COMPLEXITY ABSTRACTS 1997. Vol VII

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

Titles of Abstracts

The Complexity of Controlled Stochastic Processes

Eric Allender, Dept. of Computer Science, Rutgers University, Piscataway NJ 08855-1179 (`allender@cs.rutgers.edu`)
Judy Goldsmith, University of Kentucky, 763 Anderson Hall, Lexington, KY 40506-0046 (`goldsmit@cs.engr.uky.edu`)
Michael L. Littman, Dept. of Computer Science, Duke University, Durham, NC 27708-0129 (`mlittman@cs.duke.edu`)
Chris Lusena, University of Kentucky, 773 Anderson Hall, Lexington, KY 40506-0046 (`cdluse01@engr.uky.edu`)
Martin Mundhenk, Universität Trier, FB IV – Informatik, D-54286 Trier, Germany (`mundhenk@ti.uni-trier.de`)

Abstract Number 97-1

This research program concerns the computational complexity of problems related to mathematical models of controlled stochastic processes. The processes modelled may be assembly lines, automated medical diagnostic tools, ecological or economic systems, or robot controllers. The models may be Markov decision processes (MDPs) or others. The problems considered are the evaluation of given control policies, the existence of good policies and the construction of optimal, or good enough, policies.

In several recent papers (available from our web pages) we have shown the complexity of a large variety of decision problems of the forms, “does this control policy for this MDP have expected reward > 0,” and “is there a control policy for this MDP that has expected reward > 0”. The complexities range from NL-complete to EXPSPACE-complete, depending on the amount of information available to the controller at each stage in the process, the amount of memory the controller has, how long the process runs, the number of actions available to the controller, and the succinctness of the input. We also show NP-hardness of approximating the optimal policies for some cases.

In terms of complexity theory, our most surprising results are that the existence problem for policies for certain succinctly represented problems are $\mathrm{NP}^{\mathrm{PP}}$-complete. $\mathrm{NP}^{\mathrm{PP}}$-completeness also arises in questions about the median and average expectations of policies.

Papers are available at
`www.cs.engr.uky.edu/~goldsmit/` or at `www.informatik.uni-trier.de/~mundhenk/`.

Circuit Expressions of Low Kolmogorov Complexity

José L. Balcázar, Department of Software (LSI), Universitat Politècnica de Catalunya, Pau Gargallo 5, E-08028 Barcelona, Spain, (balqui@lsi.upc.es)
Harry Buhrman, Kruislaan 413, P.O. Box 94079, 1090 GB Amsterdam, The Netherlands, (buhrman@cwi.nl)
Montserrat Hermo, Department of Software (LSI), Universidad del País Vasco, P.O. Box 649, E-20080 San Sebastián, Spain, (jiphehum@si.ehu.es)

Abstract Number 97-2

We study circuit expressions of logarithmic and polylogarithmic polynomial-time Kolmogorov complexity, focusing on their learnability properties and complexity-theoretic characterizations. They are shown to provide a nontrivial circuit-like characterization for a natural nonuniform complexity class that seemed to lack it. We also show that circuit expressions of this kind (for fixed constants) can be learned with membership queries in polynomial time if and only if every NE-predicate is E-solvable. Thus they are learnable given that the learner is allowed the extra use of an oracle in NP. The precise way of accessing the oracle is shown to be optimal under relativization. We also present a precise characterization of the subclass defined by Kolmogorov-easy circuit expressions that can be constructed from membership queries in polynomial time, with some consequences for the structure of reduction and equivalence classes of certain tally sets.

A full paper is available by email to jiphehum@si.ehu.es

Compressibility of Infinite Binary Sequences

José L. Balcázar, Department of Software (LSI), Universitat Politècnica de Catalunya, Pau Gargallo 5, E-08028 Barcelona, Spain, (balqui@lsi.upc.es)
Ricard Gavaldà, Department of Software (LSI), Universitat Politècnica de Catalunya, Pau Gargallo 5, E-08028 Barcelona, Spain, (gavalda@lsi.upc.es)
Montserrat Hermo, Department of Software (LSI), Universidad del País Vasco, P.O. Box 649, E-20080 San Sebastián, Spain, (jiphehum@si.ehu.es)

Abstract Number 97-3

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 both the standard resource-bounded Kolmogorov complexity of infinite strings, and the uniform complexity. Some nontrivial coincidences and disagreements are proved. The resource-unbounded case is also considered.

A full paper is available by email to jiphehum@si.ehu.es

The Structure of Logarithmic Advice Complexity Classes

José L. Balcázar, Department of Software (LSI), Universitat Politècnica de Catalunya, Pau Gargallo 5, E-08028 Barcelona, Spain, (balqui@lsi.upc.es)
Montserrat Hermo, Department of Software (LSI), Universidad del País Vasco, P.O. Box 649, E-20080 San Sebastián, Spain, (jiphehum@si.ehu.es)

Abstract Number 97-4

A nonuniform class called here Full-P/log, due to Ko, is studied. It corresponds to polynomial time with logarithmically long advice. Its importance lies in the structural properties it enjoys, more interesting than those of the alternative class P/log; specifically, its introduction was motivated by the need of a logarithmic advice class closed under polynomial-time deterministic reductions. Several characterizations of Full-P/log are shown, formulated in terms of various sorts of tally sets with very small information content. A study of its inner structure is presented, by considering the most usual reducibilities and looking for the relationships among the corresponding reduction and equivalence classes defined from these special tally sets.

A full paper is available by email to jiphehum@si.ehu.es

NP Might Not Be As Easy As Detecting Unique Solutions

Richard Beigel, Yale, University of Maryland, and Lehigh University, Elect Eng Comp Science, 19 Memorial Dr W Ste 2, Bethlehem PA 18015-3084. Email: beigel@eecs.lehigh.edu
Harry Buhrman, CWI. PO Box 94079, 1090 GB Amsterdam, The Netherlands. E-mail: buhrman@cwi.nl
Lance Fortnow, CWI and University of Chicago, Department of Computer Science, 1100 E. 58th St., Chicago, IL 60637. Email: fortnow@cs.uchicago.edu.

Abstract Number 97-5

We construct an oracle A such that

$$P^A = \oplus P^A \text{ and } NP^A = EXP^A.$$

This relativized world has several amazing properties:

- The oracle A gives the first relativized world where one can solve satisfiability on formulae with at most one assignment yet $P \neq NP$.
- The oracle A is the first where

$$P^A = UP^A \neq NP^A = coNP^A.$$

- The construction gives a much simpler proof than Fenner, Fortnow and Kurtz of a relativized world where all NP-complete sets are polynomial-time isomorphic. It is the first such computable oracle.
- Relative to A we have a collapse of $\oplus EXP^A \subseteq ZPP^A \subseteq P^A$/poly.

We also create a different relativized world where there exists a set L in NP that is NP-complete under reductions that make one query to L but not complete under traditional many-one reductions. This contrasts with the result of Buhrman, Spaan and Torenvliet showing that these two completeness notions for $NEXP$ coincide.

A preliminary version is available from http://www.cs.uchicago.edu/˜fortnow/papers.

Commutative Queries

Richard Beigel, On sabbatical from the Yale University Department of Computer Science. Address: Dept. of Computer Science, University of Maryland at College Park, College Park, MD 20742-3251, USA. (`beigel@cs.umd.edu`)

Richard Chang, CSEE Department, University of Maryland Baltimore County, Baltimore, MD 21250, USA. (`chang@umbc.edu`)

Abstract Number 97-6

This paper considers polynomial-time Turing machines which have access to two oracles and investigates when the order of oracle access is significant. The oracles used here are complete languages for the Polynomial Hierarchy (PH). For language classes, the results in this paper show that the order of the oracle queries does not matter, even when the queries are truth table queries. This improves upon the previous results of Hemaspaandra, Hemaspaandra and Hempel who showed that the order of the queries does not matter if the base machine asks one query to each oracle. Furthermore, the results in this paper extend to polynomial-time machines which make more than two rounds of truth table queries to the oracles.

Let $k > j$ and let H and E be complete languages for Σ_k^{P} and Σ_j^{P} respectively. Then, the new results show that for all polynomial bounded $r(n)$ and $s(n)$,

$$\mathrm{P}^{H_{r(n)\text{-tt}};E_{s(n)\text{-tt}}} = \mathrm{P}^{E_{s(n)\text{-tt}};H_{r(n)\text{-tt}}} = \mathrm{P}^{E_{s(n)\text{-tt}}\|H_{r(n)\text{-tt}}},$$

where $\mathrm{P}^{A_{a(n)\text{-tt}};B_{b(n)\text{-tt}}}$ denotes the class of languages recognized by polynomial-time Turing machines that ask $a(n)$ parallel queries to A followed by $b(n)$ parallel queries to B, and $\mathrm{P}^{A_{a(n)\text{-tt}}\|B_{b(n)\text{-tt}}}$ denotes the class of languages recognized by polynomial-time Turing machines that ask $a(n)$ parallel queries to A simultaneous with $b(n)$ parallel queries to B. In contrast, for function classes the order of access is critical. In particular, for all constants r and s, $\mathrm{PF}^{H_{r\text{-tt}};E_{s\text{-tt}}} \not\subseteq \mathrm{PF}^{E_{s\text{-tt}};H_{r\text{-tt}}}$ unless $\mathrm{PH} = \Sigma_{j+1}^{\mathrm{P}}$. This result also extends to several rounds of queries to H and E. For example, for all constants r, s and t, $\mathrm{PF}^{H_{r\text{-tt}};H_{s\text{-tt}};E_{t\text{-tt}}} \not\subseteq \mathrm{PF}^{H_{r\text{-tt}};E_{t\text{-tt}};H_{s\text{-tt}}}$ unless $\mathrm{PH} = \Sigma_{j+1}^{\mathrm{P}}$.

The full paper has appeared in the *Proceedings of the 5th Israeli Symposium on Theory of Computing and Systems,* June 1997. The paper is also available from the authors' web pages: `<http://umbc.edu/~chang/papers/>` or `<http://www.cs.yale.edu/~beigel/>`.

On the order of queries

Richard Beigel, Dept. of Computer Science, Yale University (rjb@cs.yale.edu)

Richard Chang, Dept. of Computer Science, Univ. of MD- Baltimore Campus, (chang@cs.umbc.edu)
William Gasarch, Dept. of Computer Science, Univ. of MD- College Park, (gasarch@cs.umd.edu)
Jacob Lurie, Dept. of Math, Harvard Univ. (lurie@husc.harvard.edu) *Timothy McNicholl* Dept. of Mathematics, Ottawa University, (mcnichol@iso.ott.edu)

Abstract Number 97-7

If you make a queries to A followed by b queries to B is this different than making b query to B followed by a queries to A. Our setting is recursion-theoretic. Let $Q(n, A, m, B)$ be the class of sets that can be determined with n queriest to A followed by m queries to B.

1. If A is Σ_i-complete and B is Σ_j-complete then $Q(n, A, m, B) = Q(m, B, n, A)$. (So for deciding sets, order is irrelvant. For computing functions we have shown that order is relevant.)

2. If $(\forall B)[Q(1, A, 1, B) = Q(1, B, 1, A)$ then A is recursive.

3. There exists two incomparable r.e. sets A, B such that $(\forall m, n)[Q(n, A, m, B) = Q(m, B, n, A)]$.

The paper is still under construction.

The Complexity of ODD_n^A

Richard Beigel, Dept. of Computer Science, Yale University (rjb@cs.yale.edu)
William Gasarch, Dept. of Computer Science, Univ. of MD, (gasarch@cs.umd.edu)
Martin Kummer, Technische Universität Chemnitz-Zwickau, Fakultät für Informatik (martin.kummer@informatik.tu-chemnitz.de) *Georgia Martin*, Dept. of Computer Science, Univ. of MD, (gam@cs.umd.edu) *Timothy McNicholl* Dept. of Mathematics, Ottawa University, (mcnichol@iso.ott.edu) *Frank Stephan* Mathematisches Institut, Ruprecht-Karls-Universität, (fstephan@math.uni-heidelberg.de)

Abstract Number 97-8

We consider the following sets with regard to how many queries to A are needed to compute them.
$\mathrm{ODD}_n^A = \{(x_1, \ldots, x_n) \mid |A \cap \{x_1, \ldots, x_n\}| \text{ is odd}\}$ and
$\mathrm{WMOD}(m)_n^A = \{(x_1, \ldots, x_n) \mid |A \cap \{x_1, \ldots, x_n\}| \not\equiv 0 \pmod{m}\}$.
If A, B are semirecursive then we obtain the following: (1) ODD_n^A can be computed with n parallel queries to A (obviously) but cannot be computed with any fewer; (2) ODD_n^A can be computed with $\lceil \log(n+1) \rceil$ serial queries to A but cannot be computed with any fewer; (3) $\mathrm{WMOD}(m)_n^A$ can be computed with $\lceil \frac{n}{m} \rceil + \lfloor \frac{n}{m} \rfloor$ parallel queries to A but cannot be computed with any fewer, even if the oracle is B. (4) $\mathrm{WMOD}(m)_n^A$ can be computed with $\lceil \log(\lceil \frac{n}{m} \rceil + \lfloor \frac{n}{m} \rfloor + 1) \rceil$ queries to A but cannot be computed with any fewer, even if the oracle is B
The lower bounds hold for any nonrecursive A, B r.e. and are derived *from* the lower bounds for A semirecursive. We also show that every truth table degree contains a set B such that ODD_n^B can be decided with one query to B. Hence, for bounded query complexity, how information is packaged is more important than Turing degree.

The paper is available from gasarch@cs.umd.edu

The Power of Not Converging

Richard Beigel, Dept. of Computer Science, Yale University (rjb@cs.yale.edu)
William Gasarch, Dept. of Computer Science, Univ. of MD, (gasarch@cs.umd.edu)
Martin Kummer, Technische Universität Chemnitz-Zwickau, Fakultät für Informatik (martin.kummer@informatik.tu-chemnitz.de) *Georgia Martin*, Dept. of Computer Science, Univ. of MD, (gam@cs.umd.edu) *Timothy McNicholl* Dept. of Mathematics, Ottawa University, (mcnichol@iso.ott.edu) *Frank Stephan* Mathematisches Institut, Ruprecht-Karls-Universität, (fstephan@math.uni-heidelberg.de)

Abstract Number 97-9

We consider the number of queries as a measure of complexity. We consider issues of convergence. Let A, B be sets and $n \in N$. (1) $A \in Q(n, B)$ if A can be decided with n queries to B, (2) $A \in QC(n, B)$ if $A \in Q(n, B)$ via a machine where all paths converge. Clearly $QC(n, A) \subseteq Q(n, A)$. The question arises as to for which A these are equal. The sets we deal with are on the extremes, and our definitions reflect this: (1) A is *universally convergent* (u.c.) $(\forall n \geq 1)[Q(n, A) \subseteq QC(n, A)]$. (2)$A$ is *strongly non-universally convergent* (s.n.u.c.) if $Q(1, A) - \bigcup_{n=1}^{\infty} QC(n, A) \neq \emptyset$.
We have proven the following.

1. If A is Σ_i-complete then A is u.c.
2. Every tt-degree either has an s.n.u.c set or every set in it is u.c. (We hae a characteriztion of when this happens.)
3. There are Turing degrees such that contain only u.c. sets. (Any hyperimmune-free degree will suffice.)
4. Every r.e. Turing degree contains an r.e. set that is s.n.u.c.
5. There are r.e. Turing degree whose r.e. sets are all s.n.u.c.

A rough draft is available from gasarch@cs.umd.edu

When do more queries help?

Richard Beigel, Dept. of Computer Science, Yale University (rjb@cs.yale.edu)
William Gasarch, Dept. of Computer Science, Univ. of MD, (gasarch@cs.umd.edu)
Martin Kummer, Technische Universität Chemnitz-Zwickau, Fakultät für Informatik (martin.kummer@informatik.tu-chemnitz.de) *Georgia Martin*, Dept. of Computer Science, Univ. of MD, (gam@cs.umd.edu) *Timothy McNicholl* Dept. of Mathematics, Ottawa University, (mcnichol@iso.ott.edu) *Frank Stephan* Mathematisches Institut, Ruprecht-Karls-Universität, (fstephan@math.uni-heidelberg.de)

Abstract Number 97-10

We consider the number of queries as a measure of complexity. A key question is 'do more queries help?' We present here results on this issue. Let A, B be sets and $n \in N$. (1) $f \in FQ(n, B)$ if f can be computed with n queries to B, (2) $f \in FQ_p(n, B)$ if f can be computed with n parallel queries to B. (3) $A \in Q(n, B)$ if A can be decided with n queries to B, (4) $A \in Q_p(n, B)$ if A can be decided with n parallel queries to B.

For computing functions more queries always help: if A is nonrecursive then $(\forall n)[FQ(n, B) \subset FQ(n+1, B)]$ and $(\forall n)[FQ_p(n, B) \subset FQ_p(n+1, B)]$.

For sets results are more complicated.

1. If A is r.e., semirecursive, or $A = B'$ for some B then $Q(n, A) \subset Q(n+1, A)$ and $Q_p(n, A) \subset Q_p(n+1, A)$. Note that this includes most natural sets.
2. There exists sets A such that $(\forall n)[Q(n, A) = Q_p(n, A) = Q(1, A)]$. (If B is hyperimmune-free then $A = B^{\text{tt}}$ suffices. There are other examples.)
3. There exists sets A such that $(\forall n)[Q(n, A) \subset Q(n+1, A)]$ but $(\forall n)[Q_p(n, A) = Q(1, A)]$. ($A = K^{\text{tt}}$ is one such example.)

The results are corollaries of results in other papers which are available from gasarch@cs.umd.edu.

DNA Computation: Models and Algorithms

Richard Beigel, Elect. Eng. Comp. Science, 19 Memorial Dr. W. Ste. 2, Bethlehem, PA 18015-3084, USA. (mailto:beigel@eecs.lehigh.edu, http://www.eecs.lehigh.edu/~beigel.)
Bin Fu, Dept. of Computer Science, P.O. Box 208285, New Haven, CT 06520-8285, USA. (mailto:binfu@cs.yale.edu).

Abstract Number 97-11

The maximum number of strands used is an important measure of a molecular algorithm's complexity. This measure is also called the *space* or *volume* used by the algorithm. We consider three $s(n)$-volume, polynomial-time bounded models of DNA computation:

- MOL($s(n)$), which allows the operations Separate, Pour, Append and Merge,
- MOL$'$($s(n)$), which allows the operations Separate, Pour, Append, Merge, and *Split*, and
- MOL-A($s(n)$), which allows the operations Separate, Pour, Append, Merge, and *Amplify*.

We relate these models to bounded nondeterminism. Define

- NPinit($s(n)$) $=$ the class of languages accepted by NP machines that nondeterministically choose a number between 1 and $s(n)$ and then behave deterministically.
- NPpaths($s(n)$) $=$ the class of languages accepted by NP machines that have at most $s(n)$ paths on inputs of length n.

We prove that

- MOL($s(n)$) $=$ MOL$'$($s(n)$) $=$ NPinit($s(n)$)
- MOL-A($s(n)$) $=$ NPpaths($s(n)$)

Thus the Split operation does not increase the power of volume-bounded polynomial-time DNA computation. However, Append does increase the power of volume-bounded polynomial-time DNA computation, assuming NPinit($s(n)$) $\neq$NPpaths($s(n)$). We present an oracle for which this separation holds.

Furthermore, we identify a large class of recursive algorithms that can be implemented in the NPinit model. This yields improved molecular algorithms for important problems like 3-SAT, independent set, and 3-colorability. Applying this idea to approximation problems, we construct algorithms that exhibit a useful volume–accuracy tradeoff.

Finally, we design an approximation algorithm for the Covering problem of Hochbaum and Maass in the NPpaths model. Our solution uses fewer paths than any known solution in the NPinit model. This is the first real problem for which the Amplify operation seems to increase the power of DNA computation.

Research supported in part by the National Science Foundation under grants CCR-8958528 and CCR-9415410.

Extended abstracts are available as "Molecular Computing, Bounded Nondeterminism, and Efficient Recursion" in ICALP 1997, "A Comparison of Resource-Bounded Molecular Computation" in ISTCS 1997, and "On Molecular Approximation Algorithms for NP Optimization Problems" in the International Workshop on DNA Computation (DIMACS), 1997.

Powers-of-Two Acceptance Suffices for Equivalence and Bounded Ambiguity Problems

Bernd Borchert, Mathematisches Institut, Universität Heidelberg, 69120 Heidelberg, Germany. Email: `bb@math.uni-heidelberg.de`.
Lane A. Hemaspaandra, Department of Computer Science, University of Rochester, Rochester, NY 14627, USA. Email: `lane@cs.rochester.edu`.
Jörg Rothe, Institut für Informatik, Friedrich-Schiller-Universität Jena, 07743 Jena, Germany. Email: `rothe@informatik.uni-jena.de`.

Abstract Number 97-12

We study EP, the subclass of NP consisting of those languages accepted by NP machines that when they accept always have a number of accepting paths that is a power of two. We show that the negation equivalence problem for OBDDs (ordered binary decision diagrams [FHS78]) and the interchange equivalence problem for 2-dags are in EP. We also show that for boolean negation the equivalence problem is in $\mathrm{EP}^{\mathrm{NP}}$, thus tightening the existing $\mathrm{NP}^{\mathrm{NP}}$ upper bound.

We also show that FewP [All86, AR88], bounded ambiguity polynomial time, is contained in EP, a result that seems incomparable with the previous SPP upper bound. Finally, we show that EP can be viewed as the promise-class analog of $\mathrm{C}_=\mathrm{P}$.

References

[All86] E. Allender. The complexity of sparse sets in P. In *Proceedings of the 1st Structure in Complexity Theory Conference*, pages 1–11. Springer-Verlag *Lecture Notes in Computer Science #223*, June 1986.

[AR88] E. Allender and R. Rubinstein. P-printable sets. *SIAM Journal on Computing*, 17(6):1193–1202, 1988.

[FHS78] S. Fortune, J. Hopcroft, and E. Schmidt. The complexity of equivalence and containment for free single program schemes. In *Proceedings of the 5th International Colloquium on Automata, Languages, and Programming*, pages 227–240. Springer-Verlag *Lecture Notes in Computer Science #62*, 1978.

A full paper is available as UR-DCS-TR-97-628 at `http://www.cs.rochester.edu/trs`.

Results on Resource-Bounded Measure

Harry Buhrman, CWI. PO Box 94079, 1090 GB Amsterdam, The Netherlands. E-mail: buhrman@cwi.nl
Steve Fenner, University of Southern Maine, 96 Falmouth St., Portland, ME 04103. Email: fenner@cs.usm.maine.edu.
Lance Fortnow, CWI and University of Chicago, Department of Computer Science, 1100 E. 58th St., Chicago, IL 60637. Email: fortnow@cs.uchicago.edu.

Abstract Number 97-13

We construct an oracle relative to which NP has p-measure 0 but D^p has measure 1 in EXP. This gives a strong relativized negative answer to a question posed by Lutz. Secondly, we give strong evidence that BPP is small. We show that BPP has p-measure 0 unless $EXP = MA$ and thus the polynomial-time hierarchy collapses. This contrasts with the work of Regan et. al., where it is shown that $P/poly$ does *not* have p-measure 0 if exponentially strong pseudorandom generators exist.

This paper appeared in the Proceedings of the 24th International Colloquium on Automata, Languages and Programming. A preliminary version is also available from http://www.cs.uchicago.edu/~fortnow/papers.

Two Queries

Harry Buhrman, CWI. PO Box 94079, 1090 GB Amsterdam, The Netherlands. E-mail: buhrman@cwi.nl
Lance Fortnow, CWI and University of Chicago, Department of Computer Science, 1100 E. 58th St., Chicago, IL 60637. Email: fortnow@cs.uchicago.edu.

Abstract Number 97-14

We consider the question whether two queries to SAT are as powerful as one query. We show that if $P^{NP[1]} = P^{NP[2]}$ then

- Locally either $NP = coNP$ or NP has polynomial-size circuits.
- $P^{NP} = P^{NP[1]}$.
- $\Sigma_2^p = UP^{NP[1]} \cap RP^{NP[1]}$.
- $PH = BPP^{NP[1]}$.

Moreover we extend work of Hemaspaandra, Hemaspaandra and Hempel to show that if $P^{\Sigma_2^p[1]} = P^{\Sigma_2^p[2]}$ then $\Sigma_2^p = \Pi_2^p$. We also give a relativized world where $P^{NP[1]} = P^{NP[2]}$ but $NP \neq coNP$.

A preliminary version is available from http://www.cs.uchicago.edu/˜fortnow/papers.

Nonrelativizing Separations

Harry Buhrman, CWI. PO Box 94079, 1090 GB Amsterdam, The Netherlands. E-mail: buhrman@cwi.nl
Lance Fortnow, CWI and University of Chicago, Department of Computer Science, 1100 E. 58th St., Chicago, IL 60637. Email: fortnow@cs.uchicago.edu.

Abstract Number 97-15

Consider the class MAEXP, exponentially long publishable proofs, the variation of the class MA where "Arthur" can run in exponential time. We show that not every language in MA ∩ coMA has polynomial-size circuits. This result was independently proven by Thierauf.

One can think of MAEXP as the weakest form of interactive proofs with an exponential-time verifier. The strongest notion would be that of MIPEXP. By padding the MIP = NEXP result of Babai, Fortnow and Lund, we get that MIPEXP equals NEEXP, the class of languages accepted in nondeterministic double exponential time.

Nevertheless we create an oracle A where every language in MIPEXP^A is in P^A/poly. We also create relativized worlds where MIPEXP is in P^{NP} and $\oplus$P even though NEEXP is also known to strictly contain these classes.

A preliminary version of this paper will be available shortly at
http://www.cs.uchicago.edu/˜fortnow/papers.

Complete Sets under Non-Adaptive Reductions are Scarce

Harry Buhrman, CWI, afdeling INS4, Kruislaan 413, P.O. Box 94079, NL-1090 GB Amsterdam, THE NETHERLANDS, (buhrman@cwi.nl)
Dieter van Melkebeek, Department of Computer Science, The University of Chicago, 1100 East 58th Street, Chicago, IL 60637, USA, (dieter@cs.uchicago.edu)

Abstract Number 97-16

We investigate the frequency of complete sets for various complexity classes within EXP under non-adaptive reductions in the sense of resource bounded measure. We show that these sets are rare:

- The sets that are complete under $\leq^p_{n^\alpha-\mathrm{tt}}$-reductions for NP, the levels of the polynomial-time hierarchy, PSPACE, and EXP have p_2-measure zero for any constant $\alpha < 1$.
- Assuming MA $\neq$ EXP, the $\leq^p_{\mathrm{tt}}$-complete sets for the Δ-levels of the polynomial-time hierarchy have p-measure zero.

We also prove that the hard sets for E and EXP under $\leq^p_{n^\alpha-\mathrm{tt}}$-reductions have p_2-measure zero for any $\alpha < 1$.
A key ingredient of the first result is the Small Span Theorem, which states that for any set A in EXP at least one of its lower span (i.e., the sets that reduce to A) or its upper span (i.e., the sets that A reduces to) has p_2-measure zero. Previous to our work, the theorem was only known to hold for $\leq^p_{k-\mathrm{tt}}$-reductions for any constant k. We establish it for $\leq^p_{n^{o(1)}-\mathrm{tt}}$-reductions.
The second result is based on the connection between completeness and autoreducibility, and on the use of pseudo-random generators.

A full paper is available from URL http://www.cs.uchicago.edu/~dieter.

Robust Reductions

Jin-Yi Cai, Department of Computer Science, SUNY at Buffalo, Buffalo, NY 14260, USA. Email: cai@cs.buffalo.edu.
Lane A. Hemaspaandra, Department of Computer Science, University of Rochester, Rochester, NY 14627, USA. Email: lane@cs.rochester.edu.
Gerd Wechsung, Institut für Informatik, Friedrich-Schiller-Universität Jena, 07743 Jena, Germany. Email: wechsung@informatik.uni-jena.de.

Abstract Number 97-17

We continue the study of robust reductions initiated by Gavaldà and Balcázar in [GB91]. In particular, [GB91] claims an optimal separation between the power of robust and nondeterministic strong reductions; unfortunately the proof in [GB91] is invalid. We re-establish that sweeping theorem.

Generalizing robust reductions, we note that robustly strong reductions are built from two restrictions—robust underproductivity and robust overproductivity—both of which have been studied separately before in other contexts. By analyzing systematically the power of these reductions, we explore the extent to which each restriction weakens the power of reductions. We apply this to extend known theorems regarding sparse complete sets.

References

[GB91] R. Gavaldà and J. Balcázar. Strong and robustly strong polynomial time reducibilities to sparse sets. *Theoretical Computer Science*, 88(1):1–14, 1991.

A full paper will be available shortly by email to the authors.

Bounded Queries, Approximations and the Boolean Hierarchy

Richard Chang, CSEE Department, University of Maryland Baltimore County, Baltimore, MD 21250, USA. (chang@umbc.edu)

Abstract Number 97-18

This paper investigates some connections linking nondeterministic bounded query classes, the complexity of NP-hard approximation problems and the Boolean Hierarchy. Nondeterministic bounded query classes turn out be rather suitable for describing the complexity of NP-hard approximation problems. For example, finding the vertices of a 2-approximate clique is complete for the class $\mathrm{NPF}^{\mathrm{SAT}[\log\log n]}$, where $\mathrm{NPF}^{\mathrm{SAT}[q(n)]}$ denotes the class of total multi-valued functions computed by nondeterministic polynomial-time Turing machines which ask at most $q(n)$ queries to the SAT oracle in the entire nondeterministic computation tree. Similar completeness results can be proven for Graph Coloring, the Traveling Salesman Problem on general graphs (TSP) and several other NP-optimization problems for which finding approximate solutions is known to be NP-hard.

We take advantage of this machine-based model to prove that in many cases, NP-approximation problems have the upward collapse property. That is, a reduction between NP-approximation problems of apparently different complexity at a lower level results in a similar reduction at a higher level. For example, one might expect that finding a $(\log n)$-approximation of MaxClique is easier than finding the exact solution to MaxClique. On the other hand, if MaxClique does reduce to $(\log n)$-approximating MaxClique, our new results show that TSP also reduces to 2-approximating TSP. Since 2-approximating TSP is equivalent in complexity to MaxClique, we have a total collapse of the hierarchy of approximation problems from solving TSP exactly all the way down to $(\log n)$-approximating MaxClique: MaxClique $\leq_{\mathrm{m}}^{\mathrm{P}}$ $(\log n)$-approximating MaxClique $\Longrightarrow$ TSP $\equiv_{\mathrm{m}}^{\mathrm{P}}$ MaxClique $\equiv_{\mathrm{m}}^{\mathrm{P}}$ $(\log n)$-approximating MaxClique.

Several upward collapse theorems are presented in this paper. In each of these cases, the proof of the result relies heavily on the machinery provided by the nondeterministic bounded query classes and the Boolean Hierarchy — even though the statement of the result does not make any mention of oracle queries. For example, we can show that $\mathrm{BH}_{2^k} = \mathrm{coBH}_{2^k} \Longrightarrow \mathrm{NPF}^{\mathrm{SAT}[n^{O(1)}]} \subseteq \mathrm{NPF}^{\mathrm{SAT}[k]}$. This and similar results are used to prove upward collapse theorems for the nondeterministic bounded query classes. Since finding approximate solutions to MaxClique and TSP are complete for various levels of the nondeterministic bounded query hierarchy, we are able to obtain upward collapse results for those NP-approximation problems as well.

A full paper will be available shortly from: `<http://umbc.edu/~chang/papers/>`.

On Spectral Lower Bound Arguments for Decision Trees

Carsten Damm, Universität Trier, Fachbereich IV — Informatik D-54286 Trier (damm@informatik.uni-trier.de)

Abstract Number 97-19

A decision tree is a rooted binary tree with inner nodes labeled by Boolean variables and edges and leaves labeled by Boolean constants. A decision tree T defines a Boolean function f_T in a natural way: given an input a, start at the root and follow at each inner node the edge according to the value of the variable that labels this node. The label of the terminal node is $f_T(a)$. The *size of a decision tree is its number of leaves, the* average depth is the expectation of the depth of the leaf that is reached by a randomly chosen input. Denote by $\mathsf{DT}(f)$ and $\overline{\mathsf{depth}}(f)$ the minimal size and the minimal average depth, respectively, of decision trees that compute a given Boolean function $f : \{0,1\}^n \to \{+1,-1\}$.

We give an new proof and generalization for the following lower bounds due to Brandman, Orlitsky, and Hennessy (1990):

$$\mathsf{DT}(f) \geq \sum_{S \subseteq [n]} 2^{|S|} \cdot \hat{f}(S)^2, \overline{\mathsf{depth}}(f) \geq \sum_{S \subseteq [n]} |S| \cdot \hat{f}(S)^2.$$

Here the $\hat{f}(S)$ are defined by the linear decomposition $f = \sum_{S \subseteq [n]} \hat{f}(S)\chi_S$, where χ_S is the ± 1-valued parity of the variables $x_i, S \subseteq [n]$.

Our argument is extremely easy and is directly applicable to spectral decompositions with respect to bases different from the standard Fourier basis $\chi_S, S \subseteq [n]$.

Full paper under preparation—a draft is available by email to damm@informatik.uni-trier.de

Extractors for Kolmogorov Complexity

Lance Fortnow, CWI and University of Chicago, Department of Computer Science, 1100 E. 58th St., Chicago, IL 60637 (fortnow@cs.uchicago.edu)
Sophie Laplante, University of Chicago, Department of Computer Science (laplante@cs.uchicago.edu)

Abstract Number 97-20

Extractors are bipartite graphs designed to "extract" randomness. One would expect some connections with Kolmogorov complexity, one of the best known measures of "randomness". Previously no known connection has been established.

We show two sets of results applying the theory of extractors to resource-bounded Kolmogorov complexity:

1. Most strings in easy sets have nearly optimal polynomial-time CD (distinguishing) complexity. This extends work of Sipser [*A complexity theoretic approach to randomness*, STOC 83] and Buhrman and Fortnow [*Resource-bounded Kolmogorov complexity revisited*, STACS 97].

2. We use extractors to extract the randomness of strings. In particular we show how to get a random string of high polynomial-time C complexity from a potentially nonrandom string of high polynomial-time CND complexity (nondeterministic distinguishing complexity).

Sipser shows that for every set A in P, for all strings x of length n in A, the CD^p complexity of x given a "random" string r is bounded by $\log |A| + O(\log n)$. Buhrman and Fortnow remove the dependency on the random string but at a cost of only bounding the CD^p complexity of x by $2 \log |A| + O(\log n)$. We nearly achieve the optimal bound of Sipser without the random string by bounding the CD^p complexity of most strings x in A by $\log |A| + \log^{O(1)} n$. Following Buhrman and Fortnow, we also establish a similar relationship between sets in NP and CND complexity. We can also achieve Sipser's bound for most strings at the cost of only polylogarithmic random bits.

How hard is it given a string x to find a string y such that y is random and y has roughly the same length as x? Note that y "extracts" out the randomness from x. In traditional Kolmogorov complexity one can describe y by x and only $\log n$ additional bits–the size of the smallest program for x. For polynomial-time complexity this attack appears not to work. However, we can use extractors to extract the randomness. We show that given a string x of high CND^p complexity we can find a string y that captures most of the randomness of x using only a small additional number of bits.

A full paper is available at http://www.cs.uchicago.edu/˜fortnow/papers/extr.ps.Z.

Exp. Sums and Circuits with a Single Threshold Gate and Mod-Gates

Frederic Green, Department of Mathematics and Computer Science, Clark University, Worcester, MA 01610 (fgreen@black.clarku.edu)

Abstract Number 97-21

Consider circuits consisting of a threshold gate at the top, Mod$_m$ gates at the next level (for a fixed m), and polylog fan-in AND gates at the lowest level. It is a difficult and important open problem to obtain exponential lower bounds for such circuits. Here we prove exponential lower bounds for restricted versions of this model, in which each Mod$_m$-of-AND subcircuit is a symmetric function of the inputs to that subcircuit. We show that if q is a prime not dividing m, the Mod$_q$ function requires exponential size circuits of this type. This generalizes recent results and techniques of Cai, Green and Thierauf [CGT] (which held only for $q = 2$) and Goldmann (which held only for depth two threshold over Mod$_m$ circuits). As a further generalization of the [CGT] result, the symmetry condition on the Mod$_m$ sub-circuits can be relaxed somewhat, still resulting in an exponential lower bound. The basis of the proof is to reduce the problem to estimating an exponential sum, which generalizes the notion of "correlation" studied by [CGT]. This identifies the type of exponential sum that will be instrumental in proving the general case. Along the way we substantially simplify previous proofs.

A full paper is available at http://aleph0.clarku.edu/~fgreen/papers/exp.ps or by e-mail at fgreen@black.clarku.edu.

Distinguishing Robust m-1 and T-Completeness on a Natural Class

Edith Hemaspaandra, Dept. of Mathematics, Le Moyne College, Syracuse, NY 13214, USA. Email: `edith@bamboo.lemoyne.edu`.

Lane A. Hemaspaandra, Department of Computer Science, University of Rochester, Rochester, NY 14627, USA. Email: `lane@cs.rochester.edu`.

Harald Hempel, Institut für Informatik, Friedrich-Schiller-Universität Jena, 07743 Jena, Germany. Email: `hempel@informatik.uni-jena.de`.

Abstract Number 97-22

Do complexity classes have many-one complete sets if and only if they have Turing-complete sets? We prove that there is a relativized world in which a relatively natural complexity class—namely a downward closure of NP—has Turing-complete sets but has no many-one complete sets. In fact, we show that in the same relativized world this class has 2-truth-table complete sets but lacks 1-truth-table complete sets. As part of the groundwork for our result, we prove that the class has many equivalent forms having to do with ordered and parallel access to NP and NP $\cap$ coNP.

A full paper is available by email to the authors.

Query Order in the Polynomial Hierarchy

Edith Hemaspaandra, Dept. of Mathematics, Le Moyne College, Syracuse, NY 13214, USA. Email: `edith@bamboo.lemoyne.edu`.
Lane A. Hemaspaandra, Department of Computer Science, University of Rochester, Rochester, NY 14627, USA. Email: `lane@cs.rochester.edu`.
Harald Hempel, Institut für Informatik, Friedrich-Schiller-Universität Jena, 07743 Jena, Germany. Email: `hempel@informatik.uni-jena.de`.

Abstract Number 97-23

The study of query order was initiated by Hemaspaandra, Hempel, and Wechsung [HHW]. Their goal was to learn whether the order of access to information sources affects the class of problems that can be solved. They showed that in the *boolean* hierarchy over NP, order matters. In the present paper, we study the power of query order when accessing levels of the *polynomial* hierarchy, and we show that here order does not matter. In particular, let $\mathrm{P}^{\mathcal{C}:\mathcal{D}}$ denote the class of languages computable by a polynomial-time machine that is allowed one query to $\mathcal{C}$ followed by one query to $\mathcal{D}$ [HHW]. We prove that the levels of the polynomial hierarchy are *order-oblivious*:

$$\mathrm{P}^{\Sigma_j^p:\Sigma_k^p} = \mathrm{P}^{\Sigma_k^p:\Sigma_j^p}.$$

Yet, we also show that these ordered query classes form new levels in the polynomial hierarchy unless the polynomial hierarchy collapses. We prove that a wide range of other classes (UP, BPP, $\oplus$P, PP, etc.) inherit all order-obliviousness results that hold for deterministic polynomial-time transducers.

References

[HHW] L. Hemaspaandra, H. Hempel, and G. Wechsung. Query order. *SIAM Journal on Computing.* To appear.

A full paper is available as UR-DCS-TR-96-634 at `http://www.cs.rochester.edu/trs`.

Lewis Carroll's 1876 Election System is Complete for Parallel Access to NP

Edith Hemaspaandra, Dept. of Mathematics, Le Moyne College, Syracuse, NY 13214, USA. Email: edith@bamboo.lemoyne.edu.
Lane A. Hemaspaandra, Department of Computer Science, University of Rochester, Rochester, NY 14627, USA. Email: lane@cs.rochester.edu.
Jörg Rothe, Inst. für Informatik, Friedrich-Schiller-Universität Jena, 07743 Jena, Germany. Email: rothe@informatik.uni-jena.de.

Abstract Number 97-24

In 1876, Lewis Carroll proposed an election system in which the winner is the candidate who with the fewest changes in voters' preferences becomes a Condorcet winner—a candidate who beats all other candidates in pairwise majority-rule elections. We establish the exactly computational complexity of determining the election winner in Carroll's system: Determining the winner in Carroll's system is complete for parallel access to NP. It is by far the most natural complete problem for this class.

It follows from our result that determining the winner in Carroll's elections is not NP-complete unless the polynomial hierarchy collapses.

A full paper is available by email to the authors.

Self-Specifying Machines

Lane A. Hemaspaandra, Department of Computer Science, University of Rochester, Rochester, NY 14627, USA. Email: `lane@cs.rochester.edu`.
Harald Hempel, Institut für Informatik, Friedrich-Schiller-Universität Jena, 07743 Jena, Germany. Email: `hempel@informatik.uni-jena.de`.
Gerd Wechsung, Institut für Informatik, Friedrich-Schiller-Universität Jena, 07743 Jena, Germany. Email: `wechsung@informatik.uni-jena.de`.

Abstract Number 97-25

We study the computational power of machines that specify their own acceptance types, and show that they accept exactly the languages in $\mathrm{R}_m^{\#\mathrm{P}}(\mathrm{NP})$. A natural variant accepts exactly the languages in $\mathrm{R}_m^{\#\mathrm{P}}(\mathrm{P})$. We show that these two classes coincide if and only if $\mathrm{P}^{\#\mathrm{P}[1]} = \mathrm{P}^{\#\mathrm{P}[1]:\mathrm{NP}[\mathcal{O}(1)]}$, where the latter class denotes the sets acceptable via at most one question to #P followed by at most a constant number of questions to NP.

A full paper is available as UR-DCS-TR-97-654 at `http://www.cs.rochester.edu/trs`.

Power Balance and Congressional Apportionment

Lane A. Hemaspaandra, Department of Computer Science, University of Rochester, Rochester, NY 14627, USA. Email: `lane@cs.rochester.edu`.
Kulathur S. Rajasethupathy, Department of Computer Science, SUNY–Brockport, Brockport, NY 14420. Email: `kraja@acspr1.acs.brockport.edu`.
Prasanna Sethupathy, P.O. Box 12315, Stanford University, Palo Alto, CA 94309. Email: `prasanna@leland.stanford.edu`.
Marius Zimand, School of Computer & Applied Sciences, Georgia Southwestern State University, Americus, GA 31709. Email: `zimand@gswrs6k1.gsw.peachnet.edu`.

Abstract Number 97-26

Can seemingly difficult functions in $\mathrm{FP}^{\mathrm{NP}^{\#\mathrm{P}}}$ (actually, merely "$(\mathrm{OptP})^{\#\mathrm{P}}$") be reasonably solved in practice? We consider the task of apportioning the Congress of the United States, and propose an approach that combines heuristic and exact computation. We establish that on every set of census data in this country's history, our approach *provably* (in the rigorous sense of the concept, from political science, of power indices) yields fairer apportionments than those of any of the historical approaches, including the algorithm currently used for Congressional apportionment.

A full paper is available as UR-DCS-TR-96-637 at `http://www.cs.rochester.edu/trs`.

Recognizing When Greed Can Approximate Maximum Independent Sets is Complete for Parallel Access to NP

Edith Hemaspaandra, Department of Mathematics, Le Moyne College, Syracuse, NY 13214, USA. Email: edith@bamboo.lemoyne.edu.
Jörg Rothe, Institut für Informatik, Friedrich-Schiller-Universität Jena, 07743 Jena, GERMANY. Email: rothe@informatik.uni-jena.de.

Abstract Number 97-27

Bodlaender, Thilikos, and Yamazaki [BTY97] investigate the computational complexity of the problem of whether the Minimum Degree Greedy Algorithm can approximate a maximum independent set of a graph within a constant factor of r, for fixed rational $r \geq 1$. They denote this problem by $\mathcal{S}_r$ and prove that for each rational $r \geq 1$, $\mathcal{S}_r$ is coNP-hard. They also provide a P^{NP} upper bound of $\mathcal{S}_r$, leaving open the question of whether this gap between the upper and the lower bound of $\mathcal{S}_r$ can be closed. For the special case of $r = 1$, they show that $\mathcal{S}_1$ is DP-hard (where DP denotes the class of sets that can be represented as the difference of two NP sets), again leaving open the question of whether $\mathcal{S}_1$ can be shown to be complete for DP or some larger class such as P^{NP}.

In this note, we completely solve all the questions left open by Bodlaender et al. in [BTY97]. Our main result is that for each rational $r \geq 1$, $\mathcal{S}_r$ is complete for $\mathrm{P}_{||}^{\mathrm{NP}}$ (a.k.a. Θ_2^p or $\mathrm{P}^{\mathrm{NP}[\log]}$), the class of sets solvable via parallel access to NP.

References

[BTY97] H. L. Bodlaender, D. Thilikos, and K. Yamazaki. It is hard to know when greedy is good for finding independent sets. *Information Processing Letters*, 61:101–106, 1997.

A full paper is available via email to the authors.

Compressibility and Uniform Complexity

Montserrat Hermo, Department of Software (LSI), Universidad del País Vasco, P.O. Box 649, E-20080 San Sebastián, Spain, (jiphehum@si.ehu.es)

Abstract Number 97-28

We focus on notions of resource-bounded complexity for infinite binary sequences, and compare both, a definition based on Kobayashi's concept of compressibility, and the uniform approach studied by Loveland.

It is known that for constant bounds on the complexity these definitions exactly coincide, and characterize the polynomial-time computable sequences when the running time is bounded by a polynomial, together with the recursive sequences when there is no time bound.

We show here how for complexity functions that are monotonic, and recursive, the Kobayashi and Loveland complexity concepts are equivalent under a small constant factor. This also works under time bounds if instead of bounding functions that are recursive, those that are computed within the allowed time are considered.

A full paper is available by email to jiphehum@si.ehu.es

Resource-bounded Randomness and Compressibility with Respect to Nonuniform Measures

Steven M. Kautz, Department of Mathematics, Randolph-Macon Woman's College, 2500 Rivermont Avenue, Lynchburg, VA 24503, USA (`skautz@rmwc.edu`)

Abstract Number 97-29

Most research on resource-bounded measure and randomness has focused on the uniform probability density, or Lebesgue measure, on $\{0,1\}^{\infty}$; the study of resource-bounded measure theory with respect to a *non*uniform underlying measure was recently initiated by Breutzmann and Lutz [1]. In this paper we prove a series of fundamental results on the role of nonuniform measures in resource-bounded measure theory. These results provide new tools for analyzing and constructing martingales and, in particular, offer new insight into the compressibility characterization of randomness given recently by Buhrman and Longpré [2]. We give several new characterizations of resource-bounded randomness with respect to an underlying measure μ: the first identifies those martingales whose rate of success is asymptotically *optimal* on the given sequence; the second identifies martingales which induce a *maximal compression* of the sequence; the third is a (nontrivial) extension of the compressibility characterization to the nonuniform case. In addition we prove several technical results of independent interest, including an extension to resource-bounded measure of the classical theorem of Kakutani on the equivalence of product measures; this answers an open question in [1].

An extended abstract will appear in the proceedings of RANDOM '97, July 1997, to be published by Springer. A version of the full paper is available from the author (`skautz@rmwc.edu`, `http://www2.rmwc.edu/skautz`).

1. J.M. Breutzmann and J.H. Lutz. Equivalence of measures of complexity classes. STACS '97.

2. H. Buhrman and L. Longpré. Compressibility and resource bounded measure. STACS '95.

On Cluster Machines and Function Classes

Sven Kosub, Theoretische Informatik, Universität Würzburg, Am Exerzierplatz 3, D-97072 Würzburg, GERMANY. (`kosub@informatik.uni-wuerzburg.de`)

Abstract Number 97-30

We consider a special kind of non-deterministic Turing machines. Cluster machines are distinguished by a neighbourhood relationship between accepting paths. Based on a formalization using equivalence relations some subtle properties of these machines are proven. Moreover, by abstraction we gain the machine-independend concept of cluster sets which is the starting point to establish cluster operators. Cluster operators map complexity classes of sets into complexity classes of functions where for the domain classes only cluster sets are allowed. For the counting operator $c\#\cdot$ and the optimization operators $\mathrm{cmax}\cdot$ and $\mathrm{cmin}\cdot$ the structural relationships between images resulting from these operators on the polynomial-time hierarchy are investigated. Furthermore, we compare cluster operators with the corresponding common operators $\#\cdot$, $\max\cdot$ and $\min\cdot$.

A full paper is available by email to kosub@informatik.uni-wuerzburg.de

Uniformly Defining Complexity Classes of Functions

Sven Kosub, Heinz Schmitz, and Heribert Vollmer, Theoretische Informatik, Universität Würzburg, Am Exerzierplatz 3, D-97072 Würzburg, GERMANY ({`kosub, schmitz, vollmer`}`@informatik.uni-wuerzburg.de`)

Abstract Number 97-31

We introduce a general framework for the definition of function classes. Our model, which is based on polynomial time nondeterministic Turing transducers, allows uniform characterizations of deterministic classes (FP), counting classes (#·P, #·NP, #·coNP, GapP, GapNP), optimization classes (max·P, min·P, max·NP, min·NP), promise classes (NPSV, $\#_{\mathrm{few}}$·P, c#·P), multivalued classes (FewPF, NPMV) and many more. Each such class is defined in our model by a certain family of functions. We introduce a reducibility notion between such families, which allows us to develop a necessary and sufficient criterion for relativizable inclusion between function classes. As it turns out, our criterion is very easily applicable and we get as a consequence e.g. that there are oracles A, B, such that $\mathrm{min}\cdot\mathrm{P}^A \not\subseteq \#\cdot\mathrm{NP}^A$, and $\mathrm{max}\cdot\mathrm{NP}^B \not\subseteq \mathrm{c}\#\cdot\mathrm{coNP}^B$. (Note that no structural consequences are known to follow from a collapse of these classes.)

A full paper will be available shortly. Send e-mail to one of the authors.

Computational Limitations of Stochastic Turing Machinesand Arthur-Merlin Games with Small Space Bounds

Maciej Liśkiewicz, Instytut Informatyki, Uniwersytet Wrocławski, 51-151 Wrocław, POLAND, (liskiewi@tcs.uni.wroc.pl)
Rüdiger Reischuk, Institut für Theoretische Informatik, Med. Universität zu Lübeck, D-23560 Lübeck, GERMANY. (reischuk@informatik.mu-luebeck.de)

Abstract Number 97-32

A stochastic Turing machine (STM) is a nondeterministic machine with the additional ability to perform random moves, also called games against nature by Papadimitriou. Alternative characterizations can be given by Arthur-Merlin-games of Babai and interactive proof systems with public coins of Goldwasser, Micali and Rackoff. Dwork/Stockmeyer, Condon and others have investigated stochastic Turing machines and interactive proof systems with small space bounds. Among others, it has been shown that for sublogarithmic bounds it makes a difference whether the random moves are known, as it is the case for a STM, resp. for Arthur-Merlin games, or whether they are hidden as in interactive proof systems. For any $S \in o(\log)$ the following separations have been shown:

$$BPSpace(S) =: AM_1 Space(S) \subset AMSpace(S) \subset AMSpace(\log) = \mathcal{P} \ ,$$

where $AMSpace(S)$ denotes the complexity class defined by S-space bounded STMs. By limiting the number of alternations (noted as $AM_k Space(S)$, resp. $MA_k Space(S)$ depending on whether the STM starts in a probabilistic, resp. nondeterministic configuration) we refine this chain. Our approach will be to define a sequence of simple languages parameterized by an index k, and to show that in order for a stochastic machine to accept them a certain number of alternations are necessary and sufficient, where the bound depends on k. This gives that for any integer $k \geq 1$ it holds

$$MA_{3k+2} Space(\log\log) \ \not\subseteq \ AM_k Space(o(\log)) \ \cup \ MA_k Space(o(\log)) \ .$$

As a consequence, almost tight separations for the corresponding classes and an infinite round/alternation hierarchy are obtained: for any $S \in o(\log) \cap O(\log\log)$ and any $k \geq 1$,

$$AM_k Space(S) \ \cup \ MA_k Space(S) \ \ \subset \ \ MA_{3k+2} Space(S) \ .$$

A full paper is available by email to liskiewi@tcs.uni.wroc.pl

Optimal proof systems for Propositional Logic and complete sets

Jochen Meßner and Jacobo Torán, Universität Ulm Theoretische Informatik
D-89069 Ulm, Germany
messner,toran@informatik.uni-ulm.de

Abstract Number 97-33

A polynomial time computable function $h : \Sigma^* \rightarrow \Sigma^*$ whose range is the set of tautologies in Propositional Logic (TAUT), is called a proof system. Cook and Reckhow defined this concept and in order to compare the relative strenth of different proof systems, they considered the notion of p-simulation. Intuitively a proof system h p-simulates a second one h' if there is a polynomial time computable function γ translating proofs in h' into proofs in h. A proof system is called optimal if it p-simulates every other proof system. The question of whether p-optimal proof systems exist is an important one in the field. Krajíček and Pudlák have given a sufficient condition for the existence of such optimal systems, showing that if the deterministic and nondeterministic exponential time classes coincide, then p-optimal proof systems exist. They also give a condition implying the existence of optimal proof systems (a related concept to the one of p-optimal systems) exist. In this paper we improve this result giving a weaker sufficient condition for this fact. We show that if a particular class of sets with low information content in nondeterministic double exponential time is included in the corresponding nondeterministic class, then p-optimal proof systems exist. We also show some complexity theoretical consequences that follow from the assumption of the existence of p-optimal systems. We prove that if p-optimal systems exist the the class UP (an some other related complexity classes) have many-one complete languages, and that many-one complete sets for NP $\cap$ SPARSE follow from the existence of optimal proof systems.

A full paper is available from the authors.

NP-hard sets have many hard instances

Martin Mundhenk, Universität Trier, FB IV – Informatik, D-54286 Trier, Germany (mundhenk@ti.uni-trier.de)

Abstract Number 97-34

The notion of *instance complexity* was introduced by Ko, Orponen, Schöning, and Watanabe (1986) as a measure of the complexity of individual instances of a decision problem. Comparing instance complexity to Kolmogorov complexity, they stated the "instance complexity conjecture," that every set not in P has p-hard instances. Whereas this conjecture is still unsettled, Buhrman and Orponen (1994) showed that E-complete sets have exponentially dense hard instances, and Fortnow and Kummer (1995) proved that NP-hard sets have p-hard instances unless P=NP. We introduce a slightly weaker notion of hard instances and obtain a superpolynomial lower bound on the density of hard instances in the case of NP-hard sets, unless P=NP.

Kummer (1995) proved that the class of recursive sets cannot be characterized by a respective version of the instance complexity conjecture, i.e. there exist nonrecursive sets without hard instances. We give a complete characterization of the class of recursive sets comparing the instance complexity to a relativized Kolmogorov complexity of strings. A set A is shown to be recursive iff $\mathrm{ic}(x : A) \leq \mathrm{C}^{K_0 \oplus A}(x)$ for almost all x. This translates to a characterization of P.

The paper is available at `www.informatik.uni-trier.de/~mundhenk/`.

Distributionally Hard Languages and Distributional Complete Problems

A. Pavan (aduri@cs.buffalo.edu,) *Alan L. Selman* (selman@cs.buffalo.edu)
Department of Computer Science, University at Buffalo, 226 Bell Hall, Box 602000, Buffalo, NY 14260-2000

Abstract Number 97-35

Cai and Selman (STACS, 1996, LNCS, v. 1046, 307–318, Springer-Verlag) defined a modification and extension of Levin's notion of average polynomial time to arbitrary time-bounds and proved that if L is P-bi-immune, then L is *distributionally hard*, meaning, that for every polynomial-time computable distribution μ, the distributional problem (L, μ) is not polynomial on the μ-average. We prove the following results, which suggest that distributional hardness is closely related to more traditional notions of hardness.

1. If NP contains a distributionally hard set, then NP contains a P-immune set.
2. There exists a language L that is distributionally hard but not P-bi-immune if and only if P contains a set that is immune to all P-printable sets.

The following corollaries follow readily

1. If the p-measure of NP is not zero, then there exists a language L that is distributionally hard but not P-bi-immune.
2. If the p_2-measure of NP is not zero, then there exists a language L in NP that is distributionally hard but not P-bi-immune.

We say that a distribution μ is *reasonable* if there exists a constant $s \geq 0$ such that $\mu(\{x \mid |x| \geq n\}) = \Omega(\frac{1}{n^s})$. Cai and Selman proved that if μ is reasonable, then for any language L, (L, μ) is polynomial on average with respect to Levin's definition if and only if it is polynomial on average by the definition of Cai-Selman. We prove the following results, which suggest that all DistNP-complete problems have reasonable distributions.

1. If the p-measure of NP is not zero, then for every $\leq_m^p$-complete distributional problem (L, μ) in DistNP, μ is reasonable.
2. If the p-measure of NP is not zero, then for every $\leq_m^{ap}$-complete distributional oblem (L, μ) in DistNP, μ is reasonable.

A full paper is available by email to aduri@cs.buffalo.edu or selman@cs.buffalo.edu, or on the web at www.ncstrl.org.

An Oracle Relative to which $R = NP$ but $NP \neq coNP$

Randall Pruim, Department of Computer Science, Boston University, Boston, MA, USA (rpruim@cs.bu.edu, rpruim@calvin.edu)

Abstract Number 97-36

An oracle A is constructed such that $R^A = NP^A ! = coNP^A$.

A rough sketch is currently available by email to to rpruim@cs.bu.edu

Betting Games, Resource-Bounded Measure, and Autoreducibility

Kenneth Regan, Dept. of Computer Science, SUNY at Buffalo, Buffalo, NY 14260, USA (regan@cs.buffalo.edu)
D. Sivakumar, Dept. of CS, Univ. of Houston, Houston, TX 77204, USA (siva@cs.uh.edu)
Martin Strauss, AT&T Labs,Florham Park,NJ 07932,USA (mstrauss@research.att.com)

Abstract Number 97-37

The question of whether the class of autoreducible languages has measure zero in exponential time (EXP) is of significant interest in complexity theory: On the one hand, Allender and Strauss (FOCS '94) showed that the class of languages Turing-hard for BPP has measure one in EXP, and on the other, Buhrman, Fortnow, and Torenvliet (FOCS '95) showed that the class of languages Turing-complete for EXP are all autoreducible. Thus if the class of autoreducible languages is shown to have measure zero in EXP, it would follow (using the fact that if $\mathcal{C}_1$ and $\mathcal{C}_2$ have measure zero in EXP, then so does $\mathcal{C}_1 \cup \mathcal{C}_2$) that BPP $\neq$ EXP.

Whereas various classes of languages that possess some form of structural redundancy have been shown to have measure zero in EXP (*eg.* P-selective sets, approximable sets, self-reducible sets, etc.), showing that autoreducible sets have measure zero has proved to be notoriously hard. To make progress on this and related matters, we introduce the notion of a *betting game* that generalizes Lutz's notion of a martingale. The difference is that while a Lutz martingale is required to bet on strings of Σ^* in the standard lexicographic ordering, our betting games can bet on strings in any (complexity-bounded) computable ordering.

We show that the class of autoreducible sets does have measure zero in EXP under the (more liberal) notion of measure zero via a betting game. Therefore, it follows that either of the following two conditions would imply BPP $\neq$ EXP: (1) The betting game notion of measure zero in EXP is identical to the standard Lutzian notion of measure zero in EXP; (2) If $\mathcal{C}_1$ and $\mathcal{C}_2$ have measure zero in EXP via betting games, then so does $\mathcal{C}_1 \cup \mathcal{C}_2$.

Unfortunately, at the present time, we don't know how to prove either of the two conditions above. However, we show that the existence of pseudorandom generators secure against probabilistic TMs that run in time 2^{n^ϵ} for some fixed $\epsilon > 0$ implies condition (1) (and hence (2)) above. We also have a preliminary result where we show that a much weaker hypothesis, namely the existence of a pseudorandom generator secure against (mildly) superpolynomial time PTMs, implies that the class of autoreducible sets has (Lutz) measure zero in EXP. (Note that this only implies that if there is a pseudorandom generator secure against superpolynomial time PTMs, then BPP $\neq$ EXP, which is obvious.)

A preliminary draft is available by email to the authors; a version fully treating the connections to BPP vs. EXP and weaker pseudorandom generators will be available shortly.

Making Nondeterminism Unambiguous

Klaus Reinhardt, Wilhelm-Schickard Institut für Informatik, Universität Tübingen, Sand 13, D-72076 Tübingen, GERMANY. (`reinhard@informatik.uni-tuebingen.de`)
Eric Allender, Department of Computer Science, Rutgers University, P.O. Box 1179, Piscataway, NJ 08855-1179, USA (`allender@cs.rutgers.edu`)

Abstract Number 97-38

We show that in the context of nonuniform complexity, nondeterministic logarithmic space bounded computation can be made unambiguous. An analogous result holds for the class of problems reducible to context-free languages. In terms of complexity classes, this can be stated as:

$$\mathrm{NL/poly} = \mathrm{UL/poly}$$
$$\mathrm{LogCFL/poly} = \mathrm{UAuxPDA}(\log n, n^{O(1)})/\mathrm{poly}$$

The proof makes use of the isolation lemma and a new extended version of the inductive counting technique.

A full paper is available at the Electronic Colloquium on Computational Complexity (ECCC):

`http://www.eccc.uni-trier.de/eccc`

or at our home pages:

`http://www-fs.informatik.uni-tuebingen.de/ reinhard`
`http://www.cs.rutgers.edu/ allender/publications`

Quantum computation and one-way functions

John D. Rogers, School of CTI, DePaul University, Chicago IL 60604, USA, (rogers@cs.depaul.edu)

Abstract Number 97-39

In his paper "On the power of quantum computation," Simon asks whether it is possible that the existence of one-way functions implies a separation between BPP and BQP. Building on work in the paper "Strengths and weaknesses of quantum computing," by Bennett, et al., we demonstrate an oracle relative to which one-way functions exist but BPP and BQP are the same. Thus, a proof of the implication will require nonrelativizing techniques.

A full paper will soon be available.

Characterizations of the Existence of Partial and Total One-Way Permutations

Jörg Rothe, Institut für Informatik, Friedrich-Schiller-Universität Jena, 07743 Jena, Germany. Email: `rothe@informatik.uni-jena.de`.
Lane A. Hemaspaandra, Department of Computer Science, University of Rochester, Rochester, NY 14627, USA. Email: `lane@cs.rochester.edu`.

Abstract Number 97-40

In this note, we study the easy certificate classes introduced by Hemaspaandra, Rothe, and Wechsung [HRW], with regard to the question of whether or not surjective one-way functions exist. This is an important open question in cryptology. We show that the existence of partial one-way permutations can be characterized by separating P from the class of UP sets that, for all unambiguous polynomial-time Turing machines accepting them, always have easy (i.e., polynomial-time computable) certificates. This extends the well-known results of Grollmann and Selman [GS88]. By Grädel's recent results about one-way functions [Grä94], this also links statements about easy certificates of NP sets with statements in finite model theory. Similarly, there exist surjective poly-one one-way functions if and only if there is a set L in P such that not all FewP machines accepting L always have easy certificates. We also establish a condition necessary and sufficient for the existence of (total) one-way permutations.

References

[Grä94] E. Grädel. Definability on finite structures and the existence of one-way functions. *Methods of Logic in Computer Science*, 1:299–314, 1994.

[GS88] J. Grollmann and A. Selman. Complexity measures for public-key cryptosystems. *SIAM Journal on Computing*, 17(2):309–335, 1988.

[HRW] L. Hemaspaandra, J. Rothe, and G. Wechsung. Easy sets and hard certificate schemes. *Acta Informatica.* To appear.

A full paper is available by email to the authors.

A Note on Parallel vs. Adaptive Queries when Computing Functions

Heinz Schmitz, Klaus W. Wagner, Theoretische Informatik, Universität Würzburg, Am Exerzierplatz 3, D-97072 Würzburg, GERMANY
({schmitz, wagner}@informatik.uni-wuerzburg.de)

Abstract Number 97-41

We contribute to the still open question $\mathrm{FP}_{||}^{\mathrm{NP}} \subseteq \mathrm{FP}_{\log}^{\mathrm{NP}}$ and equivalently restate it for subclasses $\mathcal{F}$ of $\mathrm{FP}_{||}^{\mathrm{NP}}$ as $\mathcal{F} \subseteq \mathrm{FP}_{\log}^{\mathrm{NP}}$. Each of these subclasses corresponds to a certain level of the boolean hierarchy over NP and together they form a proper hierarchy of function classes between NPSV and $\mathrm{FP}_{||}^{\mathrm{NP}}$, i. e. if two of them should coincide then the boolean hierarchy over NP collapses. Moreover, all these new classes $\mathcal{F}$ characterize the difference between $\mathrm{FP}_{||}^{\mathrm{NP}}$ and $\mathrm{FP}_{\log}^{\mathrm{NP}}$ as $\mathrm{FP}_{||}^{\mathrm{NP}} = \mathcal{F} \circ \mathrm{FP}_{\log}^{\mathrm{NP}}$. As a natural extension of NPSV when omitting the promise condition we introduce NPUV (*uniquevalued* functions), the smallest class of functions with the above property, and investigate its relation to other well–known function classes. All results are obtained in a more general setting using restricted maximum operators and remain valid for NP and many other oracle classes.

A full paper will be available soon. Send e-mail to schmitz@informatik.uni-wuerzburg.de

Randomness, Stochasticity and Approximations

Yongge Wang, Dept of CS, Univ. of Auckland, Private Bag 92019, Auckland, NZ(wang@cs.auckland.ac.nz)

Abstract Number 97-42

Polynomial time unsafe approximations for intractable sets were introduced by Meyer and Paterson [4] and Yesha [8] respectively. The question of which sets have optimal unsafe approximations has been investigated extensively, see, e.g., [1,3,6,7]. Recently, Wang [6,7] showed that polynomial time random sets are neither optimally unsafe approximable nor Δ-levelable. In this paper, we will show that: (1) There exists a polynomial time stochastic set in $\mathbf{E}_2$ which has an optimal unsafe approximation. (2) There exists a polynomial time stochastic set in $\mathbf{E}_2$ which is Δ-levelable. The above two results answer a question asked by Ambos-Spies and Lutz et al. [2]: What kind of natural complexity property can be characterized by p-randomness but not by p-stochasticity? Our above results also extend Ville's [5] historical result. The proof of our first result shows that, for Ville's stochastic sequence, we can find an optimal betting strategy (prediction function) such that we will never lose our own money (except the money we have earned), that is to say, if at the beginning we have only one dollar and we always bet one dollar that the next selected bit is 1, then we always have enough money to bet on the next bit. Our second result shows that there is a stochastic sequence for which there is a betting strategy such that we will never lose our own money (except the money we have earned), but there is no such kind of optimal betting strategy. That is to say, for any such kind of betting strategy, we can find another betting strategy which could be used to make money more quickly.

1. K. Ambos-Spies. On opt. poly. time approx.: **P**-levelability vs. Δ-levelability. In *Proc. 22nd ICALP*, LNCS 944, pp. 384–392. Springer Verlag, 1995.
2. K. Ambos-Spies, and J. Lutz. Dagstuhl Workshop on *Randomness and Information* 1996.
3. P. Duris and J. D. P. Rolim. **E**-complete sets do not have optimal polynomial time approximations. In *Proc. 19th MFCS*, LNCS, 841, pages 38–51. Springer Verlag, 1994.
4. A. R. Meyer and M. S. Paterson. With what frequency are apparently intractable problems difficult? Technical Report TM-126, Laboratory for Computer Science, MIT, 1979.
5. J. Ville. *Etude Critique de la Notion de Collectif.* Gauthiers-Villars, Paris, 1939.
6. Y. Wang. *Randomness and Complexity.* PhD thesis, Heidelberg, 1996.
7. Y. Wang. Genericity, randomness, and poly time approx. To appear in *SICOMP*
8. Y. Yesha. On certain polynomial-time truth-table reducibilities of complete sets to sparse sets. *SIAM J. Comput.*, 12:411–425, 1983.

A full paper is available by email to wang@cs.auckland.ac.nz