Structures Abstracts 1995. Vol V

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.

Titles of Abstracts

Measure on P: Robustness of the Notion
The Complexity of Matrix Rank and Feasible Systems of Linear Equations
Other Logics that Capture NP and Have Normal Forms
Optimal Universal Parallel Computer, Neural Networks, and Kolgmorov's Theorem
Using Autoreducibility to Separate Complexity Classes
Compressibility and Resource Bounded Measure
The Complexity of Generating and Checking Proofs of Membership
On the Existence of Hard Sparse Sets under Weak Reductions
Sparse Hard Sets for P: Resolution of a Conjecture of Hartmanis
Sparse Parameterized Problems
Helping by Unambiguous Computation and Probabilistic Computation
A Formal Framework for Evaluating Heuristic Programs
Automata That Take Advice
Fragments of Binary NP
On Random-self-reducibility: Adaptiveness, Advice, and Self-correctability
On Inverting Onto Functions
Optimal Advice
Dense Hierarchy between Monotone NC_1 and Monotone NC_2
Improved Hardness Results for Approximating the Chromatic Number
Graph Isomorphism Testing without Numerics
Lower Bounds for Circuits with Mod Gates and One Exact Threshold Gate
Universally Serializable Computation
Polynomial-Time Semi-Rankable Sets
Optimal Advice
Computability and Complexity Over Structures of Finite Type
An Algebraic Characterization of Tractable Constraints
Completeness and Weak Completeness under Polynomial-Size Circuits
Random Elements, Composite Measures, and Quantum Mechanics
A Non-Algorithmic Analogue of Kolmogorov-Martin-Lof Randomness
Why Are Symmetries a Universal Language of Physics? A Remark
A Constant-Space Sequential Model of Computation for First-Order Logic
On the Power of Additional Output Values
The PL Hierarchy Collapses
Sparse Hard Sets for P Yield Space-efficient Algorithms
Function Computable with Limited Access to NP
Pseudorandom Generators, Measure Theory, and Natural Proofs
Improved Resource-Bounded Borel-Cantelli and Stochasticity Theorems
On the Power of Bio-Computers
Sets Computable in Polynomial Time on Average
A Tight Upper Bd on Kolm. Comp. by Hausdorff Dim. and Unif. Opt. Prediction
Probabilistic Boolean Decision Trees: Several Remarks
The Chain Method to Separate Counting Classes
Lectures on the Fusion Method and Derandomization
On the Size of Classes with Weak Membership Properties
On randomized cryptographic primitives
Large sets in AC^0: a Kolmogorov complexity related property and some applications

Measure on P: Robustness of the Notion

Eric Allender Department of Computer Science, Rutgers University, PO Box 1179, Piscataway, NJ 08855-1179, USA. (allender@cs.rutgers.edu)
Martin Strauss Department of Mathematics, Rutgers University, PO Box 1179, Piscataway, NJ 08855-1179, USA. (mstrauss@math.rutgers.edu)

Abstract Number 95-1

In (Allender and Strauss, FOCS '95), we defined a notion of measure on the complexity class P (in the spirit of the work of (Lutz, JCSS '92) that provides a notion of measure on complexity classes at least as large as E, and the work of (Mayordomo, Phd. Thesis, 1994) that provides a measure on PSPACE). In this paper, we show that several other ways of defining measure in terms of covers and martingales yield precisely the same notion as in (Allender and Strauss). (Similar "robustness" results have been obtained previously for the notions of measure defined by Lutz and Mayordomo, but – for reasons that will become apparent below – different proofs are required in our setting.)

To our surprise, and in contrast to the measures of Lutz and Mayordomo, one obtains strictly more measurable sets if one considers "nonconservative" martingales that succeed merely in the lim sup rather than having a limit of infinity. For example, it is shown in (Allender and Strauss) that the class of sparse sets does not have measure zero in P, whereas here we show that using the "nonconservative" measure, the class of sparse sets (and in fact the class of sets with density $\epsilon < 1/2$) does have measure zero. We also show that our "nonconservative" measure on PSPACE is incomparable with that of Mayordomo.

An extended abstract announcing these results will be be presented at MFCS '95. A full version of the paper is available as ECCC report number 95-028.

The Complexity of Matrix Rank and Feasible Systems of Linear Equations

Eric Allender Department of Computer Science, Rutgers University, PO Box 1179, Piscataway, NJ 08855-1179, USA. (allender@cs.rutgers.edu)
Robert Beals DIMACS, Rutgers University, PO Box 1179, Piscataway, NJ 08855-1179, USA, and School for Mathematics, Institute for Advanced Study, Olden Lane, Princeton, NJ 08540, USA. (rbeals@dimacs.rutgers.edu)
Mitsunori Ogihara Department of Computer Science, University of Rochester, Rochester, NY, 14627, USA (ogihara@cs.rochester.edu)

Abstract Number 95-2

We consider some natural and important computational problems in linear algebra whose exact characterization in terms of computational complexity has long been unknown. In particular, we consider the following problems about integer matrices:

$$\mathit{Ver.RANK} = \{(A,r) : A \in \mathbf{Z}^{n\times n}, r \in \mathbf{N}, \mathrm{rank}(A) = r\}.$$
$$\mathit{Comp.RANK} = \{(A,i,b) : A \in \mathbf{Z}^{n\times n}, \mathrm{rank}(A) = r, \text{ and bit number } i \text{ of } r \text{ is } b\}$$
$$\mathit{FSLE} = \{(A,\vec{b}) : A \in \mathbf{Z}^{n\times n}, \vec{b} \in \mathbf{Z}^{n\times 1}, \exists X \in \mathbf{Q}^{n\times 1} : AX = \vec{b}\}.$$

(*FSLE* stands for Feasible Systems of Linear Equations.)

We show that *FSLE* and *Comp.RANK* are complete for the complexity class $\mathrm{L(C_{=}L)}$ consisting of sets that are logspace-Turing reducible to sets in $\mathrm{C_{=}L}$. (Equivalently, this is the class of languages reducible to the set of singular matrices, since $\{A : \mathit{DET}(A) = 0\}$ is complete for $\mathrm{C_{=}L}$.) Also, we show that *Ver.RANK* is complete for the second level of the Boolean Hierarchy above $\mathrm{C_{=}L}$. If $\mathrm{C_{=}L}$ is closed under complement, then all of these classes collapse to $\mathrm{C_{=}L}$.

One of our main results is the collapse of the $\mathrm{C_{=}L}$ hierarchy defined by [Allender, Ogihara; Structures 1994]. This hierarchy can be defined equivalently as $\mathrm{AC^0(C_{=}L)}$, or as the union of the classes

$$\mathrm{L^{C_{=}L}} \subseteq \mathrm{NL^{C_{=}L}} \subseteq \mathrm{C_{=}L^{C_{=}L}} \subseteq \mathrm{C_{=}L^{C_{=}L^{C_{=}L}}} \subseteq \dots$$

We show that all of these classes collapse to the lowest level (i.e., to the class of problems reducible to *FSLE*); and this class is itself logspace disjunctive-truth-table reducible to *Ver.RANK*.

A similar collapse of the PL hierarchy was recently proved by Ogihara. Note that these classes are the logspace-analogs of the counting hierarchy consisting of PP, $\mathrm{PP^{PP}}$, ...

A complete version of the paper is not yet available.

Other Logics that Capture NP and Have Normal Forms

Argimiro A. Arratia-Quesada,
University of Wisconsin-Madison, Department of Mathematics, 480 Lincoln Drive, Madison, WI 53706, USA
(quesada@math.wisc.edu)

Abstract Number 95-3

We present the operators ELP and OLP, which correspond to the NP-complete problems *even length path* and *odd length path*: Given a directed graph $G = (V, E)$, together with two specified vertices $s, t \in V$, to find a simple path from s to t in G which contains an even (resp. odd) number of arcs. We show that the logics $ELP^*[FO_s]$ and $OLP^*[FO_s]$, constructed by adjoining to first order logic with successor relation the operator ELP (resp. OLP), captures NP and have a normal form (i.e., nested applications of the operator is equivalent to one application). Specifically, we show

Theorem: Every formula $\phi \in ELP^*[FO_s](\tau)$ (resp. $OLP^*[FO_s](\tau)$) is equivalent to a formula of the form $ELP[\lambda\,\overline{x}\,\overline{y}\,\psi](\overline{0}, \overline{max})$, (resp. $OLP[\lambda\,\overline{x}\,\overline{y}\,\psi](\overline{0}, \overline{max})$), where $\psi \in FO_s(\tau)$, ψ projective and over the distinct k-tuples of variables $\overline{x}$ and $\overline{y}$, for some $k \geq 1$, and where $\overline{0}$ (resp. $\overline{max}$) is the constant symbol 0 (resp. max) repeated k-times.

Thus, ELP and OLP have similar properties to the Hamiltonian path operator, HP, studied by I. A. Stewart in *J. of Comp. and System Sci., 45, 1992, 127–151.* As a corollary, we obtain that the problem ELP (resp. OLP) is complete for NP via first order projections, just as HP is. Assuming $NP \neq coNP$, we observe that, in general, problems that generate logics with a normal form, like Stewart's $HP^*[FO_s]$, can not be complete via first order *monotone* projections. So, we have a lower bound for the type of reducibilities under which these problems are complete (relative to the NP =?$coNP$ question). Our ultimate goal is to understand the reasons that govern the existence of normal forms for this type of logics, and we hope that these examples help illuminate this problem.

A full paper will be available shortly.

Optimal Universal Parallel Computer, Neural Networks, and Kolmogorov's Theorem

Andrew Bernat, Vladik Kreinovich, Luc Longpré, Department of Computer Science, University of Texas at El Paso, El Paso, TX 79968 ({abernat,vladik,longpre}@cs.utep.edu)
David A. Sprecher, Department of Mathematics, University of California at Santa Barbara, Santa Barbara, CA 93106, (sprecher@math.ucsb.edu)

Abstract Number 95-4

How can we design the fastest parallel computer architecture that is *universal* in the sense that it will be able to perform arbitrary computations? To make computations faster, we must divide them into the simplest possible (and thus, fastest possible) procesing elements working in parallel. The simplest possible operation with real numbers $x_1, ..., x_n$ is computing their linear combination. However, if we only have these *linear* processing elements, we will only be able to compute linear functions. So, to make the computer universal, we also need some *nonlinear* processing elements that compute non-linear functions $y = f(x_1, ..., x_n)$. In general, the greater the number n of inputs, the more time it takes to process them and compute n. So, the simplest nonlinear procesing element computes a function of one variable $f(x)$. To get a general computation, we must combine the resulting processing elements. The resulting time of parallel computation increases with the number of layers. So, the fewer layers, the faster the computations. We show that:

- with one or two layers, we do not get a universal computer;
- for an appropriate three-layer architecture, we get a *neural* architecture that enables us to *approximate* an arbitrary non-linear function; we also prove that three layers are not sufficient to *exactly represent* all non-linear functions;
- finally, for four layers, Kolmogorov's superposition theorem enables us to *exactly represent* all non-linear functions.

We also discuss whether these results remain valid if, in addition to computation time (as described by the number of layers), we take communication time into consideration.

A preliminary version is available by email request to vladik@cs.utep.edu. A full paper will be available shortly.

Using Autoreducibility to Separate Complexity Classes

Harry Buhrman, CWI. PO Box 94079, 1090 GB Amsterdam, The Netherlands. E-mail: buhrman@cwi.nl
Lance Fortnow, Department of Computer Science, University of Chicago, 1100 E. 58th St., Chicago, IL 60637. Email: fortnow@cs.uchicago.edu.
Leen Torenvliet, University of Amsterdam, Plantage Muidergracht 24, 1024 TV, Amsterdam. E-mail: leen@fwi.uva.nl

Abstract Number 95-5

A language is autoreducible if it can be reduced to itself by a Turing machine that does not ask its own input to the oracle. We use autoreducibility to separate exponential space from doubly exponential space by showing that all Turing-complete sets for exponential space are autoreducible but there exists some Turing-complete set for doubly exponential space that is not. We immediately also get a separation of logarithmic space from polynomial space.

Although we already know how to separate these classes using diagonalization, our proofs separate classes solely by showing they have different structural properties, thus applying Post's Program to complexity theory. We feel such techniques may prove unknown separations in the future. In particular if we could settle the question as to whether all complete sets for doubly exponential time were autoreducible we would separate polynomial time from either logarithmic space or polynomial space.

We also show several other theorems about autoreducibility.

An extended abstract is available from
ftp://cs.uchicago.edu/pub/users/fortnow/papers/auto.ps.Z

Compressibility and Resource Bounded Measure

Harry Buhrman, Centrum voor Wishkunde en Informatica, PO Box 94079, 1090 GB Amsterdam, The Netherlands. (buhrman@cwi.nl)
Luc Longpré, Computer Science Department, University of Texas at El Paso, El Paso, TX 79968, USA. (longpre@cs.utep.edu)

Abstract Number 95-6

We give a new definition of resource bounded measure based on compressibility of infinite binary strings. We prove that the new definition is equivalent to the one commonly used. This new characterization offers us a different way to look at resource bounded measure, shedding more light on the meaning of measure zero results and providing one more tool to prove such results.

We then show how this new characterization can be used to prove that the class of linear auto-reducible sets has p-measure 0. We also prove that the class of sets that are truth-table reducible to a p-selective set has p-measure 0 and that the class of sets that Turing reduce to a sub-polynomial dense set has p-measure 0. This strengthens various results.

A full paper is available by email to longpre@cs.utep.edu

The Complexity of Generating and Checking Proofs of Membership

Harry Buhrman, CWI Amsterdam, PO Box 94079, 1090 GB Amsterdam, The Netherlands. (`buhrman@cwi.nl`)
Thomas Thierauf, Abt. Theoretische Informatik, Universität Ulm, Oberer Eselsberg, 89069 Ulm, Germany. (`thierauf@informatik.uni-ulm.de`)

Abstract Number 95-7

We consider the following questions:

1. Can one compute satisfying assignments for satisfiable Boolean formulas in polynomial time with parallel queries to NP?
2. Is the unique optimal clique problem (UOCLIQUE) complete for $\mathrm{P}^{\mathrm{NP[log]}}$?
3. Is the unique satisfiability problem (USAT) NP hard?

We investigate the complexity of generating proofs of membership for sets in NP and $\mathrm{P}^{\mathrm{NP[log]}}$ and the complexity of checking these proofs. We show that such *proof-systems* can be used to distinguish the complexity of NP hard or $\mathrm{P}^{\mathrm{NP[log]}}$ complete sets from the complexity of USAT or UOCLIQUE, thereby giving some evidence that the answer to all the above questions is 'no'. Furthermore, we show the existence of an oracle relative to which $\mathrm{FP}_{||}^{\mathrm{NP}}$ is not powerful enough to compute satisfying assignments for satisfiable Boolean formulas, answering a question of Ogihara.

A full paper is available.

On the Existence of Hard Sparse Sets under Weak Reductions

Jin-yi Cai, State University of New York at Buffalo, (cai@cs.buffalo.edu)
Ashish V. Naik, University of Chicago, (naik@cs.uchicago.edu)
D. Sivakumar, State University of New York at Buffalo (sivak-d@cs.buffalo.edu)

Abstract Number 95-8

Recently a 1978 conjecture by Hartmanis was resolved by Cai and Sivakumar, following progress made by Ogihara. It was shown that *many-one hard* sparse sets for P do not exist unless P = LOGSPACE. We extend the results to the case of sparse sets that are hard under more general reducibilities. Our main results are as follows.

(1) If there exists a sparse set that is hard for P under bounded truth-table reductions, then P = NC^2.

(2) If there exists sparse that is hard for $O(\log n)$-positive truth-table reductions, then every language in P is computable by a family of randomized circuits of size $2^{O(\log^2 n)}$ and depth $O(\log^2 n)$.

(3) If there exists a sparse set that is hard for P under RNC^2 reductions with one-sided error, then P $\subseteq$ RNC^2.

(4) If there exists an NP-hard sparse set under randomized polynomial-time reductions with one-sided error, then NP = RP. This answers an open question by Ranjan and Rohatgi.

(5) If there exists a $2^{(\log n)^{O(1)}}$-sparse hard set for P under truth-table reductions, then $P \subseteq$ DSPACE$[(\log n)^{O(1)}]$.

Also, as a by-product of (5), we obtain a uniform $O(\log^2 n \log\log n)$ time parallel algorithm for computing the rank of a $2^{\log^2 n} \times n$ matrix over an arbitrary field, generalizing a result of Mulmuley. This algorithm may be of independent interest in solving non-square linear equation systems.

A full paper is available from the authors.

Sparse Hard Sets for P: Resolution of a Conjecture of Hartmanis

Jin-yi Cai and D. Sivakumar, Dept. of Computer Science, State Univ. of NY at Buffalo, Buffalo, NY 14260, USA. ({cai,sivak-d}@cs.buffalo.edu)

Abstract Number 95-9

A set S is called sparse if there are at most a polynomial number of strings in S up to length n. The study of sparse hard sets originated with the famous Berman–Hartmanis conjecture about the isomorphism of NP-complete sets. Sparse sets have been the subject of study in complexity theory for the past 20 years, as they reveal inherent structure and limitations of computation. For instance, it is well known that the class of languages Turing-reducible to a sparse set is precisely the class of languages with polynomial size circuits.

Some fundamental results have been established concerning the existence of sparse sets hard for various classes: Karp and Lipton proved that if a Turing hard sparse set exists for NP, then the polynomial time hierarchy collapses to its second level. Mahaney showed that if a sparse NP-hard set exists under polynomial-time many-one reductions, then NP = P.

Hartmanis conjectured in 1978 that there are no sparse complete sets for P under logspace many-one reductions. We resolve this conjecture of Hartmanis: we show that if sparse hard set exists for P under logspace many-one reductions, then P = LOGSPACE.

An interesting aspect of our work is that the techniques we employ are probabilistic and algebraic in nature. Following recent work by M. Ogihara, we first show that if a sparse set exists for P under logspace many-one reductions, then P = NC^2. We first give a randomized construction that shows P = $\mathcal{R}\mathrm{NC}^2$, under the given hypothesis. Then we use techniques from finite field theory to derandomize this construction. The techniques are relevant to constructions of small sample spaces.

Using more finite field theory and the discrete Fourier Transform, we finally prove the following result: if a sparse set S is hard for P under many-one reductions, then P collapses to NC^1 (with oracle access to the reduction to S). It follows that if a sparse hard set exists for P under logspace many-one reductions, then P = LOGSPACE.

We combine the above techniques with a novel application of the famous Immerman–Szelepcsényi theorem (NL = co-NL) to affirm another conjecture of Hartmanis: we show that if a sparse set S is hard for NL (nondeterministic logspace) under logspace many-one reductions, then NL = LOGSPACE.

The first author was supported in part by NSF grants CCR-9319393 and CCR-9057486, and by a Sloan fellowship; the second author was supported in part by NSF grant CCR-9409104.

An extended abstract is available by email to the authors.

Sparse Parameterized Problems

Marco Cesati,
Department of Computer Science, University of Rome “La Sapienza”,
via Salaria 113, 00198 Roma, ITALY. E-mail: `cesati@dsi.uniroma1.it`

Michael R. Fellows,
Department of Computer Science, University of Victoria,
Victoria, British Columbia, V8W 3P6 CANADA. E-mail: `mfellows@csr.uvic.ca`

Abstract Number 95-10

Many natural computational problems have input that consists of a pair of items, and often one element of the pair should be regarded as a *parameter*. A parameterized problem is *fixed-parameter tractable* (i.e., in FPT) if there exists an algorithm to solve the problem in time bounded by $f(k)n^\alpha$ for any instance (x, k) where $n = |x|$. Here f is an arbitrary function (even not recursive) and α is a constant not depending on k.

Downey and Fellows have established in a series of recent papers the framework of a completeness theory with which to address the apparent fixed-parameter intractability of many parameterized problems. In particular, they defined a hierarchy of classes of parameterized problems FPT $\subseteq$ W[1] $\subseteq$ W[2] $\subseteq \cdots \subseteq$ W[P] (the *W hierarchy*) and showed that a variety of natural problems are complete for various levels of this hierarchy.

The setting of parameterized complexity introduces substantial technical challenges for nearly every conjectured analog of classical structural results. Experience so far seems to indicate that new and more powerful techniques than in the classical case are often required for headway on analogous parameterized structural questions.

In this paper we prove a full analog of Mahaney's theorem. A parameterized problem L is *sparse* if there exist an arbitrary function $g : N \to N$ and a constant β such that for all $n > 0$ and $k \geq 0$, $|\{(x, k) \in L : |x| \leq n\}| \leq g(k)n^\beta$. Then:

If there is a sparse parameterized problem which is hard for $W[t]$ $(t \geq 1)$*, then* $W[t] = FPT$.

The proof is based on substantial modifications and extensions of the method of *left set* introduced in the classical setting by Ogiwara and Watanabe; however, we must deal with two sources of difficulty. The first one arises from the definition of the W-classes, which essentially limits us to very restricted computational power, especially in the case of W[1]. We address this with several combinatorial tricks in the design of bounded-depth circuits. The second problem arises from the fact that the parameter functions might not be recursive. We handle this by incorporating the left sets algorithm inside of a diagonalization against all possible values of the relevant parameter function.

A full paper is available. See also the WWW page on Parameterized Complexity (at URL `http://www-csc.uvic.ca/home/mhallett/research.html`).

Helping by Unambiguous Computation and Probabilistic Computation

Patrizio Cintioli, Dipartimento di Matematica, Università di Siena, via del Capitano 15, 53100 Siena, Italy. (`cintioli@sivax.cineca.it`)
Riccardo Silvestri, Dipartimento di Scienze dell'Informazione, Università di Roma "La Sapienza", via Salaria 113, 00198 Roma, Italy. (`silvestri@dsi.uniroma1.it`)

Abstract Number 95-11

Schöning [*TCS* **40** (1985), 57–66] introduced a notion of helping, based on robust machines, and suggested the study of the class $\mathrm{P}_{\mathrm{help}}(\mathcal{C})$ of languages that can be helped by oracles in a given class $\mathcal{C}$. Among the other results, he showed that $\mathrm{P}_{\mathrm{help}}(\mathrm{BPP})$ is included in ZPP. Later, Ko [*TCS* **52** (1987), 15–36] introduced a weaker notion of helping, called one-sided helping, and proved that $\mathrm{P}_{1\text{-help}}(\mathrm{BPP})$ is included in R and that UP is included in $\mathrm{P}_{1\text{-help}}(\mathrm{UP})$. The three inverse inclusions are open problems (see [Hemachandra, *Proc. 20th ICALP*, (1993)]). Cai et al. [*Proc. 17th MFCS*, LNCS **629** (1992), 162–171] constructed a relativized world in which the third open inclusion fails. We show relativized worlds in which all the three open inclusions fail in a strong way.
By using a uniform approach to define complexity classes, introduced by Bovet et al. [*TCS* **104** (1992), 263–283] and by Vereshchagin [*Russian Academy of Sciences. Izvestiya. Mathematics (AMS)* **42** (1994), 261–298], we find quite general conditions on a complexity class $\mathcal{C}$ to ensure the relativized separation of $\mathrm{P}_{\mathrm{help}}(\mathrm{UP})$ from $\mathcal{C}$. Among the many corollaries, we strengthens the result of Cai et al., showing that $\mathrm{P}_{\mathrm{help}}(\mathrm{UP})$ is not included in Few. The other two open inclusions are showed to strongly fail by the relativized separation of ZPP from $\mathrm{P}_{1\text{-help}}(\mathrm{AM} \cap \text{co-AM})$. Another consequence of this separation is the existence of a relativized world in which ZPP is not included in $\mathrm{P}_{1\text{-help}}(\mathrm{NP} \cap \text{co-NP})$.

A full paper is available by email to silvestri@dsi.uniroma1.it

A Formal Framework for Evaluating Heuristic Programs

Lenore Cowen, Mathematical Sciences Department, The Johns Hopkins University, Baltimore, MD 21218-2689, USA (`cowen@brutus.mts.jhu.edu`)
Joan Feigenbaum, AT&T Bell Laboratories, Room 2C-473, 600 Mountain Avenue, Murray Hill, NJ 07974-0636, USA (`jf@research.att.com`)
Sampath Kannan, Department of Computer and Information Science, University of Pennsylvania, Philadelphia, PA 19104-6389, USA (`kannan@central.cis.upenn.edu`)

Abstract Number 95-12

We address the question of how one evaluates the usefulness of a heuristic program on a particular input. If theoretical tools do not allow us to decide for every instance whether a particular heuristic is fast enough, might we at least write a simple, fast companion program that makes this decision on some inputs of interest? We call such a companion program a *timer* for the heuristic. Timers are related to program checkers, as defined by Blum, in the following sense: Checkers are companion programs that check the *correctness* of the output produced by (unproven but bounded-time) programs on particular instances; timers, on the other hand, are companion programs that attempt to *bound the running time* on particular instances of correct programs whose running times have not been fully analyzed. This paper provides a family of definitions that formalize the notion of a timer and some preliminary results that demonstrate the utility of these definitions.

An extended abstract is available by email to any of the authors.

Automata That Take Advice

Carsten Damm, FB IV—Informatik, Universität Trier, 54286 Trier, GERMANY. (damm@uni-trier.de)
Markus Holzer, Fakultät f. Informatik, Universität Tübingen, 72076 Tübingen, GERMANY. (holzer@informatik.uni-tuebingen.de)

Abstract Number 95-13

A universal formalization of the idea of nonuniformity has been proposed and studied in depth by Karp and Lipton: Given a class $\mathcal{B}$ of languages and a set $\mathcal{F}$ of sequences (*advices*) $\alpha = (\alpha_n)$ of strings, define the nonuniform counterpart $\mathcal{B}/\mathcal{F}$ of $\mathcal{B}$ as the class of sets of the form $L : \alpha = \{ w \mid \alpha_{|w|} w \in L \}$, with $L \in \mathcal{B}$ and $\alpha \in \mathcal{F}$.

Although several models of nonuniformity were studied in connection with automata and formal language theory, this approach—despite of it's unifying power—has not been investigated in this field. We try to fill this gap in studying the Chomsky Hierarchy **REG** $\subset$ **CFL** $\subset$ **CS** $\subset$ **RE** relative to advices.

We relate this to grammar-based nonuniform cost measures μ for formal language classes: For a language L let $\mu_L(n)$ denote the minimum size of a Chomsky-grammar of the appropriate type such that the set of words of length n generated by this grammar equals the set of words of length n in L. Similar measures have been considered by several other authors.

1. **REG** $\subset$ **CFL** $\subset$ **CS** $\subset$ **RE** relative to constant length and to polynomial length advices.

   The classes of the Chomsky Hierarchy relative to constant length advices are strictly contained in the corresponding classes relative to polynomial length advices except for **REG** where equality holds.

2. Allowing constant length advices is equivalent to allowing constantly bounded grammar sizes.

   Allowing polynomial length advices is equivalent to allowing polynomially bounded grammar sizes for **CS** and for **RE**. For **REG** this is not the case and for **CFL** this is unknown.

A full paper is available:
ftp.informatik.uni-trier.de:/pub/users/Damm/Automata.ps.

Fragments of Binary NP

Arnaud Durand
Université de Caen
arnaud@calvin.info.unicaen.fr

Clemens Lautemann & Thomas Schwentick
Johannes Gutenberg–Universität Mainz
{cl,tick}@informatik.mathematik.uni-mainz.de

Abstract Number 95-14

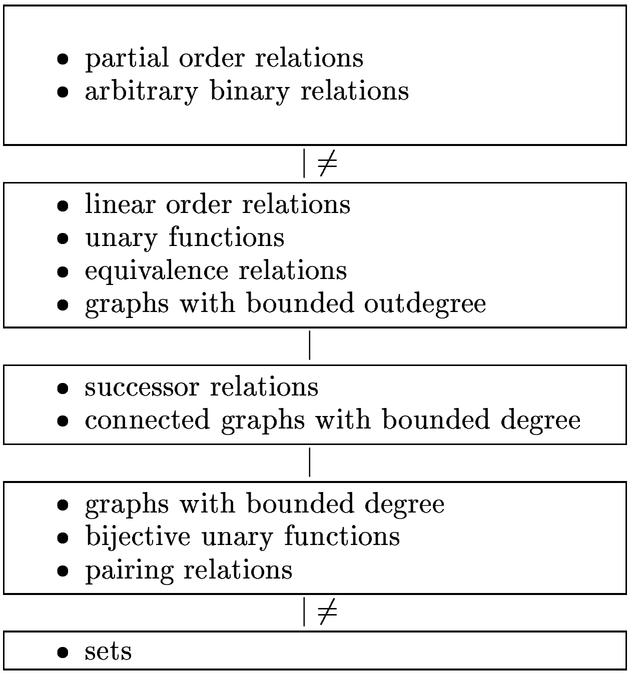
In the last few years most computational complexity classes have been characterized in terms of *descriptional* complexity. One of the earliest, and the most influential such result was Fagin's theorem, which characterizes the complexity class NP through Σ^1_1, i.e., existential second order logic. This result created hopes that it might be possible to attack the main open problems of complexity theory with methods of logic. In an attempt to tackle the NP vs. CoNP problem Fagin considered MonNP, that is the class of sets of structures characterized by those Σ^1_1–sentences, in which second order quantifiers range only over *monadic* relations. He then proved that the set of connected graphs (which is in MonCoNP) is not in MonNP thus showing that MonNP is not closed under complements.

Since then many non-expressibility results for MonNP have been shown.

In our paper we study BinNP, the class obtained by allowing quantification over *binary* relations. We look at *semantical* restrictions, where these quantifiers range only over certain classes of relations. For instance, in order to express that a graph has a Hamiltonian cycle, it is enough to quantify over a linear order, or even a successor relation.

Some such restrictions have been considered in the literature: edge sets of graphs, unary functions (which suffice for a characterization of nondeterministic linear time) and certain pairing relations on strings. In our paper we consider three types of classes of binary relations: unary functions, order relations and graphs with degree bounds.

We obtain the hierarchy indicated in the following figure, where classes within one box are of the same expressive power, and inclusion is upwards.



- partial order relations
- arbitrary binary relations

| $\neq$

- linear order relations
- unary functions
- equivalence relations
- graphs with bounded outdegree

|

- successor relations
- connected graphs with bounded degree

|

- graphs with bounded degree
- bijective unary functions
- pairing relations

| $\neq$

- sets

All our results are based on techniques for expressing one kind of relations by another. We systematize this argument with the notion of representability of a class of relations by another class of relations. A paper is available.

On Random-self-reducibility: Adaptiveness, Advice, and Self-correctability

Joan Feigenbaum, AT&T Bell Laboratories, Room 2C-473, Murray Hill, NJ 07974, USA (jf@research.att.com)
Lance Fortnow, University of Chicago, Department of Computer Science, 1100 E. 58th St., Chicago, IL 60637, USA, (fortnow@cs.uchicago.edu)
Sophie Laplante, University of Chicago (laplante@cs.uchicago.edu)
Ashish V. Naik, University of Chicago (naik@cs.uchicago.edu)

Abstract Number 95-15

A function f is *random-self-reducible* if there is a probabilistic, polynomial-time procedure M that computes f using f as an oracle with the following randomness property: For all strings x, y with $|x| = |y|$, the distributions of oracle queries made by M on inputs x and y are identical. Random-self-reducible functions have several applications in the areas of average-case complexity, probabilistically checkable proofs, cryptography, etc., but many questions remain about their structural properties. In this paper, we study some of these properties.

Our first result addresses the power of adaptiveness and advice in random-self-reductions. Feigenbaum, Fortnow, Lund, and Spielman showed that there exists a random-self-reducible function f that is not *nonadaptively* random-self-reducible. The function f that they construct belongs to P/*poly*, the class of languages computable with polynomial-size circuits. We extend this result as follows.

Theorem: *There exists a random-self-reducible function f that is* not *nonadatively random-self-reducible, even with sub-exponential advice (that is, advice length bounded by 2^{n^ϵ}, for some $\epsilon < 1$).*

Next, we examine the relationship between random-self-reducible functions and *self-correctable* functions, as defined by Blum, Luby, and Rubinfeld. They show that, if a function is random-self-reducible, then it is also self-correctable; 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:

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

Theorem: *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.*

This work is an extension of *Two Remarks on Self-Correctability versus Random-Self-Reducibility.* The full paper is available by email to the authors.

On Inverting Onto Functions

Stephen Fenner, University of Southern Maine, (fenner@usm.maine.edu)
Lance Fortnow, University of Chicago, (fortnow@cs.uchicago.edu)
Ashish V. Naik, University of Chicago, (naik@cs.uchicago.edu)
John Rogers, University of Chicago, (rogers@cs.uchicago.edu)

Abstract Number 95-16

We study the complexity of inverting onto functions. Asserting that every polynomial-time computable, honest, onto function is invertible is equivalent to the following proposition that we call **Q**.

> **Proposition Q:** For all NP machines M that accept Σ^*, there exists a polynomial-time computable function g_M such that for all x, $g_M(x)$ outputs an accepting computation of M on x.

We show that **Q** is equivalent to several, seemingly unrelated, propositions in complexity theory. For example, **Q** is equivalent to the proposition *Tautology Search* that was studied by Impagliazzo and Naor. Also, in terms of function classes **Q** is equivalent to $\mathrm{NPMV}_t \subseteq_c \mathrm{PF}_t$. Perhaps the most intriguing equivalent assertion to **Q** is: for all NP machines M that accept SAT, there exists a polynomial-time algorithm g_M that, on input x and an accepting computation of M on x, outputs a satisfying assignment of x.

We also define and study the following weaker version of **Q** called **Q**': for all NP machines accepting Σ^* there is a polynomial-time computable function g_M that computes *the first bit* of an accepting computation of M. **Q**' is interesting since it is equivalent to another well-studied proposition: All disjoint sets of coNP languages are p-separable.

We study the relationship of **Q** and **Q**' with other complexity hypothesis. We show that **Q**' implies that $\mathrm{AM} \cap \mathrm{coAM} \subseteq \mathrm{BPP}$, and $\mathrm{NP} \cap coAM \subseteq \mathrm{RP}$. Also, **Q'** and $\mathrm{NP} = \mathrm{UP}$ implies that the polynomial hierarchy collapses to $\mathrm{ZPP}^{\mathrm{NP}}$.

A full paper is available as a University of Chicago Technical Report-95-05, or at URL http://www.cs.uchicago.edu/users/fortnow/papers.

Witness-Isomoprhic Reductions and the Local Search Problem

Sophie Fischer, Dept. of Math. and Comp. Sci., University of Amsterdam, 1018 TV Amsterdam, The Netherlands, sophie@fwi.uva.nl.
Lane A. Hemaspaandra, Department of Computer Science, University of Rochester, Rochester, NY 14627, lane@cs.rochester.edu.
Leen Torenvliet, Dept. of Math. and Comp. Sci., University of Amsterdam, 1018 TV Amsterdam, The Netherlands, leen@fwi.uva.nl.

Abstract Number 95-17

We study witness-isomorphic reductions, a type of structure-preserving reduction between NP decision problems. We show that witness-isomorphic reductions can be used in a uniform approach to the local search problem. We completely classify the relative strengths of the natural witness-isomorphic reduction types. Valiant has shown that even some P sets have #P-complete counting versions. We show that under certain complexity-theoretic assumptions, not all counting versions of NP-complete sets are $\leq^{p}_{1\text{-}T}$-complete for #P.

A full paper is available from the authors.

Dense Hierarchy between Monotone $\mathbf{NC}_1$ and Monotone $\mathbf{NC}_2$

Bin Fu, Department of Computer Science, Princeton University, Princeton New Jersey, NJ, 08544 (binfu@cs.princeton.edu)

Abstract Number 95-18

We study the monotonic circuit depth lower bound for a special (s, t)-connectivity problem. For a graph G with source node v and target node t, there v levels of nodes between s and t such that each level contains n nodes and each edge connects two nodes in the neighbor levels. The problem is to tests if G contains a path from s to t. We show that the upper bound of the monotone depth is $O(\log v \cdot \log n)$, and the lower bound is $\Omega(\log v \cdot \log n / \log \log v)$ for all $v \leq n^c$, where c is a constant. The following hierarchy is obtained: For $1 \leq r < 2$ and $0 < \epsilon$, $\mathrm{mNC}_r \neq \mathrm{mNC}_{r+\epsilon}$, where mNC_r is the class of monotone NC_r.

Improved Hardness Results for Approximating the Chromatic Number

Martin Fürer, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA 16802, USA (furer@cse.psu.edu)

Abstract Number 95-19

First, a simplified geometric proof is presented for the result of Lund and Yannakakis saying that the chromatic number cannot be approximated by a factor of N^{ϵ} for some $\epsilon > 0$ (without trying to maximize ϵ). Then, more sophisticated techniques are employed to improve ϵ. A randomized twisting method allows us to completely pack a certain space with copies of a graph without much affecting the independence number. This implies improvements under reasonable complexity assumptions. Under the $Z\tilde{PP} \neq N\tilde{P}$ assumption, we improve the lower bound of $N^{1/10-o(1)}$ to $N^{1/7-o(1)}$ based on published results on the number of free bits. Together with the newest results on the number of free bits, this bound increases to $N^{1/5-o(1)}$ under the weaker assumption of *ZPP* $\neq$ *NP*.

Finally, we get polynomial lower bounds in terms of $\chi(G)$. Unless *ZPP* = *NP*, the performance ratio of every algorithm approximating the chromatic number in polynomial time is $\chi(G)^{6/5-\epsilon}$ for every $\epsilon > 0$.

A preliminary paper is available by email to furer@cse.psu.edu

Graph Isomorphism Testing without Numerics

Martin Fürer, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA 16802, USA (furer@cse.psu.edu)

Abstract Number 95-20

There are several parameterized classes of graphs for which polynomial time isomorphism tests are known. Attempts have been made to develop one conceptionally simple parameterized class of algorithms to solve the graph isomorphism problem for all of these classes. Such unified algorithms have been designed to handle almost all of these classes except for the case of bounded eigenvalue multiplicity. It is shown here that this case can also be handled in a more direct way by discrete methods. The new algorithm uses combinatorics and group theory closely related to the methods used for the other feasible classes of graphs. The classical polynomial time graph isomorphism test of Babai, Grigoriev and Mount for graphs of bounded eigenvalue multiplicity consists of two distinct parts. First, in the linear algebra part, numerical approximations of all eigenvalues and projections of the basis vectors into the eigenspaces are computed. The precision has to be chosen carefully to ensure that it is decidable whether two such projections are equal or have equal length. Also equal angles between such projections have to be recognized. In a second combinatorial and group theoretical part, this information is used to try isomorphisms in the projections and either to combine them to a global isomorphism or to detect that none exists.

The numerical part is alien to such a discrete mathematical problem. A direct combinatorial approach is more natural and gives more insight. It is shown that such an approach is indeed possible. It is an important step towards one unified algorithm for the graph isomorphism problem for all natural polynomially solvable classes. It helps understanding under which circumstances computationally feasible isomorphism tests are possible.

A preliminary paper is available by email to furer@cse.psu.edu

Lower Bounds for Circuits with Mod Gates and One Exact Threshold Gate

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

Abstract Number 95-21

We say an integer polynomial p, on Boolean inputs, weakly m-represents a Boolean function f if p is non-constant and is zero (mod m), whenever f is zero. In this paper we prove that if a polynomial weakly m-represents the Mod_q function on n inputs, where q and m are relatively prime and m is otherwise arbitrary, then the degree of the polynomial is $\Omega(n)$. This generalizes previous results of Barrington, Beigel and Rudich (STOC 1992, pp. 455-461) and Tsai (Structures 1993, pp. 96-101), which held only for constant or slowly growing m. In addition, the proof technique given here is quite different. We use a method (adapted from Barrington and Straubing, LATIN '92, pp. 24-31) in which the inputs are represented as complex q^{th} roots of unity. In this representation it is possible to compute the Fourier transform using some elementary properties of the algebraic integers. As a corollary of the main theorem and the proof of Toda's theorem, if q, p are distinct primes, any depth-three circuit which computes the Mod_q function, and consists of an exact threshold gate at the output, Mod_p-gates at the next level, and AND-gates of polylog fan-in at the inputs, must be of exponential size. We also consider the question of how well circuits consisting of one exact gate over ACC(p)-type circuits (where p is an odd prime) can approximate parity. It is shown that such circuits must have exponential size in order to agree with parity for more than $1/2 + o(1)$ of the inputs.

This is a revised and expanded version of "Lower Bounds for Depth-Three Circuits with Equals and Mod-Gates," in *12th Annual Symposium on Theoretical Aspects of Computer Science*, Springer-Verlag (1995) 71-82.

A full paper is available by email to fgreen@black.clarku.edu.

Universally Serializable Computation

Lane A. Hemaspaandra and Mitsunori Ogihara
Department of Computer Science, University of Rochester
Rochester, NY 14627
(lane@cs.rochester.edu, ogihara@cs.rochester.edu)

Abstract Number 95-22

Cai and Furst proved that every PSPACE language can be solved via a large number of identical, simple tasks, each of which is provided with the original input, its own unique task number, and at most three bits of output from the previous task.

In the Cai-Furst model, the tasks are required to be run in the order specified by the task numbers. To study the extent to which the Cai-Furst PSPACE result is due to this strict scheduling, we remove their ordering restriction, allowing tasks to execute in any serial order. That is, we study the extent to which complex tasks can be decomposed into large numbers of simple tasks that can be scheduled arbitrarily. We provide upper bounds on the complexity of the sets thus accepted. Our bounds suggest that Cai and Furst's surprising PSPACE result is due in large part to the fixed order of their task execution. In fact, our bounds suggest the possibility that even relatively low levels of the polynomial hierarchy cannot be accepted via large numbers of simple tasks that can be scheduled arbitrarily.

However, adding randomization recaptures the polynomial hierarchy: the entire polynomial hierarchy can be accepted by large numbers of arbitrarily scheduled probabilistic tasks passing only a single bit of information between successive tasks (and using J. Simon's "exact counting" acceptance mechanism). In fact, we show that the class of languages so accepted is exactly $\mathrm{NP}^{\mathrm{PP}}$.

A full paper is available as Department of Computer Science Technical Report TR520, University of Rochester.

Polynomial-Time Semi-Rankable Sets

Lane A. Hemaspaandra, Mohammed J. Zaki, and Marius Zimand, Department of Computer Science, University of Rochester, Rochester, NY 14627, e-mail: {lane, zaki, zimand}@cs.rochester.edu

Abstract Number 95-23

We study the polynomial-time semi-rankable sets (P-sr), the ranking analog of the P-selective sets. Informally, a set A is polynomial-time semi-rankable if there is a polynomial-time two-argument function f that, whenever at least one of its inputs, say x, is in A, outputs that input and its rank within A, i.e., $||\{z \mid z \in A \text{ and } z \leq_{lexicographical} x\}||$. We prove that P-sr is a strict subset of the P-selective sets, and indeed that the two classes differ with respect to closure under complementation, closure under union with P sets, and closure under join with P sets. We also show that P-sr is closed under intersection with P sets if and only if $\mathrm{P} = \mathrm{P}^{\#\mathrm{P}}$. On the other hand, we argue that P-sr seem just as hard in terms of the extended lowness hierarchy as the P-selective sets: both these classes are in the EL_2 level of the extended low hierarchy and there are oracles relative to which they are not in $\widehat{\mathrm{EL}}_2$. We also show that though P-sr falls between the P-rankable and the weakly-P-rankable sets in its inclusiveness, it equals neither of these classes.

A full paper is available as University of Rochester Department of Computer Science Technical Report TR-584 (which can be obtained, for example, at http://www.cs.rochester.edu/trs/).

Optimal Advice

Lane A. Hemaspaandra, Department of Computer Science, University of Rochester, Rochester, NY 14627, lane@cs.rochester.edu.
Leen Torenvliet, Dept. of Math. and Comp. Sci., University of Amsterdam, 1018 TV Amsterdam, The Netherlands, leen@fwi.uva.nl.

Abstract Number 95-24

Ko proved that the P-selective sets are in the advice class P/quadratic, and E. Hemaspaandra, Naik, Ogihara, and Selman showed that they are in PP/linear. We strengthen the latter result by establishing that the P-selective sets are in NP/linear $\cap$ coNP/linear. We show linear advice to be optimal.

A full paper is available as University of Rochester Department of Computer Science Technical Report TR-527 (which can be obtained, for example, at http://www.cs.rochester.edu/trs/).

Computability and Complexity Over Structures of Finite Type

Armin Hemmerling,
Ernst Moritz Arndt University, Dept. of Mathematics and Computer Science, D – 17487 Greifswald, GERMANY, (hemmerling@math-inf.uni-greifswald.d400.de)

Abstract Number 95-25

We present a general approach to computability and (time) complexity over an arbitrary structure of finite type.

More precisely, concepts of $\mathcal{S}$–computability of string functions over the universe of the structure $\mathcal{S}$ are defined and shown to be general enough to include classical recursion theory. Moreover, nondeterministic computations of two kinds are considered, namely by nondeterministic branching within programs and by guessing of elements of the universe.

The approach allows a straightforward definition of time complexity yielding in particular the complexity classes

$$\mathcal{S}\text{–}\mathbf{P} \subseteq \mathcal{S}\text{–}\mathbf{N_1P} \subseteq \mathcal{S}\text{–}\mathbf{N_2P}$$

of recognition problems over $\mathcal{S}$, which are solvable by polynomially bounded deterministic resp. nondeterministic programs, of the both kinds of nondeterminism. By considering quasiprograms, in which arbitrary elements of the universe are allowed to be used as direct operands ("quasiconstants"), we obtain the classes

$$\mathcal{S}\text{–}\mathbf{PQ} \subseteq \mathcal{S}\text{–}\mathbf{N_1PQ} \subseteq \mathcal{S}\text{–}\mathbf{N_2PQ}\ .$$

The main result shows the $\mathcal{S}$–$\mathbf{N_2P}[\mathbf{Q}]$–completeness of the satisfiability problem for boolean quasiexpressions over $\mathcal{S}$; these are the quantifier–free expressions in which again arbitrary elements of the universe can occur as quasiconstants. Some modifications of this problem and $\mathcal{S}$–$\mathbf{N_1P}[\mathbf{Q}]$–complete variants of satisfiability are presented.

Thus, this paper shows how to generalize the Blum–Shub–Smale theory of computability and complexity over the reals and other rings to arbitrary structures, and it gives correspondingly general results of **NP**–completeness including both Cook's basic theorem on the **NP**–completeness of SAT and Meggido's generalization of the completeness results by Blum–Shub–Smale. Some of the crucial ideas and results can already be found in a recent paper by Goode.

A full paper is available as technical report by mail or email from the author.

An Algebraic Characterization of Tractable Constraints

Peter Jeavons
Department of Computer Science,
Royal Holloway, University of London,
Egham, Surrey TW20 0EX, UK,
(pete@dcs.rhbnc.ac.uk)

Abstract Number 95-26

Many combinatorial search problems may be expressed as 'constraint satisfaction problems', and this class of problems is known to be NP-complete. In this paper we investigate what restrictions must be imposed on the allowed constraints in order to ensure tractability. We describe a simple algebraic closure condition, and demonstrate that this is both necessary and sufficient to ensure tractability in Boolean valued problems. This result shows that Schaefer's (1978) six criteria for tractability in the SATISFIABILITY problem [a] can be reduced to one simple algebraic criterion. We also demonstrate that this condition is necessary to ensure tractability in problems with arbitrary finite domains.

This paper is due to be presented at COCOON 95, Xi'an, China, and is available by email to pete@dcs.rhbnc.ac.uk

[a] Schaefer, T.J., "The complexity of satisfiability problems", Proc. ACM STOC (1978) pp. 216–226.

Completeness and Weak Completeness under Polynomial-Size Circuits

David W. Juedes, Department of Computer Science, Ohio University, Athens, Ohio 45701, U.S.A., (juedes@ohiou.edu)
Jack H. Lutz, Department of Computer Science, Iowa State University, Ames, Iowa 50011, U.S.A., (lutz@cs.iastate.edu)

Abstract Number 95-27

This paper investigates the distribution and nonuniform complexity of problems that are complete or weakly complete for ESPACE under nonuniform reductions that are computed by polynomial-size circuits (P/Poly-Turing reductions and P/Poly-many-one reductions). A tight, exponential lower bound on the space-bounded Kolmogorov complexities of weakly P/Poly-Turing-complete problems is established. A Small Span Theorem for P/Poly-Turing reductions in ESPACE is proven and used to show that *every* P/Poly-Turing degree — including the complete degree — has measure 0 in ESPACE. (In contrast, it is known that almost every element of ESPACE is weakly P-many-one complete.) Every weakly P/Poly-many-one-complete problem is shown to have a dense, exponential, nonuniform complexity core. More importantly, the P/Poly-many-one-complete problems are shown to be *unusually simple* elements of ESPACE, in the sense that they obey nontrivial *upper* bounds on nonuniform complexity (size of nonuniform complexity cores and space-bounded Kolmogorov complexity) that are violated by almost every element of ESPACE.

A full paper is available by email to lutz@cs.iastate.edu

Random Elements, Composite Measures, and Quantum Mechanics

Vladik Kreinovich, Luc Longpré, Department of Computer Science, University of Texas at El Paso, El Paso, TX 79968 ({vladik,longpre}@cs.utep.edu)

Abstract Number 95-28

Definition. Let a mathematical language L be fixed (e.g., language of set theory, or language of recursive objects). Sets defined by formulas from L will be called *($L-$)definable.* Let μ be a probability measure on a set X. An element $x \in X$ is called *random* w.r.t. μ if x does not belong to any $L-$definable set of $\mu-$measure 0 (for recursive L, we get Kolmorogov-Martin-Löf's definition of randomness).

Theorem. Let $\mu_1, ..., \mu_n$ be measures on X, and let $\alpha_i > 0$, $\alpha_1 + ... + \alpha_n = 1$. Then, an element $x \in X$ is random w.r.t. a composite measure $\mu = \alpha_1 \cdot \mu_1 + ... + \alpha_n \cdot \mu_n$ iff x is random w.r.t. one of the measures μ_i.

Comment. This property was *postulated* when Levin defined tests of randomness for arbitrary measures. In our definition, it is a theorem.

Application to quantum mechanics (QM): In QM, if we are in a state ψ, and we measure an observable A with eigenvectors φ_i and corresponding eigenvalues λ_i, then, with probability $p_i = |(\varphi_i, \psi)|^2$, the result of this measurement is λ_i, and the measured object "jumps" into the state φ_i. The corresponding probability measure $\mu_A(\psi)$ on the real line R is therefore located at λ_i with probability p_i. If we make repeated experiments with several objects (e.g., particles) in the same state ψ, then we can conclude that the result of this sequence of measurements is random w.r.t. $\mu_A(\psi)$.

After having measured A, we may want to measure a sequence of other observables $\mathcal{B} = B_1, ..., B_n, ...$ There are two ways to describe this situation:

- We can say that with probability p_i, the particle is in the state φ_i, and therefore, the result of the measurement will be distributed according to the probability measure $\mu_{\mathcal{B}}(\varphi_i)$.
- We can also say that a particle is in a *composite* state, and that therefore, the result of measuring B is distributed according to the composute measure $\mu_{\mathcal{B}} = p_1 \cdot \mu_{\mathcal{B}}(\varphi_1) + p_2 \cdot \mu_{\mathcal{B}}(\varphi_2) + ...$

Our theorem says that every sequence random w.r.t. $\mu_{\mathcal{B}}$ is random w.r.t. one of the measures $\mu_{\mathcal{B}}(\varphi_i)$. We can reformulate it by saying that *if a particle is in a composite state, it actually is in one one of the pure states.* This conclusion is in accordance with the opinion of many physicists who view pure states as *real*, and composite states as a useful *mathematical* construction.

A full paper will be available shortly.

A Non-Algorithmic Analogue of Kolmogorov-Martin-Löf Randomness

Vladik Kreinovich, Luc Longpré, Department of Computer Science, University of Texas at El Paso, El Paso, TX 79968 ({vladik,longpre}@cs.utep.edu)

Abstract Number 95-29

According to the original Kolmogorov-Martin-Löf (KML), a sequence ω is *random* iff it cannot be compressed, i.e., iff for every n, the Kolmogorov complexity (i.e., the length of the shortest possible compression) of ω's $n-$fragment $\omega_{1:n}$ is close to n.

At first glance, this definition is purely algorithmic and cannot have a non-algorithmic analogue: indeed, if we consider *arbitrary* (not necessarily algorithmic) compression schemes, then, whatever sequence ω we have, we can always have a (non-algorithmic) compression scheme that compresses every fragment $\omega_{1:n}$ of a given sequence into a binary code of n.

In this paper, we will show that if we consider sets of measure 0 instead of random sequences, then we get a direct statistical (non-algorithmic) analogue of the KML idea.

Definitions and Denotations.

- By a *coding procedure*, we mean a function $f : \{0,1\}^* \to \{0,1\}^*$ for which $x \neq y$ implies $f(x) \neq f(y)$. For each binary word α, the result $f(\alpha)$ of applying f to α will be called a *code* of α.
- The length of a binary sequence α will be denoted by $|\alpha|$.
- Let $C > 0$ be an integer. We say that a coding procedure f $C-$*compresses* an infinite binary sequence ω iff there exists an integer N such that for all $n \geq N$, the code $f(\omega_{1:n})$ of an $n-$fragment $\omega_{1:n}$ of the sequence ω is at least C bits shorter than the $n-$fragment itself, i.e., $|f(\omega_{1:n})| \leq n - C$.

Theorem. A set $A \subseteq \{0,1\}^\infty$ is of (Lebesgue) measure 0 iff for every C, there exists a coding procedure that $C-$compresses all elements of A.

Comment. This theorem provides an additional justification for a compression-based definition of resource-bounded randomness that one of the authors (L.L.) is currently working on.

A preliminary version is available by email request. A full paper will be available shortly.

Why Are Symmetries a Universal Language of Physics? A Remark

Vladik Kreinovich, Luc Longpré, Department of Computer Science, University of Texas at El Paso, El Paso, TX 79968 ({vladik,longpre}@cs.utep.edu)

Abstract Number 95-30

Intuitively, whatever we measure, is either completely random ("lawless", in the informal sense of this word), or there is some law that controls these measurements. There are different mathematical formalisms for describing such laws. The formalism that is among most frequently used in modern physics is *symmetries*: modern theories (starting from quarks) are often formulated not in terms of differential equations (as in Newton's days), but it terms of the corresponding symmetry groups. Symmetry approach has been very successful. A natural question is: how universal is it? Can we describe any non-randomness in terms of a symmetry? Our answer is "yes".

Definitions.

- Let a language L be fixed (e.g., the language of set theory). We say that a set X is *definable* if in the language L there is a formula $P(Z)$ with one free set variable Z that is true for only one object: this set X.
- Let U be a set with a probability measure μ. We say that an element $u \in U$ is *random* w.r.t. μ is it does not belong to any definable set of $\mu-$measure 0.
- By a *symmetry* S, we mean a 1-1, measure preserving, definable mapping $S : U \to U$ for which $\mu\{u \,|\, S(u) = u\} = 0$ (i.e., almost always $S(u) \neq u$).
- A probability space (U, μ) is *non-trivial* is it has at least one symmetry S_0.
- We say that an element u is *invariant* (or *symmetric*) w.r.t. S if $S(u) = u$.

Comment. A symmetry (e.g., a rotation of the plane) must be invertible and therefore, 1-1. It must preserve apriori probability measure μ, and it must be *non-trivial* in the sense that being symmetric must be a very informative property (i.e., only very few elements must be symmetric).

Theorem. An element u of a non-trivial probability space U is random w.r.t. μ iff u is not invariant w.r.t. any symmetry.

Idea of the proof. If u is invariant w.r.t. some symmetry S, then u belongs to the set $I(S)$ of invariant elements of S. Since S is definable, this set $I(S)$ is also definable, and it is of measure 0. So, u is not random. Vice versa, assume that u is not random, then u belongs to a definable set E of measure 0. Define $S(u)$ as u for all u from $E \cup S_0(E) \cup S_0^2(E) \cup \ldots \cup S_0^{-1}(E) \cup \ldots$, and $S(u) = S_0(u)$ for all other u. It is relatively easy to check that S is a symmetry, and that $S(u) = u$.

A full paper will be available shortly.

A Constant-Space Sequential Model of Computation for First-Order Logic

Steven Lindell, Department of Computer Science, Haverford College, Haverford PA 19041-1392 (slindell@haverford.edu)

Abstract Number 95-31

We define and justify a natural sequential model of computation with a constant amount of read/write work space, despite unlimited (polynomial) access to read-only input and write-only output. The model is deterministic, uniform, and sequential. The constant work space is modeled by a finite number of destructive read boolean variables, assignable by formulas over the canonical boolean operations. We then show that computation on this model is equivalent to expressibility in first-order logic, giving a duality between (read-once) constant-space serial algorithms and constant-time parallel algorithms.

A full paper (preliminary draft) is available upon request by e-mail.

On the Power of Additional Output Values

Ashish V. Naik, University of Chicago, (naik@cs.uchicago.edu)
Kenneth Regan, State University of New York at Buffalo, (regan@cs.buffalo.edu)
James Royer, Syracuse University, (royer@top.cis.syr.edu)
Alan Selman, State University of New York at Buffalo (selman@cs.buffalo.edu)

Abstract Number 95-32

Recall that NPMV is the class of partial multivalued functions computable by a nondeterministic transducer in polynomial time. Hemaspaandra et al. [1] recently showed that if the polynomial hierarchy does not collapse to $\mathbf{ZPP}^{\mathbf{NP}}$, then there are functions that are 2-valued that cannot be simulated by any single-valued transducer. This suggests that the number of output values in a Turing machine is a *computational resource*, somewhat analogous to the number of bounded queries.

We define an NPkV-hierarchy of partial multivalued functions. A function f is at the k^{th} level of this hierarchy ($f \in$ NPkV) if $f \in$ NPMV and for all x, $f(x)$ has atmost k values. Hemaspaandra et al. showed that the first two levels of this hierarchy are likely to be distinct. We show that the hierarchy is proper relative to a random oracle.

> **Theorem:** Relative to a random oracle, for all $k > 0$, there exists a k-valued nondeterministic function f such that no $k-1$-valued transducer can compute a refinement of f.

We also show that NP $\neq$ UP relative to a random oracle, and our technique yields simpler proofs of NP $\neq$ coNP and coNP $\not\subseteq$ IP relative to random oracles.

A full paper will be available soon. Please send requests for a copy to the first author.

[1] L. Hemaspaandra, A. Naik, M. Ogihara, and A. Selman. *Computing Unique Solutions Collapses the Polynomial Hierarchy*, In proceedings of *ISAAC* '94, pages 57-64, 1994

The PL Hierarchy Collapses

Mitsunori Ogihara

Department of Computer Science, University of Rochester

Rochester, NY 14627 (ogihara@cs.rochester.edu)

Abstract Number 95-33

It is shown that the PL hierarchy $\mathrm{PLH} = \mathrm{PL} \bigcup \mathrm{PL}^{\mathrm{PL}} \bigcup \mathrm{PL}^{\mathrm{PL}^{\mathrm{PL}}} \bigcup \cdots$, defined in terms of the Ruzzo-Simon-Tompa relativization, collapses to PL. Also, it is shown that PL is closed under logspace-uniform AC^0-reductions.

A full paper is available as Department of Computer Science Technical Report 587.

Sparse Hard Sets for P Yield Space-efficient Algorithms

Mitsunori Ogihara

Department of Computer Science, University of Rochester

Rochester, NY 14627 (ogihara@cs.rochester.edu)

Abstract Number 95-34

In 1978, Hartmanis conjectured that there exist no sparse complete sets for P under logspace many-one reductions. In this paper, in support of the conjecture, it is shown that if P has sparse hard sets under logspace many-one reductions, then P $\subseteq$ DSPACE$[\log^2 n]$. The result is derived from a more general statement that if P has $2^{polylog}$ sparse hard sets under poly-logarithmic space-computable many-one reductions, then P $\subseteq$ DSPACE$[polylog]$.

A full paper is available as Department of Computer Science Technical Report 569.

Function Computable with Limited Access to NP

Mitsunori Ogihara

Department of Computer Science, University of Rochester

Rochester, NY 14627 (ogihara@cs.rochester.edu)

Abstract Number 95-35

Hemaspaandra, Naik, Ogihara, and Selman showed that if all NPMV functions have refinements in NPSV, then PH $= \Sigma_2^p$. Burhman, Thierauf, and Kadin extended the result and showed that if all NPMV functions have refinements in $\mathrm{PF}^{\mathrm{NPSV}}_{1\text{-}tt}$, then PH $= \Sigma_2^p$. We further extend the result and show for any constant $c < 1$, that if all NPMV functions have refinements in $\mathrm{PF}^{\mathrm{NPSV}}_{c \log n\text{-}tt}$, then PH $= \Sigma_2^p$.

A full paper is available as Department of Computer Science Technical Report 583.

Pseudorandom Generators, Measure Theory, and Natural Proofs

Kenneth Regan, D. Sivakumar, and Jin-yi Cai, Dept. of Computer Science, State Univ. of NY at Buffalo, Buffalo, NY 14260, USA. ({regan,sivak-d,cai}@cs.buffalo.edu)

Abstract Number 95-36

We prove that if strong pseudorandom number generators (PSRGs) exist, then the class of languages that have polynomial-sized circuits (P/poly) is not small within exponential time, in terms of the resource-bounded measure theory of Lutz. More precisely, if there is a PSRG that cannot be predicted by circuits of size less than 2^{n^ϵ} for some $\epsilon > 0$, then P/poly is not measurable in EXP ($= 2^{\mathrm{poly}}$).

Our proof uses the framework of *natural proofs* introduced by Razborov and Rudich (Proc. 26th STOC, 1994). Razborov and Rudich showed that superpolynomial lower bound arguments of a certain kind, which they call *natural proofs*, translate into *statistical tests* that prevent the existence of strong PSRGs. We prove that if P/poly has measure zero in EXP, then there is a natural proof against P/poly. Hence if strong PSRGs exist, then P/poly cannot have measure zero in EXP. We further prove that if strong PSRGs exist, then P/poly cannot have measure one in EXP, either; this yields the *non*-measurability result. We also show that NP and many other classes cannot have measure one in EXP unless they equal EXP. This answers a question of Lutz, and tightens his interesting hypothesis concerning the measure of NP in EXP.

The second half of this paper takes a closer look at the nature of statistical tests, and at the size and strength parameters of natural proofs in the Razborov–Rudich framework. We show a partial converse to the main theorem: if there is a P-natural proof of sufficient density and strength against P/poly, then there is a randomized martingale that "succeeds on" P/poly. Here, a deterministic martingale would imply that P/poly has measure zero. We also note that there are oracles relative to which a stronger converse, namely that non-measurability of P/poly implies the existence of strong PSRGs, does not hold.

Using recent developments in the construction of random variables with limited independence, we also prove unconditionally that non-uniform AC^0 plus parity does not have measure zero under either of the measures defined by Allender and Strauss [FOCS'94].

The first and second authors were supported in part NSF grant CCR-9409104; the third author was supported in part by by NSF grants CCR-9319393 and CCR-9057486, and by a Sloan fellowship.

Available by anonymous ftp as SUNY Buffalo CS TR 95-02, Jan. 1995. A slightly updated version is available by email to the authors.

Improved Resource-Bounded Borel-Cantelli and Stochasticity Theorems

Kenneth Regan and D. Sivakumar, Dept. of Computer Science, State Univ. of NY at Buffalo, Buffalo, NY 14260, USA. ({regan,sivak-d}@cs.buffalo.edu)

Abstract Number 95-37

This note strengthens and simplifies Lutz's resource-bounded version of the Borel-Cantelli lemma for density systems and martingales. We give simple and tight conditions, in terms of the convergence of a certain "payoff sequence," under which a martingale can make unbounded profit on a class of languages. We observe that the technique can be used to construct martingales that are "additively honest"—martingales that can be computed by knowing the membership of strings only of the "current length,"— and also martingales that are "multiplicatively honest." We use this to improve the "Weak Stochasticity Theorem" of Lutz and Mayordomo: their result does not address the issue of how rapidly the bias away from 1/2 converges toward zero in a "stochastic" language, while we show that the bias must vanish exponentially.

The authors were supported in part by NSF Grant CCR-9409104.

Available electronically as SUNY Buffalo CS TR 95-08, Feb. 1995, or by email to the authors.

On the Power of Bio-Computers

Diana Rooß, Institut für Informatik, Universität Würzburg, Am Exerzierplatz 3, 97072 Würzburg, GERMANY, (diana@informatik.uni-wuerzburg.de)
Klaus W. Wagner, Department of Mathematics, University of California at Santa Barbara, Santa Barbara, CA 93106, USA, (wagner@math.ucsb.edu)

Abstract Number 95-38

In 1994 Leonard Adleman describes his experiments to compute with DNA-strings. He is successful in solving special instances of the NP-complete *Hamiltonian Path Problem* with biological manipulations of such strings in test tubes. Richard Lipton formalizes this approach of 'molecular computing'; and, what is more, he can show that any NP-complete problem can be solved with Adleman's method, manipulating the strings in the test tubes only polynomially often.

Our model of biological computing is Bio-Pascal, which is a reduced version of Pascal, supplied by operations and tests for set variables. Set variables are modelled after test tubes, DNA-strings are represented by words over the alphabet $\{0,1\}$, and set operations and tests take over the function of biological manipulations. By varying the collections of set operations and set tests, different programming languages are defined. One of them describes exactly Lipton's model.

In this paper we characterize the power of various polynomially time-bounded Bio-Pascal models by well known 'classical' complexity classes. Thus, for example, the power of Lipton's model, like some other types of Bio-Pascal, is equivalent to P^{NP}. On the other hand, if length decreasing operations and subset tests are allowed, the class of solvable problems coincides with $\mathrm{P}^{\Sigma_2^p}$. Moreover, we prove that the additional use of the operation *intersection* increases the power of the model to PSPACE, what is everything we can expect from parallel polynomially time-bounded computations.

Another interesting question is, what happens to Bio-Pascal, if all variables (including every string contained in a set variable) are restricted to logarithmic length. Things turn out to have a simpler structure than in the polynomially time-bounded case. Now already the collection of operations and tests that Lipton uses, gives logarithmically space-bounded Bio-Pascal programs the whole power of P.

A full paper is available by email (diana@informatik.uni-wuerzburg.de)
or ftp (ftp://haegar.informatik.uni-wuerzburg.de/pub/TRs/ro-wa95.ps.gz).

Sets Computable in Polynomial Time on Average

Rainer Schuler
Abteilung Theoretische Informatik, Universität Ulm, D-89069 Ulm, Germany (schuler@informatik.uni-ulm.de)
Tomoyuki Yamakami
Department of Computer Science, University of Toronto, Toronto, Ontario, Canada M5S 1A4 (yamakami@cs.toronto.edu)

Abstract Number 95-39

In this paper, we discuss the complexity and properties of the sets which are computable in polynomial-time on average. This study is motivated by Levin's question of whether all sets in NP are solvable in polynomial time on average for ever reasonable (i.e., polynomial-time computable) distribution on the instances. Let $\mathrm{P}_{\mathrm{P}\text{-comp}}$ denote the class of all those sets which are computable in polynomial time on average for every polynomial time computable distribution on the instances [2]. It is known that $\mathrm{P} \subset \mathrm{P}_{\mathrm{P}\text{-comp}} \subset \mathrm{E}$ [1,2]. In this paper, we show that $\mathrm{P}_{\mathrm{P}\text{-comp}}$ is not contained in DTIME(2^{cn}) for any constant c and that it lacks some basic structural properties: for example, it is not closed under many-one reducibility or for the existential operator. From these results, it follows that $\mathrm{P}_{\mathrm{P}\text{-comp}}$ contains P-immune sets but no P-bi-immune sets; it is not included in P/cn for any constant c; and it is different from most of the well-known complexity classes, such as UP, NP, BPP, and PP. Finally, we show that, relative to a random oracle, NP is not included in $\mathrm{P}_{\mathrm{P}\text{-comp}}$ and $\mathrm{P}_{\mathrm{P}\text{-comp}}$ is not in PSPACE with probability 1.

References

[1] R. Schuler, On average polynomial time, Technical Report Nr.94-12, 1994.

[2] R. Schuler and T. Yamakami, Structural average case complexity, in: Proceedings of the 12th Annual Conference on Foundations of Software Technology and Theoretical Computer Science, Lecture Notes in Computer Science, Vol.652, pp.128–139, 1992.

A full paper is available by email and will appear in the *Proceedings of the First Annual International Computing and Combinatorics Conference* in Xi'an, China, in August, 1995.

A Tight Upper Bound on Kolmogorov Complexity by Hausdorff Dimension and Uniformly Optimal Prediction

Ludwig Staiger, Martin-Luther-Universität Halle-Wittenberg, Institut für Informatik, Weinbergweg 17, D-06120 Halle (Saale), Germany (staiger@informatik.uni-halle.de)

Abstract Number 95-40

The present paper links the concepts of Kolmogorov complexity (in Complexity theory) and Hausdorff dimension (in Fractal geometry) for a class of recursive (computable) ω-languages. It is shown that the complexity of an infinite string contained in a Σ_2-definable set of strings is upper bounded by the Hausdorff dimension of this set and that this upper bound is tight. Moreover, we show that there are computable gambling strategies guaranteeing a uniform prediction quality arbitrarily close to the optimal one estimated by Hausdorff dimension and Kolmogorov complexity provided the gambler's adversary plays according to a sequence chosen from a Σ_2-definable set of strings.
We provide also examples which give evidence that our results do not extend further in the Arithmetical hierarchy.

A full paper is available by email to staiger@informatik.uni-halle.de or by anonymous ftp from ftp.informatik.rwth-aachen.de (137.226.225.3):/pub/reports/95-03.ps.gz

Probabilistic Boolean Decision Trees: Several Remarks

Nikolai K. Vereshchagin, Department of Mathematical Logic, Faculty of Mechanics and Mathematics, Moscow State University, Moscow 119899, Russia (E-mail: ver@ium.ac.msk.su)

Abstract Number 95-41

Suppose there is a probability distribution over the set of all assignments to variables of a Boolean function according to which the expected complexity of any deterministic decision tree computing that function is at least c. Then we can conclude that the complexity of any probabilistic decision tree computing that function is at least c, too. Yao in 1977 proved that the converse is true, too, that is, this method is universal for proving lower bounds for probabilistic errorless decision trees. In the present paper we prove that this is the case also for probabilistic decision trees which are allowed to make errors. This gives the positive answer to the question posed by Yao.

In the second part of the paper we exhibit an example when probabilistic directional algorithms defined by Saks and Wigderson to evaluate read once formulae are not optimal. We construct a formula F_n of n Boolean variables such that the complexity of the optimal directional algorithm computing F_n is $\Omega(n^\alpha)$ and there is an undirectional probabilistic algorithm computing F_n of complexity $O(n^\beta)$ for some $\beta < \alpha$.

A full paper is available by email to ver@ium.ac.msk.su.

The Chain Method to Separate Counting Classes

Katja Cronauer, Theoretische Informatik, Universität Würzburg, Am Exerzierplatz 3, D-97072 Würzburg, GERMANY (cronauer@informatik.uni-wuerzburg.de),
Ulrich Hertrampf, Theoretische Informatik, Medizinische Universität zu Lübeck, Wallstraße 40, D-23560 Lübeck, GERMANY (hertramp@informatik.mu-luebeck.de),
Heribert Vollmer, Department of Mathematics, University of California at Santa Barbara, Santa Barbara, CA 93106, USA (vollmer@math.ucsb.edu),
Klaus W. Wagner, Theoretische Informatik, Universität Würzburg, Am Exerzierplatz 3, D-97072 Würzburg, GERMANY (wagner@informatik.uni-wuerzburg.de).

Abstract Number 95-42

We introduce a new method to separate counting classes of a special type by oracles. Among the classes, for which this method is applicable, are NP, coNP, US (also called 1NP), $\bigoplus$P and all other MOD-classes, PP and $C_=P$, classes of boolean hierarchies over the named classes, classes of finite acceptance type, and many more. As an important special case, we completely characterize all relativizable inclusions between classes NP(k) from the Boolean hierarchy over NP and other classes defined by what we call bounded counting.

A full paper is available.

Lectures on the Fusion Method and Derandomization

Avi Wigderson, Hebrew University of Jerusalem

Abstract Number 95-43

The 1994 McGill–Montréal Invitational Workshop on Complexity Theory was held at McGill University's Bellairs Research Institute in Barbados from January 28 to February 3, organized by Pierre McKenzie (U. de Montréal) and Denis Thérien (McGill U.).

The core of the workshop was a series of lectures given by Avi Wigderson from the Hebrew University of Jerusalem. Two main themes were treated: the fusion method for proving lower bounds, and the question of deterministic amplification of probabilistic algorithms using expanders and universal hashing. This technical report consists of notes taken by the attendees on the content of the five two-hour lectures.

Available by anonymous ftp from ftp.cs.mcgill.ca, cd pub/tech-reports/library/reports/95, get TR95.2.ps.gz or get TR95.2.ps. Send correspondence to Denis Thérien, School of Computer Science, McGill University, Montréal (Québec), Canada, H3A 2A7; `denis@cs.mcgill.ca`.

On the Size of Classes with Weak Membership Properties

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

Abstract Number 95-44

We attempt to identify an as weak as possible membership related property computable in polynomial time which yields a small class in E in the resource-bounded measure-theoretical sense. We show that the class of sets that are p-isomorphic to P-quasi-approximable sets has measure 0 in E. A set A is P-quasi-approximable if there exists a constant q and a polynomial-time algorithm M that is allowed to answer "don't know" such that for infinitely many q-tuples $(x_1, \ldots, x_q)$, with x_{i+1} being the lexicographical successor of x_i for $i = 1, \ldots, q-1$, M outputs a q-long binary string that is different from $A(x_1) \ldots A(x_q)$. The above result cannot be extended to the class of sets that are equivalent to some P-quasi-approximable set under one-one reducibility since this equivalence class is a superset of E. As an immediate corollary we obtain that the following classes have measure 0 in E: the class of P-selective sets, the class of P-multiselective sets, the class of cheatable sets, the class of easily countable sets, the class of easily approximable sets, the class of near-testable sets, the class of nearly near-testable sets, the class of sets that are not P-bi-immune. By considering the recent approach of Allender and Strauss for measuring in subexponential classes, we obtain similar results with respect to P for classes having weak logarithmic time membership properties.

A full paper is available as University of Rochester Department of Computer Science Technical Report TR-557 (which can be obtained, for example, at http://www.cs.rochester.edu/users/grads/zimand/).

On randomized cryptographic primitives

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

Abstract Number 95-45

It is shown that if a public source of random bits is available, then strong hard functions, strong one-way functions and strong pseudo-random generators exist. For example, there is a polynomial-time computable pseudo-random generator $g : \Sigma^n \to \Sigma^{2n}$ using a random source such that with probability $1 - 2^{-\Omega(n)}$ any circuit of size less than $2^{n/8}$ cannot distinguish with an accuracy larger than $16 \cdot 2^{-n/8}$ between a random string y in Σ^{2n} and $g(x)$ for a random x in Σ^n even if the circuit has access at the random source used by g. Similar parameters can be achieved for one-way functions and hard functions. It follows that the above cryptographic primitives exist in worlds relativized with random oracles. As an application, using a result of Regan, Sivakumar and Cai, it is shown that with respect to a random oracle, P$/poly$ is not measurable in EXP in the resource-bounded theoretical sense.

A full paper is available as University of Rochester Department of Computer Science Technical Report TR-586 (which can be obtained, for example, at http://www.cs.rochester.edu/users/grads/zimand/).

Large sets in AC^0: a Kolmogorov complexity related property and some applications

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

Abstract Number 95-46

We show that sets in AC^0 that have a large density at infinitely many lengths contain many strings of relatively low Kolmogorov complexity. More precisely, if A is a set in AC^0 such that for some $q > 0$ and infinitely many n, $|A^n| > 2^{n-\log^q n}$, then A contains more than quasipolynomially many strings with polynomial-time bounded length-conditioned Kolmogorov complexity below n^ϵ, for arbitrary $\epsilon > 0$, at each length n where A satisfies the above density condition. This property allows some form of strong separations from AC^0. Many sets known not to be in AC^0 (like PARITY or EXACT-HALF) have however close approximations recognizable by AC^0 circuits. We exhibit a set A in NP such that all sets consisting of strings x that are within Hamming distance less than $|x|/(3\log|x|)$ to some string in A are bi-immune to sets in AC^0 that satisfy the above density condition.

A full paper is available as University of Rochester Department of Computer Science Technical Report TR-556 (which can be obtained, for example, at http://www.cs.rochester.edu/users/grads/zimand/).