COMPLEXITY ABSTRACTS 2006. Volume XVI

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

Worst-Case Running Times for Average-Case Algorithms

The Multiparty Communication Complexity of EXACT-T Revisited

Depth-Universal Quantum Circuits

Very Sparse Leaf Languages

Worst-Case Running Times for Average-Case Algorithms

Luis Antunes, Porto University (`lfa@ncc.up.pt`)
Lance Fortnow, University of Chicago (`fortnow@cs.uchicago.edu`)

Abstract Number 06-1

Under a standard hardness assumption we exactly characterize the worst-case running time of languages that are in average polynomial-time over all polynomial-time samplable distributions.

More precisely we show that if exponential time is not in subexponential space, then the following are equivalent for any algorithm A:

- For all polynomial-time samplable distributions μ, A runs in time polynomial on μ-average.
- For all polynomial p, the running time for A is bounded by $2^{O(K^p(x)-K(x)+log(|x|))}$ for *all* inputs x.

To prove this result we explore the time-bounded Kolmogorov distribution, $m^t(x) = 2^{-K^t(x)}$ where $K^t(x)$ is the Kolmogorov complexity (smallest program size to generate x) with programs limited to run in time $t(|x|)$ and show that under the hardness assumption, the time-bounded Kolmogorov distribution is a universal samplable distribution.

An extended abstract is available at http://people.cs.uchicago.edu/~fortnow/papers/ud.pdf.

The Multiparty Communication Complexity of EXACT-T Revisited

Richard Beigel, Department of Computer Science, Temple University, Philadelphia, PA, 19122 (`professorb@gmail.com`)
William Gasarch, University of Maryland, Dept. of Computer Science and Institute for Advanced Computer Studies, College Park, MD 20742. (`gasarch@cs.umd.edu`)
James Glenn, Dept. of Computer Science, Loyola College in Maryland, Baltimore, MD, 21210. (`jglenn@cs.loyola.edu`)

Abstract Number 06-2

Let $x_1, \ldots, x_k$ be n-bit numbers and T∈N. Assume that $P_1, \ldots, P_k$ are players such that P_i knows all of the numbers *except* x_i. The players want to determine if $\sum_{j=1}^{k} x_j = T$ by broadcasting as few bits as possible. Chandra, Furst, and Lipton obtained an upper bound of $O(\sqrt{n})$ bits for the k=3 case, and a lower bound of $\omega(1)$ for k≥ 3 when T=$\Theta(2^n)$. We obtain (1) for general k≥ 3 an upper bound of k+$O(n^{1/(\lfloor \lg(2k-2) \rfloor)})$, (2) for k=3, T=$\Theta(2^n)$, a lower bound of $\Omega(\log \log n)$, (3) a generalization of the protocol to abelian groups, (4) lower bounds on the multiparty communication complexity of some regular languages, (5) lower bounds on branching programs, and (6) empirical results for the k=3 case.

A full paper is available by email to gasarch@cs.umd.edu

Depth-Universal Quantum Circuits

Stephen Fenner, University of South Carolina (`fenner@cse.sc.edu`)
Frederic Green, Clark University (`green@black.clarku.edu`)
Steven Homer, Boston University (`homer@cs.bu.edu`)

Abstract Number 06-3

A *universal circuit* is one that takes two types of inputs: regular input bits (data bits) and control bits. Depending on the values of the control bits (the "program"), the universal circuit can simulate *any* circuit on the regular inputs, up to some bound on the size/depth of the circuit to be simulated.

A depth-universal circuit is one that can simulate circuits up to depth d and size s with only a constant factor blow-up in depth (that is, depth $O(d)$) and size poly(d, s). Cook & Hoover [1985] constructed depth-universal NC circuits (i.e., circuits with Boolean gates of fan-in two) provided $d = \Omega(\log s)$.

We construct depth-universal quantum circuits with fan-out gates for any depth (even constant). In particular, we show that for any n and d there exists a quantum circuit $U_{n,d}$ on $n + m$ qubits such that, for any quantum circuit C on n qubits with depth at most d, there exists a (classical) program $p \in \{0,1\}^m$ such that for all $x \in \{0,1\}^n$,

$$U_{n,d}(|x\rangle \otimes |p\rangle) = (C|x\rangle) \otimes |p\rangle.$$

Further, we have the following:

1. $U_{n,d}$ has depth $O(d)$ and $m = O(dn^2)$.
2. The circuit C may use any gates from the family $\{H, T\} \cup \{F_n \mid n \geq 1\}$, where H is the one-qubit Hadamard gate, T is the $\pi/8$ gate, and F_n is the n-qubit fan-out gate.
3. The circuit $U_{n,d}$ only uses gates from the same family.
4. The program p can be computed easily (and classically) from a description of C.
5. Depth-universal quantum circuits exist for other families of allowed gates.

Our construction can be easily adapted to build depth-universal AC circuits (unbounded fan-in AND and OR, NOT) for any depth bound.

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

Very Sparse Leaf Languages

Lance Fortnow, University of Chicago (`fortnow@cs.uchicago.edu`)
Mitsunori Ogihara, University of Rochester (`ogihara@cs.rochester.edu`)

Abstract Number 06-4

Unger studied the balanced leaf languages defined via poly-logarithmically sparse leaf pattern sets. Unger shows that NP-complete sets are not polynomial-time many-one reducible to such balanced leaf language unless the polynomial hierarchy collapses to θ_2^p and that Σ_2^p-complete sets are not polynomial-time bounded-truth-table reducible (respectively, polynomial-time Turing reducible) to any such balanced leaf language unless the polynomial hierarchy collapses to Δ_2^p (respectively, Σ_4^p).
This paper studies the complexity of the class of such balanced leaf languages, which will be denoted by VSLL. In particular, the following tight upper and lower bounds of VSLL are shown:

1. co-NP $\subseteq$ VSLL $\subseteq$ co-NP/poly (the former inclusion is already shown by Unger).
2. $\mathrm{co}-\mathrm{NP}/1 \not\subseteq$ VSLL unless PH $= \theta_2^p$.
3. For all constant $c > 0$, VSLL $\not\subseteq \mathrm{co}-\mathrm{NP}/n^c$.
4. $\mathrm{P}/(\log\log(n) + O(1)) \subseteq$ VSLL.
5. For all $h(n) = \log\log(n) + \omega(1)$, $\mathrm{P}/h \not\subseteq$ VSLL.

An extended abstract is available at http://people.cs.uchicago.edu/~fortnow/papers/vsll.pdf.