Klaus Ambos-Spies, Steven Homer,
Uwe Schöning (editors):

Structure and Complexity Theory

Dagstuhl-Seminar-Report; 30
3.-7.2.92 (9206)

ISSN 0940-1121

Copyright © 1992 by IBFI GmbH, Schloß Dagstuhl, W-6648 Wadern, Germany
Tel.: +49-6871 - 2458
Fax: +49-6871 - 5942

Das Internationale Begegnungs- und Forschungszentrum für Informatik (IBFI) ist eine gemeinnützige GmbH. Sie veranstaltet regelmäßig wissenschaftliche Seminare, welche nach Antrag der Tagungsleiter und Begutachtung durch das wissenschaftliche Direktorium mit persönlich eingeladenen Gästen durchgeführt werden.

Verantwortlich für das Programm:
Prof. Dr.-Ing. José Encarnaçao,
Prof. Dr. Winfried Görke,
Prof. Dr. Theo Härder,
Dr. Michael Laska,
Prof. Dr. Thomas Lengauer,
Prof. Ph. D. Walter Tichy,
Prof. Dr. Reinhard Wilhelm (wissenschaftlicher Direktor)

Gesellschafter: Universität des Saarlandes,
Universität Kaiserslautern,
Universität Karlsruhe,
Gesellschaft für Informatik e.V., Bonn

Träger: Die Bundesländer Saarland und Rheinland-Pfalz

Bezugsadresse: Geschäftsstelle Schloß Dagstuhl
Informatik, Bau 36
Universität des Saarlandes
W - 6600 Saarbrücken
Germany
Tel.: +49 -681 - 302 - 4396
Fax: +49 -681 - 302 - 4397
e-mail: office@dag.uni-sb.de

PROGRAM

Eric Allender, Rutgers University
A Uniform Circuit Lower Bound for the Permanent

Klaus Ambos-Spies, Universität Heidelberg
On the Theory of the Polynomial Degrees of Exponential Time Sets

Vikraman Arvind, Indian Institute of Technology, Delhi
Conjunctive (and other) Reductions to Sparse Sets

José L. Balcazar, U. Politecnica de Catalunia, Barcelona
Characteriazations of Logarithmic Advice Complexity Classes

Ronald V. Book, University of Santa Barbara
On Languages with High Information Content

Harry Buhrman, University of Amsterdam/ILLC
Structure of Complete Sets for Exponential Time

Rod Downey, Victoria University of Wellington, New Zealand
A Completeness Theory for Parameterised Intractability

Lance Fortnow, University of Chicago
Gap-Definable Counting Classes

Willian I. Gasarch, University of Maryland, U.S.A.
Some Open Problems in Concrete Complexity

Johan Håstad, Royal Institute Stockholm
Majority Gates us General Weighted Threshold Gates

Lane A. Hemachandra, University of Rochester
Access to Unambiguous Computation

Ulrich Hertrampf, Universität Würzburg
Locally Definable Acceptance Types

Steven Homer, University of Boston
Reductions to Sparse and Almost-Sparse Sets

Neil Immerman, University of Massachusetts, Amherst
Tradeoffs in Descriptive Complexity

Birgit Jenner, Technische Universität München
A Note on LOGSPACE OPTIMIZATION

Johannes Köbler, Universität Ulm
The Power of the Middle Bit

Martin Kummer, Universität Karlsruhe
Frequency Computation and Bounded Queries

Klaus-Jörn Lange, Technische Universität München
Oblivious PRAMs Characterize P, NC^k, and $DSPACE(logn)$

Timothy J. Long, Ohio State University
The Structure of the Extended Low Hierarchy

Christoph Meinel, Universität Trier
Separating Complexity Classes Related to Bounded Alternating ω-Branching Programs

André Nies, Universität Heidelberg
The Theory of the Polynomial Many-one Degrees of Recursive Sets is Undecidable

Kenneth Regan, SUNY Buffalo
Parsimonious and Truly Linear Time Computation

Uwe Schöning, Universität Ulm
Graph Isomorphism is Low for PP

Thomas Schwentick, Universität Mainz
On the Power of One Bit of a $\#P$-Function

Alan L. Selman, SUNY Buffalo
A Taxonomy of Complexity Classes of Functions

Theodore A. Slaman, University of Chicago
On The Complexity Types of Recursive Sets

Jacobo Torán, U. Politecnica de Catalunia, Barcelona
On the Non-uniform Complexity of the Graph Isomorphism Problem

Peter van Emde Boas, University of Amsterdam
Embedding is as Hard as Separation

Paul Vitányi, CWI & University of Amsterdam
Learning Simple Concepts under Simple Distributions

Klaus W. Wagner, Universität Würzburg
Complexity of Functions vs. Complexity of Sets

A Uniform Circuit Lower Bound for the Permanent

Eric Allender
Rutgers University
(Joint work with V. Gore, Rutgers University)

We show that there are sets in PP that are not accepted by uniform ACC circuits of subexponential size, and that there are no subexponential-size uniform ACC circuits computing the permanent.
This is in contrast to the fact that it remains an open question if $D\text{time}(2^{\text{Poly}})$ is contained in non-uniform ACC. This seems to be the first proof of a lower bound in circuit complexity where uniformity plays an essential role.

On the Theory of the Polynomial Degrees of Exponential Time Sets

Klaus Ambos-Spies
University of Heidelberg

We show that the theory of the polynomial Turing degrees of the Exponential Time sets has infinitely many 1-types. As a consequence this theory - and, relative to some oracle, the theory of the p-T-degrees of the NP-sets - have a nonstandard model.
We obtain the types by considering a hierarchy of bounded distributivity notions. To realize these types we consider a hierarchy of very sparse sets – called k-supersparse ($k \geq 1$) – which automatically induce some distributivity but leave enough room for enforcing certain nondistributive configurations by diagonalization.

Conjunctive (and other) Reductions to Sparse Sets

Vikraman Arvind
Indian Institute of Technology, Delhi
(Joint work with J. Han, L. Hemachandra, J. Köbler, A. Lozano, M. Mundhenk, M. Ogiwara, U. Schöning, T. Thierauf)

We study the consequence of complete sets for various complexity classes reducing conjunctively in polynomial time to a sparse set. One such central result is that if an NP-complete set conjunctively reduces in polynomial time to a sparse set then $P = NP$. Indeed, we establish similar consequences with far more flexible, polynomial time reductions. Another problem we study is: if a set A is reducible to a sparse set then how hard need the sparse set be relative to the set A? We partially answer this question by giving upper-bound results

for various types of truth-table reductions. Turning to a different, but related, problem we give a complete characterization of IC [log, poly] (languages of low instance complexity) as the intersection of polynomial-time conjunctive and disjunctive closure of tally sets.

Characteriazations of Logarithmic Advice Complexity Classes

José L. Balcazar
U. Politecnica de Catalunia, Barcelona
(Joint work with Montserrat Hermo and Elvira Mayordomo)

The complexity classes P/log and Full-P/log, corresponding to the two standard forms of logarithmic advice for polynomial time, are studied. The novel proof technique of "doubly exponential skip" is introduced, and characterizations for these classes are found in terms of several other concepts, among them easy-to-describe boolean circuits and reduction classes of tally sets with high regularity. Similar results hold for many other complexity classes.

On Languages with High Information Content

Ronald V. Book
University of Santa Barbara
(Joint work with Jack Lutz)

Language B is in HIGH if for every polynomial q, $KS^q(B_{\leq n}) > 2^{n+1} - 2n$ a.e.
Languages in HIGH have essentially maximal information content. Almost every language is in HIGH, that is, $\text{PROB}_A[A \in \text{HIGH}] = 1$.

Main Theorem: Let $A \in \text{DSPACE}(2^{lin})$ and let $k > 0$ be an integer. If there exists $B \in \text{HIGH}$ such that $A \leq^p_{k-tt} B$, then there exists a sparse set S such that $A \leq^p_{k-tt} S$.

Corollary Let $K \in \{NP, PP, MOD_qP(q \geq 1), PSPACE)$. If there exists $B \in \text{HIGH}$ such that B is $\leq^p_{btt}$-hard for K, then $K = P$.

Corollary No set in HIGH is $\leq^p_{btt}$-hard for Dtime (2^{lin}).

Structure of Complete Sets for Exponential Time

Harry Buhrman
University of Amsterdam/ILLC

We investigated the structure of exponential time complete sets. We considered the robustness of the completeness notion, with respect to substraction of "sparse" easy to compute sets. We proved that for $\leq^p_{2tt}$ - complete sets, this does not destroy the completeness. Furthermore we look at the mitoticity of exponential time complete sets; can we split a complete set A into A_0 and A_1, $A_1 \cap A_0 = \emptyset$, $A_1 \cup A_0 = A$ and A_0 and A_1 are both complete again.
We prove that this is indeed the case for $\leq^p_m$ - complete sets. Furthermore we showed the existence of a $\leq^p_{2tt}$ - complete set that is not m-mitotic.
These results can be found in the paper: "ROBUSTNESS AND SPLITTINGS OF EXPONENTIAL TIME COMPLETE SETS"
Buhrman, H.; Hoene, A.; Torenvliet, L. (Manuscript, avialable via email from: buhrman@fwi.uvd.nl).

A Completeness Theory for Parameterised Intractability

Rod Downey
Victoria University of Wellington, New Zealand

This work, jointly with Mike Fellows of the University of Victoria, British Columbia, concerns the structure of P-time. Some of the work is also with Karl Abrahamson of Washington state. It is meant to capture the fact that many classically intractable problems such as graph genus have tractable parameterised versions (fix k ; does g have genus k, is $0(|g|^3)$ by the Robertson-Seymour theorem), and there are other problems such as 2CNF-SAT having intractable parameterised versions (fix k; does X have a satisfying asignment with exaclty k literals true?).
Furthermore virtually all classical NP reductions do not carry the structure of the problems, that is they show that problems one has a solution if problem two does, but say nothing about the spectrum of solutions.
We have a completeness theory to explain the above phenomena. It seems to be very rich and widely applicable. It is still full of open questions.

Gap-Definable Counting Classes

Lance Fortnow
University of Chicago
(Joint with Steve Fenner, Stuart Kurtz)

The function class $\#P$ lacks an important closure property; it is not closed under subtraction. To remedy this problem, we introduce the function class Gap-P as a natural alternative to $\#P$. Gap-P is the closure of $\#P$ under subtraction, and has all the other useful closure properties of $\#P$ as well. We show that most previosly studied counting classes, including PP, $C{=}P$, and Mod_kP are "gap-definable", i. e. definable using the values of Gap-P functions alone. We show that there is a smallest gap-definable class, SPP, which is still large enough to contain Few. We also show that SPP consists of exactly those languages low for Gap-P and thus SPP languages are low for any gap-definable class. These results unify and improve earlier desparate results of Cai & Hemachandra and Köbler, Schöning, Toda & Torán. We show further that any countable collection of languages is contained in a unique minimum gap-definable class, which implies that the gap-definable classes form a lattice under inclusion. Subtraction seems necessary for this result, since nothing similar is known for the $\#P$-definable classes.

Some Open Problems in Concrete Complexity

Willian I. Gasarch
University of Maryland, U.S.A.

Let $F(x_i, \ldots, x_m)$ be a boolean formula. Normally it takes m probes to evaluate. Are there natural example that can be evaluated in less than m probes? Yes! (That wasn't the open problem.) The thing to look at is the group of permutations that preserve the function. Let $\Gamma_F = \{0 \in S_m : F(x_1, \ldots, x_m) = F(x_{0(1)}, \ldots, x_{0(m)})\}$ We can study what happens, if Γ_F has certain properties. If Γ_F is <u>transitive</u> then the following is known

1. $\exists\ F(x_1, \ldots, x_m)$ can be evaluated in $\sqrt{m}$ probes.
2. If $F(0) \neq F(1)$, m is prime power, <u>requires</u> m probes.
3. Monotone graph properties require $\Omega(n^2)(n = \#$ of vertices). We have looked at $\Gamma_F = \mathbb{Z}_m$. We have
   1. $\exists\ F(x_1, \ldots, x_m)$ can do $\frac{m}{2} + O(\sqrt{m})$ probes.
   2. if $n = pq$, $p << q$, $F(0) \neq F(1)$, require n probes.

Majority Gates vs. General Weighted Threshold Gates

Johan Håstad
(Joint work with Mikael Goldmann and Alexander Razborow)

We study small-depth polynomial size circuits that contain threshold gates (with or without weights) and parity gates. We prove

1. A single threshold gate with weights cannot in general be replaced by a polynomial fan-in unweighted threshold gate of parities.
2. On the other hand it can be replaced by a depth 2 unweighted threshold circuit at polynomial size. In general can depth d weighted threshold circuit be computed by depth $d+1$ unweighted threshold circuits (constant d).
3. A polynomial fan-in threshold gate (with weights) at parity gates cannot in general be replaced by a depth 2 unweighted threshold circuit of polynomial size.

Access to Unambiguous Computation

Lane A. Hemachandra
University of Rochester
(Joint work with J. Cai and J. Vyskoč)

We study the power of three types of access to unambiguous computation: nonadaptive access, fault-tolerant access, and guarded access. Though for NP it is known that nonadaptive access has exponentially succinct adaptive simulations, we show that UP does not robustly admit any non-trivial simulations. Though fault-tolerant access to NP is known to be no more powerful than NP itself, we give structural and relativized evidence that fault-tolerant access to UP suffices to recognize even sets beyond UP. Finally, we show that promise probabilistic classes, under fault-tolerant access, are characterized as standard probabilistic classes, and we show that "guarded" access to unambiguous computation seems to bestow great power upon adaptive reductions.

Locally Definable Acceptance Types

Ulrich Hertrampf
University of Würzburg

We introduce k-valued locally definable acceptance types, a new model generalizing the idea of alternating machines and their acceptance behaviour. The model can be described as follows:

Let F be a set of functions from k-valued logic. Let M be an F-machine, i.e. a machine where the computation tree on a given input x associates with each node a function from $F \cup \{id\} \cup$ constant functions, such that the arity coincides with the number of successors. Evaluate the tree from the leaves to the root. Let $L(M) := \{x : \text{the root evaluates to } 1\}$. Define $F(P) := \{L(M) : M \text{ is an } F\text{-machine }\}$.
We prove a normal form theorem for finite sets F:
$\forall\, F\ \exists\, g : g$ is a binary function and $(F)P = (\{g\})P$.

If F is a set of boolean functions, i. e. $k = 2$, then $(F)P$ is one of $P, NP, coNP, \oplus P, PSPACE$. (Post 1921, Goldschlager, Parberry 1986.)

We show for $g : \{0,1,2\}^2 \to \{0,1,2\}$ that $(\{g\})P$ is one of 20 classes including $\Sigma_2^p, \Pi_2^p, \Delta_2^p, \Theta_2^p$, as well as $P^{NP}[1]$ or MOD_3P.
We give several closure properties of the system of classes definable as $(F)P$ for some set F, including closure under the operations $co-, \exists, \forall$, but also restricted types of $\leq_{k-tt}^p$-closure and several types of Turing-closure.

Reductions to Sparse and Almost-Sparse Sets

Steven Homer
University of Boston
Joint work with Luc Longpré and Harry Buhrman

The consequences of polynomial-time reductions from NP-complete sets to sets of polynomial and other subexponential densities are considered. For $\leq_m^p$ and $\leq_{btt}^p$ reductions the methods of Ogiwara and Watanabe and of Homer and Longpré are used to show that if $SAT \leq_m^p S$ and S has subexponential density then NP is contained in subexponential time. Next the results of Karp and Lipton concerning $\leq_T^p$-reductions to sparse sets are extended. In particular, if $SAT \leq_T^p S$ and $||S|| \leq 2^{\text{POLYLOG}}$ then the exponential-time hierarchy collapses to the second level. Finally, it is suggested that a single approach might be found which yields both the theorem of Ogiwara and Watanabe and the results of Karp and Lipton.

Tradeoffs in Descriptive Complexity

Neil Immerman
University of Massachusetts, Amherst

In descriptive complexity one analyzes the computational complexity of a property in terms of the complexity of describing the property in first-order logic. A property is a set of finite, ordered structures of some vocabulary. The quantifier-depth and number of

variables needed to express the property is closely related to the parallel time and amount of hardware needed to check whether an input has the property. For a long time, the basic question of complexity – namely what are the trade-offs between time and hardware – has remained quite open. We have been attempting to understand this question in terms of the trade-off between number of variables and quantifier-depth. In this talk we demonstrate a tight relationship between number of variables and deterministic space. We show that the set of properties checkable by a Turing machine in DSPACE[n^k] is exactly equal to the set of properties describable by a uniform sequence of first-order sentences using at most $k+1$ distinct variables. We suggest some directions for exploiting this result to derive trade-offs between the number of variables and the quantifier-depth in descriptive complexity.

A Note on LOGSPACE OPTIMIZATION

Birgit Jenner
Technische Universität München

Logspace optimization functions compute the maximum of all output values of an NL-transducer. The corresponding class $optL$ was shown to lie between NL^*, the class of NL-functions, and AC^1. Some characterizations of NL^* in terms of restricted $optL$-functions were discussed and it was claimed that $optL$ could be a candidate of a fairly natural function class in AC^1 that might not be contained in LOGCFL*. It was shown that the problem of computing the $(MAX, \circ)$ iterated matrix product of wordmatrices with entries from $\{0,1\}^* \cup \perp$ (where $\perp$ is an additional absorbing element for $\circ$) is complete for $optL$. This nicely contrasts $optL$ with the logspace country class $\# L$ for which computing the iterated matrix product of positive integer matrices is complete.

The Power of the Middle Bit

Johannes Köbler
Universität Ulm
(Joint work with Frederic Green a. Jacobo Torán)

We study the class of languages that can be recognized in polynomial time with the additional information of one bit from a $\# P$ function. In particular we show that every MOD_k class and every class contained in PH are low for this class.
We translate these results to the area of circuit complexity using MidBit (middle bit) gates. A MidBit gate over m inputs $x_1, \ldots, x_m$ is a gate which outputs the value of the $\lfloor log(m)/2 \rfloor$ the bit in the binary representation of the number Σx_i. We show that every language in ACC can be computed by a family of depth-2 deterministic circuits of size 2^{POLYLOG} with a MidBit gate at the root and AND-gates of famin POLYLOG at the leaves.

Frequency Computation and Bounded Queries

Martin Kummer
Universität Karlsruhe

We presented an overview of some recent results from [1], [2], concentrating on the inclusion structure of the classes of (m, n)-recursive and (m, n)-verbose sets. Also their polynomial-time analogs were treated. For the verbose-classes, a complete description of the inclusion relation and an explicit description of the quality relation is obtained. For frequency-classes, we have an explicit solution of the equality in the general recursive case, and a decision procedure for the inclusion problem in the polynomial-time case. The complementary question are still open.

[1] Kummer, M., Stephan, F.
Some aspects of frequency computation
Interner Bericht Nr. 21/91, Fak. für Informatik, Univ. Karlsruhe (1991)

[2] Beigel, R., Kummer, M., Stephan, F.
Quantifying the amount of verboseness
Manuscript (-LaTeX version available via email from: kummer@ira.uka.de) (1992)

Oblivious PRAMs Characterize P, NC^k, and DSPACE($log\ n$)

Klaus-Jörn Lange
Technische Universität München

Usually, PRAMs are classified according to their ability to access the global memory simultaneously. A new classification concerning the communication structure and its dependence of the input is introduced. By requiring *oblibious* CRCW-PRAMs to use indirect addressing in read and/or write statements independently of the actual input, we get new characterizations of classes like P, NC^k, and DSPACE($log\ n$). These investigations were motivated by some attempts to classify those PRAM algorithms which are efficiently implementable on existing parallel machines.

The Structure of the Extended Low Hierarchy

Timothy J. Long
Ohio State University

Balcázar, Book, and Schöning introduced the extended low hierarchy based on the Σ-levels of the polynomial-time hierarchy as follows: for $k \geq 1$, level k of the extended

low hierarchy is the set $EL_k^{P,\Sigma} = \{A|\Sigma_k^P(A) \subseteq \Sigma_{k-1}^P(A \oplus SAT)\}$. Allender and Hemachandra and Long and Sheu introduced refinements of the extended low hierarchy based on the Δ and Θ-levels, respectively, of the polynomial-time hierarchy: for $k \geq 2$, $EL_k^{P,\Sigma} = \{A \mid \Delta_k^P(A) \subseteq \Delta_{k-1}^P(A \oplus SAT)\}$ and $EL_k^{P,\Theta} = \{A \mid \Theta_k^P(A) \subseteq \Theta_{k-1}^P(A \oplus SAT)\}$. In this paper we show that the extended low hierarchy is properly infinite by showing, for $k \geq 2$, that $EL_k^{P,\Sigma} \subset EL_{k+1}^{P,\Theta} \subset EL_{k+1}^{P,\Delta} \subset EL_{k+1}^{P,\Sigma}$. Our proofs use in circuit lower bound techniques of Hastad and Ko. As corollaries to our constructions, we obtain, for $k \geq 2$, oracle sets B_k, C_k and D_k, such that $PH(B_k) = \Sigma_k^P(B_k) \neq \Delta_k^P(B_k), PH(C_k) = \Delta_k^P(C_k) \neq \Theta_k^P(C_k)$, and $PH(D_k) = \Theta_k^P(D_k) \neq \Sigma_{k-1}^P(D_k)$.

Separating Complexity Classes Related to Bounded Alternating ω-Branching Programs

Christoph Meinel
Universität Trier
(Joint work with Stephan Waack)

We develop a theory of communication within branching programs that provides exponential lower bounds on the size of branching programs that are bounded alternating. Our theory is based on the algebraic concept of co-branching programs, $\omega : I\!N \twoheadrightarrow R$ semiring homomorphism, that generalizes ordinary branching programs, SL-branching programs and MOD_p-branching programs.
Due to certain exponential lower and polynomial upper bounds on the size of bounded alternating ω-branching programs we are able to separate the corresponding classical complexity classes $N2_{ba}, co-N2_{ba}, \oplus 2_{ba}, MOD_p \cdot 2_{ba}$ (p prime) from each other and from that classes corresponding to oblivious linear length-bounded branching programs investigated in the past.

The Theory of the Polynomial Many-one Degrees of Recursive Sets is Undecidable

André Nies
Universität Heidelberg
(Joint work with Klaus Ambos-Spies)

To obtain undecidability of the polynomial m-degrees of recursive sets, we show that the lattice of Σ_2^0 sets under inclusion is elementary definable with parameters. The model theoretic and algebraic tools are the same as in a previous paper (joint work with R. Shore) where we show undecidablity of the recursively enumerable weak truth table degrees. To get a uniformly recursive independent sequence which is definable, we apply results of Ambos-Spies on polynomial m-degrees: an exact pair theorem as well as the fact that, for

each $a \neq 0$ there is a degree b such that a, b form a minimal pair and b is not the supremum of a minimal pair.

Parsimonious and Truly Linear Time Computation

Kenneth Regan
SUNY Buffalo

The standard multitape Turing Machine model provides only a very restricted form of access to data stored in its one-dimensional types. This becomes very noticeable when one studies linear-time computation. Unit-cast RAM models remove this restriction, but these assume that every individual memory register can be addressed in the same unit time. B. Alpern, A. Aggarwal, A. Chandra, and M. Snir introduced a "more-realistic" model based on the concept of a "hierarchical memory", whereby some memory close to the CPU is "fast" (such as in a processor cache), and other memory B more distant and "slow" (such as on a disk drive). Generally, they considered an access time charge function $M(i)$ on register number i, such as $M(i) = log(i)$ (S. Cook's log-cost criterion), $M(i) = \sqrt[3]{i}, M(i) = \sqrt[2]{i}$, or $M(i) = i$ (similar to a TM tape).
A computation is parsimonious in the cost measure μ (Alpern, Carter, Fery, FOCS 1990) if its runtime under $\mu(i)$ access charges is still within a constant factor of its runtime under unit cost – intuitively, such a computation uses a processor cache efficiently. Aggarwal, Chandra, and Snir [FOCS 1987] enhanced their model by allowing blocks of data to be copied, with the μ charge applied only for addressing the block and not for each data item inside. All of their models are still based on RAMs with unlimited-size registers.
We introduce an analogue "BM" of the HMM-Block Transfer model for fixed-size registers, where any finite transduction (not just "copy") can be applied to data in a block-move. We show that several list-processing operations, among them member, shuttle, unshuttle, maximum element, and normalize can be canied out in linear time on this model, even under the strictest cost measure $\mu(i) = i$. These operation are not linear time on the HMM-BT model (no nontrivial operation is), and really use tricks on individual bits of the data. For this reasons it is interesting to study to what extent other lower bounds on the HMM-BT model carry over.

Graph Isomorphism is Low for PP

Uwe Schöning
Universität Ulm
(Joint work with Johannes Köbler und Jacobo Torán)

It is shown that the graph automorphism problem is located in the class SPP (introduced by Fenner-Fortnow-Kurtz) implying that this problem is low for $\oplus P$, $C{=}P$, and PP.

Similarly, but a little weaker, the graph isormorphism problem is located in $LWPP$, and therefore low for $C{=}P$ and PP. These results show an interesting difference between the graph automorphism and isomorphism problems, and both problems are very unlikely to be NP-complete.

On the Power of One Bit of a $\#P$-Function

Thomas Schwentick
Universität Mainz
(Joint work with Ken Regan, SUNY/Buffalo)

We introduce the class MP of languages L which can be solved in polynomial time with an oracle for one selected bit of the value $f(y)$ of a $\#P$-function on a selected argument y. This extends the much-studied language classes $\oplus P$ and PP, which correspond to the power of the least and most significant bits, respectively. We show that MP is captured by the power of the middle bit; namely a language L is in MP if for some $\#P$-function f' and all $x, x \in L \Leftrightarrow$ the middle bit of $f'(x)$ in binary notation is '1'. Also S. Toda's proof that PH $\subseteq P^{\#P}$ actually gives

$$PH \subseteq BP \oplus P \subseteq C \oplus P \subseteq MP$$

The class MP has complete problems, and is closed under complements and under polynomial-time many-one reducibility.
We examine the subclass $AmpMP$ of languages whose MP representations can be "amplified", showing that $BP \oplus P \subseteq AmpMP$, and that for any $\leq_m$-closed subclass C of $AmpMP$, $MP^C = MP$. Hence $BP \oplus P$ is low for MP, and if $C{=}P \subseteq AmpMP$, then $PP^{PP} = MP$. Finally our work leads to a purely mathematical question about the size of integer-valued polynomials $p(x, y)$ which satisfy certain congruence relations, one which also matters to the theory of bounded-depth circuits.

A Taxonomy of Complexity Classes of Functions

Alan L. Selman
SUNY Buffalo

This paper comprises a systematic comparison of several complexity classes of functions that are computed nondeterministically in polynomial time or with an oracle in NP. There are three components to this work.

- A taxonomy is presented that demonstrates all known inclusion relations of these classes. For (nearly) each inclusion that is not shown to hold, evidence is presented

to indicate that the inclusion is false. As an example, consider $FewPF$, the class of multivalued functions that are nondeterministically computable in polynomial time such that for each x, there is a polynomial bound on the number of distinct output values of $f(x)$. We show that $FewPF \subseteq PF_{tt}^{NP}$. However, we show $PF_{tt}^{NP} \subseteq FewPF$ if and only if $NP = co-NP$, and thus $PF_{tt}^{NP} \subseteq FewPF$ is likely to be false.

- Whereas it is known that $P^{NP}(O(log\ n)) = P_{tt}^{NP} \subseteq P^{NP}$ [Hem87, Wagb, BH88], we show that $PF^{NP}(O(log\ n)) = PF_{tt}^{NP}$ implies $P = FewP$ and $R = NP$. Also, we show that $PF_{tt}^{NP} = PF^{NP}$ if and only if $P_{tt}^{NP} = P^{NP}$.

- We show that if every nondeterministic polynomial-time multivalued function has a single-valued nondeterministic refinement (equivalently, if every honest function that is computable in polynomial-time can be inverted by a single-valued nondeterministic function), then there exists a disjoint pair of NP-complete sets such that every separator is NP-hard. The latter is a previously studied open problem that is closely related to investigations on promise problems. This result motivates a study of reductions between partial multivalued functions.

On The Complexity Types of Recursive Sets

Theodore A. Slaman
University of Chicago

For recursive sets A and B say that $A \equiv_c B$ if for every time constructible f, $A \in DTIME_{RAM}(f) \leftrightarrow B \in DTIME_{RAM}(f)$. Say $A \geq_c B$ if only the forward implication holds. Let C be the induced ordering of $\equiv_c$-equivalence classes by $\leq_c$.

Theorem (Groszek-Slaman). For every nonlinear A and every recursive function f, there is an automorphism π of C sending the equivalence class of A to that of a set $\pi\ A$ such that $\pi\ A \notin \mathrm{DTIME}_{RAM}(f)$.

Corollary $PTIME, EXP, \ldots$ are not definable in C.

On the Non-uniform Complexity of the Graph Isomorphism Problem

Jacobo Torán
U. Politecnica de Catalunia, Barcelona
(Joint work with Antoni Lozano)

We study the non-uniform complexity of the graph isomorphism (GI) and graph automorphism (GA) problems considering the implications of different types of polynomial time

reducibilities from these problems to sparse sets. We show that if GI (or GA) is bounded truth-table or conjunctively reducible to a sparse set then it is in P, while if we suppose that it is in $P/poly$ then the problem is low for MA, the class of sets with publishable proofs. These results are proved using graph constructions that show new properties of the GI and GA problems.

Embedding is as Hard as Separation

Peter van Emde Boas
University of Amsterdam

It is a know classical result that the partial order of complexity classes ordered under inclusion is a universal partial order, i. e. all countable partial orders can be represented in this structure. The classical formulation for this result is the Embedding theorem as presented by E. M. McCreight in his thesis at 1969. His proof uses an intricate diagonalization and the recursion theorem. In fact he proves a stronger theorem since his result states that the system of recursive functions ordered by their complexity already represents a universal partial order. In this order $f \geq g$ provided f is computed by some program Φ_j computing g. The standard embedding theorem follows by selecting the classes generated by the individual functions used in McCreight embedding.
We show that for the universality property of the system of classes a standard diagonalization suffices, provided it is invoked in a localized way. The resulting machine independent proof shows moreover that neither the names of the embedding classes, nor the operator which actually performs the embedding needs to be arbitrary complex.
I obtained this improvement some 20 years ago while doing research leading towards my ph. d. thesis. It remained an unpublished manuscript since.

Learning Simple Concepts under Simple Distributions

Paul Vitányi
CWI & University of Amsterdam
(Joint work with Ming Li (SIAM J. Comp. 91)

We develop a learning theory were "simple" concepts are easily learnable. In Valiant's distribution-free learning model, many concepts turn out to be too hard (like NP-hard) to learn. Relatively few concept classes were shown to be learnable polynomially. In real life, almost nothing we have to learn appears to be not (polynomially) learnable. It is known that leaning under one fixed distribution (like the uniform one) is often easy. Hence we look for a class of distributions which is wide enough to be interesting, and small enough to be usable. We first prove two completeness results. Define a distribution P to be universal for a distribution class $\mathcal{P}$ if $\forall\, \varphi \in \mathcal{P}\ \exists c > O \forall x \in \mathcal{S}[P(x) \geq c\varphi(x)]$, where $\mathcal{S}$ is the simple space.

(i) $\mathcal{S}$ is a discrete (countable) simple space. Then a concept class $\mathcal{C}$ is polynomially pac (probably approximately correct) learnable under all distributions in a class X, provided we sample according to a X-universal distribution P, if $\mathcal{C}$ is polynomially pac learnable under P.

(ii) $\mathcal{S}$ is a continous sample space. A concept class $\mathcal{C}$ is pac learnable under all distributions in a class X if $\mathcal{C}$ is pac learnable under an X-universal distribution.

If we take X the class of all distributions (discrete) which are computable or semi-computable (can be approximated from below by a computable process), then $m(x) = 2^{-K(x)}$, $K(x)$ is the self-delimiting Kolmogorov complexity of x, is universal for X. Similary, $M(x)$ is the continous version of $m(x)$ and is universal for the class of computable or semi-computable measures. We call such distributions or measures simple. We develop several new learning algorithms under $m(x)$ and $M(x)$, and show for several new concept classes that they are (polynomially) learnable in our sense, while it is not known that they are polynomially learnable in Valiant's sense only if $RP = P$. Finally, we exhibit a concept class which is PAC learnable in our sense while it has infinite Vapnik-Chervonenko dimension, that is, it is not pac learnable in Valiant's pac distribution free (over all distributions) sense.
As a final curiosity we mention that, for all algorithms, the average case running time under the universal distribution equals the worst-case running time. Similary for the space complexity.

Complexity of Functions vs. Complexity of Sets

Klaus W. Wagner
Universität Würzburg
(Joint work with Heribert Vollmer)

A complexity theory of functions is developed systematically. A relation $\mathcal{F} \simeq \varphi$ between classes $\mathcal{F}$ of functions and classes φ of sets is established which preserves inclusional relationships (i. e. $\mathcal{F} \simeq \varphi$ and $\mathcal{F}' \simeq \varphi'$ implies $\mathcal{F} \subseteq \mathcal{F}' \Leftrightarrow \varphi \subseteq \varphi'$). By this relation the operators $\exists$ and $\forall$ on classes correspond to the operators Max and Min, resp., on classes of functions (i. e. $\mathcal{F} \simeq \varphi$ implies $\mathrm{Max}\mathcal{F} \simeq \exists\, \varphi$ and $\mathrm{Min}\mathcal{F} \subseteq \forall\varphi$). A slightly weaker correspondence holds between the set theoretic operator C and the function operator Med (median). The number-of-query hierarchy collapses in the function case because $\mathcal{F} \simeq \varphi$ implies $FP^{\mathcal{F}} = FP^{\mathcal{F}}[1] = \mathcal{F} - \mathcal{F} \simeq \mathrm{P}^{\varphi}$. The counting hierarchy of functions built by Med is strongly connected to the hierarchy of counting functions built by $\#P^{\#P^{\#P^{\cdots}}}$. As consequences we obtain besides others $\#P \subseteq MedFP$ and $FP^{\mathrm{Med}FP} = MedFP - MedFP$.

Dagstuhl-Seminar 9206

Participants

Eric **Allender**
Rutgers University
Dept. of Computer Science
New Brunswick NJ 08903
USA
allender@cs.rutgers.edu
tel.: +1-908-932-3629

Klaus **Ambos-Spies**
Universität Heidelberg
Mathematisches Institut
Im Neuenheimer Feld 288
W-6900 Heidelberg 1
Germany
G77@DHDURZ1.BITNET
tel.: 06221-562673

Vikraman **Arvind**
Dept. of C.S.E.
Hanz Khas
Delhi 110016
India

José L. **Balcázar**
Universidad Politecnica de Catalunya
Dept. L.S.I. (Ed. FIB)
Pau Gargallo 5
E-08028 Barcelona
Spain
balqui@lsi.upc.es
tel.: +34-3-401-7013 / 6944

Ronald **V. Book**
University of California at Santa Barbara
Department of Mathematics
Santa Barbara CA 93106
USA
book%henri@hub.ucsb.edu
tel.: +1-805-893-2778 / 2171

Harry **Buhrman**
Faculteit Wiskunde en Informatica
Plantage Muidergracht 24
NL-1018 TV Amsterdam
The Netherlands
buhrman@fwi-uva.nl
tel.: +31-20-525-6508

Rod **Downey**
Victoria University of Wellington
Department of Mathematics
P.O. Box 600
Wellington
New Zealand
downey@math.vuw.ac.nz
tel.: +64-4-4784948 / 4715344

Lance **Fortnow**
The University of Chicago
Dept. of Computer Science
Ryerson Hall
1100 East 58th Street
Chicago IL 60637
USA
FORTNOW@CS.UCHICAGO.EDU
tel.: +1-312-702-3494

William **Gasarch**
Univ. of Maryland at College Park
Dept. of Computer Science
College Park MD 20742
USA
gasarch@cs.umd.edu
tel.: +1-301-405-2698

Johan **Hastad**
Royal Institute of Technology
Kungl. Tekuiska Högskolan
Nada
10044 Stockholm
Sweden
johanh@nada.kth.se
tel.: 46-8-790 6289

Lane **Hemachandra**
University of Rochester
Dept. of Computer Science
Rochester NY 14627
USA
lane@cs.rochester.edu
tel.: +1-716-275-1203

Ulrich **Hertrampf**
Universität Würzburg
Lehrstuhl für Informatik IV
Am Exerzierplatz 3
W-8700 Würzburg
Germany
hertramp@informatik.uni-wuerzburg.de
tel.: 0931-887810

Steven **Homer**
Boston University
Computer Science Department
College of Liberal Arts
111 Cummington Street
Boston MA 02215
USA
homer@cs.bu.edu
tel.: +1-617-353-3840

Neil **Immerman**
University of Massachusetts at Amherst 2-19692
Computer Science Department
Lederle Graduate Research Center
Amherst MA 01003
USA
immerman@cs.umass.edu
tel.: +1-413-545-1862

Birgit **Jenner**
TU München
Institut für Informatik
Arcisstraße 21
W-8000 München 2
Germany
jenner@informatik.tu-muenchen.de
tel.: 089-2105-2387

Johannes **Köbler**
Universität Ulm
Fakultät für Informatik
Oberer Eselsberg
W-7900 Ulm
Germany
koebler@informatik.uni-ulm.de
tel.: 0731-502-4107

James **Kadin**
University of Maine
Dept. of Computer Science
Neville Hall
Orono Maine 04469-0122
USA
jak@gandalf.umcs.maine.edu
tel.: +1-207-581-3909

Marek **Karpinski**
Universität Bonn
Inst. für Informatik VI
Römerstr. 164
W-5300 Bonn
Germany
KARPINSKI@cs.uni-bonn.de
tel.: 0228-550-224

Martin **Kummer**
Universität Karlsruhe
IInstitut für Logik
Komplexität und
Deduktionssysteme
Postfach 6980 W-7500 Karlsruhe
Germany
0721-608-4214

Klaus-Joern **Lange**
TU München
Institut für Informatik
Arcisstraße 21
W-8000 München 2
Germany
lange@informatik.tu-muenchen.de
tel.: 089-2105-2403

Tim **Long**
New Mexico State University
Dept. of Computer Science
Dept. 3 CU
P.O. Box 30001
Las Cruces NM 88003-0001
USA
long@nmsu.edu
tel.: +1-505-646-5286

Christoph **Meinel**
Universität Trier
FB IV -7z Informatik
Postfach 38 25
W-5500 Trier
Germany
meinel@uni-trier.dbp.de
tel.: 0651-201-2827

Andre **Nies**
Universität Heidelberg
Mathematisches Institut
Im Neuenheimer Feld 288
W-6900 Heidelberg 1
Germany
b29@dhdurz1
tel.: 06221-562672

Piergiorgio **Odifreddi**
Universita di Torino
Dipartimento di Informatica
Corso Svizzera 185
10149 Torino
Italy
piergior@di.unito.it
tel.: 0039-11-771 2002

Pekka **Orponen**
University of Helsinki
Dept. of Computer Science
Teollisuuskatu 23
00510 Helsinki
Finland
orponen@cs.Helsinki.FI
tel.: +358-0-708-4224

Kenneth W. **Regan**
SUNY at Buffalo
Dept. of Computer Science
226 Bell Hall
Buffalo NY 14260
USA
regan@cs.buffalo.edu
tel.: +1-716-636-3189

Uwe **Schöning**
Universität Ulm
Fakultät für Informatik
Oberer Eselsberg
W-7900 Ulm
Germany
schoenin@informatik.uni-ulm.de
tel.: 0731-502-4100 / 4101

Thomas **Schwentick**
Johannes Gutenberg-Universität Mainz
FB 17 - Institut für Informatik
Staudingerweg 9
W-6500 Mainz
Germany
TICK@uaimzti.mathematik.uni-mainz.de
tel.: 06131-393603

Alan **Selman**
SUNY at Buffalo
Dept. of Computer Science
226 Bell Hall
Buffalo NY 14260
USA
selman@cs.buffalo.edu
tel.: +1-716-636-3182

Theodore A. **Slaman**
The University of Chicago
Dept. of Mathematics
Ryerson Hall
1100 East 58th Street
Chicago IL 60637
USA
tel.: ted@zaphod.uchicago.edu

Jacobo **Toran**
Universidad Politecnica de Catalunya
Dept. L.S.I. (Ed. FIB)
Pau Gargallo 5
E-08028 Barcelona
Spain
JACOBO@LSI.UPC.ES
tel.: +34-3-401-7340

Leen **Torenvliet**
UvA / ILLC
Faculteit Wiskunde en Informatica
Plantage Muidergracht 24
NL-1018 TV Amsterdam
The Netherlands
leen@fwi.uva.nl
tel.: +31-205-256065

Paul **Vitanyi**
CWI - Mathematisch Centrum
Kruislaan 413
NL-1098 SJ Amsterdam
The Netherlands
paulv@cwi.nl
tel.: +31-205-924124

Jörg **Vogel**
Friedrich-Schiller-Universität
Mathematische Fakultät
Universitätshochhaus 17. OG
O-6900 Jena
Germany
Joerg.Vogel@mathematik.uni-Jena.dbp.de

Klaus W. **Wagner**
Universität Würzburg
Lehrstuhl für theoretische Informatik
Am Exerzierplatz 3
D-W-8700 Würzburg
Germany
wagner@informatik.uni-wuerzburg.de
tel.: 0931/887910

Peter **van Emde Boas**
ILLC
Faculteit Wiskunde en Informatica
Plantage Muidergracht 24
NL-1018 TV Amsterdam
The Netherlands
peter@fwi.uva.nl
tel.: +31-20-525-6065

Zuletzt erschienene und geplante Titel:

J. Berstel , J.E. Pin, W. Thomas (editors):
Automata Theory and Applications in Logic and Complexity, Dagstuhl-Seminar-Report; 5, 14.-18.1.1991 (9103)

B. Becker, Ch. Meinel (editors):
Entwerfen, Prüfen, Testen, Dagstuhl-Seminar-Report; 6, 18.-22.2.1991 (9108)

J. P. Finance, S. Jähnichen, J. Loeckx, M. Wirsing (editors):
Logical Theory for Program Construction, Dagstuhl-Seminar-Report; 7, 25.2.-1.3.1991 (9109)

E. W. Mayr, F. Meyer auf der Heide (editors):
Parallel and Distributed Algorithms, Dagstuhl-Seminar-Report; 8, 4.-8.3.1991 (9110)

M. Broy, P. Deussen, E.-R. Olderog, W.P. de Roever (editors):
Concurrent Systems: Semantics, Specification, and Synthesis, Dagstuhl-Seminar-Report; 9, 11.-15.3.1991 (9111)

K. Apt, K. Indermark, M. Rodriguez-Artalejo (editors):
Integration of Functional and Logic Programming, Dagstuhl-Seminar-Report; 10, 18.-22.3.1991 (9112)

E. Novak, J. Traub, H. Wozniakowski (editors):
Algorithms and Complexity for Continuous Problems, Dagstuhl-Seminar-Report; 11, 15-19.4.1991 (9116)

B. Nebel, C. Peltason, K. v. Luck (editors):
Terminological Logics, Dagstuhl-Seminar-Report; 12, 6.5.-18.5.1991 (9119)

R. Giegerich, S. Graham (editors):
Code Generation - Concepts, Tools, Techniques, Dagstuhl-Seminar-Report; 13, 20.-24.5.1991 (9121)

M. Karpinski, M. Luby, U. Vazirani (editors):
Randomized Algorithms, Dagstuhl-Seminar-Report; 14, 10.-14.6.1991 (9124)

J. Ch. Freytag, D. Maier, G. Vossen (editors):
Query Processing in Object-Oriented, Complex-Object and Nested Relation Databases, Dagstuhl-Seminar-Report; 15, 17.-21.6.1991 (9125)

M. Droste, Y. Gurevich (editors):
Semantics of Programming Languages and Model Theory, Dagstuhl-Seminar-Report; 16, 24.-28.6.1991 (9126)

G. Farin, H. Hagen, H. Noltemeier (editors):
Geometric Modelling, Dagstuhl-Seminar-Report; 17, 1.-5.7.1991 (9127)

A. Karshmer, J. Nehmer (editors):
Operating Systems of the 90s and Beyond, Dagstuhl-Seminar-Report; 18, 8.-12.7.1991 (9128)

H. Hagen, H. Müller, G.M. Nielson (editors):
Scientific Visualization, Dagstuhl-Seminar-Report; 19, 26.8.-30.8.91 (9135)

T. Lengauer, R. Möhring, B. Preas (editors):
Theory and Practice of Physical Design of VLSI Systems, Dagstuhl-Seminar-Report; 20, 2.9.-6.9.91 (9136)

F. Bancilhon, P. Lockemann, D. Tsichritzis (editors):
Directions of Future Database Research, Dagstuhl-Seminar-Report; 21, 9.9.-12.9.91 (9137)

H. Alt , B. Chazelle, E. Welzl (editors):
Computational Geometry, Dagstuhl-Seminar-Report; 22, 07.10.-11.10.91 (9141)

F.J. Brandenburg , J. Berstel, D. Wotschke (editors):
Trends and Applications in Formal Language Theory, Dagstuhl-Seminar-Report; 23, 14.10.-18.10.91 (9142)

H. Comon , H. Ganzinger, C. Kirchner, H. Kirchner, J.-L. Lassez , G. Smolka (editors):
Theorem Proving and Logic Programming with Constraints, Dagstuhl-Seminar-Report; 24, 21.10.-25.10.91 (9143)

H. Noltemeier, T. Ottmann, D. Wood (editors):
Data Structures, Dagstuhl-Seminar-Report; 25, 4.11.-8.11.91 (9145)

A. Dress, M. Karpinski, M. Singer(editors):
Efficient Interpolation Algorithms, Dagstuhl-Seminar-Report; 26, 2.-6.12.91 (9149)

B. Buchberger, J. Davenport, F. Schwarz (editors):
Algorithms of Computeralgebra, Dagstuhl-Seminar-Report; 27, 16.-20.12.91 (9151)

K. Compton, J.E. Pin , W. Thomas (editors):
Automata Theory: Infinite Computations, Dagstuhl-Seminar-Report; 28, 6.-10.1.92 (9202)

H. Langmaack, E. Neuhold, M. Paul (editors):
Software Construction - Foundation and Application, Dagstuhl-Seminar-Report; 29, 13..-17.1.92 (9203)

K. Ambos-Spies, S. Homer, U. Schöning (editors):
Structure and Complexity Theory, Dagstuhl-Seminar-Report; 30, 3.-7.02.92 (9206)

B. Booß, W. Coy, J.-M. Pflüger (editors):
Limits of Modelling with Programmed Machines, Dagstuhl-Seminar-Report; 31, 10.-14.2.92 (9207)

K. Compton, J.E. Pin , W. Thomas (editors):
Automata Theory: Infinite Computations, Dagstuhl-Seminar-Report; 28, 6.-10.1.92 (9202)

H. Langmaack, E. Neuhold, M. Paul (editors):
Software Construction - Foundation and Application, Dagstuhl-Seminar-Report; 29, 13.-17.1.92 (9203)

K. Ambos-Spies, S. Homer, U. Schöning (editors):
Structure and Complexity Theory, Dagstuhl-Seminar-Report; 30, 3.-7.2.92 (9206)

B. Booß, W. Coy, J.-M. Pflüger (editors):
Limits of Information-technological Models, Dagstuhl-Seminar-Report; 31, 10.-14.2.92 (9207)

N. Habermann, W.F. Tichy (editors):
Future Directions in Software Engineering, Dagstuhl-Seminar-Report; 32; 17.2.-21.2.92 (9208)

R. Cole, E.W. Mayr, F. Meyer auf der Heide (editors):
Parallel and Distributed Algorithms; Dagstuhl-Seminar-Report; 33; 2.3.-6.3.92 (9210)

P. Klint, T. Reps, G. Snelting (editors):
Programming Environments; Dagstuhl-Seminar-Report; 34; 9.3.-13.3.92 (9211)

H.-D. Ehrich, J.A. Goguen, A. Sernadas (editors):
Foundations of Information Systems Specification and Design; Dagstuhl-Seminar-Report; 35; 16.3.-19.3.9 (9212)

W. Damm, Ch. Hankin, J. Hughes (editors):
Functional Languages:
Compiler Technology and Parallelism; Dagstuhl-Seminar-Report; 36; 23.3.-27.3.92 (9213)

Th. Beth, W. Diffie, G.J. Simmons (editors):
System Security; Dagstuhl-Seminar-Report; 37; 30.3.-3.4.92 (9214)

C.A. Ellis, M. Jarke (editors):
Distributed Cooperation in Integrated Information Systems; Dagstuhl-Seminar-Report; 38; 5.4.-9.4.92 (9215)