, JOHAN (Stockholm)	johanh@nada.kth.se
KAIB, MICHAEL (Frankfurt)	kaib@informatik.uni-frankfurt.de
KALTOFEN, ERICH (Troy)	kaltofen@cs.rpi.edu
KARPINSKI, MAREK (Bonn)	marek@cs.bonn.edu
KIRRINIS, PETER (Bonn)	kirr@informatik.uni-bonn.de
KRAJICEK, JAN (Praha)	
LICKTEIG, THOMAS, (Bonn)	lickteig@leon.informatik.uni-bonn.de
LUBY, MICHAEL (Berkeley)	luby@icsi.Berkeley.edu
LUPANOV, O.B. (Moscow)	lup@compnet.npimsu.msk.su
MAASS, WOLFGANG (Graz)	maass@figids01
MEHLHORN, KURT (Saarbrücken)	mehlhorn@mpi-sb.mpg.de
MEYER AUF DER HEIDE, FRIEDHELM (Paderborn)	
MICALI, SILVIO (Cambridge)	
PUDLAK, PAVEL (Praha)	
REISCHUK, RÜDIGER (Darmstadt)	reischuk@iti.informatik.th-darmstadt.de
SINCLAIR, ALISTAIR (Berkeley)	sinclair@icsi.berkeley.edu
SCHNORR, CLAUS-PETER (Frankfurt)	schnorr@informatik.uni-frankfurt.de
SCHÖNHAGE, ARNOLD (Bonn)	
SHAMIR, ADI (Revohot)	shamir@wisdom.weizmann.ac.il
SHOKROLLAHI, MOHAMMAD AMIN (Bonn)	
STRASSEN, VOLKER (Konstanz)	
VALIANT, LESLIE (Cambridge)	
VALLÉE, BRIGITTE (Caen)	vallee@geocub.greco-prog.fr
VAZIRANI, UMESH (Berkeley)	
WEGENER, INGO (Dortmund)	
WIGDERSON, AVLI (Jerusalem)	avi@cs.huji.ac.il

Programm der Tagung "Komplexitätstheorie"

Monday, 16.11.1992

Morning session. Chair: Shafi Goldwasser

9.00-9.15	Opening	
9.15-10.00	Silvio Micali	Fair Cryptosystems
10.10-10.50	Ingo Wegener	Graph Driven BDD's — A New Data Structure for Boolean Functions
11.10-11.55	P. Pudlak	Communication Complexity, Circuits and Tensor Rank

Afternoon session. Chair: Michael Luby

17.00-17.40	Wolfgang Maass	Bounds for the Computational Power and Learning Complexity of Analog Neural Nets
17.50-18.20	Peter Kirrinnis	Fast Computation of Numerical Partial Fraction Decompositions and Contour Integrals of Rational Functions

Tuesday, 17.11.1992

Morning session. Chair: Silvio Micali

9.00-10.00	Umesh Vazirani	Quantum Complexity Theory
10.05-10.35	Kurt Mehlhorn	Variation on the Dictionary Problem
10.45-11.30	Ulrich Baum	Computing Irreducible Representations of Supersolvable Groups
11.35-12.15	Eric Bach	Statistical Evidence for Small Generating Sets

Afternoon session. Chair: Kurt Mehlhorn

16.00-16.30	Leslie Valiant	Models in Parallel Computation
16.35-17.15	Peter Bürgisser	Decision Complexity of Generic Complete Intersections
17.25-17.55	Ingrid Biehl	Models for Average-Case Complexity
18.00-18.30	Friedhelm Meyer auf der Heide	Computation with Integer Division

Wednesday, 18.11.1992

Morning session. Chair: Avi Wigderson

8.45-9.15	Merrick Furst	Are Relevant Bits Hard to Find?
9.20-10.00	Michael Luby	Efficient Construction of a Small Hitting Set for Combinatorical Rectangles
10.05-10.50	Alistair Sinclair	Quadratic Dynamical Systems
10.55-11.25	Arnold Schönhage	Power Sums mod p and a generalized Padé Approximation Problem
11.30-12.00	Michael Kaib	A Sharp Worst-Case-Analysis of the Gauß Lattice Basis Reduction Algorithm for any Norm

Evening session. Chair: Ingo Wegener

19.30-20.15	O. B. Lupanov	On the Realization Complexity of Iterations of Boolean Maps

Thursday, 19.11.1992

Morning session. Chair: Merrick Furst

9.00-9.40	Marc Giusti	Complexity of Effective Nullstellensätze
9.45-10.25	Jan Krajicek	Complexity of Propositional Logic
10.35-11.15	Oded Goldreich	Towards a Theory of Statistical Tests
11.20-11.55	Shafi Goldwasser	Low-Error and Efficient Probabilistically Checkable Proofs; Applications to Approximation
12.00-12.30	Thomas Lickteig	On Randomized Algebraic Decision Complexity

Afternoon session. Chair: Umesh Vazirani

16.00-16.30	Erich Kaltofen	Parallel Sparse Linear System Solving
16.40-17.30	Marek Karpinski	An Approximation Algorithm for Counting the Number of Zeros of Polynomials over $GF(q)$
17.40-18.30	Brigitte Valleé	Average-Case Analysis of the LLL Algorithm

Friday, 20.11.1992

Morning session. Chair: Leslie Valiant

9.00-9.45	Avi Wigderson	Undirected Connectivity in $O(\log^{1.5} n)$ Space
9.50-10.35	Johan Håstad	The Shrinkage Constant is 2
10.40-11.00	Martin Fürer	Minimum Degree Steiner Tree Approximation
11.10-11.55	Rüdiger Reischuk	Average Case Analysis
12.00-12.30	Adi Shamir	On the Generation of Multivariate Polynomials which are Hard to Factor

Gefördert durch
DFG Deutsche Forschungsgemeinschaft