Report on the Dagstuhl-Seminar

"Structure and Complexity"

Organizers:
Klaus Ambos-Spies (Heidelberg)
Steven Homer (Boston)
Uwe Schöning (Ulm)

February 14-18, 1994

The seminar "Structure and Complexity" was the second Dagstuhl Seminar devoted to the structural aspects of Computational Complexity Theory. It was attented by 47 scientists who in 37 talks presented new results in this field. The following topics were among the main subjects covered by the talks: Kolmogorov complexity, resource bounded genericity and randomness, relativizations, descriptive complexity theory, and computational models.

PROGRAM

Eric Allender
Pseudorandom Sources and Oracles for BPP

Klaus Ambos-Spies
Genericity and Measure for Exponential Time

Ingrid Biehl
Definition and Existence of Super Complexity Cores

Ronald V. Book
On Collapsing the Polynomial-Time Hierarchy

Bernd Borchert
Predicate Classes and Promise Classes

Harry Buhrman
Separating PSPACE and EXP using autoreducibility

Gerhard Buntrock
On the Computational Power of Restricted Two-Pushdown Automata

Cristian Calude
Information and Randomness – An Overview

Anne Condon
Finite State Automata with Nondeterministic and Probabilistic States

Rod Downey
The Density Problem for Parameterized Polynomial Reducibilities

Mike Fellows
The Natural Degrees of Parameterized Complexity: Recent Results and Open Problems

Stephen Fenner
Inverting the Turing Jump in Complexity Theory

Lance Fortnow
The Role of Relativization in Complexity Theory

William Gasarch
Frequency Computation and Bounded Queries

Judy Goldsmith
Limits on Nondeterminism and Upward Collapse

Neil Immerman
NP-Completeness via Syntax

Birgit Jenner
Logspace Leaf Languages

Johannes Köbler
Nondeterministic Kolmogorov Complexity and Sparse Sets in NP

Phokion G. Kolaitis
How to Define a Linear Order on Finite Structures

Martin Kummer
Kolmogorov Complexity and its Relation to Instance Complexity

Jack H. Lutz
Feasible Martingales, Weak Completeness, and Strong Hypotheses

Elvira Mayordomo
Separating NP-Completeness Notions if NP is not Small

Christoph Meinel
Lower Bounds on the MOD_k- and MAJ-Communication Complexity of Various Graph-Accessability Problems

Martin Mundhenk
Reductions to Sparse Sets

Noam Nisan
Pseudorandomness for Network Algorithms

Kenneth W. Regan
The Block Move Model and Circuit Complexity

Rüdiger Reischuk
Average Case Complexity

Michel de Rougemont
Interactive Complexity in Graph theory

Rainer Schuler
Bounding Prover Complexity in Interactive Proof Systems

Thomas Schwentick
On Monadic NP

Alan Selman
Computing Solutions Uniquely Collapses the Polynomial Hierarchy

Thomas Thierauf
On the Correlation of Symmetric Functions

Leen Torenvliet
The Resource Bounded Injury Method

Paul Vitanyi
Two Heads are better than Two Tapes

Klaus W. Wagner
Complexity Classes Defined by Symmetric Leaf Languages

Jie Wang
An Average-Case Complete Word Problem for Finitely Presented Groups

Xizhong Zheng
n^k-Random Sets are Weakly Complete for Exponential Time

ABSTRACTS

Pseudorandom Sources and Oracles for BPP

Eric Allender
Rutgers University
(joint work with Martin Strauss, Rutgers University)

Lutz defined the notion of a pseudorandom oracle for BPP, and showed that almost every set in ESPACE is a source in this sense. We improve this result, showing that almost every set in PSPACE is a source. Using a new notion of measure for P, we show that the set of sources for BPP does *not* have measure 1 in P, although there are sources for BPP in AC^0. These results depend on our characterization of Pseudorandom Sources for BPP as exactly the Borel-normal binary sequences.

Our main result shows that, for almost every set A in E, $BPP^A = E^A$. (This improves an earlier result of Lutz, showing that this property holds for almost every $A \in$ ESPACE.) A similar construction can be carried out in PSPACE, although we do not know if it holds with measure 1.

Notions of measure for classes such as PSPACE and DTIME($T(n)$) for $T(n) << 2^n$ do not seem to relativize in a meaningful way. The talk concludes with speculation as to whether probabilistic methods can be applied in this way to yield fast simulations of BPP.

Genericity and Measure for Exponential Time

Klaus Ambos-Spies
Universität Heidelberg
(joint work with C. Neis, Freiburg, and S. Terwijn, Amsterdam)

We relate the genericity concepts of Ambos-Spies, Fleischhack and Huwig to Lutz's resource bounded measure. We show that the class of n^k-generic sets has p-measure 1. This allows us to simplify and extend some p-measure-1-results. We illustrate this approach by proving a new small span theorem for p-k-tt-reductions.

Definition and Existence of Super Complexity Cores

Ingrid Biehl
Universität des Saarlandes

I define and study *super complexity cores* of languages L with respect to classes $\mathcal{C}$ with $L \notin \mathcal{C}$. For example let $\mathcal{C} = \mathcal{P}$ and S be a super complexity core of L. Then S is infinite and for all polynomials $p \in I\!N[X]$ and all deterministic Turing machines M which output 1 on input $x \in S \cap L$ and which output 0 on input $x \in S \cap \overline{L}$ it follows that the running time of M on all but finitely many inputs $x \in S$ exceeds $p(|x|)$. I prove that for all non-empty, countable classes of languages $\mathcal{C}$ which are closed under finite variation, finite union and under complement and for all languages $L \notin \mathcal{C}$ it follows that such a super complexity core of L with respect to $\mathcal{C}$ exists. Moreover one can show: Given a recursively enumerable class $\mathcal{C}$ of recursive languages and a recursive language L. If there is a super complexity core of L with respect to $\mathcal{C}$, then there exists a recursive super complexity core too.

On Collapsing the Polynomial-Time Hierarchy

Ronald V. Book
University of California at Santa Barbara

Theorem: If for almost every oracle set A the polynomial-time hierarchy relative to A collapses, then the (unrelativized) polynomial-time hierarchy collapses.

Predicate Classes and Promise Classes

Bernd Borchert
Universität Heidelberg

Considering computation trees produced by polynomial time nondeterministic computations one can define a complexity class by any predicate on computation trees, such classes will be called *predicate classes*. It will be shown that these classes are exactly the principal ideals of the polynomial time many-one reducibility. Additionally, the set of classes – which will be called *recursive promise classes* – definable by recursive promise functions instead of predicates will be shown to be equal to the set of the recursively presentable ideals.

Separating PSPACE and EXP using autoreducibility

Harry Buhrman
Universidad Politecnica de Catalunya

We investigate the complete sets of all the levels of the Polynomial Time Hierarchy, PSPACE and EXP. We show that all the Turing complete sets for each level of the Polynomial Time Hierarchy as well as PSPACE are *autoreducible*. On the other hand we give some evidence for the existence of a Turing complete non-auto-reducible set for EXP, for we prove that for every k there exists a Turing complete set in EXP that is not auto-reducible with n^k adaptive queries. Improving this result to a non auto-reducible Turing complete set will (with the previous result) separate PSPACE from EXP. Since there are oracles where PSPACE = EXP, our results are in some sense optimal.

Addendum: Recently we have been informed that the results on the autoreducibility for PSPACE appear in "On Being Incoherent without Being Very Hard," by Richard Beigel and Joan Feigenbaum, journal Computational Complexity in 1992 (vol. 2, 1992, pp. 1-17).

On the Computational Power of Restricted Two-Pushdown Automata

Gerhard Buntrock
Universität Würzburg

We introduce a model of two pushdown automata without input tape (TPDA); i. e. the input is assumed to be in one of the pushdowns initially. With the concept of weight functions we define shrinking automata and prove that shrinking TPDA (sTPDA) characterize the growing context-sensitive languages. The fact that growing context-sensitive languages are contained in LOGCFL is sharpened to the containment in One-Way-LOGCFL. This is shown by using a characterization of One-Way-LOGCFL by oneway auxiliary pushdown automata with polynomial time and logarithmic space bounds (OWauxPDA). On the other hand it is shown that deterministic sTPDA (sDTPDA) cannot be simulated by deterministic OWauxPDA. Surprisingly for unambiguous GCSL we can give a simulation with unambiguous OWauxPDA.

Information and Randomness – An Overview

Cristian Calude
University of Auckland

We survey the core constructions and results in our forthcoming book *Information and Randomness – An Algorithmic Perspective* to be published by Springer-Verlag.

- philosophy of the book
- computers and complexities
- binary vs non-binary coding
- a model for random strings
- from random strings to random sequences

- topological methods in the study of randomness
- open problems.

Finite State Automata with Nondeterministic and Probabilistic States

Anne Condon
University of Wisconsin-Madison
(joint work with Lisa Hellerstein, Sam Pottle and Avi Wigderson)

We study finite automata with both nondeterministic and random states (npfa's). We restrict our attention to those npfa's that accept their languages with a small probability of error and run in polynomial expected time. Equivalently, we study Arthur-Merlin games where Arthur is limited to polynomial time and constant space.

Dwork and Stockmeyer asked whether these npfa's accept only the regular languages (this was known if the automaton has only randomness or only nondeterminism). We show that the answer is yes in the case of npfa's with a 1-way input head. We also show that if L is a nonregular language, then either L or its complement is not accepted by any npfa with a 2-way input head.

Toward this end, we define a new measure of the complexity of a language L, called its 1-tiling complexity. For each n, this is the number of tiles needed to cover the 1's in the "characteristic matrix" of L, namely the binary matrix with a row and column for each string of length at most n, where entry [x,y]=1 if and only if the string xy in L. We show that a language has constant 1-tiling complexity if and only if it is regular, from which the result on 1-way input follows. Our main result regarding the general 2-way input tape follows by contrasting two bounds: an upper bound of polylog(n) on the 1-tiling complexity of every language computed by our model, and a lower bound stating that the 1-tiling complexity of a nonregular language or its complement exceeds a function in $2^{\Omega(\sqrt{\log n})}$ infinitely often.

The last lower bound follows by proving that the characteristic matrix of every nonregular language has rank n for infinitely many n. This is our

main technical result, and its proof uses techniques of Frobenius and Iohvidov developed for Hankel matrices.

The Density Problem for Parameterized Polynomial Reducibilities

Rod Downey, Victoria University
(joint work with Mike Fellows)

A parameterized language is $L \in \Sigma^* \times N$. The talk studies the degree structure of parameterized languguages under parameterized reducibilities. For instance, we say $L_1 \leq_m^u L_2$ if there exist f, g, h, α such that $\langle x, k\rangle \in L_1$ iff $\langle f(x,k), g(x,k)\rangle \in L_2$ where the running times for f and g are $h(k)|x|^\alpha$ and $g(x,k) \leq h(k)$. If $h(k)$ is recursive, say that $L_1 \leq_m^s L_2$ (strong parameterized m-reducibility). Theorem: The strong parameterized m-degrees of recursive sets are dense. Open: is this true for $\leq_m^u$?

The Natural Degrees of Parameterized Complexity: Recent Results and Open Problems

Mike Fellows
University of Victoria, Canada
(Joint work with Rod Downey)

Many natural and important computational problems involve a parameter. For example, a large number of familiar computational problems take as input a graph G and a positive integer k. An important qualitative distinction concerns the complexity of such problems for fixed parameter values. Vertex Cover and Min Cut Linear Arrangement are examples of problems of this kind that can be solved in linear time for each fixed k, while the best known algorithms for Dominating Set and Bandwidth require time $O(n^{k+1})$. This qualitative distinction forms the basis of a theory of parameterized complexity that is widely applicable to concrete problems of combinatorial

computing. Recent classification and structural results and open problems will be surveyed. Among these new results, we show that W[t] is randomly reducible to Unique W[t], and formulate some problems about the computational power of bounded depth circuits for input of fixed Hamming weight that may shed some light on whether the W[t] hierarchy can be expected to be proper.

Inverting the Turing Jump in Complexity Theory

Stephen Fenner
University of Southern Maine

We investigate the range of the resource-bounded Turing jump for various complexity classes, in analogy with the Friedberg completeness criterion of recursion theory. We show that there is a PSPACE-hard set which is not in the complete polynomial-time Turing degree of PSPACE^A for any A. This set is $G \oplus \mathrm{QBF}$, where G is 1-generic. For NP, we conjecture that there is an NP-hard set that is not in the complete p-time Turing degree of NP^A for any A, and thus the NP-jump is not invertible in the sense of Friedberg. As evidence, we show that if any NP-hard set is not in the complete degree of NP^A for any A, then $G \oplus \mathrm{SAT}$ is also not jump invertible as well, where G is 1-generic. If $G \oplus \mathrm{SAT} \equiv_T^p \mathrm{SAT}^A$ for some A then we show a number of consequences, including NP$\neq$co-NP. Any proof of noninvertibility of the jump that involves 1-generic sets can be used to construct a recursive jump-noninvertible set.

The Role of Relativization in Complexity Theory

Lance Fortnow
University of Chicago

Several recent non-relativizing results in the area of interactive proofs have caused many people to review the importance of relativization. In this

talk we looked at how complexity theorists use and misuse oracles, paying special attention to the new interactive proof system and program checking results and trying to understand why these results do not relativize. We give some new results that may help us to understand these questions better.

Frequency Computation and Bounded Queries

William Gasarch
University of Maryland
(joint work with Richard Beigel, Yale)

For a set A and a number n let $F_n^A n(x_1, \ldots, x_n) = \chi_A(x_1) \cdots \chi_A(x_n)$. We study how hard it is to approximate this function in terms of the number of queries required. We obtain matching upper and lower bounds for the case $A = K$ (the halting set), A semirecursive, and (assuming $P \neq NP$) $A = SAT$. Some of our bounds depend on functions from coding theory.

Limits on Nondeterminism and Upward Collapse

Judy Goldsmith
University of Kentucky
(joint work with Richard Beigel, Yale)

We know that the Polynomial Hierarchy has the property that if the $k + 1^{st}$ level collapses to the k^{th} level, then all higher levels also collapse to the k^{th} level, and that this holds relative to any oracle. We consider two types of limits on nondeterminism, and their effects on upward collapse.

The first limit considered is the number of nondeterministic bits, or choices, each computation may make. Buss and Goldsmith considered a hierarchy of classes $N^m P_s$ based on polynomial time ($P_s = \cup_k \mathrm{DTIME}(n^s \log^k n)$) and $m \log n$ bits of nondeterminism, for constants m and s. They showed that upward collapse holds in both dimensions: if $N^1 P_s = P_s$ then $\forall r\ N^1 P_{m+r} = P_{m+r}$, and if $N^{m+1} P_s = N^m P_s$ then $\forall k\ N^{m+k} P_s = N^m P_s$.

Kintala and Fisher introduced a hierarchy of classes $\beta_k = NP[\log^k n]$ (NP with $\mathcal{O}(\log^k n)$ bits of nondeterminism) in NP. We show that padding arguments will not prove an upward collapse theorem for this hierarchy, since for any sets A, B, and C, with $1 \in A$ and $A \cap B = \emptyset$, there is an oracle relative to which

$$\forall i \in A\ \forall j \in B\ \forall k \in C[\beta_{i+1} = \beta_i \wedge \beta_{k+1 automat} \neq \beta_k \wedge \beta_j = \overline{\beta}_j].$$

The second type of limitation considered is the number of accepting computations. We say that $A \in k(n)UP$ iff there is a polynomial time NTM N such that $\forall x\ N(x)$ has no more than $k(|x|)$ accepting computations. Beigel showed that, for any polynomial function $k(n)$,there was an oracle relative to which the following classes are distinct: P, UP, $k(n)UP$, $(k(n)+1)UP$, $FewP$, and NP. Watanabe showed that, for k constant, $P = UP$ iff $\exists k\ P = kUP$ iff $\forall k\ P = kUP$. We do not know if upward collapse holds for the kUP hierarchy above P, but we show that the hierarchy defined by $U_{qk} = 2^{\log^k n}UP$ is also *malleable* in the sense that for any consistent set of collapses (above P) and separations, there is an oracle relative to which those collapses and separations hold.

NP-Completeness via Syntax

Neil Immerman
University of Massachusetts, Amherst
(joint work with J.Antonio Medina, Amherst)

Fagin proved in 1974 that NP is equal to the set of problems expressible in second-order existential logic (SO$\exists$). We consider problems that are NP-complete via first-order projections (fops). These low-level reductions are known to have nice properties, including the fact that every pair of problems that are NP-complete via fops are isomorphic via a first-order definable isomorphism. However, before this paper, fewer than five natural problems had actually been shown to be NP-complete via fops.

We give a necessary and sufficient syntactic condition for an SO$\exists$ formula to represent a problem that is NP-complete via fops. Using this condition we prove *syntactically* that 29 natural NP-complete problems remain complete via fops.

Logspace Leaf Languages

Birgit Jenner
Dept L.S.I., UPC Barcelona/ TU München
(joint work with Pierre McKenzie, Université de Montréal,
and Denis Thérien, McGill University)

In 1991, Bovet, Crescenzi and Silvestri used leaf languages in the context of polynomial-time computation to capture complexity classes and to study machine-independent relativizations. Given a "leaf language" $Y \subseteq \Sigma^*$, they (essentially) defined the class $\mathsf{Leaf}^P(Y)$ of all languages $A \subseteq \{0,1\}^*$ such that, for some nondeterministic polynomial-time Turing machine M, $x \in A$ iff $\mathit{leafstring}^M(x) \in Y$. Hertrampf *et al* in 1993 studied $\mathsf{Leaf}^P(Y)$ as a function of the complexity of Y. They proved for instance that $PSPACE$ and PH are attainable using appropriate regular languages.

In this talk, we investigate leaf languages of nondeterministic *logspace*-bounded Turing machines, and obtain characterizations of the classes $\mathsf{Leaf}^L(Y)$, where the logspace leaf languages Y ranges over a wealth of different complexities, e.g., subclasses of regular languages (the dot depth hierarchy, periodic p-groups, periodic solvable, solvable), regular, deterministic context-free, context-free, context-sensitive languages, languages in the logtime hierarchy, AC^0, NC^1, polylogtime, semi-unbounded circuits of depth $O(\log\log\ n)$, polylogspace, P, and NP. One's first intuition might be that a routine adaptation of known proofs will characterize these classes. However, new subtleties arise here; in particular, the intuition that the behavior of a complete language for a class C in a sense captures the behavior of all languages in C fails. For instance, let OR be the regular language $\{0,1\}^*1\{0,1\}^*$ and let $\leq_{dlogtime}(OR)$ denote the set of languages reducible to OR in $DLOGTIME$. We show that $\mathsf{Leaf}^L(OR) = NL$ and yet $\mathsf{Leaf}^L(\leq_{dlogtime}(OR)) = NP$, where $\mathsf{Leaf}^L(\text{class } C) = \cup_{Y \in C}\mathsf{Leaf}^L(Y)$. As another example, let REG denote the regular languages, known to contain NC^1-complete languages under $\leq_{dlogtime}$. We prove that $\mathsf{Leaf}^L(REG) = P$ and yet $\mathsf{Leaf}^L(NC^1) = PSPACE$. These results indicate that logspace leaf languages can be as powerful as polynomial-time leaf languages, when the class of leaf languages is closed under $\leq_{dlogtime}$; and in fact, it holds for arbitrary language Y, $\mathsf{Leaf}^P(\mathrm{Y}) = \mathsf{Leaf}^L(\leq dlogtime(Y))$.

In some cases our characterizations are similar on the surface to those previously known, yet which require completely different proofs. An exam-

ple of this situation is our challenging proof that $PSPACE = \mathsf{Leaf}^L(DCFL)$, a striking result nonetheless similar at first glance to the known characterization of $PSPACE$ as $\mathsf{Leaf}^P(DCFL)$ by Hertrampf *et al.*

Nondeterministic Kolmogorov Complexity and Sparse Sets in NP

Johannes Köbler
Universität Ulm
(joint work with V. Arvind, Madras, and M. Mundhenk, Trier)

We use the notion of nondeterministic time-bounded Kolmogorov complexity to show that there is a sparse subset of SAT in Θ_2^p that is hard under polynomial time many-one reductions for all sparse sets in NP. The proof uses ideas developed by Hartmanis to show that the sparse set $\mathrm{SAT} \cap K[\log n, n^2]$ is Turing complete for all sparse sets in NP. The nondeterministic Kolmogorov complexity of a string x with respect to a time bound t is defined as the size of the smallest input y for a universal nondeterministic transducer U such that U on input y produces on some path the output string x in time $t(|x|)$, but does not output any string different from x within time $t(|x|)$.

How to Define a Linear Order on Finite Structures

Phokion G. Kolaitis
University of California, Santa Cruz
(joint work with L. Hella and K. Luosto, University of Helsinki)

Descriptive complexity theory is the area of research whose goal is to unveil the relationship between the computational complexity of algorithmic problems and their expressibility in various logics on finite structures. Many results in descriptive complexity, including the well known characterization of PTIME in terms of fixpoint logic FP, require the existence of a "built-in" linear order on the classes of finite structures under consideration. This

phenomenon raises the question of analyzing the uniform definability of linear order on classes of finite unordered structures.

Notice that if C is a class of finite structures and L is a logic such that some formula of L defines a linear order on every structure in C, then every member of C must be a rigid structure, i.e., a structure whose only automorphism is the identity mapping. Our goal in the work reported here is to embark on a systematic investigation of the uniform definability of linear order on classes of finite rigid structures. We obtain upper and lower bounds for the expressibility of linear orders in various logics that have been studied extensively in finite model theory, such as fixpoint logic FP, partial fixpoint logic PFP, infinitary logic with finitely many variables, as well as the closures of these logics under implicit definitions. Moreover, we show that the upper and lower bounds established here can not be improved substantially, unless outstanding conjectures in complexity theory are resolved at the same time.

Kolmogorov Complexity and its Relation to Instance Complexity

Martin Kummer
Universität Karlsruhe

We treat the instance complexity as defined by Ko, Orponen, Schöning and Watanabe (1st Structures 1986; JACM, 1994). We show that for every nonrecursive set the instance complexity is at least logarithmic in the Kolmogorov complexity. Since the instance complexity of any recursive set is constant, we get a logarithmic gap between recursive and nonrecursive sets. As our main result we construct an r.e. nonrecursive set witnessing that this bound tight up to additive constants. This shows that the "instance complexity conjecture" of Orponen et. al. (1994) fails in its original form.

We also consider the polynomial-time bounded version of the conjecture and show that it holds for all recursive tally sets. Also, if P = NP then the conjecture holds, but there is a relativized world where is fails. In Orponen et. al. (JACM, 1994) a weak form of the conjecture is shown where the time-bounds depend on the complexity of A. We show that the dependence

on A can be removed. It follows that the polynomial-space bounded and the exponential-time bounded version of the conjecture hold.

Feasible Martingales, Weak Completeness, and Strong Hypotheses

Jack H. Lutz
Iowa State University

This talk surveys recent results on weak completeness, a measure-theoretic generalization of the completeness phenomenon, in the exponential time complexity classes E=DTIME(2^{linear}) and E_2=DTIME(2^{poly}). Particular attention is paid to the following three developments.

1. The use of feasible martingales (betting strategies computable in polynomial or quasi-polynomial time) enables us to investigate the internal measure structure of E and E_2. An element C of one of these classes is then *weakly* $\leq^{\text{P}}_{\text{m}}$*-complete* if the set $\text{P}_{\text{m}}(C)$, consisting of all languages $A \leq^{\text{P}}_{\text{m}} C$, does not have measure 0 in the class.

2. Let C_{E}, C_{E_2}, WC_{E}, WC_{E_2} be the sets of languages in E that are $\leq^{\text{P}}_{\text{m}}$-complete for E, $\leq^{\text{P}}_{\text{m}}$-complete for E_2, weakly $\leq^{\text{P}}_{\text{m}}$-complete for E, weakly $\leq^{\text{P}}_{\text{m}}$-complete for E_2, respectively. Let $\subset$ denote proper inclusion, then

$$C_{\text{E}} = C_{\text{E}_2} \subset WC_{\text{E}} \subset WC_{\text{E}_2}.$$

   (The fact that $WC_{\text{E}} \neq WC_{\text{E}_2}$ was observed by Juedes.)

3. The strong hypothesis, "SAT is weakly $\leq^{\text{P}}_{\text{m}}$-complete for E_2" is discussed. Recent work of Mayordomo, Juedes, and Lutz shows that this hypothesis has a number of reasonable consequences not known to follow from "P $\neq$ NP" or other traditional complexity-theoretic hypotheses.

Separating NP-Completeness Notions if NP is not Small

Elvira Mayordomo
Universidad de Zaragoza
(joint work with Jack H. Lutz, Iowa State University)

Under the hypothesis that NP does not have p-measure 0 (roughly, that NP contains more than a negligible subset of exponential time), it is shown that there is a language that is $\leq^{\mathrm{p}}_{\mathrm{T}}$-complete ("Cook complete"), but not $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete ("Karp-Levin complete"), for NP. This conclusion, widely believed to be true, is not known to follow from P $\neq$ NP or other traditional complexity-theoretic hypotheses.

Evidence is presented that "NP does not have p-measure 0" is a reasonable hypothesis with many credible consequences. Additional such consequences proven here include the separation of many truth-table reducibilities in NP (e.g., k queries versus $k+1$ queries), the class separation E $\neq$ NE, and the existence of NP search problems that are not reducible to the corresponding decision problems.

Lower Bounds on the MOD $_{\mathbf{k}}$- and MAJ-Communication Complexity of Various Graph-Accessability Problems

Christoph Meinel
Universität Trier
(joint work with Stephan Waack, Universität Göttingen)

We give some new lower bounds on the complexity of various graph accessibility problems. Beside of the ordinary GAP=(GAP$_N$), $N = n^2 - n$ where n is the number of nodes, we consider the counting variants MOD$_m$-GAP = (MOD$_m$-GAP$_N$), m arbitrary. Deriving some lower bounds on the variation-rank of certain matrices being mod-k-equivalent, or order-equivalent to certain communication matrices, respectively, in the end we are able to generalize the well-known lower bound on the deterministic communication complex-

ity $\mathrm{comm}(\mathrm{GAP}_N) = \Omega(n)$ to the MOD_k- as well as to the MAJ-communication complexity mode:

$\mathrm{MOD}_k\text{-comm}(\mathrm{GAP}_N)$, $\mathrm{MOD}_k\text{-comm}(\mathrm{MOD}_k\text{-}\mathrm{GAP}_N) = \Omega(n)$

$\text{MAJ-comm}(\mathrm{GAP}_N)$, $\text{MAJ-comm}(\mathrm{MOD}_k\text{-}\mathrm{GAP}_N) = \Omega(n)$

Reductions to Sparse Sets

Martin Mundhenk
Universität Trier
(joint work with V. Arvind, Madras, and J. Köbler, Ulm)

We define a type of restricted oracle machine, called *monotonous* oracle machine and show how to charaterize different types of polynomial-time reducibilities by polynomial-time oracle machines which are monotonous, positive, or non-adaptive, or combinations thereof (cf. Ladner, Lynch, and Selman (1975)). For example, we show that A conjunctively reduces to B iff $A = L(M_{mp}, B)$ for an oracle machine M_{mp} which is (at the same time) monotonous *and* positive. Structural properties of classes consisting of sets which are decidable by those oracle machines using tally or sparse oracles are considered. We locate self-reducible sets A contained in these classes into the generalized low hierarchy in the following way: if $A = L(M_{mp}, S)$ and $\overline{A} = L(M'_{mp}, S')$ for monotonous *and* positive M_{mp}, M'_{mp} and sparse sets S, S', then A is low in NP; if $A = L(M_m, S)$ or if $A = L(M_{mp}, \overline{S})$ for a monotonous M_m resp. monotonous *and* positive M_{mp} and sparse S, then A is low in P^{NP}. This extends results by Karp and Lipton (1980), and by Lozano and Torán (1991).

Pseudorandomness for Network Algorithms

Noam Nisan
Hebrew University
(joint work with Russell Impagliazzo and Avi Wigderson)

We define pseudorandom generators for Yao's two-party communication complexity model and exhibit a simple construction, based on expanders, for it. We then use a recursive composition of such generators to obtain pseudorandom generators that fool distributed network algorithms. While the construction and the proofs are simple, we demonstrate the generality of such generators by giving several applications.

The Block Move Model and Circuit Complexity

Kenneth W. Regan
State University of New York at Buffalo

At the 1992 "Structures Dagstuhl," I introduced a model of computation in which the basic operations are *block moves* of the form

$$S[a_1 \ldots b_1] \textit{ into } [a_2 \ldots b_2].$$

Here S is a finite transducer (specifically, a DGSM) that reads some string z from $[a_1 \ldots b_1]$ and writes its output $S(z)$ into $[a_2 \ldots b_2]$. The output overwrites the previous content of $[a_2 \ldots b_2]$, except that any blank B output by S leaves its target cell unchanged.

At this meeting I discussed the characterization of uniform circuit classes by the classes $\mathrm{BM}^k(\mathcal{V})$ of languages accepted in $O(\log^k n)$ block moves and polynomial work by BMs allowed to use DGSMs from the variety $\mathcal{V}$. The intent is to extend work by Barrington, Straubing, Thérien, et al. from NC^1 to classes higher in the NC hierarchy, and also to refinements of AC^0.

Theorem [Regan, STACS'94]: For all $k \geq 1$, $\mathrm{BM}^k(d{:}e \text{ homomorphisms}) = \mathrm{NC}^k$.

Problem: For all $k \geq 0$, is $\mathrm{BM}^k(\text{aperiodic}) = \mathrm{AC}^k$?

Problem: For all $k \geq 0$, is BM^k(all DGSMs) properly contained in NC^{k+1}?

I also described problems in sequential complexity for the BM. The sequential time for a block move is $|z| + a^{1/d}$, where $a = \max\{a_1, b_1, a_2, b_2\}$ and d is a parameter that reflects the dimension of the memory. I sketched a Kolmogorov complexity technique that gives tight nonlinear lower bounds for a certain string-editing problem of $\Omega(n \log n)$ for $d = 1$, and $\Omega(n \operatorname{loglog} n)$ for $d > 1$. The intent is to extend these bounds to natural problems such as sorting, FFTs, integer mutliplication, and universal hashing, for which no nonlinear lower bounds on Turing machines are yet known. This led to interesting problems about nonoblivious branching programs.

Average Case Complexity

Rüdiger Reischuk
TH Darmstadt
(joint work with A. Jakoby and C. Schindelhauer)

We give an overview on current work concerning average case complexity. Computational models and complexity measures for a meaningful average case analysis are discussed. We define Turing Machine average case complexity classes with respect to sets of distributions and show hierarchies for these classes. For the circuit model a concept of average delay is introduced. It makes use of the observation that in certain cases a gate can compute its value at an earlier step than what is given by its depth. We also define a notion how to measure the complexity of a probability distribution D within the circuit model. For this purpose depth-bounded circuits are considered that transform a uniform random vector into a random variable with distribution D.

For explicitely defined Boolean functions almost matching upper and lower bounds can be obtained this way. In several cases an exponential speedup of the average delay compared to the worst case is achieved. Finally, we investigate the asymptotic behaviour of average delay complexity. Among others, it can be shown that for almost all Boolean functions of n

arguments the average delay is at least n - log n - loglog n -1, that means at most log n smaller than the worst case delay.

Interactive Complexity in Graph theory

Michel de Rougemont
Universite Paris Sud
(joint work with J.M. Couveignes, J.F. Diaz-Frias, M. Santha)

We give an interactive protocol for $s-t$ RELIABILITY, the well known reliability problem on graphs. Our protocol shows that if $IP(f(n))$ denotes the class of languages whose interactive complexity is $O(f(n))$, that is the set of languages which can be accepted by an interactive proof system with $O(f(n))$ number of rounds, then $s-t$ RELIABILITY $\in IP(n)$. This complexity is significantly smaller than what one could get via reduction to QBF, tha standard $PSPACE$-complete language. Another interesting aspect of our protocol is that it includes a general method to deal with rational numbers in interactive proof systems.

Bounding Prover Complexity in Interactive Proof Systems

Rainer Schuler
Universität Ulm
(joint work with V. Arvind, Madras, and J. Köbler, Ulm

We consider the complexity of MIP protocols with bounded prover complexity. We prove that for every language in FewEXP there is an MIP protocol such that the prover complexity is bounded by $\mathrm{NP}^{\mathrm{FewEXP}}$. Next we show that the class of languages accepted by MIP protocols with provers in P/poly is low for Σ_2^p. As a consequence it follows that for any class $\mathcal{C}$ whose languages have prover-complexity bounded by $\mathrm{P}^{\mathcal{C}}$, if $\mathcal{C} \subseteq$ P/poly then $\mathcal{C}$ is low for Σ_2^p. Stronger consequences follow if $\mathcal{C}$ is also closed under complement. Finally, we show that MIP protocols with provers that are polynomial-time reducible to $\log^*$-sparse or strong-P/log sets accept precisely languages in BPP.

On Monadic NP

Thomas Schwentick
Universität Mainz

We introduce a new method for proving that duplicator has a winning strategy in Ehrenfeucht games on finite structures. As applications we show: (1) There is a class of graphs that can be characterized in Monadic CoNP without any built-in relations, but not in Monadic NP even in the presence of a built-in linear order. (2) If a certain group-theoretical conjecture is true, then connectivity cannot be expressed in Monadic NP, even in the presence of a built-in linear order. (3) Monadic NP is strictly more powerful in the presence of a built-in linear order than in the presence of a built-in successor relation.

Computing Solutions Uniquely Collapses the Polynomial Hierarchy

Alan Selman
SUNY at Buffalo
(joint work with Lane Hemaspaandra, Ashish Naik, and Mitsunori Ogiwara)

Is there a single-valued NP function that, when given a satisfiable formula as input, outputs a satisfying assignment? That is, can a nondeterministic function cull just one satisfying assignment from a possibly exponentially large collection of assignments? We show that if there is such a nondeterministic function, then the polynomial hierarchy collapses to its second level.

The second part of the talk is described in the next abstract.

On P-selective sets and Adaptive versus Nonadaptive Queries to NP

Alan Selman
SUNY at Buffalo
(joint work with Jin-Yi Cai and Ashish Naik)

We show that if there exists a p-selective set that is NP-hard under truth-table reductions, then every function that is computable in polynomial time by truth-table access to an NP oracle is computable in polynomial time by making at most $O(\log n)$ queries to an NP oracle. As a consequence, it follows that if there exists a tt-hard p-selective set for NP, then for all $k > 0$, $NP \subseteq DTIME[2^{n/\log^k n}]$.

Reporting progress on the question of whether every function that is computable in polynomial time by truth-table access to an NP oracle is computable in polynomial time by making at most $O(\log n)$ queries to an NP oracle, we show that if there is a constant k such that

$$\mathrm{PF}^{\mathrm{NP}}_{n^k\text{-tt}} \subseteq \mathrm{PF}^{\mathrm{NP}}[k\lceil \log n \rceil - 1],$$

then P = NP.

On the Correlation of Symmetric Functions

Thomas Thierauf
Universität Ulm
(joint work with Jin-Yi Cai and Frederic Green)

The correlation between two Boolean functions of n inputs is defined as the number of times the functions agree minus the number of times they disagree, all divided by 2^n. We derive a closed form for the correlation between any two *symmetric, periodic* Boolean functions. Our main corollary is that every symmetric function having an odd period has an exponentially small correlation (in n) with the parity function. This result is an improvement of a result of Smolensky restricted to symmetric Boolean functions: if q is odd, the fraction of agreement between parity and a circuit consisting of a Mod_q gate over AND-gates of small fan-in is $\frac{1}{2} + 2^{-n^{\Omega(1)}}$, if the function computed by the sum of the AND-gates is symmetric. In addition, we find that for a large class of symmetric functions the correlation with parity is *identically* zero for infinitely many n. We characterize exactly those symmetric Boolean functions having this property.

The Resource Bounded Injury Method

Leen Torenvliet
University of Amsterdam
(joint work with Harry Buhrman, Universidad Polytècnica de Catalunya)

In this paper we present a new method of diagonalization that is a refinement of the well-known finite injury priority method discovered independently by Friedberg and Muchnik in 1957. In the *resource bounded injury method*, it is necessary in addition to proving that the number injuries for a given requirement is finite to carefully count these injuries and prove that this number does not exceed a bound given by the index of the requirement. The method is used to construct an oracle relative to which the polynomial time hierarchy collapses to an extent that the second level of this hierarchy (P^{NP^A}) captures nondeterministic exponential time. This oracle is an answer to an open problem posed by Heller in 1984 that has thus far resisted existing methods and that has recently regained interest by work of Fu et. al. and by work of Homer and Mocas. Moreover, our oracle provides a constructive counterexample to Sewelson's conjecture that does not make use of information theoretical lowerbounds, and answers several other questions.

Two Heads are better than Two Tapes

Paul Vitanyi
CWI/University of Amsterdam
(joint work with Tao Jiang and Joel Seiferas)

Consider two variants of Turing machines (TM) with linear tapes: the version with two heads on a single worktape (called a two-head machine) and the version with two heads on two separate worktapes (called a two-tape machine). Whether or not two-head machines are more powerful than two-tape machines in real-time has remained open for at least 25 years. We settle the problem by proving that a two-tape machine cannot simulate a queue in real-time. The techniques used are Kolmogorov complexity, symmetry of information, a novel notion of holographic coding, and the incompressibility method.

Complexity Classes Defined by Symmetric Leaf Languages

Klaus. W. Wagner
Universität Würzburg
(joint work with Katja Cronauer and Ulrich Hertrampf)

A language $L \subset \Sigma^*$ defines the complexity class L-P by using nondeterministic polynomial time machines that produce for an input x on every computation path a symbol from Σ. The input is accepted if the string of all these symbols is in L. A theorem by Bovet, Crescenzi and Silvestri says that , given two leaf languages L_1 and L_2, L_1-P$\subseteq$ L_2-P in every relativized world if and only if L_1 is polylogtime m-reducible to L_2. We make this criterion easier to apply for the subclass of symmetric leaf languages, i.e. the languages where membership depends only on the number of occurences of each symbol and not on their position in the word. We assign to every symmetric language some easy-to-compute charcteristics which are preserved by the polylogtime m-reducibility. So, for many complexity classes defined by symmetric leaf languages (like NP, 1NP, $\oplus$P, PP, C=P) we obtain as an immediate consequence oracle separation results, some of them already known and some new ones.

An Average-Case Complete Word Problem for Finitely Presented Groups

Jie Wang
University of North Carolina at Greensboro

Ever since Levin (1986) proved that randomized tiling is average-case NP-complete, researchers have been working very hard to find more average-case complete problems in the areas such as algebra and graph theory. This paper presents an average-case NP-complete problem for finitely presented groups, which is a bounded version of Novikov and Boone's theorem stating that there is a finitely presented group with an unsolvable word problem. Our result indicates that it is hard on the average-case to answer a bounded

sequence of elementary questions about finitely presented groups. Our word problem is defined as follows:

Instances: A finitely presented group $G = [A; R]$, strings u, v, w, and a unary notation 1^n for a positive integer n, where $A = \{a_1, ..., a_l\}$ of symbols and $R = \{s_1, ..., s_m\}$ of statements on relations, all coded in binary form.

Question: Is $(u^{-1}vu)w = w(u^{-1}vu)$ using relations for at most n times?

Probability: Uniform distribution proportional to

$$\frac{2^{-(|u|+|v|+|w|+\sum_{i=1}^{l}|a_i|+\sum_{i=1}^{m}|s_i|)}}{l^2m^2n^2\Pi_{i=1}^{l}|a_i|^2\Pi_{i=1}^{m}|s_i|^2}.$$

Theorem The word problem defined above is average-case NP-complete.

n^{k}-Random Sets are Weakly Complete for Exponential Time

Xizhong Zheng
Nanjing University
(joint work with Klaus Ambos-Spies)

We show that any n^k-random set A in $E = DTIME(2^{\text{lin}})$ is weakly complete, i.e. the class of the predecessors of A under p-m-reducibility has nonzero p-measure in E. This implies extensions of Lutz's recent results that there is a weakly complete set in E which is not p-m-complete for E in two directions: First we see that the class of weakly complete sets in E has measure 1 in E; Second, for any $k \geq 1$ we obtain a weakly complete set in E which is not p-k-tt-complete.

PLAY

Roomer: Room, room, give us room to play,
In winter in Saarland, when icy blows the breeze,
and and brooks and rivulets have a tendency to freeze,
we come to bring you action, drama, poetry and more,
as you can see, we're all complexity hard core.
If you don't believe what I do say, step in Prover,
and prove away.
Prover: In comes I, the prover bold, with eyes of green and logic cold.
Theorems rise up for me to meet, lemmas fall down at my feet.
My vitae is long, my career is rising,
although my colleagues think I'm compromising.
This formula I'll show is in SAT
[enter Formula]
Verifier, what do you think of that?
If you don't believe what I do say,
come in verifier, and query away.
Verifier: In comes I, the verifier,
with random bits and heart of fire.
I interact with all and sundry,
and someone else does my laundry.
Your lemmas I'll challenge, your theorems disprove
You'll lose your job and have to move.
I think your career I will end right here,
so why not sit down first and have a beer?
Prover: Your challenge I scorn, I can prove what I claim,
as long as you interact within the rules of the game.
I'll write all my bits and make you decide
which ones I'll show and which ones I'll hide.
I'll always be right, you'll look like a fool,
and I'll never let down my professional cool.
Verifier: Which interaction will you choose?
Prover: It doesn't matter, since you're gonna lose.
Verifier: We should use MIP.
Prover: We can't do that, it's only me.

Verifier: Coins are public, don't you see?
Prover: Private coins don't bother me.
Verifier: How many coins will you allow?
Roomer: Shut up, you're making such a row!
[P. and V. circle each other, brandishing pointers.]
Verifier: Weak prover!
Prover: Logspace verifier!
Verifier: Oracle lover!
Formula I resemble that remark!
Verifier: Algebraic entity!
Prover: Now do your job and verify.
If it's wrong you're gonna die.
[P. lifts up pointer and stabs F., who is behind him. F. dies dramatically.]
Roomer: You've killed it! Is there a doctor in the house?
10 marks for a doctor! 20? 20 marks 10 pfennig!
Doctor: I'm a doctor.
Roomer: We're all doctors in this schloss!
How did you get to be a doctor?
Doctor: I traveled for it.
Roomer: Where did you travel?
Doctor: To Italy, Spitaly, France and Spain,
to Boston and Dagstuhl and back again.
Roomer: What can you cure?
Doctor: I can cure the itch, the stitch, the palsy and the gout,
the pains within and the pains without.
Combinatorial quirks, hung screens, and oracle blues,
false counterexamples, trivial theorems, and pc news.
Roomer: Did my paper get in?
Doctor: I can't tell you, but for 3 coauthorships and 5 citations,
I'll nod yes or no.
Roomer: Too expensive.
Doctor: How about 2 papers and 4 acknowledgements?
Roomer: A theorem and a beer – that's my final offer.
Doctor: Okay. *[nods ambiguously]* Where's the patient?
Roomer: There.
[Dr. looks at a member of the audience, mutters about a terrible case, consults a very large algorithms book, ...]

Roomer: Not that one, this one *[points to corpse].*

Doctor: That's too bad – I could have cured that one.

waves the algorithms book threateningly].

Roomer leads Doctor to the dead formula. The Dr checks pulse in patient's ankle holds mirror to F's stomach, then preens in the mirror. R. gets irritated.]

Roomer: The patient. The patient!

Doctor: Oh, yes. How long has this been dead?

Roomer: Two parallel sessions. Can you cure it?

Doctor: Why, I could cure it if it had been disproved 20 times! I have here in the waistcoat of my pocket, a little book with the solutions to all our problems *[pulls out Vitanyi and Li].* It says here to open at random, and read. *[He does so. Nothing happens.]*

Roomer: He's still dead.

Doctor: Well, it says here that the probability of this occurrence is very small, but perhaps I can find another cure.

[A phone rings. The Doctor pulls a phone receiver from his bag and answers it. The receiver is not attached to anything.]

Doctor: It's for you – they want to discuss the budget for your grant.

[Formula leaps up and starts arguing about the budget....]

Formula: ... At least half a grad student. I need a half a grad student. The half with a brain, of course....

Roomer: Our play is ended, and now we will go,
so enjoy the music, and on with the show.

Production notes, Dagstuhl, Feb. 1994. The players were Judy Goldsmith as Roomer, Mike Fellows as Prover, Lance Fortnow as Formula, Steve Fenner as Verifier, and Harry Buhrman as Doctor. Fellows' Prover said his colleagues sometimes thought he was parametrizing, *and Fenner's Verifier jumped in backwards, with* In jump I,.... *The text was adapted by Gasarch and Goldsmith from a traditional English mummers' play.*