COMPLEXITY ABSTRACTS 2004. Volume XIV

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.

TABLE OF CONTENTS

Toward a Topology for NC^1

Eric Allender, Department of Computer Science, Rutgers University, 110 Frelinghuysen Road, Piscataway, NJ 08854-8019, USA. (allender@cs.rutgers.edu)
Samir Datta, WINLAB, Rutgers University, 73 Brett Road, Piscataway, NJ 08854-8060, USA. (sdatta@winlab.rutgers.edu)
Sambuddha Roy, Department of Computer Science, Rutgers University, 110 Frelinghuysen Road, Piscataway, NJ 08854-8019, USA. (samroy@paul.rutgers.edu)

Abstract Number 04-1

Hansen recently provided a characterization of ACC^0 as precisely the class of problems computable by constant-width *planar* circuits of polynomial size (with AND and OR gates, with negation available at the inputs). Barrington's theorem shows that, without the restriction of planarity, constant-width circuits characterize NC^1. We consider possible generalizations of Hansen's theorem, by considering circuits with small *genus* and *thickness*.
Every problem in NC^1 is computed by a constant-width circuit of thickness two, and thus thickness does not seem to be a useful parameter for investigating the structure of NC^1.
In contrast, we show that restricting constant-width circuits to have genus $O(1)$ again yields a characterization of ACC^0.
It remains an intriguing open question if there are problems that are not believed to lie in ACC^0 that can be computed by constant-width, polynomial-size circuits of small (say, logarithmic) genus.

A full paper will be available soon at http://www.cs.rutgers.edu/~allender

Robust PCPs of Proximity, Shorter PCPs and Applications to Coding

Eli Ben-Sasson, Radcliffe Institute for Advanced Study, Cambridge, MA 02139. (eli@eecs.harvard.edu)
Oded Goldreich, Department of Computer Science, Weizmann Institute of Science, Rehovot, ISRAEL. (oded.goldreich@weizmann.ac.il).
Prahladh Harsha, Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, Cambridge, MA 02139. (prahladh@mit.edu).
Madhu Sudan, Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, Cambridge, MA 02139. (madhu@mit.edu).
Salil Vadhan, Division of Engineering and Applied Sciences, Harvard University, Cambridge, MA 02138. (salil@eecs.harvard.edu).

Abstract Number 04-2

We continue the study of trade-offs between the length of PCPs and their query complexity, establishing these main results (referring to proofs of satisfiability of circuits of size n):

1. PCPs of length $\exp(\tilde{O}(\log\log n)^2) \cdot n$, verified by $o(\log\log n)$ Boolean queries.

2. For every $\epsilon > 0$, PCPs of length $\exp(\log^\epsilon n) \cdot n$ verified by a constant number of Boolean queries.

In both cases, false assertions are rejected with constant probability (which may be set to be arbitrarily close to 1). The multiplicative overhead on the length of the proof, introduced by transforming a proof into a probabilistically checkable one, is just quasi-polylogarithmic in the first case (of query complexity $o(\log\log n)$), and $2^{(\log n)^\epsilon}$, for any $\epsilon > 0$, in the second case (of constant query complexity). In contrast, previous results required at least $2^{\sqrt{\log n}}$ overhead in the length, even to get query complexity $2^{\sqrt{\log n}}$.
Our techniques include the introduction of a new variant of PCPs that we call "Robust PCPs of Proximity". These new PCPs facilitate proof composition, which is a central ingredient in construction of PCP systems. (A related notion and its composition properties were discovered independently by Dinur and Reingold.) Our main technical contribution is a construction of a "length-efficient" Robust PCP of Proximity. While the new construction uses many of the standard techniques in PCPs, it does differ from previous constructions in fundamental ways, and in particular does not use the "parallelization" step of Arora et. al. The alternative approach may be of independent interest.
We also obtain analogous quantitative results for locally testable codes. In addition, we introduce a relaxed notion of locally decodable codes, and present such codes mapping k information bits to codewords of length $k^{1+\epsilon}$, for any $\epsilon > 0$.

Full version at http://eccc.uni-trier.de/eccc-reports/2004/TR04-021/index.html

Simple PCPs with Poly-log Rate and Query Complexity

Eli Ben-Sasson, Radcliffe Institute for Advanced Study, Cambridge, MA 02139. (eli@eecs.harvard.edu)
Madhu Sudan, Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, Cambridge, MA 02139. (madhu@mit.edu).

Abstract Number 04-3

We give constructions of PCPs of length $n \cdot \mathrm{poly}(\log n)$ (with respect to circuits of size n) that can be verified by making $\mathrm{poly}(\log n)$ queries to bits of the proof. These PCPs are not only shorter than previous ones, but also simpler. Our (only) building blocks are Reed-Solomon codes and the Bivariate Low Degree Test of Polischuk and Spielman.
First, we present a novel reduction of SAT to the following problem. Given oracle access to a string of length $n' = n \cdot \mathrm{poly}(\log n)$, verify whether it is close to being an evaluation of a univariate polynomial of degree $n'/10$. While somewhat similar reductions have been extensively used in previous PCP constructions, our new reduction favors over them in its simplicity. Notice the degree of the polynomial is larger than the size of the original SAT problem. Thus, testing low degree of this string seems to cost more queries than required for reading the original satisfying assignment in its entirety!
To overcome this, we present a short PCP of Proximity for certain Reed-Solomon codes. For these codes, verifying that a string of length n' is close to an evaluation of a degree $n'/10$ polynomial can be done with $\mathrm{poly}(\log n')$ queries into the string and into an additional proof of length $n' \cdot \mathrm{poly}(\log n')$. Such PCPs of proximity also gives rise to locally testable codes with poly-logarithmic rate and query complexity.

Full version to appear soon at http://www.eecs.harvard.edu/~eli/ and will be submitted to Electronic Colloquium on Computational Complexity.

The Degree of Threshold mod 6 and Diophantine Equations

Nayantara Bhatnagar, (nand@cc.gatech.edu)
Parikshit Gopalan, (parik@cc.gatech.edu)
Richard J. Lipton, (rjl@cc.gatech.edu)
College of Computing, Georgia Tech., 801 Atlantic Drive, Atlanta, GA, 303332.

Abstract Number 04-4

The study of polynomials which represent Threshold functions modulo 6 was initiated by Barrington, Beigel and Rudich who proved that OR can be represented by a polynomial of degree $O(\sqrt{n})$ over Z_6. The AND function requires degree $\Omega(n)$ for a strong representation, but can be weakly represented by polynomials of degree $O(\sqrt{n})$. This raises the natural question

What is the (strong/weak) degree of Threshold k for $1 < k < n$?

We study this question using the connection between representations by symmetric polynomials and simultaneous communication protocols previously established by the authors. We show that proving bounds on the degree of Threshold functions is equivalent to counting the number of solutions to certain Diophantine equations. Using this connection, we prove nearly tight bounds on the degree of symmetric polynomials representing Threshold k for all k.

We show that the strong degree of T_k modulo 6, is roughly $O(\sqrt{nk})$. We show a lower bound of $\Omega(\sqrt{nk})$ using Dirichlet's Theorem on simultaneous Diophantine approximation. We show an upper bound of $O(nk)^{\frac{1}{2}+\varepsilon}$ assuming the *abc*-conjecture. We prove the bound unconditionally for k constant. We show nearly tight bounds for weak representations.

The $O(\sqrt{n})$ upper bound for the OR function can be interpreted as follows: for suitably chosen parameters (k_1, k_2) if $0 \leq w \leq n$ and $w \bmod 2^{k_2}$ and $w \bmod 3^{k_3}$ are both zero, then in fact $w = 0$. Our bounds on T_k give a similar result about the size of w. For n sufficiently large, and suitably chosen k_1, k_2 if $w \bmod 2^{k_2}$ and $w \bmod 3^{k_3}$ are both less than k, then in fact they are both equal to w itself and $w < k$. Conversely if $w \geq k$, then one of the residues must be large.

A full paper is available at http://eccc.uni-trier.de/eccc-reports/2004/TR04-022/

Quantum Lower Bounds for Fanout

Maosen Fang, Computer Science Department, Boston University, Boston, MA 02215 USA, (heroes@bu.edu)
Stephen Fenner, Dept. of CS and Eng., University of South Carolina, Columbia, SC 29208 USA, (fenner@cse.sc.edu)
Frederic Green, Dept. of Math and CS, Clark University, Worcester, MA 01610 USA, (fgreen@black.clarku.edu)
Steven Homer, Computer Science Department, Boston University, Boston, MA 02215 USA, (homer@bu.edu)
Yong Zhang, Dept. of CS and Eng., University of South Carolina, Columbia, SC 29208 USA. (zhang29@cse.sc.edu)

Abstract Number 04-5

The *fanout* gate F_n copies the (classical) value of a qubit into n other qubits, that is,

$$F_n|x_1, x_2 \ldots, x_n, x_{n+1}\rangle = |x_1 \oplus x_{n+1}, \ldots, x_n \oplus x_{n+1}, x_{n+1}\rangle.$$

The fanout operator has recently been shown to be a powerful primitive for very fast (i.e., constant-depth) quantum computation. Moore (quant-ph/9903046) observed that the fanout and parity gates are constant-depth equivalent in the quantum world. Høyer & Špalek (STACS 2003) showed how F_n can be used to compute threshold functions and approximate the Quantum Fourier Transform in constant depth. Thus $\mathbf{QAC}^0_{wf} = \mathbf{QTC}^0$, in contrast to the classical case.

An obvious question is whether fanout is necessary for such power.

We help to answer this question affirmatively by proving several new lower bounds for constant-depth quantum circuits. The main result is that approximating F_n requires $\Omega(\log n)$-depth circuits, when the circuits are composed of single-qubit and arbitrary size Toffoli gates, and when they use only constantly many ancillæ. Under this constraint, this bound is close to optimal. In the case of a non-constant number a of ancillae, we give a tradeoff between a and the required depth, that results in a non-trivial depth lower bound for fanout when $a = n^{1-o(1)}$.

A full paper is available at http://arxiv.org/abs/quant-ph/0312208.

Bounds on the Power of Constant-Depth Quantum Circuits

Stephen Fenner, Dept. of CS and Eng., University of South Carolina, Columbia, SC 29208 USA, (`fenner@cse.sc.edu`)
Frederic Green, Dept. of Math and CS, Clark University, Worcester, MA 01610 USA, (`fgreen@black.clarku.edu`)
Steven Homer, Computer Science Department, Boston University, Boston, MA 02215 USA, (`homer@bu.edu`)
Yong Zhang, Dept. of CS and Eng., University of South Carolina, Columbia, SC 29208 USA. (`zhang29@cse.sc.edu`)

Abstract Number 04-6

We show that constant-depth quantum circuits (over a fixed finite family of gates) are hard to simulate exactly classically, but are in some cases easy to approximate.
Given a finite family $\mathcal{F}$ of quantum gates, a $\mathbf{QNC}_{\mathcal{F}}$ *circuit* is a tuple $\langle C, n, S \rangle$, where

- C is a quantum circuit on at least n qubits, with gates drawn from $\mathcal{F}$,
- C takes a classical input x on its first n qubits, the other qubits initially set to 0, and
- S is some set of *output* qubits, which are measured in the computational basis.

(C, n, S) *accepts* an input $x \in \{0,1\}^n$ if all the qubits in S are found to be 0 when the final state is measured.
We investiate language classes defined using uniform families of **QNC** circuits of constant depth. In particular, the bounded-error class $\mathbf{BQNC}^0_{\epsilon,\delta}$ is defined by **QNC** circuits whose acceptance probability is either $< \epsilon$ (for rejection) or $\geq \delta$ (for acceptance). Here the error thresholds satisfy $0 < \epsilon \leq \delta \leq 1$, and they may depend on the circuit. $\mathbf{BQNC}^0_{\epsilon,\delta}$ is the constant-depth analogue of the class **BQP**.
We show first that

$$\mathbf{BQNC}^0_{\epsilon,\delta} \subseteq \mathbf{P}$$

if ϵ and δ are ptime computable and $1 - \delta = 2^{-2d}(1 - \epsilon)$, where d is the circuit depth. This inclusion holds over any family $\mathcal{F}$ of gates.
By contrast, we adapt and extend ideas of Terhal & DiVincenzo (quant-ph/0205133) to show that, for any family $\mathcal{F}$ of quantum gates that includes the Hadamard and CNOT gates, computing the acceptance probabilities of depth-five circuits over $\mathcal{F}$ is just as hard as computing these probabilities for arbitrary quantum circuits over $\mathcal{F}$. In particular, this implies that

$$\mathbf{NQNC}^0 = \mathbf{NQACC} = \mathbf{NQP} = \mathrm{co}\mathbf{C}_=\mathbf{P},$$

where $\mathbf{NQNC}^0$ is the constant-depth analog of the class **NQP**: the circuit accepts iff its acceptance probability is nonzero. This essentially refutes a conjecture of Green et al. (quant-ph/0106017) that $\mathbf{NQACC} \subseteq \mathbf{TC}^0$.

A full paper is available at `http://arxiv.org/abs/quant-ph/0312209`.

Quantum algorithms for a set of group theoretic problems

Stephen A. Fenner, Department of Computer Science and Engineering, University of South Carolina, Columbia, South Carolina 29205, USA. (fenner@cse.sc.edu)
Yong Zhang, Department of Computer Science and Engineering, University of South Carolina, Columbia, South Carolina 29205, USA. (zhang29@cse.sc.edu)

Abstract Number 04-7

Group intersection and coset intersection over solvable groups are two open problems posted in Watrous [STOC'02]. In this paper, we show that a set of group theoretic problems, including group intersection, coset intersection and double coset membership, can be solved in quantum polynomial time for solvable groups of bounded exponent and of bounded derived series.
We study these problems in the setting of black box groups. We prove our results by reducing the above problems to Orbit Coset. In fact we show that Group Intersection over solvable groups is reducible to Orbit Superposition, which is known to be reducible to Orbit Coset. An important component in our proof is the use of the uniform superposition of groups and cosets.
We also give an alternative quantum algorithm for decomposing finite abelian groups.

A full paper will be available soon at http://www.cse.sc.edu/~fenner/papers.

Communication vs. Computation

Prahladh Harsha, Computer Science and Artificial Intelligence Laboratory, MIT, Cambridge, MA 02139, USA, (prahladh@mit.edu).
Yuval Ishai, Computer Science Department, Technion, Haifa 32000, Israel, (yuvali@cs.technion.ac.il).
Joe Kilian, NEC Laboratories America Inc, Princeton, NJ 08540, USA, (joe@nec-labs.com).
Kobbi Nissim, Microsoft Research, SVC. 1065 La Avenida, Mountain View, CA 94043, USA, (kobbi@microsoft.com).
S. Venkatesh, Computer Science Department, University of Victoria, Victoria, BC, Canada V8W 3P6, (venkat@cs.uvic.ca).

Abstract Number 04-8

We initiate a study of tradeoffs between communication and computation in well-known communication models and in other related models. The fundamental question we investigate is the following: Is there a computational task that exhibits a strong tradeoff behavior between the amount of communication and the amount of time needed for local computation?

Under various standard assumptions, we exhibit boolean functions that show strong tradeoffs in the following computation models: (1) two-party randomized communication complexity; (2) query complexity; (3) property testing. For the model of deterministic communication complexity, we show a similar result relative to a random oracle.

Finally, we study a time-degree tradeoff problem that arises in arithmetization of boolean functions, and relate it to time-communication tradeoff questions in multi-party communication complexity and in cryptography.

An extended abstract of this paper is to appear in *ICALP '04*. A full version of this paper is available at http://theory.csail.mit.edu/~prahladh/papers/.

Using Nondeterminism to Amplify Hardness

Alexander Healy ahealy@fas.harvard.edu

Salil Vadhan salil@eecs.harvard.edu

Emanuele Viola viola@eecs.harvard.edu

Division of Engineering and Applied Sciences
Harvard University
Cambridge, MA 02138

Abstract Number 04-9

We revisit the problem of hardness amplification in $\mathcal{NP}$, as recently studied by O'Donnell (STOC '02). We prove that if $\mathcal{NP}$ has a balanced function f such that any circuit of size $s(n)$ fails to compute f on a $1/\text{poly}(n)$ fraction of inputs, then $\mathcal{NP}$ has a function f' such that any circuit of size $s'(n) = s(\sqrt{n})^{\Omega(1)}$ fails to compute f' on a $1/2 - 1/s'(n)$ fraction of inputs. In particular,

1. If $s(n) = n^{\omega(1)}$, we amplify to hardness $1/2 - 1/n^{\omega(1)}$.
2. If $s(n) = 2^{n^{\Omega(1)}}$, we amplify to hardness $1/2 - 1/2^{n^{\Omega(1)}}$.
3. If $s(n) = 2^{\Omega(n)}$, we amplify to hardness $1/2 - 1/2^{\Omega(\sqrt{n})}$.

These improve the results of O'Donnell, which only amplified to $1/2-1/\sqrt{n}$. O'Donnell also proved that no construction of a certain general form could amplify beyond $1/2 - 1/n$. We bypass this barrier by using both *derandomization* and *nondeterminism* in the construction of f'.

We also prove impossibility results demonstrating that both our use of nondeterminism and the hypothesis that f is balanced are necessary for "black-box" hardness amplification procedures (such as ours).

Dichotomy Theorems for Alternation-Bounded Quantified Boolean Formulas

Edith Hemaspaandra, Department of Computer Science, Rochester Institute of Technology, Rochester, NY 14623, U.S.A., (eh@cs.rit.edu).

Abstract Number 04-10

In 1978, Schaefer proved his famous dichotomy theorem for generalized satisfiability problems. He defined an infinite number of propositional satisfiability problems, showed that all these problems are either in P or NP-complete, and gave a simple criterion to determine which of the two cases holds. This result is surprising in light of Ladner's theorem, which implies that there are an infinite number of complexity classes between P and NP-complete (under the assumption that P is not equal to NP).

Schaefer also stated a dichotomy theorem for quantified generalized Boolean formulas, but this theorem was only recently proven by Creignou, Khanna, and Sudan, and independently by Dalmau: Determining truth of quantified Boolean formulas is either PSPACE-complete or in P.

This paper looks at alternation-bounded quantified generalized Boolean formulas. In their unrestricted forms, these problems are the canonical problems complete for the levels of the polynomial hierarchy. In this paper, we prove dichotomy theorems for alternation-bounded quantified generalized Boolean formulas, by showing that these problems are either Σ_i^p-complete or in P, and we give a simple criterion to determine which of the two cases holds. This is the first result that obtains dichotomy for an infinite number of classes at once.

A full paper is available as ACM Computing Research Repository Technical Report cs.CC/0406006.

All Superlinear Inverse Schemes are coNP-Hard[a]

Edith Hemaspaandra, Department of Computer Science, Rochester Institute of Technology, Rochester, NY 14623-5608, USA. (eh@cs.rit.edu)
Lane A. Hemaspaandra, Department of Computer Science, University of Rochester, Rochester, NY 14627-0226, USA. (lane@cs.rochester.edu)
Harald Hempel, Institut für Informatik, Friedrich-Schiller-Universität Jena, D-07743 Jena, Germany. (hempel@informatik.uni-jena.de)

Abstract Number 04-11

How hard is it to invert NP-problems? We show that all superlinearly certified inverses of NP problems are coNP-hard. As part of our work we develop a novel proof technique that builds diagonalizations against certificates directly into a circuit.

A full paper will soon be available by email to hempel@informatik.uni-jena.de

[a] Supported in part by grants NSF-CCR-9322513, NSF-INT-9815095/DAAD-315-PPP-gü-ab, and NSF-CCR-0311021.

Linear-time algorithms for Monadic Logic

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

Abstract Number 04-12

Abstract

In general, the computation effort required solving a problem described by a first-order or fixed-point query (logical formula) requires time polynomial in the size of the database (finite structure). We show how a linear-time evaluation algorithm for first-order logic on bounded-degree data structures can be extended to monadic fixed-point formulas.

First-order queries can always be evaluated in logarithmic-space. On bounded-degree graphs, it is surprising that first-order sentences can be evaluated in linear-time [1]. In this short presentation we illustrate how to also do this for monadic fixed-point formulas. Let $\phi(x; S)$ be a first-order formula of one free variable in the language of graphs (vertices V with one binary edge relation E) with equality, with an additional unary relation S, appearing only positively. Write $\phi(S) = \{s : G \vDash \phi(s; S)\}$ where the finite graph $G = \langle V, E \rangle$ is understood to have degree at most d.

Def: The *least fixed-point* of ϕ, denoted ϕ^∞, is the smallest relation S satisfying $\phi(S) = S$. It can be computed by any monotone method which states below the fixed-point. So, a greedy method can be used in which only one element is thrown in at each step.

Fact: If $s_i \in \phi(\{s_1, \ldots, s_{i-1}\})$ is a maximal length k sequence of distinct nodes, then $\{s_1, \ldots, s_k\} = \phi^\infty$.

Realize our graphs now include a unary relation S. The r-type of a node is the isomorphism type of the radius r neighborhood about it. It turns out satisfaction depends only upon a limited quantity of types.

Fact: Let $\tau(v)$ be the r-type of v in G, and let $\#\tau^G = |\{v \in G : \tau(v) = \tau\}|$ for any r-type τ. Then $\mathrm{T}(G) = \{(\tau, \min\{t, \#\tau\}) : \tau \text{ is an } r\text{-type}\}$, together with $\tau(v)$, determines whether $G \vDash \phi(v)$.

The algorithm assumes a unit-cost RAM model with $O(\log n)$-bit word size, in which the edge relation of the degree d graph is represented by a doubly-linked incoming and outgoing pointers at each vertex. Our method starts with $S = \emptyset$, and marks one element at a time until $S = \phi^\infty$. We always select an element in constant time that currently satisfies $\phi(S)$, keeping track of S by directly marking nodes in G, obtaining

Theorem: Over bounded-degree graphs, there is a linear-time algorithm to compute monadic fixed-points.

[1] Detlef Seese, "Linear-time computable problems and first-order descriptions" *Mathematical Structures in Computer Science*, 6(6):505–526, December 1996.

A full paper is available by email to slindell@haverford.edu