MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

Tagungsbericht 43/1996

Komplexitätstheorie

10.11. – 16.11.1996

Complexity Theory is concerned with the study of the intrinsic difficulty of computational tasks. Complexity Theory is a central field of Theoretical Computer Science, with a remarkable list of celebrated achievements as well as a very vibrant present research activity.

The 12$^{\text{th}}$ Oberwolfach Conference on Complexity Theory has been organized by Oded Goldreich (Rehovot), Joachim von zur Gathen (Paderborn) and Claus Peter Schnorr (Frankfurt).

The 1996 Meeting on Complexity Theory brought together about 50 scientists with a major interest in this field. Among them were many prominent senior researchers as well as many promising young researchers. They came from various countries in Europe, America and Asia.

The meeting took place November 10th-16th. It consisted of 6 General Sessions and 7 Specialized Sessions. The General Sessions hosted less than 20 talks, ranging from high-level expositions of various sub-areas and research directions in Complexity Theory to highly technical talks dedicated to a single recent result. The topics of the Specialized Sessions included

- Algebraic Complexity (2 sessions)
- Approximation Algorithms
- Boolean Function Complexity
- Cryptography and Coding
- Probabilistically Checkable Proofs

- Proof Complexity

Some of the Specialized Sessions took place in parallel and were marked by talks intended for experts in the sub-area. Some sessions had very detailed technical expositions of new results and one had an open-panel discussion in which many attendees took part. In total, there were about 3 dozen talks in the specialized sessions.

VORTRAGSAUSZÜGE

S. ARORA:

Polynomial-time Approximation Schemes for Euclidean TSP and other Geometric Problems

We give an algorithm that, given any $\varepsilon > 0$ and n points in the plane, finds a $1 + \varepsilon$-approximate travelings salesman tour in $n^{O(1/\varepsilon)}$ time.
The algorithm generalizes to points in $\mathbb{R}^d$; its running time then becomes $n^{O(\log^{d-2} n/\varepsilon^{d-1})}$.
It also generalizes to many other geometric Problems, including Minimum Steiner Tree, k-Minimum Spanning Tree, k-TSP, Degree-restricted Minimum Spanning Tree, etc.

P. BEAME:

New Directions in Propositional Proof Complexity

It is a fundamental open question, equivalent to one of the main outstanding questions of computational complexity, whether or not there is a method of proof that permits efficient proofs of all propositional tautologies. With this question as a lens, propositional proof complexity developed as a pleasing theory, settling questions of the relative efficiency of many traditional proof methods and, by focusing on the limitations of existing methods, raising the question of whether or not better proof methods could be found by escaping the confines of traditional approaches.
Over the last decade, powerful techniques from computational complexity have been combined with ideas from the method of forcing and from commutative algebra to produce remarkable advances in our understanding of traditional propositional proof methods, such as resolution and its generalizations.
One product of these new techniques has been a better understanding of the range of proof methods possible. As a result, several new methods of propositional proofs have been developed. Of particular note are new algebraic methods based

on Hilbert's Nullstellensatz which are in some cases provably more efficient than traditional methods and which have the promising feature that their associated search procedures are provably efficient relative to the size of the proof they seek. This talk will survey these new developments, particularly concentrating on applications of circuit complexity techniques and on the new algebraic proof methods.

M. BEN-OR:

Randomized Analytic Decision Trees

We present an $O(\log^2 n)$ depth randomized unbounded degree algebraic decision tree for finding the maximal element of a general n element set of real numbers. This generalizes the $O(\log^2 n)$ depth tree of Yao and Ting who solved this problem when all inputs are distinct.
Our second result is an $\Omega(n)$ lower bound for randomized analytic Decision Trees for verifying the median with polynomially small error probability (or $\Omega(n/\log n)$ lower bound for constant error rate).

M. BEN-OR:

Fault tolerant Quantum Computation

We present Quantum Computation Codes that can tolerate a constant error rate, thereby improving P. Shor's Computation Codes that could tolerate only polylogarithmicly small error rate.

U. FEIGE:

Zero knowledge and the Chromatic Number

A new approach is described for proving the hardness of approximating the chromatic number of a graph. This approach is inspired by zero knowledge proof systems. The main result is that the chromatic number cannot be efficiently approximated within a multiplicative factor of $O(n^{1-\varepsilon})$ unless NP has randomized expected polynomial time algorithms.

L. FORTNOW:

Resource-Bounded Kolmogorov Complexity Revisited

We take a fresh look at CD complexity, where $\mathrm{CD}^t(x)$ is the smallest program that distinguishes x from all other strings in time $t(|x|)$. We also look at a CND complexity, a new nondeterministic variant of CD complexity.

We show several results relating time-bounded C, CD and CND complexity and their applications to a variety of questions in computational complexity theory including:

- Showing how to approximate the size of a set using CD complexity avoiding the random string needed by Sipser. Also we give a new simpler proof of Sipser's lemma.
- A proof of the Valiant-Vazirani lemma directly from Sipser's earlier CD lemma.
- A relativized lower bound for CND complexity.
- Various other relationships and applications to complexity theory.

M. FÜRER:

Approximation of k-Set Cover by Semi-Local Optimization

We define a new approximation technique called semi-local optimization. It provides very natural heuristics that are distinctly more powerful than those based on local optimization. With an appropriate metric, semi-local optimization can still be viewed as a local optimization, but it has the advantage of making global changes to an approximate solution. Semi-local optimization generalizes recent heuristics of Halldórsson for 3-Set Cover, Color Saving, and k-Set Cover. Greatly improved performance ratios of 4/3 for 3-Set Cover and very close to 6/5 for Color Saving (i.e., for approximating n minus the number of colors used) are obtained and shown to be the best possible with semi-local optimization. Also, the performance ratio for k-Set Cover is improved.

M. GIUSTI:

The relevance of data structures for elimination problems

Solving elimination problems requires only a moderate amount of bit operations if one uses appropriate data structures (as e.g. straight-line programs) for the encoding of polynomials with integer coefficients. We present an elimination procedure whose bit complexity is polynomial in the input size and in the value of two suitably defined invariants which reflect the geometric degree and the arithmetic height of the input system. From our complexity bound we deduce by means of an appropriate effective Nullstellensatz a multivariate and intrinsic version of Liouville's classical theorem on approximation of algebraic numbers by rationals. Consequences for practically solving systems of polynomial equations are drawn.

Eventually we give as application a fast procedure to find a representative point in every connected component of a smooth compact real hypersurface defined by a polynomial with integer coefficients.

S. GOLDWASSER:

Property Testing with Applications to Learning and Approximation

We consider the question of determining whether a function f has property P or is ε-far from any function with property P. The property testing algorithm is given a sample of the value of f on instances drawn according to some distribution. In some cases, it is also allowed to query f on instances of its choice. We study this question for different properties and establish some connection to problems in learning theory and approximation.

In particular we focus our attention on testing graph properties. Given access to a graph G in the form of being able to query whether an edge exists or not between a pair of vertices, we devise algorithms to test whether the underlying graph has properties such as being bipartite, k-colorable, or having a ρ-clique (clique of density ρ w.r.t. the vertex set). Our graph property testing algorithms are probabilistic and make assertions which are correct with high probability, utilizing only a constant number of queries into the graph. Moreover, the property testing algorithms can be used to efficiently (i.e., in time linear in the number of vertices) construct partitions of the graph which correspond to the property being tested, if it holds for the input graph. For k-colorability this sheds new light on the problem of approximatly coloring a k-colorable graph.

D. GRIGORIEV:

Quadratic randomized lower bound for the knapsack problem

We prove a quadratic lower bound for the knapsack problem on a randomized computation tree. Formerly, a similiar bound for the deterministic computation trees was known. The proof relies essentially on the lower bound on the border complexity which could be of independent interest.

J. HÅSTAD:

Inapproximability results for Max SNP-hard optimization problems

Consider the problem of satisfying the maximal number of linear equations in an overdetermined system of linear equations. We prove that over $\mathbb{Z}_p$ this problem is NP-hard within $p-\varepsilon$ for all $\varepsilon > 0$. We also derive results for other Max SNP-hard problems like MAX SAT, MAX CUT and MIN VERTEX COVER.

E. KALTOFEN:

Polynomial factorization over high extensions of finite fields

Suppose $q = 2^k$, n an integer, and $k = O(n^{1+x})$ where $x > 0$. We present an algorithm that can factor a polynomial of degree n over a field with q elements in

$$O(n^{3+x+o(1)} + n^{2.69+1.69x})$$

fixed precision (i.e. bit) operations. Here the field is assumed to be represented by an irreducible polynomial of degree k mod 2. Our algorithm is a twist of the method by von zur Gathen and Shoup (1992) which would require $O(n^{3+2x+o(1)})$ fixed precision operations. Generalization to $q = p^k$ is possible.

M. KARPINSKI:

Randomized lower bounds for algebraic decision trees

We prove the first nontrivial lower bounds on the depth of randomized algebraic decision trees for problems being finite unions of hyperplanes and the intersections of halfspaces, solving a long standing open problem. As an application, among other things, we derive an $\Omega(n^2)$ randomized lower bound for the knapsack problem and the element distinctness problem. For the case of linear arrangements our proof method yields also a new elementary technique for deterministic algebraic decision trees without making use of Milnor's bound on Betti number of algebraic varieties.

L. LOVÁSZ:

A proof system of linear and quadratic polynomials

Given a family of linear inequalities, we can derive other inequalities valid for their 0–1 solutions by multiplying them by x_i or $1-x_i$, and then combining them with non-negative coefficients and with $x_i^2 = x_i$ so as to kill all quadratic terms. This proof system is complete. Further, this family of all inequalities derivable in $O(1)$ iterations has a polynomial time seperator routine. One can add steps of taking the square of any linear polynomial to get a stronger system with the same properties. One can use these results to design polynomial time algorithms for stable sets and other problems.

M. LUBY:

Practical Erasure Codes

We present encoding and decoding algorithms for erasure codes that can run in time $n \log(1/\varepsilon)$ (for both decoding and encoding) and have the guarantee that, with high probability over the random coin flips of the algorithm are able to decode the message of length Rn from any $(1+\varepsilon)Rn$ portion of the encoding. $R < 1$, n, and ε are input parameters of the algorithm.

E.W. MAYR:

Gröbner bases and space optimal normal form computation

We consider ideals in the polynomial ring $\mathbb{Q}[x_1, \ldots, x_n]$, given by a basis $p_1, \ldots, p_w$, and some test polynomial p. Given some term ordering $\prec$ on the monomials over $\{x_1, \ldots, x_n\}$, we can distinguish the (w.r.t. $\prec$) minimal polynomial in $p + < p_1, \ldots, p_w >$ as the uniquely determined normal form of p. We show that computing this normal form is EXPSPACE-complete, as is the computation of the uniquely determined reduced Gröbner basis for $< p_1, \ldots, p_w >$ together with $\prec$. Using Gröbner bases to compute normal forms would on the other hand, require doubly exponential space in the worst case.

C. MEINEL:

On the modular communication complexity

We show that the modular communication complexity of a problem can be exactly characterized in terms of the logarithm of a certain rigidity function of the communication matrix. Thus, we are able to exactly determine the modular communication complexity of several problems, such as e.g. set disjointness, comparability, and undirected graph connectivity. From the obtained bounds we can conclude exponential lower bounds on the size of depth-two-circuits having arbitrary symmetric gates at the bottom level and MOD_m-gates at the top.

M. NAOR:

Pseudo-random synthesizers

We introduce a new cryptographic primitive called pseudo-random synthesizer. It is a two-variable function $S(x, y)$ s.t. if polynomially many $x_1, \ldots, x_m$, $y_1, \ldots, y_m$ are chosen uniformly at random, the matrix defined by $S(x_i, y_j)$, $1 \leq i \leq m$, $1 \leq j \leq m$, is indistinguishable from a truly random one. We show how one can construct a pseudo-random function from a pseudo-random synthesizer in $\log n$ levels. We show an NC^1 construction of synthesizers based on either Diffie-Hellman assumption, RSA and a hard-to-learn function. In general, we can construct synthesizers from trapdoor permutations. Combining our results we achive an NC^2 construction of pseudo-random functions.

M. OGIHARA:

Recent progress on sparse hard sets

Sparse hard sets is the research area which investigates the problem whether difficult problems can be efficiently reduced to sets with small information content. In the 1990s we have seen remarkable progress in this research area, proven using highly combinatorial arguments. This talk reviews two such results: NP has no sparse $\leq^{\mathrm{p}}_{\mathrm{btt}}$-hard sets unless $\mathsf{NP} = \mathsf{P}$, and P has no sparse $\leq^{\mathrm{log}}_{\mathrm{m}}$-hard sets unless $\mathsf{P} = \mathsf{LOGSPACE}$.

L.M. PARDO:

Time-Space tradeoff lower bounds for univariate polynomial evaluation

In this talk I exhibit a new method for showing lower bounds for time-space tradeoffs of polynomial evaluation procedures given by straight-line programs.
From the tradeoff results obtained by this method we deduce lower space bounds for polynomial evaluation procedures running in optimal nonscalar time. Time, denoted by L, is measured in terms of nonscalar arithmetic operations and space, denoted by S, is measured by the maximal number of pebbles (registers) used during the given evaluation procedure. The time-space tradeoff function considered in this paper is LS^2.
We show that for "almost all" univariate polynomials of degree at most d our time-space tradeoff functions satisfy the inequality: $LS^2 \geq \frac{d}{8}$.
From this we conclude that for "almost all" degree d univariate polynomials, any nonscalar time optimal evaluation procedure requires space at least $S \geq c\sqrt[4]{d}$, where $c > 0$ is a suitable universal constant. In particular, this lower bound applies for the optimality in terms of space of the Paterson-Stockmeyer procedure for univariate polynomial evaluation. The main part of this talk is devoted to the exhibition of specific families of univariate polynomials which are "hard to compute" in the sense of time-space tradeoff (this means that our tradeoff function increases linearly in the degree).

P. PUDLÁK:

Interpolations theorems in propositional calculus

"Effective interpolation theorem" for a propositional proof system means that one can construct an interpolent $I(\overline{p})$ for an implication $\phi(\overline{p}, \overline{q}) \rightarrow \psi(\overline{p}, \overline{r})$ from its proof in polynomial time. We sketch an idea of a proof of such a theorem for cutting plane proof systems and discuss possible extension and limitations of this method of proving lower bounds on the lengths of proofs.

R. RAZ:

Sub-Constant Error Probability PCP Characterization of NP

We establish a new characterization of NP in terms of PCP, exhibiting a sub-constant error-probability with constant number of accesses.
Specifically, our theorems state the following:

- For any $\beta < 1$, membership in any NP language can be verified with a constant number of accesses, each reading $\log^{\beta} n \cdot \log\log^{c} n$ bits (for some fixed constant c), and such that the error-probability is at most $2^{-\log^{\beta} n}$.

- For any $\beta < \beta'$ (for some $0 < \beta' < 1$), membership in any NP language can be verified with a constant number of accesses, each reading $O(\log^{\beta} n)$ bits, and such that the error-probability is at most exponentially small in the number of bits read, i.e., $2^{-\log^{\beta} n}$.

Using known results, this new characterization of NP implies approximating set-cover to within logarithmic factors to be NP-hard.
The main technical lemma utilized for that purpose presents a new consistency-test, implying a new low-degree-test, which is the first to exhibit sub-constant error-probability with constant number of accesses.

R. REISCHUK:

Arthur-Merlin games within Small Space

Stochastic Turing machines are Turing machines that can perform nondeterministic and probabilistic moves. Such devices are also called games against nature, Arthur-Merlin games, or interactive proof systems with public coins. We investigate stochastic machines with space ressources strictly between constant logarithmic size and constant or sublinear bounds on the number of alternations between nondeterministic and probabilistic moves. Seperation results are proven for the corresponding complexity classes by showing the inclusion, resp. noninclusion of certain languages. The lower bounds hold without any restriction on the run time and will follow from general combinatorial properties. These results imply an infinite hierarchy with linear distance based on the number of alternations.
The seperations are obtained by extending and improving lower bound techniques developed for probabilistic automata and stochastic machines by which previously the lower levels have been seperated, resp. a hierarchy with exponential distance has been shown. Furthermore, we establish a hierarchy for stochastic Turing machines with arbitrary small nonconstant space bounds.

S. RUDICH:

Gaps, isomorphism and stop gaps

We show that all sets complete for NP under AC^0-reductions remain complete under NC^0-reductions. Furthermore, they are all isomorphic under AC^0-isomorphisms. This resolves the Berman-Hartmanis conjecture for the case of AC^0-reductions. We exhibit a set that is complete under $\mathsf{AC}^0[2]$-reductions, but not under AC^0-reductions. arbitrary small nonconstant space bounds.

M. SAKS:

Randomization and space bounded complexity

This talk is a historical survey of results about probabilistic space bounded complexity. The fundamental question in the area is whether any time bounded probabilistic computation can be simulated deterministically in log space. There has been substantial progress towards an affirmative answer to this question.

G. SCHNITGER:

Nondeterministic communication with a limited number of advice bits

We present a new technique to differentiate deterministic from nondeterministic communication complexity. As a consequence we give almost tight lower bounds for the nondeterministic communication complexity with a restricted number of advice bits (i.e., nondeterministic guesses). In particular, for any function $s : \mathbb{N} \to \mathbb{N}$ we construct a family $(L_n \ : \ n \in \mathbb{N})$ of languages such that

- $L_n \subseteq \{0,1\}^{2n}$,
- $\mathrm{ncc}_{s(n)}(L_n) = O(s(n))$ and $\mathrm{ncc}_{\log_2 n}(\overline{L_n}) = O(\frac{n \cdot \log_2 n}{s(n)})$,
- but $\mathrm{ncc}_{o(s(n)/\log_2 n)}(L_n) = \Omega(\frac{n}{\log_2(n/s(n))})$.

($\mathrm{ncc}_r(L)$ is the nondeterministic communication complexity of L, assuming that at most r advice bits are used for any input.) Thus, in contrast to probabilistic communication complexity, a small reduction in the number of advice bits results in almost maximal communication, *even* if the original number of advice bits is superlogarithmic. Moreover, also an almost maximal increase results, if “verified” nondeterminism (yes- and no-answers have to be error-free with the additional answer “?” allowed) is considered.

C.P. SCHNORR:

More RSA and Rabin bits are secure

We present a novel method for the deciphering of RSA-ciphertexts $E_N(x)$ with the help of an oracle that predicts the least significant bit of the message x with non-negligible advantage. The new method proceeds by refining approximations of random multiples of the message. The new method doubles the number of RSA-message bits that are simultaneously secure while it decreases the reduction time. We give practical and provable security guarantees for the RSA-random bit generator provided that factoring N or RSA-inversion is hard. With the new method we also invert the Rabin function $E_N(x) = x^2 \bmod N$

J.-P. SEIFERT:

Approximate Optima for Greatest Common Divisor Computations

We investigate the approximability of the following NP-complete (in their feasibility recognition forms) number theoretic optimization problems: given n numbers $a_1, \ldots, a_n \in \mathbb{Z}$, find a *minimum* gcd *set for* $a_1, \ldots, a_n$, i.e., a subset $S \subseteq \{a_1, \ldots, a_n\}$ with minimum cardinality satisfying $\gcd(S) = \gcd(a_1, \ldots, a_n)$, and given n numbers $a_1, \ldots, a_n \in \mathbb{Z}$, find a ℓ_∞*-minimum* gcd *multiplier for* $a_1, \ldots, a_n$, i.e., a vector $\mathbf{x} \in \mathbb{Z}^n$ with minimum $\max_{1 \le i \le n} |x_i|$ satisfying $\sum_{i=1}^n x_i a_i = \gcd(a_1, \ldots, a_n)$.
We present a polynomial-time algorithm which approximates a minimum gcd set for $a_1, \ldots, a_n$ within a factor $1 + \ln n$ and prove that this algorithm is best possible in the sense that unless $\mathsf{NP} \subseteq \mathsf{DTIME}(n^{O(\log\log n)})$, there is no polynomial-time algorithm which approximates a minimum gcd set within a factor $(1 - \varepsilon) \ln n$. Concerning the second problem, we prove under the slightly stronger complexity theory assumption, $\mathsf{NP} \not\subseteq \mathsf{DTIME}(n^{\mathrm{poly}(\log n)})$, that there is no polynomial-time algorithm which approximates a ℓ_∞-minimum gcd multiplier within a factor $2^{\log^{1-\gamma} n}$, where γ is an arbitrary small positive constant. Complementary to this result, there exists a polynomial-time algorithm, which computes a gcd multiplier $\mathbf{x} \in \mathbb{Z}^n$ for $a_1, \ldots, a_n \in \mathbb{Z}$ with $\|\mathbf{x}\|_\infty \le 0.5 \|\mathbf{a}\|_\infty$. We also present a simple polynomial-time algorithm which computes a gcd multiplier $\mathbf{x} \in \mathbb{Z}^n$ with Euclidean length $\|\mathbf{x}\| \le 1.5^n \|\mathbf{a}\| / \gcd(a_1, \ldots, a_n)$.

A. SHAMIR:

Differential fault analysis, or how to break cryptosystems by mistake

In this talk we describe a new method of cryptanalysis which is based on the idea of introducing computational errors by applying physical stress to sealed tamperproof devices. The model was first described in September 1996 by Boneh, Demillo and Lipton, who used it to break several public key cryptosystems. In this talk we extend the attack to virtually all the known secret key algorithms, and show, how to break it even when the structure of the cryptosystem is completely unknown.

M. SUDAN:

Decoding of Reed Solomon codes beyond the error correction bound

Given n pairs of points $\{(x_i, y_i)\}$, $1 \leq i \leq n$, from a field $\mathbb{F}$ and integers t and d, we present a polynomial time algorithm that reconstructs all degree d polynomials p s.t. $p(x_i) = y_i$ for at least t values of i, provided $t = \Omega(\sqrt{dn})$. The algorithm is deterministic if $\mathbb{F}$ is the field of real numbers or rationals and randomized if $\mathbb{F}$ is a field of finite characteristic. This provides a decoding algorithm for Reed Solomon codes which works beyond the error-correcting (BCH) bounds.

A. TA-SHMA:

$\mathsf{SL} \subseteq \mathsf{L}^{4/3}$

We show that undirected $s-t$-connectivity can be solved in $O(\log^{4/3} n)$ space. This improves the previous bound that was $O(\log^{3/2} n)$.
We also believe that the new derandomization technique we use might be useful in other cases.

S. VAUDENAY:

On Provable Security for Digital Signature Algorithms

In this paper we consider provable security for ElGamal-like digital signature schemes. We point out that the good the security criterion on the underlying hash function is pseudorandomness. We extend Pointcheval-Stern's results about the use of the random oracle model to prove the security of two variants of the US Digital Signature Algorithm against adaptive attacks which issue an existential forgery. We prove that a very practical use of the random oracle model is possible whith tamper-resistant modules.

I. WEGENER:

Optimal attribute-efficient learning of disjunction, parity, and threshold functions

Decision trees are a very general computation model. Here the problem is to identify a Boolean function f out of a given set of Boolean functions F by asking for the value of f at adaptively chosen inputs. For classes F consisting of functions which may be obtained from one function g on n inputs by replacing arbitrary $n-$

k inputs by given constants this problem is known as attribute-efficient learning with k essential attributes. Results on general classes of functions are known. More precise and often optimal results are presented for the cases where g is one of the functions disjunction, parity or threshold

V. WEISPFENNIG:

Complexity issues in Presburger Arithmetic and integer optimization

Presburger Arithmetic (PrA) is the first-order theory of integers in the language $L = \{0, 1, +, -, \leq, \{\equiv_n\}\}$. Replacing the constant number coefficients in L-terms by scalar variables or scalar-terms, we arrive at uniform Presburger Arithmetic (UPrA). Scalar variabels may not be quantified; operations on scalars are $0, 1, +, -, \cdot,$ lcm with cofactors and max. A bounded quantifier in UPrA is of the form $\exists x(0 \leq x \leq \alpha 1 \wedge \ldots)$ or $\forall x(0 \leq x \leq \alpha 1 \implies \ldots)$ for some scalar term α. Bounded quantifier elimination (BQE) is the reduction of an arbitrary formula to an equivalent formula having only bounded quantifiers.

Theorem 1. PrA and UPrA admit BQE in time polynomial $\ell^{O(n^b)}$, where ℓ is the formula-lngth, n the number of quantified variables and b the number of quantifier-blocks. Moreover, the length of atomic formulas grows polynomially.
2. Any BQE for PrA or UPrA requires doubly exponential space in the worst case.
3. UPrA does not admit quantifier elimination.

The theorem solves an open problem in a paper of van den Dries and Holly (1992). It has applications to parametric, non-necessary convex integer optimization with linear constraints and a linear or quadratic objective function.

A. WIGDERSON:

$\mathsf{P} = \mathsf{BBP}$ unless E has sub-exponential circuits: Derandomizing the XOR Lemma

Yao showed that the *XOR* of independent random instances of a somewhat hard Boolean function becomes almost completely unpredictable. In this talk we show that, in non-uniform settings, total independence is not necessary for this result to hold. We give a pseudo-random generator which produces n instances of the function for which the analog of the *XOR* lemma holds. This is the first derandomization of a "direct product" result. Our generator is a combination of two known ones — the random walks on expander graphs and the nearly disjoint subsets generator. The quality of the generator is proved via a new proof of the *XOR* lemma, which may be useful for other direct product results.
Combining our generator with the approach of Nisan, Wigderson and Babai, Fortnow, Nisan, Wigderson and the generator of Impagliazzo gives substantially

improved results for hardness vs. randomness trade-offs. In particular, we show that if any problem in $\mathsf{E} = \mathsf{DTIME}(2^{O(n)})$ has circuit complexity $2^{\Omega(n)}$, then $\mathsf{P} = \mathsf{BBP}$.

A. C.-C. YAO:

Branching programs, rectangular proofs, and transversal calculus

We investigate read-once branching programs for the following search problem: given a boolean $m \times n$ matrix, $m > n$, find either an all-zero row, or two 1's in some column. Our primary motivation is that this models regular resolution proofs of the pigeon principle PHP_n^m, which for $m > n^2$ has no known strong lower bounds for the length of such branching programs. Along a different line, we consider another class of resolution proofs which we call rectangular proofs (not necessarily regular), and derive exponential lower bounds. Finally, a natural proof system, transversal calculus, is introduced for estimating from below the transversal size of set families. We show that transversal calculus and rectangular proofs are strongly related.

A. C.-C. YAO:

Lower bounds for MAX finding

We present two results. The first one is an exponential lower bound on the minimum size of ternary bounded-degree algebraic decision tree for finding the maximum of n numbers. The second one is an $\Omega(\log^2 n)$ lower bound on the depth of probabilistic decision trees for finding maximum using $\chi : A$ $(A \subseteq \{\chi_1, \ldots, \chi_n\})$ as primitives.

D. ZUCKERMANN:

Asymptotically good codes correcting insertions, deletions and transpositions

We present efficiently encodable and decodable codes which have constant rate and correct a constant fraction of insertions and deletions. If the codewords are of length n, they also correct $\Omega(n/\log n)$ transpositions. All rates and error-correcting is optimal up to constant factors.

Berichterstatter: J.-P. Seifert