COMPLEXITY ABSTRACTS 2000. Vol X

Abstract

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

Monotone Proofs of the Pigeon Hole Principle
The Complexity of Tensor Circuit Evaluation
Strengths and weaknesses of LH arithmetic
The Enumerability of Kolmogorov functions
Relativized Separation of EQP from P^{NP}
The Complexity of Poor Man's Logic
Modal Satisfiability is in Deterministic Linear Space
Computational Politics: Comp. Complexity and Electoral Sys.
Almost-Everywhere Superiority for Quantum Polynomial Time
Algebraic Properties for P-Selectivity
Reducing the Number of Solutions of NP Functions
New Algorithms for Fast Matrix Multiplication
Separation of Reducibilities within NP
Combinatorial interpretation of Kolmogorov complexity
On the Hardness of Graph Isomorphism
Independent minimum length programs to translate between
How Important Is Theory for Practical Problems?

Monotone Proofs of the Pigeon Hole Principle

Albert Atserias, Departament of Software, Technical University of Catalonia, Jordi Girona Salgado 1–3, 08034 Barcelona, SPAIN, (atserias@lsi.upc.es)
Ricard Gavaldà, Departament of Software, Technical University of Catalonia, Jordi Girona Salgado 1–3, 08034 Barcelona, SPAIN, (gavalda@lsi.upc.es)
Nicola Galesi, Departament of Software, Technical University of Catalonia, Jordi Girona Salgado 1–3, 08034 Barcelona, SPAIN, (galesi@lsi.upc.es)

Abstract Number 00-1

We study the complexity of proving the Pigeon Hole Principle (PHP) in a monotone variant of the Gentzen Calculus, also known as Geometric Logic. We show that the standard encoding of the PHP as a monotone sequent admits quasipolynomial-size proofs in this system. This result is a consequence of deriving the basic properties of certain quasipolynomial-size monotone formulas computing the boolean threshold functions. Since it is known that the shortest proofs of the PHP in systems such as Resolution or Bounded Depth Frege are exponentially long, it follows from our result that these systems are exponentially separated from the monotone Gentzen Calculus. We also consider the monotone sequent (CLIQUE) expressing the *clique-coclique* principle defined by Bonet, Pitassi and Raz (1997). We show that monotone proofs for this sequent can be easily reduced to monotone proofs of the one-to-one and onto PHP, and so CLIQUE also has quasipolynomial-size monotone proofs. As a consequence, Cutting Planes with polynomially bounded coefficients is also exponentially separated from the monotone Gentzen Calculus. Finally, a simple simulation argument implies that these results extend to the Intuitionistic Gentzen Calculus. Our results partially answer some questions left open by P. Pudlák.

To be presented in ICALP'00. A full paper is available by email to gavalda@lsi.upc.es

The Complexity of Tensor Circuit Evaluation

Martin Beaudry, Département de mathématiques et d'informatique, Université de Sherbrooke, 2500 boul. Université, Sherbrooke (Québec), J1K 2R1 Canada (beaudry@dmi.usherb.ca)
Markus Holzer, Département d'I.R.O., Université de Montréal, C.P. 6128, succ. Centre-Ville, Montréal (Québec), H3C 3J7 Canada (holzer@iro.umontreal.ca)

Abstract Number 00-2

The study of the computational complexity of tensor calculus over semirings was recently initiated by Damm, Holzer, and McKenzie (paper presented at this conference). Central to their work is the analysis of the *non-zero tensor problem*, denoted by $0 \neq \mathrm{val}_{\mathcal{S}}$, which consists in asking whether a given *formula* yields a 1×1 matrix whose unique entry is equal to the zero of the semiring $\mathcal{S}$.
First, we solve an open problem mentioned by Damm *et al.*, namely the extension of their work from formulas to circuits. Our main results on this problem are:

1. evaluating a tensor circuit over the natural numbers is #E-complete under polytime linear-space reductions, and
2. $0 \neq \mathrm{val}_{\mathbb{B}}$ and $0 \neq \mathrm{val}_{\mathbb{F}_2}$ are respectively NE-complete and $\oplus$E-complete under polytime linear-space reductions;

here E denotes the class $\mathrm{DTIME}(2^{O(n)})$. We also look at some common-sense restrictions such as imposing a logarithmic upper bound on circuit depth (this particular restriction turns out to define a PSPACE-complete problem).
Next, we consider a number of natural problems concerning tensor formulas and circuits, such as asking whether the output of a formula/circuit is diagonal, or the identity, or a permutation matrix. These problems capture the classes Π_2^p for formulas and Π_2^e for circuits over the Boolean semiring; other semirings are also discussed.

A full paper is in preparation; it will be available by email at beaudry@dmi.usherb.ca

Strengths and weaknesses of LH arithmetic

Chris Pollett, Dept. of Mathematics, 405 Hilgard Ave., Box 951555, University of California, Los Angeles, CA., 90095 (cpollett@willow.math.ucla.edu)
Randall Pruim, Department of Mathematics and Statistics Calvin College, Grand Rapids, MI rpruim@calvin.edu (rpruim@calvin.edu)

Abstract Number 00-3

The first author had previously exhibited a bounded arithmetic theory Z which was shown not to be able to prove the collapse of the polynomial hierarchy. This theory also had the property that if $Z \subseteq S_2^i$ for any $i \geq 1$ then the polynomial hierarchy collapses. Here S_2^i are the theories of Buss. Unfortunately, despite this property Z seemed too weak a theory to formalize many of the arguments that have been used in computational complexity. In this new paper, we give a new arithmetic characterization of the levels of log-time hierarchy. Using this characterization, we propose a variant of the theory TAC^0 of Clote and Takeuti. This variant has nice deductive fragments which in some sense correspond to the levels of the log-time hierarchy. We show that this theory (like Z) cannot prove the collapse of the polynomial hierarchy. Furthermore, we give some evidence that this theory may be strong enough to prove that the log-time hierarchy is infinite, so unlike Z it can carry out useful complexity arguments.

A full paper is available by email to cpollett@willow.math.ucla.edu

The Enumerability of Kolmogorov functions

Frederic Green, Department of Computer Science, University of Maryland, College Park, MD 20742 (gasarch@cs.umd.edu).
Luc Longpre, Department of Computer Science, University of Texas at El Paso, TX 79968 (longpre@cs.utep.edu).

Abstract Number 00-4

A function f is g-enumerable if there is a computable function h such that such that $h(x)$ produces $g(x)$ candidates for $f(x)$, one of which is correct.
Let KP be the function that computes the shortest program that outputs x. KP is 2^{n+c} enumerable: on input x, $|x| = n$, the program that just prints x by having x hardcoded is of size $n + c - 1$ for some c, hence you need only print all programs of size $\leq 2^{n+c-1}$, of which there are 2^{n+c}. KP is not 1-enumerable since then it would be computable. The question arises, where does it fit?
We have shown that KP is not $\frac{n}{\log n}$-enumerable. It is an open problem to narrow the gap. Other functions associated to Kolmogorov complexity can also be looked at such as the size of the shortest program to compute x (rather than the program itself).

A sketch is available by email to either author.

Relativized Separation of EQP from P^{NP}

Frederic Green, Department of Mathematics and Computer Science, Clark University, Worcester, MA 01610 (fgreen@black.clarku.edu).
Randall Pruim, Department of Mathematics and Statistics, Calvin College, Grand Rapids, MI 49546 (rpruim@calvin.edu).

Abstract Number 00-5

An oracle is constructed relative to which quantum polynomial time (EQP) is not polynomial-time Turing reducible to NP. That is, there is an A such that $\mathrm{EQP}^A \not\subseteq \mathrm{P}^{\mathrm{NP}^A}$. This generalizes and simplifies previous separations of EQP from NP and ZPP, due to Berthiaume and Brassard. A key element of the proof is the use of a special property of Grover's algorithm for database search, in order to show that the test language is in EQP^A.

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

The Complexity of Poor Man's Logic

Edith Hemaspaandra, Department of Computer Science, Rochester Institute of Technology, Rochester, NY 14623, USA. Email: eh@cs.rit.edu.

Abstract Number 00-6

Motivated by description logics, we investigate what happens to the complexity of modal satisfiability problems if we only allow formulas built from literals, $\wedge$, $\Diamond$, and $\Box$. Previously, the only known result was that the complexity of the satisfiability problem for K dropped from PSPACE-complete to coNP-complete (Schmidt-Schauss and Smolka and Donini et al.). In this paper we show that not all modal logics behave like K. In particular, we show that the complexity of the satisfiability problem with respect to frames in which each world has at least one successor drops from PSPACE-complete to P, but that in contrast the satisfiability problem with respect to the class of frames in which each world has at most two successors remains PSPACE-complete. As a corollary of the latter result, we also solve the open problem from Donini et al.'s complexity classification of description logics. In the last section, we classify the complexity of the satisfiability problem for K for all other restrictions on the set of operators.

A full paper is available via email to eh@cs.rit.edu.

Modal Satisfiability is in Deterministic Linear Space

Edith Hemaspaandra, Department of Computer Science, Rochester Institute of Technology, Rochester, NY 14623, USA. Email: eh@cs.rit.edu.

Abstract Number 00-7

In recent years, there has been a lot of interest in analyzing the space requirements for modal logics. In this paper, we prove that modal satisfiability is in deterministic linear space. This improves the best previously-known $O(n \log n)$ bound and it is the first linear space result in this area.

A full paper is available via email to eh@cs.rit.edu.

Computational Politics: Computational Complexity and Electoral Systems

Edith Hemaspaandra, Department of Computer Science, Rochester Institute of Technology, Rochester, NY 14623, USA. Email: eh@cs.rit.edu.
Lane A. Hemaspaandra, Department of Computer Science, University of Rochester, Rochester, NY 14627, USA. Email: lane@cs.rochester.edu.

Abstract Number 00-8

This paper discusses some recent results in the study of electoral systems:

1. Determining the winner in Lewis Carroll's 1876 electoral system is complete for parallel access to NP [HHR].

2. For any electoral system that is neutral, consistent, and Condorcet, determining the winner is complete for parallel access to NP [Hem1].

3. The manipulation problem for Lewis Carroll's 1876 electoral system is $\mathrm{NP}^{\mathrm{NP}}$-complete [Hem2].

4. For each census in US history, a simulated annealing algorithm yields *provably* fairer (in a mathematically rigorous sense) congressional apportionments than any of the classical algorithms—even the one currently mandated by law [HRSZ].

The full paper will be soon available via email to the authors.

Almost-Everywhere Superiority for Quantum Polynomial Time

Edith Hemaspaandra, Department of Computer Science, Rochester Institute of Technology, Rochester, NY 14623, USA. Email: eh@cs.rit.edu.
Lane A. Hemaspaandra, Department of Computer Science, University of Rochester, Rochester, NY 14627, USA. Email: lane@cs.rochester.edu.
Marius Zimand, Department of Computer and Information Sciences, Towson University, Towson, MD 21252, USA. Email: mzimand@saber.towson.edu.

Abstract Number 00-9

Simon as extended by Brassard and Høyer shows that there are tasks on which polynomial-time quantum machines are exponentially faster than each classical machine infinitely often. The present paper shows that there are tasks on which polynomial-time quantum machines are exponentially faster than each classical machine almost everywhere.

A full paper is available via email to lane@cs.rochester.edu.

Algebraic Properties for P-Selectivity

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 00-10

We study the effect on P-selective sets when their P-selector functions have algebraic structure—commutativity and associativity. We show that sets that are P-selective via associative P-selector functions have a wide range of simplicity properties.

In particular, we show that all associatively P-selective sets are associatively, commutatively P-selective. We show that all associatively P-selective sets have linear deterministic advice. This contrasts with the general case for P-selective sets, where the best known upper bound on deterministic advice is quadratic [Ko83]. We give a sufficient condition for all P-selective sets to be associatively P-selective.

A full paper is available as UR-CS-TR-2000-730.

Reducing the Number of Solutions of NP Functions

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

Abstract Number 00-11

We study whether one can prune solutions from NP functions. Though it is known that, unless surprising complexity class collapses occur, one cannot reduce the number of accepting paths of NP machines (*A Complexity Theory for Feasible Closure Properties*, Ogiwara and Hemachandra, JCSS, 1993), we nonetheless show that it often is possible to reduce the number of solutions of NP functions. For finite cardinality types, we give a sufficient condition for such solution reduction. We also give absolute and conditional necessary conditions for solution reduction, and in particular we show that in many cases solution reduction is impossible unless the polynomial hierarchy collapses.

A full paper is available as UR-CS-TR-2000-727.

New Algorithms for Fast Matrix Multiplication

Aileen M. McLoughlin, School of Computer Applications, Dublin City University, Dublin 9, IRELAND, (amcloughlin@compapp.dcu.ie)

Abstract Number 00-12

In previous work R. Johnson and A. McLoughlin, by a computer-aided search, found new noncommutative bilinear algorithms for 3 by 3 matrix multiplication that require only 23 essential multiplications rather than the 27 required by the conventional method—the same complexity as the algorithm earlier found by J. Laderman, but inequivalent to it (and each other) in a sense that is made precise. Such algorithms, like Strassen's algorithm for the 2 by 2 case, lead to fast algorithms for matrices of arbitrary size. We have extended the search and are seeking improved upper bounds on the number of essential multiplications required for the 3 by 3 case and other small sizes, in particular 4 by 4. We are also considering non-square matrices and admitting complex coefficients. Results to date include additional new algorithms using 23 essential multiplications for the 3 by 3 case.

A full paper is in preparation and will be available by email to amcloughlin@compapp.dcu.ie

Separation of Reducibilities within NP

A. Pavan (aduri@cse.buffalo.edu) and *A. Selman* (selman@cse.buffalo.edu)
Department of Computer Science and Engineering, University at Buffalo, 226 Bell Hall, Buffalo, NY 14260

Abstract Number 00-13

We report progress on one of our favorite old questions. Do many-one and Turing reducibilities differ on sets in NP? It has been known that if E$\cap$*co*-NE $\neq$ E, then there exist sets A and B in NP $-$ P such that $A \leq^{\mathrm{P}}_{tt} B$ but $A \not\leq^{\mathrm{P}}_{ptt} B$ (A. Selman, *Theoretical Computer Science*, 19, 287–304, 1982). Also, if NP does not have p-measure 0, then there is a language L that is $\leq^{\mathrm{P}}_{3-tt}$-complete but not $\leq^{\mathrm{P}}_{m}$-complete for NP (J. Lutz and E. Mayordomo, *Theoretical Computer Science*, 164, 141–163, 1996).

We prove that if UE $\neq$ E, then there are languages A, B, C, and D in UP $-$ P such that

1. $A \leq^{\mathrm{P}}_{tt} B$, but $A \not\leq^{\mathrm{P}}_{btt} B$, and
2. $C \leq^{\mathrm{P}}_{T} D$, but $C \not\leq^{\mathrm{P}}_{tt} D$.

Now consider the following hypothesis (Hyp. H): There is a UP-machine M that accepts 0^* such that no $2^{\sqrt{n}}$ time-bounded Turing machine can output infinitely-many accepting computations of M. Hyp. H is equivalent to the assertion that there exists a language in P with exactly one string of every length that is $2^{\sqrt{n}}$-printable immune.

We prove that if Hyp. H, then there is a language L that is $\leq^{\mathrm{P}}_{T}$-complete but not $\leq^{\mathrm{P}}_{btt}$-complete for NP.

A full paper is not yet available.

Combinatorial interpretation of Kolmogorov complexity

Andrei Romashchenko, Dept. of Mathematical Logic and Theory of Algorithms, Moscow State University, Vorobjevy Gory, 119899, Moscow, Russia (anromash@mccme.ru)
Alexander Shen, Institute of Problems of Information Transmission, Russia (shen@mccme.ru)
Nikolai Vereshchagin, Dept. of Mathematical Logic and Theory of Algorithms, Moscow State University, Vorobjevy Gory, 119899, Moscow, Russia (ver@mccme.ru)

Abstract Number 00-14

The very first Kolmogorov's paper on algorithmic information theory was entitled "Three approaches to the definition of the quantity of information". These three approaches were called *combinatorial*, *probabilistic* and *algorithmic*. Trying to establish formal connections between combinatorial and algorithmic approaches, we prove that every linear inequality including Kolmogorov complexities could be translated into an equivalent combinatorial statement.
Entropy (complexity) proofs of combinatorial inequalities given in papers of Llewellyn – Radhakrishnan and Hammer – Shen can be considered as a special cases (and a natural starting points) for this translation.

A full paper is available by email to anromash@mccme.ru

On the Hardness of Graph Isomorphism

Jacobo Torán Abteilung Theoretische Informatik Universität Ulm Oberer Eselsberg 89069 Ulm, Germany (toran@informatik.uni-ulm.de)

Abstract Number 00-15

We show that the graph isomorphism problem is hard under logarithmic space many-one reductions for the complexity classes NL, PL (probabilistic logarithmic space), for every logarithmic space modular class $\mathrm{Mod}_k\mathrm{L}$ and for the class DET of problems NC_1 reducible to the determinant. These are the strongest existing hardness results for the graph isomorphism problem, and imply a randomized logarithmic space reduction from the perfect matching problem to graph isomorphism.

A full paper is available by email to toran@informatik.uni-ulm.de

Independent minimum length programs to translate between given strings

Nikolai K. Vereshchagin, Moscow State University, Dept. of Mathematical Logic and Theory of Algorithms, Vorobjevy Gory, Moscow, Russia 119899. (ver@mccme.ru)
Michael V. Vyugin, Moscow State University, Dept. of Mathematical Logic and Theory of Algorithms, Vorobjevy Gory, Moscow, Russia 119899. (misha@vyugin.mccme.ru)

Abstract Number 00-16

A string p is called a program to compute y given x if $U(p,x)=y$, where U denotes universal programming language. Kolmogorov complexity $K(y|x)$ of y relative to x is defined as minimum length of a program to compute y given x. Let $K(x)$ denote $K(x|\text{emptystring})$ (Kolmogorov complexity of x) and let $I(x:y)=K(x)+K(y)-K(\langle x,y\rangle)$ (the amount of mutual information in x,y). In the present paper we answer in negative the following question posed in [C.H. Bennett, P. Gács, M. Li, P.M.B. Vitányi, and W.H. Zurek. "Information Distance", IEEE Trans. on Information Theory **44** (1998), No 4, 1407–1423]: Is it true that for any strings x,y there are independent minimum length programs p,q to translate between x,y, that is, is it true that for any x,y there are p,q such that $U(p,x)=y$, $U(q,y)=x$, the length of p is $K(y|x)$, the length of q is $K(x|y)$, and $I(p:q)=0$ (where the last three equalities hold up to an additive $O(\log(K(x|y)+K(y|x)))$ term)?
If we allow the equalities hold up to an additive $O(\log(K(x)+K(y)))$ term, the answer becomes positive: for any x,y there are p,q such that $U(p,x)=y$, $U(q,y)=x$, the length of p is $K(y|x)$, the length of q is $K(x|y)$, and $I(p:q)=0$ (where the last three equalities hold up to an additive $O(\log(K(x)+K(y)))$ term).

A full paper is available by email to ver@mccme.ru.

How Important Is Theory for Practical Problems? On Hartmanis' Observation

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

Abstract Number 00-17

J. Hartmanis recently observed that if a theoretical result is very difficult to prove or disprove, then usually, this result has little or no practical usefulness. We explain this seemingly paradoxical observation by proving that a (simple) formalization of this observation is indeed true.

By a *potential application* of a statement S, we mean the fact that from S, we can conclude that $\forall x\, P(x)$, where x runs over all binary strings, and $P(x)$ is a feasible predicate. For example, the Generalized Riemann hypothesis implies that a certain feasible algorithm $\mathcal{U}$ is a universal primality test, i.e., that $\forall \langle n_1, n_2 \rangle\, (\mathcal{U}(n_1 \cdot n_2) =$"false"$)$.

By the *potential complexity* of a proof, we mean the total number of its steps. In addition to deduction steps (in the sense of some deduction system), we allow steps typical for computer proofs, such as checking whether a given feasible predicate $Q(x)$ holds for a given binary string x, and generating a random binary string α of a given length n (we mean a true random number generator, in which random numbers come from the physical process like a resistor noise). This addition is useful: e.g., the easiest proof that two analytical functions $f_i : [0,1] \to R$ differ is comparing $f_1(\alpha)$ and $f_2(\alpha)$ for a random $\alpha \in [0,1]$; this proof succeeds with probability ≈ 1.

Let $\varepsilon \in (0,1)$ be fixed. We say that a proof is *correct* if it succeeds with probability $\geq 1 - \varepsilon$. A statement S is called *C-potentially complex* if any correct proof of S or $\neg S$ has potential complexity $\geq C$.

PROPOSITION. *Let S be a C-potentially complex statement, and let $P(x)$ be its potential application (with a proof p of length* $\mathrm{len}(p)$*). Then, regardless of whether S is true or not, for every integer n, the portion P_n of strings x of length n for which the predicate $P(x)$ is true satisfies the inequality $P_n \geq \varepsilon^{n/(C-\mathrm{len}(p)-2)}$.*

When the statement S is very complex, and the strings are of reasonable length n, then $P_n \approx 1$, so even without S, we can guarantee that $P(x)$ is true for "almost all" strings of this length. Thus, for the application $P(x)$, the difficult-to-prove statement S is, indeed, not very useful.

A full paper is available at http://www.cs.utep.edu/vladik/2000/tr00-21.ps.gz