Structures Abstracts 1994. Vol IV

Abstract

This is a collection of one page abstracts of recent results of interest to the Structural Complexity community. The purpose of this document is to spread this information, not to judge the truth or interest of the results therein.

List of Titles of Abstracts

This is a list of the titles of the abstracts in the order they appear. The order alphabetical by the author.

On the Kolmogorov Complexity of Boolean Query Languages
On Balanced vs. Unbalanced Computation Trees
Recursion Theoretic Characterizations of Comp. Classes of Counting Functions
Weighted NP optimization problems: logical definability and approx. properties

From Disjunctive Self-reducibility to Self-reducibility

Manindra Agrawal, School of Mathematics, SPIC Science Foundation, 92, G. N. Chetty Road, T. Nagar, Madras 600 017, INDIA. manindra@ssf.ernet.in

Abstract Number 94-01

Different notions of self-reducibility play an important role in showing that the classes of low-information sets are not hard. For example, Mahaney used the disjunctive self-reducibility of SAT to show that no sparse set can be many-one hard for NP unless P = NP. Similarly, Ogiwara and Watanabe showed that no *left* set (these sets have a special kind of one-word decreasing self-reducibility) can bounded truth-table reduce to a sparse set unless it is already in P.

These results suggest the following question: for which notions of self-reducibility can a result of the above kind be shown? In particular, can it be shown for two of the most common notions, viz., disjunctive self-reducibility and polynomially-related self-reducibility? As there are relativized worlds where a disjunctive self-reducible sparse set exists that is not in P, this question is difficult to answer. Can we say that the hardness results hold for a disjunctive (or, polynomially-related) self-reducible set with some additional properties? There has been some progress towards this recently: Agrawal and Arvind (see abstract titled *Geometric Sets of Low-information Content* in this volume) have shown that no disjunctive self-reducible bd-cylinder (set A is a *bd-cylinder* if there exists an FP function OR such that $\mathrm{OR}(x, y) \in A$ iff $x \in A \vee y \in A$) reduces to a sparse set via a composition of bounded truth-table and conjunctive reductions unless it is already in P.

We propose a technique to translate results on disjunctive self-reducible sets that are based on a breadth-first search pruning algorithm, to polynomially-related self-reducible sets. We show that no polynomially-related self-reducible bd-cylinder can conjunctively reduce to a sparse set unless it is already in P. Similarly, we show that no polynomially-related self-reducible set such that both the set and its complement are bd-cylinders, can bounded truth-table reduce to a sparse set unless it is already in P.

Another class of low-information sets is that of approximable sets (these sets contain bounded truth-table closure of p-selective sets). Recently, it has been shown (see Structures '94 proceedings) that no disjunctive self-reducible bd-cylinder can be approximable unless it is already in P. We use our technique to show that no polynomially-related self-reducible set such that both the set and its complement are bd-cylinders, can be approximable unless it is already in P.

These results are the best obtainable via relativizable techniques as there is a relativized world (exhibited by Beigel, Kummer, and Stephan) that has a disjunctive self-reducible set that is both sparse and approximable with its complement being a bd-cylinder, but the set is not in P.

A preliminary version will be available by July-end.

Geometric Sets of Low Information Content

Manindra Agrawal, School of Mathematics, SPIC Science Foundation, 92, G. N. Chetty Road, T. Nagar, Madras 600 017, INDIA. manindra@ssf.ernet.in,
V. Arvind, Department of Computer Science, Institute of Mathematical Sciences, C. I. T. Campus, Madras 600 113, INDIA. arvind@imsc.ernet.in

Abstract Number 94-02

Arithmetization of boolean formulas has found several applications in complexity theory. An immediate consequence of arithmetization is that corresponding to every NP language A there is a family of multilinear forms $\{M_n\}_{n>0}$ where M_n is n-variate, such that $x = x_1x_2\cdots x_n \in A$ iff $M_n(x_1, x_2, \ldots, x_n) > 0$. This raises the following question: for which kinds of algebraic surfaces M_n can NP be captured in the above sense? More precisely, letting $M_= = \bigcup_{n>0}\{\langle x_1, x_2, \ldots, x_n\rangle \in Q^n \mid M_n(x_1, x_2, \ldots, x_n) = 0\}$ and $M_+ = \bigcup_{n>0}\{\langle x_1, x_2, \ldots, x_n\rangle \in Q^n \mid M_n(x_1, x_2, \ldots, x_n) > 0\}$, for which kinds of surfaces M_n is NP polynomial-time reducible to either $M_=$ or M_+ (Q is the field of rationals)?
In this paper, we consider families of hyperplanes $\{M_n\}_{n>0}$ over the field of rationals. We show that any disjunctively self-reducible bd-cylinder (set A is a *bd-cylinder* if there exists an FP function OR such that $\mathrm{OR}(x, y) \in A$ iff $x \in A \vee y \in A$) that polynomial-time many-one reduces to either $M_=$ or M_+, for any family $\{M_n\}_{n>0}$ of hyperplanes, is in P. Similarly, we show that any *left set* that polynomial-time many-one reduces to $M_=$, for any family $\{M_n\}_{n>0}$ of hyperplanes, is in P.
Furthermore, for families of hyperplanes $\{M_n\}_{n>0}$ over finite fields, we show that

- Any polynomially-related self-reducible set that polynomial-time many-one reduces to $M_=$ is in P.
- Any word-decreasing self-reducible set that polynomial-time many-one reduces to $M_=$ is in NP $\cap$ co-NP.
- Any strictly one word-decreasing self-reducible set that polynomial-time many-one reduces to $M_=$ is in P.

As an immediate consequence of these results, we have that if any class $\mathcal{K}$ in { NP, Mod_kP, C$_=$P, PP, PSPACE } is many-one reducible to M_+ or $M_=$ for a family $\{M_n\}_{n>0}$ of hyperplanes over rationals then $\mathcal{K} =$ P.
The above results have the following interesting consequences for reductions to sparse and tally sets.

- Any disjunctive self-reducible bd-cylinder that reduces to a sparse set via a composition of bounded truth-table and conjunctive reductions is in P.
- Any disjunctively self-reducible bd-cylinder that reduces to a tally set either via a composition of bounded truth-table and exact count truth-table reductions, or via threshold truth-table reductions is in P.
- Any polynomially-related self-reducible set that reduces to a tally set via parity truth-table reductions is in P.

A preliminary version is available. Contact address: manindra@ssf.ernet.in

Measure on Small Complexity Classes, with Applications for BPP

Eric Allender, Department of Computer Science, Rutgers University, New Brunswick, NJ 08903. Email: `allender@cs.rutgers.edu`.
Martin Strauss, Department of Mathematics, Rutgers University, New Brunswick, NJ 08903. Email: `mstrauss@math.rutgers.edu`.

Abstract Number 94-03

The main contributions of this work are:

1. We present a notion of resource-bounded measure for P and other subexponential-time classes. This is a generalization of Lutz's notion of measure, but Lutz's definitions apply only to classes at least as large as E, and several obstacles needed to be overcome to give a meaningful notion of measure for smaller classes. We present some of the basic properties of this measure; for example, $\forall k$ DTIME(n^k) is a measure 0 subset of P, but neither P-uniform AC^0 nor SPARSE $\cap$ P is a measure zero subset of P.

2. We use this new notion of measure to show that for all $\epsilon > 0$ almost every set A in the subexponential class E_ϵ is hard for BPP, where $E_\epsilon = \bigcup_{\delta<\epsilon}$DTIME($2^{n^\delta}$). This is best possible without improving the known bounds on the deterministic time complexity of sets in BPP. Using similar techniques, we show that almost every set $A \in$ PSPACE also satisfies this property. (This exponentially improves on the result of [J. Lutz, A Pseudorandom Oracle Characterization of BPP, *SIAM J. Comput.*, **22** 1993, 1075-1086] showing that almost every set in ESPACE satisfies this property.)

A preliminary paper is available.

On infinite sequences (almost) as easy as Π

José L. Balcázar *Ricard Gavaldà*
Departament L.S.I., Universitat Politècnica de Catalunya,
Pau Gargallo 5, 08028 Barcelona, SPAIN

Montserrat Hermo
Departamento de Lenguajes y Sistemas Informáticos, Universidad del País Vasco, Apdo. 649, E-20080 San Sebastián, Spain.

E-mail addresses: balqui@lsi.upc.es, gavalda@lsi.upc.es, montse@si.ehu.es

Abstract Number 94-04

It is known that infinite binary sequences of constant Kolmogorov complexity are exactly the recursive ones. Such a kind of statement no longer holds in the presence of resource bounds. Contrary to what intuition might suggest, there are sequences of constant, polynomial-time bounded Kolmogorov complexity that are not polynomial-time computable. This motivates the study of several resource-bounded variants in search for a characterization, similar in spirit, of the polynomial-time computable sequences. We propose some definitions, based on Kobayashi's notion of compressibility, and compare them to the standard resource-bounded Kolmogorov complexity of infinite strings. Some nontrivial coincidences and disagreements are proved. The resource-unbounded case is also considered.

A full paper will be available shortly.

The Power of Local Self-Reductions

Richard Beigel, Department of Computer Science, Yale University, New Haven, CT 06520, USA,
Howard Straubing, Computer Science Department, Boston College, Chestnut Hill, MA 02167, USA.

Abstract Number 94-05

We study here a form of lexicographic self-reducibility. Let x be a binary string, and identify x with the integer m whose binary representation is $1x$. We say that a language L is k-locally self-reducible if membership in L can be reduced in polynomial time to the questions $m - i \in L$? for $i = 1, ..., k$. More precisely, there is a deterministic polynomial-time oracle Turing machine M such that M^L recognizes L, and on input m, M queries only $m - 1, ..., m - k$. L is locally self-reducible if it is k-locally self-reducible for some k.

The case $k = 1$ was studied by Goldsmith, Joseph, Hemachandra and Young, and by Hemachandra and Hoene, under the name 'nearly near-testable sets'.

Here are our results: *(i)* Every locally self-reducible language is in PSPACE. *(ii)* Every 2-locally self-reducible language is in $\mathrm{MOD}_6\mathrm{PH}$. ($\mathrm{MOD}_6\mathrm{PH}$ is the analogue of the polynomial-time hierarchy where we allow modular quantifiers as well as the ordinary existential and universal quantifiers. This is the exponential analogue of the circuit complexi ty class ACC(6).) In fact, all 2-locally self-reducible languages belong to a fixed level of this hierarchy. *(iii)* There is a 3-locally s elf-reducible language that is PSPACE-complete. *(iv)* There is a PSPACE-complete 6-locally self-reducible language whose self-reduction is a permutation-reduction. This means that there is a polynomial-time computabl e bijection $f : \mathbf{Z}^+ \backslash \{1, 2, 3, 4, 5\} \to \mathbf{Z}^+$ such that for all $m \in \mathbf{Z}^+ \backslash \{1, 2, 3, 4, 5\}$, $m - 6 \leq f(m) < m$, and $m \in L$ if and only if $f(m) \in L$.

We prove these statements by reducing them to questions about the algebraic structure of certain finite semigroups, and then applying the results of Barrington and Thérien on the connections between semigroups and small-depth circuits.

A preliminary version of the full paper is now available; a definitive version will be available very soon.

$Almost - IP = IP$

Josef M. Breutzmann, Department of Computer Science, Iowa State University, breutzma@cs.iastate.edu

Abstract Number 94-06

In this paper we prove that $Almost - IP = IP$. The technique used constructs an oracle interactive proof system which accepts a language $L \in Almost - IP$ for a measure $1 - \varepsilon$ set of oracles. The proof system is converted into a family of circuits. The oracle is then replaced by a pseudorandom generator of Nisan and Wigderson. The family of circuits is reconverted into a (non-oracle) proof system. The resulting proof system places L in IP.

This paper is scheduled to appear in TCS in October 1994 and is currently available as TR 93-26 from the Iowa State University Computer Science Department.

Remark on a Theorem by Savitch

Mathias Bull, Fachbereich Informatik, Universität Rostock, Albert-Einstein-Str. 21, 18051 Rostock, GERMANY. e-mail: mb@informatik.uni-rostock.de

Abstract Number 94-07

W.J. Savitch introduced (in:"Maze Recognizing Automata and Nondeterministic Tape Complexity",JCSS 7(4),389-403) the concept of Maze Recognizing Automata which work with pebbles on graphs. He established a fundamental relationship between a certain searching problem of such automata and the question whether **L**=**NL**. By a slight modification of the automata and the graphs, here called Savitch-automata and Savitch-graphs, and by using of the proof techniques, we extend this consideration in the following manner. If a property Φ of graphs is logspace-complete for a complexity class C then the following two statements are equivalent. (1) C$\subseteq$**L**. (2) There is a Savitch-automata that accepts precisely the Savitch-graphs with the property Φ.

A full paper is available.

Jumping Multihead Automata with Additional Storages in Labyrinths

Mathias Bull, Fachbereich Informatik, Universität Rostock, Albert-Einstein-Str. 21, 18051 Rostock, GERMANY. e-mail: mb@informatik.uni-rostock.de

Abstract Number 94-08

The clique of open problems concerning the complexity of graph connectivity is a motivation to consider labyrinth problems, i.e. the searching abilities of automata on connected undirected graphs equipped with special orientation systems. In the paper we consider the searching behaviour of jumping multihead automata equipped with specially restricted multi-counters here called nested comparable counters and comparable shift registers. The following new lower bound results concerning the descriptional complexity are shown.
There is no jumping multihead automata with one of the mentioned additional storages which searches all labyrinths of one of the following classes:
• cubic edge-coloured finite connected undirected graphs;
• cubic finite connected undirected graphs with rotation system;
• rectilinearly embedded 3-dimensional finite connected undirected graphs.
These results are connected with theorems by K. Etessami and N. Immerman (cf. "Reachability and the Power of Local Ordering", Proc. STACS'94, Springer LNCS 775, 123-135).
A full paper is available.

A Note on P-selective sets and on Adaptive versus Nonadaptive Queries to NP

Jin-Yi Cai, Department of Computer Science, SUNY–Buffalo, Buffalo, NY 14260
Ashish V. Naik, Department of Computer Science, SUNY–Buffalo, Buffalo, NY 14260
Alan L. Selman, Department of Computer Science, SUNY–Buffalo, Buffalo, NY 14260
email: {cai,avnaik,selman}@cs.buffalo.edu

Abstract Number 94-09

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 $k > 0$, $SAT \in DTIME[2^{n/\log^k n}]$.
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.

A full paper is available as a SUNY-Buffalo Technical Report 94-02.

Communication Complexity of Key Agreement on Limited Ranges

Jin-Yi Cai, Department of Computer Science, State Univ. of NY at Buffalo, 226 Bell Hall, Buffalo NY 14260-2000,
Richard J. Lipton, Department of Computer Science, Princeton University,
Luc Longpreé, College of Computer Science, Northeastern University,
Mitsunori Ogihara, Department of Computer Science, University of Rochester *Kenneth W. Regan*, SUNY/Buffalo,
D. Sivakumar, SUNY/Buffalo,

Abstract Number 94-10

This paper studies a variation on classical key-agreement and consensus problems in which the set S of possible keys is the range, of size k, of a random variable that can be sampled. We give tight upper and lower bounds of $\lceil \log_2 k \rceil$ bits on the randomized communication complexity of agreement on some key in S, using a form of Sperner's Lemma, and give bounds on other problems. In the case where keys are generated by a probabilistic polynomial-time Turing machine, agreement is shown to be possible with zero communication if every fully polynomial-time approximation scheme (fpras) has a certain symmetry-breaking property.

An extended abstract, close to a full paper, is available by anonymous ftp to ftp.cs.buffalo.edu, cd pub/tech-reports, get 94-22.ps.

Randomness as an Invariant for Number Representations

Cristian Calude, Department of Computer Science, The University of Auckland, Private Bag 92109, Auckland, New Zealand, email: cristian@cs.auckland.ac.nz,
Helmut Jürgensen, Department of Computer Science, The University of Western Ontario, London, Ontario, N6A 5B7 Canada, email: helmut@uwo.ca.

Abstract Number 94-11

We show that the usual positional representations of a real number are either random, in the sense of Martin-Löf, for all bases or not so for any base.
The proof is achieved in two steps. First, we consider the transformation from base q to base q^m, for any natural number m. In this case, sequential Martin-Löf tests turn out to be the appropriate proof tool and number representations do not play a rôle at all. For the transition from base $q+1$ to base q – which turned out to be the most critical step – a characterization of randomness due to Solovay seems to be the best tool. When combined, these transformations allow for the transition between any two bases while preserving randomness.
It is important to realize in this context – and it is sometimes obscured by intuition – that the required function transforms *names* of numbers into *names* of numbers and it does not deal with the numbers themselves.
All our proofs are constructive.

A full paper is available; it will appear in H. Maurer, J. Karhumäki, G. Rozenberg (eds.). *New Results and Trends in Theoretical Computer Science* , Springer-Verlag, Berlin, 1994.

The Complexity of Computing over Quasigroups

Hervé Caussinus, Dép. d'Informatique et de recherche opérationnelle, Université de Montréal, C.P. 6128, Succ. Centre-Ville, Montréal (Québec) CANADA H3C 3J7. caussinu@iro.umontreal.ca

François Lemieux, School of Computer Science, McGill University, 3480 University Street, Montréal (Québec) CANADA H3A 2A7. lemieux@cs.mcgill.ca

Abstract Number 94-12

A groupoid is a set closed under a binary operation (denoted by concatenation). Let F be a subset of a finite groupoid G and consider the word problem: given a word w over G, is there a way to parenthesize w such that it evaluates to an element in F.

An important parameter affecting the complexity of this problem is whether or not the operation is associative. For a general groupoid G the word problem is in SAC^1 (LOGCFL), but when G is associative (i.e. when G is a semigroup) it is easily seen to be in NC^1. Furthermore, there exist semigroups and groupoids whose word problems are respectively complete for NC^1 [Barrington] and SAC^1 [Bédard, Lemieux, and McKenzie].

In this paper we study the influence of an other natural parameter on the complexity of the word problem. A groupoid G is said to satisfy the cancelation laws if for every a and b in G, both equations $ax = b$ and $ya = b$ have one and only one solution. Such a groupoid is called a quasigroup. A quasigroup that is associative is a group, and there exist groups whose word problems are complete for NC^1 [Barrington]. Hence, in the presence of associativity, the cancellation laws do not reduce the complexity of the word problem. However, the general situation is quite different. We prove that the word problem over any quasigroup is in NC^1 by showing that its corresponding language is regular.

We also consider the effect of restricting the parenthesization in the definition of the word problem. While the languages corresponding to the general problem are precisely the context-free languages, those related to the restricted version are shown to be the linear languages. As a consequence, this restricted word problem is complete for NL, and we prove that it belongs to NC^1 when it is limited to quasigroups.

In another vein, we consider the problem of evaluating a well-parenthesized expression over a finite loop —a loop is a quasigroup with an identity element. This problem is in NC^1 for any finite loop, and we give algebraic conditions for its completeness. In particular we prove that it is sufficient for the loop to be nonsolvable, extending the well-known theorem of Barrington. To obtain this result, we prove a generalization for loops of a theorem due to Maurer and Rhodes. We prove that, whenever L is a simple loop that is not an abelian group, any function $f : L^n \to L$ is reducible to the problem of evaluating a well parenthesized expression over L.

A full paper is available.

On the Structure of the Classes NPO and APX

Pierluigi Crescenzi and Luca Trevisan
Department of Computer Science
Università di Roma "La Sapienza"
Via Salaria 113, 00198 Roma, Italy email: {piluc,trevisan}@dsi.uniroma1.it

Abstract Number 94-13

It has been recently proved the existence of polynomially bounded NP optimization problems which are APX-complete with respect to the PTAS-reducibility, i.e., a reducibility preserving membership in PTAS [1].
This result has been used to obtain a more significant one, that is, the equivalence between APX and (the closure of) the class MAX SNP [2]. As a consequence, many natural problems, such as MAX CUT, MIN NODE COVER, MIN Δ-TSP, and MAX COMMON SUPERSTRING, turn out to be APX-complete.
We first give some evidence that these results cannot be obtained by making use of the L-reducibility [3]. Then we prove the existence of natural APX-intermediate problems: in particular, we show that MIN BIN PACKING and MIN EDGE COLORING, which are in APX$-$PTAS, cannot be APX-complete unless the polynomial-time hierarchy collapses.
Finally, we prove that no polynomially bounded NPO-complete problem exists unless $O(\log n)$ queries to SAT are equivalent to $O(\log \log n)$ queries to SAT.

References

[1] P. Crescenzi and L. Trevisan. On approximation scheme preserving reducibility and its applications. Submitted for pubblication.

[2] S. Khanna, R. Motwani, M. Sudan, and U. Vazirani. On syntactic versus computational views of approximability. Manuscript in preparation.

[3] C.H. Papadimitriou and M. Yannakakis. Optimization, approximation, and complexity classes. *J. Comput. and Syst. Sci.*, 43:425–440, 1991.

The paper is in preparation

Inductive Counting below LOGSPACE

Carsten Damm, FB IV-Informatik, Universität Trier,
54286 Trier, GERMANY, Email: damm@uni-trier.de,
Markus Holzer, Institut für Informatik, Technische Universität München, Arcisstr. 21,
80290 München, GERMANY, Email: holzer@informatik.tu-muenchen.de.

Abstract Number 94-14

Immerman and Szelepcsényi proved that for space bounds $s(n) \geq \log n$ the class $NSpace(s(n))$ is closed under complement. In the inductive counting method used in the proofs the bound on $s(n)$ allows to implement a counter for the number of accessible configurations. It is therefore not known if the result remains true for space bounds below $\log n$. A consequence of the Immerman-Szelepcsényi-result is the collapse of the alternating space hierarchy to its first level for space bounds $s(n) \geq \log n$.
Very recently it has been proved by von Braunmühl, by Geffert, and (also independently) by Liśkiewicz and Reischuk that the alternating space hierarchy does not collapse for sublogarithmic space bounds — bounds between $\Omega(\log \log n)$ and $o(\log n)$.
In contrast to this we show that for a nonuniform model of computation the corresponding hierarchy collapses for *any* space bound. We perform inductive counting on nondeterministic branching programs without increasing the width of the programs too much. This is another application of the inductive counting technique to a circuit like model. We prove further that width restricted branching programs are equivalent in computational power to a variant of nonuniform Turing machines. This proves $NSpace(s(n)) = co\text{-}NSpace(s(n))$ in a nonuniform setting.
The nonuniform Turing machines we study are generalizations of the nonuniform finite automata introduced by Barrington and in case $s(n) \geq \log n$ coincide with the usual Karp-Lipton model of nonuniformity.

A full paper is available.

Two Remarks on Self-Correctability versus Random-Self-Reducibility (Preliminary Version)

Joan Feigenbaum, AT&T Bell Laboratories, Room 2C-473, Murray Hill, NJ 07974 USA, jf@research.att.com
Lance Fortnow, University of Chicago, Computer Science Department, Chicago, IL 60637 USA, fortnow@cs.uchicago.edu
Ashish Naik, State University of New York, Computer Science Department, Buffalo, NY 14260 USA, avnaik@cs.buffalo.edu

Abstract Number 94-15

We examine the relationship between two types of probabilistic self-reductions that play crucial roles in the theory of interactive proof systems, program-checking, and program-testing: *self-correctors* and *random-self-reductions*. It is well known that if a function is random-self-reducible, then it is also self-correctable [Blum *et al.*, Journal of Computer and System Science, 47 (1993), pp. 549–595]. Indeed all known self-correctors use some form of random-self-reducibility. However, whether self-correctability implies random-self-reducibility, i.e., whether the two properties are equivalent, remains an important open question.
We show that:

(i) If UEEEXP $\not\subseteq$ REEEXP, then there exists a function f that is nonadaptively self-correctable but *not* nonadaptively random-self-reducible.

(ii) If #P $\subseteq$ FP, then every function that is nonadaptively self-correctable with respect to a P-sampleable ensemble is also nonadaptively random-self-reducible.

A full paper is available.

A Game-Theoretic Classification of Interactive Complexity Classes

Joan Feigenbaum, AT&T Bell Laboratories, Room 2C-473, Murray Hill, NJ 07974, jf@research.att.com
Daphne Koller, Computer Science Division, University of California, Berkeley, CA 94720 daphne@cs.berkeley.edu
Peter Shor, AT&T Bell Laboratories, Room 2D-149, Murray Hill, NJ 07974 shor@research.att.com

Abstract Number 94-16

Game-theoretic characterizations of complexity classes have often proved useful in understanding the power and limitations of these classes. One well-known example tells us that PSPACE can be characterized by two-person, perfect-information games in which the length of a played game is polynomial in the length of the description of the initial position [Chandra *et al.*, Journal of the ACM, 28 (1981), pp. 114–133].

In this paper, we investigate the connection between game theory and interactive computation. We formalize the notion of a *polynomially definable game system* for the language L, which, informally, consists of two arbitrarily powerful players P_1 and P_2 and a polynomial-time referee V with a common input w. Player P_1 claims that $w \in L$, and player P_2 claims that $w \notin L$; the referee's job is to decide which of these two claims is true. In general, we wish to study the following question:

> *What is the effect of varying the system's game-theoretic properties on the class of languages recognizable by polynomially definable game systems?*

There are many possible game-theoretic properties that we could investigate in this context; in this paper, we focus on the question of what happens when one or both of the players P_1 and P_2 have *imperfect information* or *imperfect recall*.

We use polynomially definable game systems to derive new characterizations of the complexity classes NEXP and co-NEXP. We also derive partial results about other exponential complexity classes and isolate some intriguing open questions about the effects of imperfect information and imperfect recall. These results make use of recent work on complexity-theoretic aspects of games, e.g., [Koller *et al.*, Proc. of 26th ACM Symposium on Theory of Computing, 1994, pp. 750–759] and [Lipton *et al.*, Proc. of 26th ACM Symposium on Theory of Computing, 1994, pp. 734–740]. Finally, we provide a comparison of our computational model with previous models that are also influenced by game theory, e.g., [Reif, Journal of Computer and System Science, 29 (1984), pp. 274–301], [Feige *et al.*, Advances in Cryptology – CRYPTO '88, 1990, pp. 284–296], and [Kiwi *et al.*, Proc. of 9th IEEE Structure in Complexity Theory Conference, 1994].

A full paper is not yet available.

On Inverting the Turing Jump in Complexity Theory

Stephen Fenner, Computer Science Dept., University of Southern Maine, 96 Falmouth St., Portland, ME 04103, USA. fenner@usm.maine.edu

Abstract Number 94-17

Is every NP-hard set NP^A-complete for some A? An affirmative answer to the corresponding question in recursion theory ("Is the Turing jump invertible?") was found in the 1950s by Friedberg (Friedberg, "A criterion for completeness of degrees of unsolvability," J. Symbolic Logic, vol. 22 (1957), pp. 159–160). The present question regarding the NP-jump (with respect to polynomial-time Turing reductions) appears more difficult; Friedberg's techniques do not work here.

We show that if the NP-jump *is* invertible, then NP $\neq$ coNP. More generally, if the Σ_n^p-jump is invertible, then $\Sigma_n^p \neq \Pi_n^p$. We conjecture that these and other complexity theoretic jumps are not invertible.

For example, the PSPACE-jump is not invertible, as we can readily see: it is easy to verify that A has a PSPACE-jump inverse if and only if $\mathrm{P}^A = \mathrm{PSPACE}^A$, but there are clearly PSPACE-hard sets A where this is not the case.

We also show that for a wide range of classes $\mathcal{C}$, the invertibility of the $\mathcal{C}$-jump is equivalent to the single set $G \oplus C$ having a $\mathcal{C}$-jump inverse, where G is any 1-generic set, C is some $\mathcal{C}$-complete set, and $\oplus$ is the join operation. We also study the set $G \oplus \mathrm{SAT}$ and show, for example, that it always lies strictly between some set A and SAT^A.

This work was presented at the Dagstuhl seminar on Structural Complexity, February, 1994.

A full paper is available from the address above or in person.

Beyond $\mathbf{P^{NP} = NEXP}$

Stephen Fenner, Computer Science Dept., University of Southern Maine, 96 Falmouth St., Portland, ME 04103, USA. `fenner@usm.maine.edu`
Lance Fortnow, Computer Science Dept., University of Chicago, 1100 E. 58th St., Chicago, IL 60637, USA. `fortnow@cs.uchicago.edu`

Abstract Number 94-18

Using a very clever and delicate finite injury construction, Buhrman & Torenvliet recently found an oracle relative to which $\mathrm{P}^{\mathrm{NP}} = \mathrm{NEXP}$ (Buhrman & Torenvliet, ICALP 1994, to appear). Their oracle is r.e. but evidently not recursive, and they left it as an open question whether a recursive oracle exists.
We show that (1) a recursive oracle does exist, and (2) there is an oracle A such that

- $\mathrm{P}^{\mathrm{NP}^A} = \mathrm{NEXP}^A$, and
- $\mathrm{P}^A = \mathrm{UP}^A = \mathrm{NP}^A \cap \mathrm{coNP}^A$.

We thus obtain a rather odd lowness property relative to A: $\mathrm{Low}(\mathrm{NP}) = \mathrm{P}$, but $\mathrm{Low}(\mathrm{P}^{\mathrm{NP}}) = \mathrm{NEXP}$.
The recursive oracle is constructed by removing the injury from Buhrman & Torenvliet's proof and putting it in a simpler setting. To construct A, we combine our new construction with older ideas of Hartmanis & Hemachandra and Blum & Impagliazzo. Our A is not recursive, but we believe it can be made so. We hope these techniques may be of use in finding other oracles, for example, an oracle relative to which the NP-jump is invertible.

A full paper is not yet available.

Transfinite Polynomial Hierarchies

Stephen Fenner, Computer Science Dept., University of Southern Maine, 96 Falmouth St., Portland, ME 04103, USA, `fenner@usm.maine.edu`,
Steven Homer, Computer Science Dept., Boston University, 111 Cummington St., Boston, MA 02215, USA, `homer@cs.bu.edu`.

Abstract Number 94-19

It is well-known that if the polynomial hierarchy separates, then it is not equal to PSPACE. We show that if PH separates, then the gap between PH and PSPACE is quite large, in the sense that one can fit into PSPACE a proper transfinite polynomial hierarchy of height ω_1^{CK}, the first nonrecursive ordinal.
More exactly, we show that if PH separates, then there is a one-to-one embedding $\alpha \mapsto \mathbf{h}_\alpha$ of ω_1^{CK} into the ptime T-degrees in PSPACE such that

- $\mathbf{h}_0 = \mathrm{P}$, the minimum degree,
- $\mathbf{h}_{\alpha+1}$ is the NP-complete degree relative to $\mathbf{h}_\alpha$, for all $\alpha < \omega_1^{\mathrm{CK}}$, and
- for all limit $\lambda < \omega_1^{\mathrm{CK}}$, $\mathbf{h}_\lambda$ is a (recursively) uniform upper bound for $\{\mathbf{h}_\alpha\}_{\alpha<\lambda}$.

Our present result extends an earlier result of Ambos-Spies showing that if PH separates then there is a PSPACE-incomplete, PH-hard set (*Theoretical Comp. Sci.*, 63 (1989), pp. 43–61). We combine delayed diagonalization techniques similar to those of Ambos-Spies and of Ladner (*J. ACM*, 22 (1975), pp. 155–171) with effective transfinite recursion. These ideas bear some analogy with the study of the hyperarithmetic sets in recursion theory, but differ in that there is no unique, canonical way to define the mapping above. One can, however, define a natural, robust transfinite polynomial hierarchy of height ω_1^{CK} in PSPACE that contains many of the possible mappings above. This "universal" hierarchy is well-founded but not linearly ordered.
We are interested in studying the relationship between these hierarchies and other classes in PSPACE, particularly counting classes.

A full paper is not yet available.

Weakly Useful Sets

Stephen Fenner, Computer Science Dept., University of Southern Maine, 96 Falmouth St., Portland, ME 04103, USA, fenner@usm.maine.edu,
Jack Lutz, Computer Science Dept., Iowa State University, Ames, IA 50011, USA, lutz@cs.iastate.edu,
Elvira Mayordomo, Universidad de Zaragoza, Depto. Ingenieria Informatica, C.P.S., Maria de Luna 3, 50015 Zaragoza, SPAIN, emayordomo@mcps.unizar.es.

Abstract Number 94-20

We show that there is a weakly useful set that is not strongly useful.
A set A to be *strongly useful* if there is a recursive time bound $t(n)$ such that every recursive set is Turing reducible to A in time $t(n)$. Thus, strongly useful means time-$t(n)$-hard for the class REC of recursive sets, for some t (for example, the general halting problem is useful with $t(n) = n^2$. This notion was defined by Juedes, Lathrop, and Lutz ("Computational Depth and Reducibility", *Theoretical Comp. Sci.*, to appear), and is related to that of logical depth introduced by Bennett. They showed that the strongly useful Turing degrees are exactly the high degrees.
Juedes, Lathrop, and Lutz also defined a set A to be *weakly useful* if there is a recursive t such that a nonnegligible fraction of REC (in the sense of recursive measure) is reducible to A in time $t(n)$. They posed as an open problem whether there is a weakly useful set that is not strongly useful. We give an affirmative answer.
To prove our result, we adapt the method of *martingale diagonalization*, first introduced by Lutz to show that there there is a weakly m-complete set for E that is not m-complete for E (Lutz, "Weakly Hard Problems", *SIAM J. Comput.*, to appear). We also construct, for every recursive t, a "highly incompressible" set A_t whose upper span (upper cone) under time-t-bounded reductions has rec-measure 0. The sets A_t and the notion of high incompressibility may have uses in other areas of complexity theory independent of our results.
Still open is the question of whether there are weakly useful degrees which are not high.
A full paper is not yet available.

Complexity Classes Without Programming Systems

Stephen A. Fenner, Computer Science Dept., University of Southern Maine, 96 Falmouth St., Portland, ME 04103, USA, `fenner@usm.maine.edu`,
Kenneth W. Regan, Department of Computer Science, State Univ. of NY at Buffalo, 226 Bell Hall, Buffalo NY 14260-2000, USA, `regan@cs.buffalo.edu`.

Abstract Number 94-21

Several recent papers have concerned bounds on time or proof-size or other resources of the form "$n^{1+o(1)}$" or "in DTIME$[n^{1+\epsilon}]$ for all $\epsilon > 0$" or "in DTIME$[2^{n^{\epsilon+\delta}}]$ for all $\delta > \epsilon$." (Respectively, Polishchuk and Spielman, STOC'94; E. Graedel, *Int. J. Found. Comp. Sci.* 1:295–307, 1990; Stearns and Hunt, *Math. Sys. Thy.* 23:209–225, 1990, definition of "power index ϵ.") It is natural to ask whether these complexity classes have effective enumerations of machines, a familiar and important property of P, NP, and any class defined by a "nice" recursive resource bound $t(n)$.

We show that the answer is *no*. For instance, if $\mathcal{C}$ is any class such that DTIME$[n^{1+o(1)}] \subseteq \mathcal{C} \subseteq \bigcap_{\epsilon>0}$DTIME$[n^{1+\epsilon}]$, then $\mathcal{C}$ has no effective enumeration by machines, even if the machines themselves are only required to be total, not even to run in polynomial time. It follows that membership in $\mathcal{C}$ is not in general a provable property of languages. For another instance, Yao and Nisan-Wigderson showed that good pseudorandom generators yield BPP$\subseteq \bigcap_{\epsilon>0}$DTIME$[2^{n^\epsilon}]$; our result shows that this would be a proper containment. Our methods are quite general and apply to many classes defined as infinite intersections of other classes. As a consequence, there can be no "Intersection Theorem" analogous to the Union Theorem in abstract complexity.

A full paper is not yet available.

Resource-Bounded Instance Complexity

Lance Fortnow[a], Department of Computer Science, University of Chicago, 1100 E. 58th St., Chicago, IL 60637. (Email: `fortnow@cs.uchicago.edu`).
Martin Kummer, Institut für Logik, Komplexität und Deduktionssysteme, Universität Karlsruhe, D-76128 Karlsruhe, Germany. (Email: `kummer@ira.uka.de`).

Abstract Number 94-22

Instance complexity was introduced by Ko, Orponen, Schöning, and Watanabe (1st STRUCUTRES, 1986 and JACM 41:96–121, 1994) as a measure of the complexity of individual instances of a decision problem A. Informally, the instance complexity $ic(x : A)$ of x with respect to A is the length of the shortest program p which correctly computes $\chi_A(x)$ and does not make any mistakes on other inputs (it is permitted to output "don't know" answers). We consider the resource-bounded version $ic^t(x : A)$ where the running time of p is bounded by some polynomial t.

The "Instance Complexity Conjecture" of Orponen et al. states that every set $A \notin \mathrm{P}$ must have *p-hard instances*, i.e., for every polynomial t there is a polynomial t' such that $ic^t(x : A) \geq C^{t'}(x) + O(1)$ for infinitely many x, where $C^{t'}(x)$ denotes the t'-time bounded Kolmogorov complexity of x. We show that the conjecture holds for all recursive tally sets A. Orponen et al. proved that every set which is NP-complete under honest 1-tt reductions has p-hard instances, unless DEXT = NEXT. We obtain a strong improvement of this result: All sets which are NP-complete under honest Turing reductions have p-hard instances, unless P = NP.

The Instance Complexity Conjecture cannot be settled with relativizable methods, since we construct relativized worlds where it holds and where it fails. In fact, we even show that the CD-version of the conjecture—where C-complexity is replaced by Sipser's CD-complexity—fails in some relativized world. Orponen et al. obtain a weak form of the conjecture 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.

In addition, two other questions from of Orponen et al. are settled: We construct a relativized world in which p-hard instances are not inherited upwards under polynomial 1-reductions, and we show that the ic-measure is not recursive.

Finally, we compare time-bounded C- and CD-complexity and discuss the consequences when they coincide.

A full paper is available.

[a] Partially supported by NSF Grant CCR 92-53582.

Separability and One-way Functions

Lance Fortnow (fortnow@cs.uchicago.edu), John Rogers (rogers@cs.uchicago.edu)
Department of Computer Science, University of Chicago,
1100 East 58th Street, Chicago IL 60637 USA.

Abstract Number 94-23

Consider the following five complexity propositions:

1. $P = NP$;
2. $P = UP$ (which is equivalent to the nonexistence of one-way functions);
3. $P = NP \cap coNP$;
4. all disjoint pairs of sets in NP are P-separable;
5. all disjoint pairs of sets in $coNP$ are P-separable.

It is relatively easy to show that proposition (1) implies the rest and that propositions (4) and (5) imply proposition (3). Grollmann and Selman show that proposition (4) implies proposition (2).
We show that these are the only implications to hold in every relativized world by using novel applications of genericity.

A full paper is available.

On the number of Graph Automorphisms

William Gasarch, Department of Computer Science, University of Maryland, College Park, MD., 20742
Jacobo Torán, Dept L.S.I., U. Politecnica de Catalunya, Pau Gargallo 5, E-08028 Barcelona.

Abstract Number 94-24

Cai and Hemachandra (*Enumerative Counting is Hard*, Structures88 and Information and Control 89) defined $b(n)$-enumerability as follows: Let $b(n)$ be a function with range N. A function f is $b(n)$-*enumerable* if there exists $e \in$ PF, such that, for all x, $e(x)$ is a list of at most $b(|x|)$ elements of Σ^*, separated by %, at least one of which is $f(x)$.

This definition only makes sense if $b(|x|)$ is bounded by a polynomial. Amir, Beigel, and Gasarch (*Some Connections between Bounded Query Classes and Non-uniform Complexity*, Structures90) defined a more general notion of enumerability that allows superpolynomial b: Let $b(n)$ be a function with range N. A function f is $b(n)$-*enumerable* if there exists $e \in$ PF, $e : \Sigma^* \times N \to \Sigma^*$, such that, for all x, there exists an $i < b(|x|)$ such that $e(x, i) = f(x)$.

We investigate the enumerability of the function #Aut which takes a graph and outputs the number of automorphism it has. We use the number of nodes, n, as the parameter of interest instead of the length of the input.

Theorem 1: If #Aut has an $h(n)$-enumerator for some function $h(n) \leq 2^{n^\epsilon}$ for $\epsilon < 1/5$ then GA $\in$ NP(log($h(n^{15})$))/poly.
This theorem uses a protocal similar to the one that establishes $\overline{GI} \in AM$. Also, from the proof of this result follows that if #Aut has polynomial enumerators then GA $\in$ R.

Theorem 2: If #Aut has a n^ϵ enumerator for some $\epsilon < 1$ then GA $\in$ P (hence GI $\in$ P).
This theorem uses some of the machinery developed by Amir, Beigel, and Gasarch (*Some Connections between Bounded Query Classes and Non-uniform Classes*, Preprint, 1994).

Babai has shown the following upper bound:

Theorem 3: #Aut is $2^{n/2}(n/2)!$-enumerable.

NP Trees and Carnap's Modal Logic

Georg Gottlob, Institut für Informationssysteme, Technische Universität Wien, Paniglgasse 16, A-1040 Wien, AUSTRIA (gottlob@vexpert.dbai.tuwien.ac.at)

Abstract Number 94-25

We consider problems and complexity classes definable by interdependent queries to an oracle in NP. How the queries depend on each other is specified by a directed graph G. We first study the class of problems where G is a general dag and show that this class coincides with Δ_2^P. We then consider the class where G is a tree. Our main result states that this class is identical to Θ_2^P, the class of problems solvable in polynomial time with a logarithmic number of queries to an oracle in NP. This result has interesting applications in the fields of modal logic and artificial intelligence. In particular, we show that the following problems are all Θ_2^P complete: validity-checking of formulas in Carnap's modal logic, checking whether a formula is almost surely valid over finite structures in modal logics **K**, **T**, and **S4** (a problem recently considered by Halpern and Kapron), and checking whether a formula belongs to the stable set of beliefs generated by a propositional theory.

We generalize the case of dags to the case where G is a general (possibly cyclic) directed graph of NP-oracle queries and show that this class corresponds to Π_2^P. We show that such graphs are easily expressible in autoepistemic logic. Finally, we generalize our complexity results to higher classes of the polynomial-time hierarchy.

Received October 1993

Extended Abstract in Proc. FOCS'93. A full paper is available by email/ftp from the author.

Pseudorandom Generators and the Frequency of Simplicity

Yenjo Han and *Lane A. Hemaspaandra*, Department of Computer Science, University of Rochester, Rochester, NY 14627 USA.

Abstract Number 94-26

Allender [All89] showed that if there are dense P languages containing only a **finite** set of Kolmogorov-simple strings, then all pseudorandom generators are insecure. We extend this by proving that if there are dense P (or even BPP) languages containing only a **sparse** set of Kolmogorov-simple strings, then all pseudorandom generators are insecure.

[All89] E. Allender. Some consequences of the existence of pseudorandom generators. *Journal of Computer and System Sciences*, 39:101–124, 1989.

A full paper is available as TR 507, Department of Computer Science, University of Rochester, May 1994.

Advice from Nonadaptive Queries to NP

Yenjo Han, Department of Computer Science, University of Rochester, Rochester, NY 14627 USA,
Thomas Thierauf, Abteilung Theoretische Informatik, Universität Ulm, Oberer Eselsberg, 89069 Ulm, Germany.

Abstract Number 94-27

Consider the standard model of computation to decide a language that is bounded truth-table reducible to an NP set: on a given input, a polynomial-time Turing machine, called a *generator*, produces a constant number of queries to the NP oracle; then, a second polynomial-time Turing machine, called an *evaluator*, given the answers to the queries, determines the membership of the given input.
In this paper, we investigate the classes of languages that are decided by bounded truth-table reductions to an NP set in which evaluators do not have full access to the answers to the queries but get only partial information such as the number of queries that are in the oracle set or even just this number modulo some constant. We also investigate the case in which evaluators are nondeterministic.
We locate all these classes within levels of the boolean hierarchy, which allows us to compare the complexity of such classes. The result shows the various degrees to which the power of P or NP evaluators are affected as the partial information that the evaluators get from the answers to the queries produced by generators are changed.

A full paper is available as TR 470, Department of Computer Science, University of Rochester, October 1993.

Computing Solutions Uniquely Collapses the Polynomial Hierarchy

Lane A. Hemaspaandra, Department of Computer Science, University of Rochester, Rochester, NY 14627.
Ashish V. Naik, Department of Computer Science, SUNY–Buffalo, Buffalo, NY 14260.
Mitsunori Ogihara, Department of Computer Science, University of Rochester, Rochester, NY 14627.
Alan L. Selman, Department of Computer Science, SUNY–Buffalo, Buffalo, NY 14260.

Abstract Number 94-28

Is there an NP function that, when given a satisfiable formula as input, outputs one satisfying assignment uniquely? 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. As the existence of such a function is known to be equivalent to the statement "every NP function has an NP refinement with unique outputs," our result provides the strongest evidence yet that NP functions cannot be refined.

We prove our result via theorems of independent interest. We say that a set A is NPSV-selective (NPMV-selective) if there is a 2-ary partial NP function with unique values (a 2-ary partial NP function) that decides which of its inputs (if any) is "more likely" to belong to A; this is a nondeterministic analog of the recursion-theoretic notion of the semi-recursive sets and the extant complexity-theoretic notion of P-selectivity. Our hierarchy collapse result follows by combining the easy observation that every set in NP is NPMV-selective with either of the following two theorems that we prove:

(1) If $A \in \mathrm{NP}$ is NPSV-selective, then $A \in (\mathrm{NP} \cap \mathrm{co\text{-}NP})/\mathrm{poly}$.
(2) If $A \in \mathrm{NP}$ is NPSV-selective, then A is Low_2.

To wit, either result implies that if every set in NP is NPSV-selective, then the polynomial hierarchy collapses to its second level, $\mathrm{NP}^{\mathrm{NP}}$.

We prove that the polynomial hierarchy collapses even further, namely to NP, if all coNP sets are NPMV-selective. This follows from a more general result we prove: Every self-reducible NPMV-selective set is in NP.

We also prove that all sets in $\mathrm{NP/poly} \cap \mathrm{co\text{-}NP/poly}$ are in the third level of the extended low hierarchy. This solves an open question by [Köbler, 10^{th} *STACS*, pp. 28–37, 1993].

A full paper is available.

Unambiguous Computation: Boolean Hierarchies and Sparse Turing-Complete Sets

Lane A. Hemaspaandra, Department of Computer Science, University of Rochester, Rochester, NY 14627, USA,
Jörg Rothe, Fakultät für Mathematik und Informatik, Friedrich-Schiller-Universität Jena, Universitätshochhaus 17. OG, 07743 Jena, GERMANY.

Abstract Number 94-29

This paper studies, for UP, two topics that have been intensely studied for NP: Boolean hierarchies and the consequences of the existence of sparse Turing-complete sets. Unfortunately, as is often the case, the results for NP draw on special properties of NP that do not seem to carry over straightforwardly to UP. For example, it is known for NP (and more generally for any class containing Σ^* and $\emptyset$ and closed under union and intersection) that the symmetric difference hierarchy, the Boolean hierarchy, and the Boolean closure all are equal. We prove that closure under union is not needed for this claim: For any class $\mathcal{K}$ that contains Σ^* and $\emptyset$ and is closed under intersection (e.g., UP, US, and FewP), the symmetric difference hierarchy over $\mathcal{K}$, the Boolean hierarchy over $\mathcal{K}$, and the Boolean closure of $\mathcal{K}$ all are equal. On the other hand, we show that two hierarchies—the Hausdorff hierarchy and the nested difference hierarchy—which in the NP case are equal to the Boolean closure fail to be equal for the UP case in some relativized worlds. Regarding sparse Turing-complete sets for UP, we prove that if UP has sparse Turing-complete sets, then the levels of the unambiguous polynomial hierarchy are simpler than one would otherwise expect: they collapse one level in terms of their location in the promise unambiguous polynomial hierarchy. We obtain related results under the weaker assumption that UP has sparse Turing-hard sets.

A full paper is available as Technical Report 483 of the University of Rochester.

Strong Forms of Balanced Immunity

Lane A. Hemaspaandra and *Marius Zimand*, Department of Computer Science, University of Rochester, Rochester, NY 14627, e-mail: lane@cs.rochester.edu, zimand@cs.rochester.edu

Abstract Number 94-30

Many feel that when one does prove relativized separations, one should seek to establish the highest level in the relativized separation "hierarchy" whose levels are (there exists an oracle achieving): 1) separation, 2) separation with immunity, 3) separation with bi-immunity, 4) separation with balanced immunity. (Informally, a class is balanced immune to another class if the former class contains an infinite, coinfinite set such that any set from the latter class asymptotically has half it elements in the set and half its elements out of the set.) Each of the separation types listed above yields alternate, and potentially stronger, separations when it holds with respect to a generic oracle or to a random oracle (i.e., with probability one). We analyze in terms of the above hierarchy the relativized separation from P possible for the class NT. We show that NT is P bi-immune relative to a generic oracle. This is optimal as we note that NT is *not* P balanced immune (and this result itself relativizes). This verifies an intuition of Allender that, at least when both notions are driven to extremes, self-reducibility should thwart immunity. For NP, we strengthen the Bennett-Gill construction to establish that NP is P balanced immune with probability one. It follows that $\oplus$P is also P balanced immune with probability one. We also investigate the structure of ambiguity-bounded classes.

A full paper is available.

The computational complexity of recognizing permutation functions

KEJU MA AND JOACHIM VON ZUR GATHEN
Department of Computer Science, University of Toronto
Toronto, Ontario M5S 1A4, Canada
keju, gathen@cs.toronto.edu

Abstract Number 94-31

Let $\mathbf{F}_q$ be a finite field with q elements and $f \in \mathbf{F}_q(x)$ a rational function over $\mathbf{F}_q$. No polynomial-time deterministic algorithm is known for the problem PermFunction of deciding whether f induces a permutation on $\mathbf{F}_q$. The problem has been shown to be in co-$\mathcal{R} \subseteq$ co-$\mathcal{NP}$, and in this paper we prove that it is in $\mathcal{R} \subseteq \mathcal{NP}$ and hence in $\mathcal{ZPP}$, and it is deterministic polynomial-time reducible to the problem PolyFactor of factoring univariate polynomials over $\mathbf{F}_q$. Besides the problem Prime of recognizing prime numbers, it seems to be the only natural decision problem in $\mathcal{ZPP}$ unknown to be in $\mathcal{P}$. A deterministic test and a simple probabilistic test for permutation functions are also presented.

A full paper is available.

Kolmogorov Complexity and Instance Complexity of Recursively Enumerable Sets

Martin Kummer, Institut für Logik, Komplexität und Deduktionssysteme, Universität Karlsruhe, D-76128 Karlsruhe, Germany. (Email: `kummer@ira.uka.de`).

Abstract Number 94-32

Traditionally Kolmogorov complexity measures the "descriptional complexity" of a string x. It is defined as the length of the shortest program that computes x from the empty input. Accordingly, the Kolmogorov complexity of initial segments of a set A is considered as a measure of the "randomness" of A. It is well-known that for r.e. sets the Kolmogorov complexity of initial segments of length n is bounded by $2 \log n$. We show that this bound is optimal and characterize the Turing degrees of r.e. sets which attain this bound as the array nonrecursive degrees of Downey, Jockusch, and Stob (1990).

Ko, Orponen, Schöning, and Watanabe (1986, 1994) have recently introduced the notion of *instance complexity* as a measure of the complexity of individual instances of A. Informally, $ic(x : A)$, the instance complexity of x with respect to A, is the length of the shortest total program which correctly computes $\chi_A(x)$ and does not make any mistakes on other inputs, but it is permitted to output "don't know" answers. It is easy to see that the Kolmogorov complexity of x is an upper bound for the instance complexity of x (up to a constant). A set A has *hard instances* if for infinitely many x the instance complexity of x w.r.t. A is at least as high as the Kolmogorov complexity of x (up to a constant which may depend on A), i.e., the trivial upper bound is already optimal.

Orponen et al. conjectured that every nonrecursive r.e. set has hard instances ("Instance Complexity Conjecture (ICC)"). Buhrmann and Orponen (1994) proved ICC for m-complete sets. Tromp (1993) proved that the instance complexity of x w.r.t. any nonrecursive set A is infinitely often at least logarithmic in the Kolmogorov complexity of x. We construct an r.e. nonrecursive set which attains this lower bound for all x. In particular, this is a counterexample to ICC. On the positive side, we show that ICC holds for wtt-complete sets, Q-complete sets, and hyperhypersimple sets. But ICC fails for a T-complete set, since it fails for an effectively simple set. However, ICC holds for all strongly effectively simple sets. We also investigate a weak version of instance complexity, where programs may not halt instead of giving "don't know" answers.

A full paper is available.

A Kolmogorov Complexity proof of Håstad's switching lemma: An exposition

Sophie Laplante (sophie@cs.uchicago.edu)
Department of Computer Science, University of Chicago,
1100 East 58th Street, Chicago IL 60637 USA.

Abstract Number 94-33

Håstad's switching lemma[a] has played a key role in obtaining lower bound results in circuit complexity. Razborov[b] presented a new proof of Håstad's lemma with the intent of establishing the logical requirements for a variety of lower bound results. The proof itself, however, has generated independent interest as an alternative proof for the lemma. Lance Fortnow further observed that Razborov's proof could easily be expressed in terms of elementary Kolmogorov complexity. We provide the details of this version of Razborov's proof.

A technical report is available by anonymous ftp from `cs.uchicago.edu` in the file `pub/users/fortnow/switch.ps`, or from the author.

[a] J. Håstad, *Computational Limitations of Small-Depth Circuits*, ACM doctoral dissertation award, 1986. MIT Press, 1987.

[b] A. Razborov, *Bounded arithmetic and lower bounds in Boolean complexity*, Submitted to Feasible Mathematics II, 1993.

Kolmogorov indistinguishability and communication complexity

Sophie Laplante (sophie@cs.uchicago.edu), John Rogers (rogers@cs.uchicago.edu)
Department of Computer Science, University of Chicago,
1100 East 58th Street, Chicago IL 60637 USA.

Abstract Number 94-34

Two strings (of the same length) are said to be *(Kolmogorov) k-indistinguishable* if no program of length k or less will output 1 on one string and 0 on the other. We provide some elementary technical lemmas about the number of k-indistinguishable pairs and the size of sets of pairwise indistinguishable sets.

We use these results to improve slightly on the standard result on the density of recursive sets[a]. We prove that for any recursive set A, and any string x of length n in A, $|A^{=n}| \geq 2^{C(x)-O(1)}$, where $C(x)$ represents the Kolmogorov complexity of the string x.

We apply these ideas to problems in communication complexity. We prove that there are communication problems for which the nondeterministic communication complexity for both 0 and 1 instances is $n-1$.

In further research, we hope to establish a technical framework in which to prove lower bound results in communication complexity using the techniques of Kolmogorov complexity and indistinguishability.

A full paper is not yet available but we like e-mail.

[a] Li, M., and Vitányi, P., *An Introduction to Kolmogorov Complexity and its Applications*, Springer–Verlag, 1993, p. 99.

Are Parallel Machines Always Faster Than Sequential Machines?

Louis Mak, Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, 1308 W. Main St., Urbana, IL 61801. Email: `mak@grinch.csl.uiuc.edu`

Abstract Number 94-35

It is shown that parallel machines are always faster than sequential machines for a wide range of machine models, including the tree Turing machine, the multidimensional Turing machine, and the log-cost RAM (random access machine). More precisely, it is shown that every sequential machine M (in the above list) that runs in time T can be sped up by a parallel version M' of M that runs in time $o(T)$. All previous speedup results either rely on the severe limitation on the storage structure of M (e.g., M is a Turing machine with linear tapes) or require that M' has a more versatile storage structure than M (e.g., M' is a PRAM (parallel RAM), and M is a Turing machine with linear tapes). It is unclear whether it is the parallelism, or the restriction on the storage structures, or the combination of both that realizes such speedup. This paper removes all the above restrictions on storage structures in previous results. This paper presents speedup theorems where both M and M' use the same kind of storage medium, which is not linear tapes. Thus, parallelism alone suffices to achieve the speedup.

Received November 1993

A full paper is available.

Parallelism Always Helps

Louis Mak, Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, 1308 W. Main St., Urbana, IL 61801. Email: `mak@grinch.csl.uiuc.edu`

Abstract Number 94-36

It is shown that every unit-cost random access machine (RAM) that runs in time T can be simulated by a concurrent-read exclusive-write parallel random access machine (CREW PRAM) in time $O(T^{1/2} \log T)$. The proof is constructive; thus, it gives a mechanical way to translate any sequential algorithm designed to run on a unit-cost RAM into a parallel algorithm that runs on a CREW PRAM and obtain a nearly quadratic speedup. One implication is that there does not exist any recursive function that is "inherently not parallelizable."

Received December 1993

A full paper is available.

The Varying Power of a Logspace Verifier

Meena Mahajan
The Institute of Mathematical Sciences,
C.I.T. Campus, Madras 600 113, India.
email: meena@imsc.ernet.in

V Vinay
Centre for Artificial Intelligence and Robotics,
Bangalore 560 001, India.
email: vinay@yantra.ernet.in

Abstract Number 94-37

We investigate Arthur-Merlin protocols, where Arthur is logspace-resource-bounded but may have restricted access to auxiliary storage. We show that auxiliary storage in the form of a pushdown stack, along with a logarithmic number of coin tosses, exactly captures $\mathcal{NP}$. An auxiliary checking stack, with only one alternation between pushdown mode and scan mode, suffices to capture $\mathcal{PSPACE}$. Logspace-bounded Arthur-Merlin protocols are characterized, via logspace reductions, with Arithmetic Circuits on MAX and \$ gates. We show that such circuits are equivalent to Arthur-Merlin protocols, with the depth and size of the circuit equalling the rounds of interaction and the verifier's space bound respectively in the protocol. Using this, we describe an Arthur-Merlin protocol for accepting any language in $\mathcal{NC}$ after a logspace transduction, where Arthur is logspace-bounded and the protocol requires polylog time. Omitting the transduction gives a protocol with polylog rounds of interaction.

A full paper is available as Technical Report IMSc-94/27 and can be obtained from the first author or by anonymous ftp from imsc.ernet.in (144.16.253.1).

Quasilinear Time Complexity Theory

Ashish V. Naik, Department of Computer Science, State Univ. of NY at Buffalo, 226 Bell Hall, Buffalo NY 14260-2000,
Kenneth W. Regan, SUNY/Buffalo,
D. Sivakumar, SUNY/Buffalo,

Abstract Number 94-38

The accepted yardstick for a program to be feasible is that it run in (randomized) *polynomial* time. However, a running time of n^{45} or even n^3 or n^2 may not really be feasible in practice. This paper advances the study of problems solvable by algorithms that run in *quasilinear* time, namely time $n \cdot (\log n)^{O(1)}$. The quasilinear time classes DQL and NQL are analogous to P and NP for deterministic and nondeterministic Turing machines, and Schnorr [J.ACM, 1978] showed that SAT is complete for NQL under DQL reductions. We ask whether the theorem of Toda [SIAM JC, 1991] that PH $\subseteq$ BP[$\oplus$P] carries over for QLH. By a new construction involving error-correcting codes, we show that NQL $\subseteq$ BQL[$\oplus$QL], and whether this extends higher than NQL is an interesting problem.

Our main results give a new outlook on the quantitative hardness of problems in NP, in terms of the time required for *search reducing to decision* (SRD). SAT and many other problems have SRD in quadratic time. We show that if SAT has SRD in quasilinear time, then all of NP is in quasi-polynomial time, and SRD in time $O(n^{1+\epsilon})$ for some $\epsilon < 1$ would put SAT itself into $\cap_{\epsilon' > 0}$ DTIME[$2^{n^{\epsilon+\epsilon'}}$]. In the terms of Stearns and Hunt [*Math.Sys.Thy.*, 23:209–225, 1990], the latter says that SAT would have *power index* ϵ. We compare our conjecture that SRD for SAT requires quadratic time with the Hunt-Stearns conjecture that its power index is 1, and with other hypotheses by Krentel, Lutz, Beigel, Gasarch, et al. Some open questions relate to work by Gurevich and Shelah [LNCS 363, 1989] and Homer and Wang [*Math.Sys.Thy.* 22:21–35, 1989].

Journal version of STACS'94 paper, available by anonymous ftp to ftp.cs.buffalo.edu, cd pub/tech-reports, get 94-21.ps.

Linear-Time Algorithms in Memory Hierarchies-1

Kenneth W. Regan, Department of Computer Science, State Univ. of NY at Buffalo, 226 Bell Hall, Buffalo NY 14260-2000,

Abstract Number 94-39

A realistic model of computation called the *Block Move* (BM) model is developed. The BM extends the *Block Transfer* (BT) model of Aggarwal, Chandra, and Snir [FOCS 1987] by allowing any finite transduction on data in block operations, and by having shuffle and reversal of bit-strings as primitives. Like the BT, the BM takes a parameter $\mu : N \to N$ called a *memory access cost function*, and a block move which reads contiguous memory cells $[a - m \ldots a]$ is charged $\mu(a) + m$ time units. Whereas every function that depends on all of its input has a nonlinear lower bound in the BT model, the BM provides a rich theory of linear time.

In contrast to what is known for Turing machines, the BM is proved to be highly *robust* for linear time. Under a wide range of μ parameters, many forms of the BM model, ranging from a fixed-wordsize RAM down to a single finite automaton iterating itself on a single tape, are shown to simulate each other up to constant factors in running time. The BM is proved to enjoy efficient universal simulation, and to have a tight deterministic time hierarchy. Relationships among BM and TM time complexity classes are studied.

Revision of accepted paper to *SIAM J.Comput.*, UB-CS-TR 94-18, May 1994; available by anonymous ftp to ftp.cs.buffalo.edu, cd pub/tech-reports, get 94-18.ps. (¿500K) or get 94-18.ps.Z

Linear-Time Algorithms in Memory Hierarchies-2

Kenneth W. Regan, Department of Computer Science, State Univ. of NY at Buffalo, 226 Bell Hall, Buffalo NY 14260-2000,

Abstract Number 94-40

This paper shows that several basic list-processing primitives, including membership, maximum, length-normalization, and prefix sums, can be computed in linear time on the author's *Block Move* (BM) model. The BM is less restrictive than the *Block Transfer* model of Aggarwal, Chandra, and Snir [FOCS 1987], more restrictive than the LPM pipelining model of Luccio and Pagli [*Math.Sys.Thy.* 26, 1993], and when its *memory-access cost function* $\mu(a) = a^{1/d}$ is set with $d = 1$, more restrictive than a Turing machine. Merging two lists whose elements have size $\Omega(n^{\epsilon})$ is linear time for $d > 1$, but this is open for $d = 1$, and for lists with elements of size $O(\log n)$. A general Kolmogorov-complexity technique for nonlinear time lower bounds on the BM is shown, and applied for a string-editing problem.

To appear in the proceedings of IFIP'94, Hamburg, Germany, August 1994. Available by anonymous ftp to ftp.cs.buffalo.edu, cd pub/tech-reports, get 94-23.ps.

Linear-Speed-Up, Information Vicinity, and Finite-State Machines

Kenneth W. Regan, Department of Computer Science, State Univ. of NY at Buffalo, 226 Bell Hall, Buffalo NY 14260-2000,

Abstract Number 94-41

Define the *vicinity* $v(t)$ of a machine to be the maximum number of stored data bits whose values can conceivably affect the evolution of a computation over the next t steps. (Cf. Feldman and Shapiro [*Comm. ACM*, Oct. 1992].) Turing machines with k linear tapes have vicinity $2kt+1$ and TMs with d-dimensional tapes have vicinity $O(t^d)$; whereas RAMs, TMs with tree-structured tapes, and all known OTMs giving P=NP, all have exponential vicinity. The paper uses a Kolmogorov complexity "volume" argument, extending one by Hühne [IPL 47:313–318, 1993], shows that polynomial vicinity is necessary for the familiar linear speed-up property. One can artificially define models for which the converse does not hold, but the attempt to do this for the author's *Block Move* (BM) model, whose memory-cost parameter d sets the vicinity to $O(t^d)$, leads to several problems of stand-alone interest: Can the standard off-line simulation of a finite-state transducer M, which uses sorting to compose state mappings in M, be improved? (This boils down to the century-old problem of finding the most efficient representations for finite groups.) Can one always code stored programs so that the time to fetch instructions does not dominate the running time? Reasonable answers imply that the BM has a *constant-factor time hierarchy* in the fashion of the exponential-vicinity pointer model of N. Jones [STOC 1993], which negates linear-speedup.

To appear in the proceedings of IFIP'94, Hamburg, Germany, August 1994. Available by anonymous ftp to ftp.cs.buffalo.edu, cd pub/tech-reports, get 94-24.ps.

Normal Numbers and Sources for BPP

Martin Strauss Department of Mathematics, Rutgers University, New Brunswick, NJ 08903.
Email: `mstrauss@math.rutgers.edu`.

Abstract Number 94-42

In [J. Lutz, "Pseudorandom Sources for BPP." *J. Computer and System Sciences,* **41** (1990), pp. 307-320], Lutz proposed a notion of *source*, a nonrandom sequence that can substitute in a certain way for the random bits used by bounded-error probabilistic machines. He showed that almost every sequence in DSPACE($2^{\text{polynomial}}$) is a source. We improve this abundance result to PSPACE, by first showing that the sources are exactly the classical normal numbers of Borel. We go on to show there are sources in AC^0. Unfortunately, this suggests that alternate notions of source should be explored.

A preliminary paper is available.

A lower bound on the mod 6 degree of the OR function

by

G. Tardos and D. A. M. Barrington

Abstract Number 94-43

Abstract

We examine the computational power of modular counting, where the modulus m is not a prime power, in the setting of polynomials in boolean variables over Z_m. In particular, we say that a polynomial P weakly represents a boolean function f (both have n variables) if for any inputs x and y in $\{0,1\}^n$ we have $P(x) \neq P(y)$ whenever $f(x) \neq f(y)$. Barrington, Beigel, and Rudich (1992) investigated the minimal degree of a polynomial representing the OR function in this way, proving an upper bound of $O(n^{1/r})$ (where r is the number of distinct primes dividing m) and a lower bound of $\omega(1)$. Here we show a lower bound of $\Omega(\log n)$ when m is a product of two primes and $\Omega((\log n)^{1/(r-1)}$ in general. While many lower bounds are known for a much stronger form of representation of a function by a polynomial (Barrington *et al.* 1992, Tsai 1993), using this liberal (and, we argue, more natural) definition very little is known. While the degree is known to be $\Omega(\log n)$ for the generalized inner product because of its high communication complexity (Grolmusz 1994), our bound is the best known for any function of low communication complexity and any modulus not a prime power.

A full paper *is* available by email from either author at "tardos@cs.elte.hu" or "barring@cs.umass.edu". The reference to (Barrington *et al.* 1992) is STOC, to (Tsai 1993) is Structures, and to (Grolmusz 1994) is a draft.

A Note on PCP vs. MIP

Amnon Ta-Shma

Department of Computer Science, The Hebrew University,

Givat Ram, Jerusalem, ISRAEL.

email address: am@cs.huji.ac.il

Abstract Number 94-44

Two variants of interactive proof systems have been used to derive intractability of approximation results. The first is the single round multi-prover model where one verifier can query many provers who can't communicate among themselves (MIP). The second is the oracle model where the verifier queries a non-adaptive oracle (OPCP). It is known that the oracle model is at least as strong as the one-round multi-prover model but it is not known whether the opposite is true.

We show how to convert a PCP protocol to MIP, using the Lapidot and Shamir, and Feige and Lovasz parallelizing technique. Loosely speaking, we force the provers to induce the same behavior by asking them to extend their strategies and give as answers low-degree polynomials. We can check that all those low-degree polynomials reflect the same strategy by checking them in a **single** point, taking advantage of the provers' inability to interact among themselves.

Formally, we show:

If $q, \frac{1}{\epsilon}, m \ \leq \ poly(r)$ then: $OPCP(r, m, q, a, \epsilon) \subseteq \ \ MIP_1(O(r),\ m+1,\ O(r),\ a \cdot r^2,\ 3\epsilon)$

where r denotes number of random bits, m is the number of questions (queries), q question length, a answer length and ϵ is the error.

A full paper is available, though not published yet.

On the Kolmogorov Complexity of Boolean Query Languages

Jerzy Tyszkiewicz
Mathematische Grundlagen der Informatik,
RWTH Aachen, Ahornstr. 55,
D-52074 Aachen, Germany.
jurek@mephisto.informatik.rwth-aachen.de

Abstract Number 94-45

We develop a Kolmogorov complexity based tool to measure the usage of data by boolean query languages. We define a general notion of *Kolmogorov expressive power* of a boolean query language L. It is done by considering two values: the Kolmogorov complexity of the isomorphism type of finite model $\mathbf{A}$ and the number of bits of this description that can be reconstructed from truth values of all boolean queries from L in $\mathbf{A}$. These quantities over all $\mathbf{A}$ in some specified set D of finite models give the description of the power of L in D.

Further, we explore some connections between Kolmogorov expressive power of first-order sentences and the complexity of evaluation of (non necessarily boolean) *fixpoint* and *while* queries. In particular, we show how to obtain time (space) lower bounds for computations of such queries, expressed in terms of the Kolmogorov expressive power of the logic in the model.

In particular, we demonstrate that successful application of the *split* optimization method of *fixpoint* and *while* queries, based on the Abiteboul and Vianu Normal Form, always implies a bound on the Kolmogorov expressive power of boolean queries in these languages.

Extended abstract is available from the author. The full version is in preparation. The research was supported by grants from the German DFG and Polish KBN.

On Balanced vs. Unbalanced Computation Trees

Ulrich Hertrampf, Heribert Vollmer, Klaus W. Wagner, Theoretische Informatik, Universität Würzburg, Am Exerzierplatz 3, D-97072 Würzburg, GERMANY. e-mail: {hertramp,vollmer,wagner}@informatik.uni-wuerzburg.de

Abstract Number 94-46

A great number of complexity classes between P and PSPACE can be defined via leaf languages for computation trees of nondeterministic polynomial time machines. Jenner, McKenzie, and Thérien (Proceedings of the 9th Conference on Structure in Complexity Theory, 1994) addressed the question whether considering balanced or unbalanced trees makes any difference. For a number of leaf language classes, coincidence of both models was shown, but for the very prominent example of leaf language classes from the alternating logarithmic time hierarchy the question was left open. It was only proved that in the balanced case these classes characterize exactly the classes from the polynomial time hierarchy. Here, we answer the question showing that it really makes a difference: In the unbalanced case, a class from the logarithmic time hierarchy characterizes the corresponding class from the polynomial time hierarchy with a PP-oracle.
Along the way, we get an interesting normal form for PP computations.

A full paper is available via anonymous ftp from haegar.informatik.uni-wuerzburg.de (132.187.101.41).

Recursion Theoretic Characterizations of Complexity Classes of Counting Functions

Heribert Vollmer, Klaus W. Wagner, Theoretische Informatik, Universität Würzburg, Am Exerzierplatz 3, D-97072 Würzburg, GERMANY.
e-mail: {vollmer,wagner}@informatik.uni-wuerzburg.de

Abstract Number 94-47

There has been a great effort in giving machine independent, algebraic characterizations of complexity classes, especially of functions. Astonishingly, no satisfactory characterization of the prominent class #P has been known up to now. Here, we characterize #P as the closure of a set of simple arithmetical functions under summation and weak product. An analogous result is obtained for Gap-P.

Building on that result, the hierarchy of counting functions, which is the closure of #P under substitution, is characterized; remarkably without using the operator of substitution, since we can show that in the context of this hierarchy the operation of modified subtraction is as powerful as substitution.

Finally, relationships to ciruit classes are given.

A full paper is available.

Weighted NP optimization problems: logical definability and approximation properties

Marius Zimand, Department of Computer Science, University of Rochester, Rochester, NY 14627, e-mail: zimand@cs.rochester.edu

Abstract Number 94-48

An optimization problem A is defined by: (1) a set $\mathcal{I}_A$ of input instances; we assume that this set can be recognized in polynomial time, (2) for each $I \in \mathcal{I}_A$, a set $\mathcal{F}_A(I)$ of feasible solutions associated to each input instance; we assume that each element in $\mathcal{F}_A(I)$ has size polynomially bounded in the size of I, and (3) an objective function f_A which maps each feasible solution to a real number; we assume that this function is computable in polynomial time. Problem A is an NP optimization problem if the associated decision problem (e.g., given $I \in \mathcal{I}_A$ and a real value k, does there exists $J \in \mathcal{F}_A(I)$ with $f_A(J) \geq k$?) is in NP. Extending a well known property of NP optimization problems in which the value of the optimum is guaranteed to be polynomially bounded in the length of the input, we observe that, by attaching weights to tuples over the domain of the input, all NP optimization problems admit a logical characterization. We show that any NP optimization problem can be stated as a problem in which the constraint conditions can be expressed by a Π_2 first-order formula and this is the best possible result. We further analyze the weighted analogue of all syntactically defined classes of optimization problems that are known to have good approximation properties: $MAX\ NP, MAX\ SNP, MAX\ SNP(\pi), MIN\ F^+\Pi_1$ and $MIN\ F^+\Pi_2(1)$. All these classes continue to have the same approximation properties in the case of positive weights. Using reductions from multiprover interactive systems, we show that if $NP \not\subseteq DTIME[2^{\log^{O(1)} n}]$, their approximation properties deteriorates considerably when negative weights are also allowed (with the exception of $MIN\ F^+\Pi_1$, where only a weaker depreciation could be proven). It follows that the general weighted versions of MAX 2SAT, SET COVER, PRIORITY ORDERING (given a finite set X and real-valued weights $w(\cdot,\cdot)$ to all pairs of distinct elements in X find the maximum over all permutations π of X of $\sum_{\{(x,y)\ :\ x,y\in X, \pi(x)<\pi(y)\}} w(x,y)$) and of some other closely related natural problems are not approximable in quasipolynomial time within a factor of $2^{\log^{\mu} n}$ for some $\mu > 0$, unless $NP \subseteq DTIME[2^{\log^{O(1)} n}]$. Under the same hypothesis, we show that the maximization variant of SET PARTITION (given a finite set U and some subsets of it, find the maximum number of subsets that are disjoint and whose union cover U) is also not superpolylog approximable. A stronger result is proven for the minimization variant of SET PARTITION (as above, but the requirement is to find the minimum number of subsets etc.): if $P \neq NP$, then MIN SET PARTITION cannot be approximated in polynomial time within a factor of $n^{O(1)}$.

A full paper is available.