1999 IEEE Conference on Computational Complexity

Proceedings

Fourteenth Annual IEEE Conference on
Computational Complexity

(Formerly: Structure in Complexity Theory Conference)

May 4-6, 1999
Atlanta, Georgia, USA

Sponsored by

IEEE Computer Society Technical Committee on
Mathematical Foundations of Computing

In cooperation with

ACM SIGACT
EATCS

IEEE
COMPUTER
SOCIETY

Los Alamitos, California
Washington · Brussels · Tokyo

Copyright © 1999 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries may photocopy beyond the limits of US copyright law, for private use of patrons, those articles in this volume that carry a code at the bottom of the first page, provided that the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

Other copying, reprint, or republication requests should be addressed to: IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, P.O. Box 133, Piscataway, NJ 08855-1331.

The papers in this book comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and, in the interests of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors, the IEEE Computer Society, or the Institute of Electrical and Electronics Engineers, Inc.

IEEE Catalog Number 99CB36317
ISBN: 0-7695-0075-7 (Softbound)
ISBN: 0-7803-5685-3 (Casebound)
ISBN: 0-7695-0077-3 (Microfiche)
ISSN: 1093-0159
PR00075

Additional copies may be ordered from:

IEEE Computer Society
Customer Service Center
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314
Tel: + 1-714-821-8380
Fax: + 1-714-821-4641
E-mail: cs.books@computer.org

IEEE Service Center
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
Tel: + 1-732-981-0060
Fax: + 1-732-981-9667
mis.custserv@computer.org

IEEE Computer Society
Asia/Pacific Office
Watanabe Building,
1-4-2 Minami-Aoyama
Minato-ku, Tokyo 107-0062 JAPAN
Tel: + 81-3-3408-3118
Fax: + 81-3-3408-3553
tokyo.ofc@computer.org

Editorial production by Danielle C. Martin

Cover art production by Alex Torres

Printed in the United States of America by The Printing House

IEEE
COMPUTER
SOCIETY

Proceedings

Fourteenth Annual IEEE Conference on
Computational Complexity

Preface

The papers in this volume were presented at the Fourteenth Annual IEEE Conference on Computational Complexity held from May 4-6, 1999 in Atlanta, Georgia, in conjunction with the Federated Computing Research Conference. This conference was sponsored by the IEEE Computer Society Technical Committee on Mathematical Foundations of Computing, in cooperation with the ACM SIGACT (The special interest group on Algorithms and Complexity Theory) and EATCS (The European Association for Theoretical Computer Science).

The call for papers sought original research papers in all areas of computational complexity. A total of 70 papers were submitted for consideration of which 28 papers were accepted for the conference and for inclusion in these proceedings. Six of these papers were accepted to a joint STOC/Complexity session. For these papers the full conference paper appears in the STOC proceedings and a one-page summary appears in these proceedings.

The program committee invited two distinguished researchers in computational complexity – Avi Wigderson and Jin-Yi Cai – to present invited talks. These proceedings contain survey articles based on their talks.

The program committee thanks Pradyut Shah and Marcus Schaefer for their organizational and computer help, Steve Tate and the SIGACT Electronic Publishing Board for the use and help of the electronic submissions server, Peter Shor and Mike Saks for the electronic conference meeting software and Danielle Martin of the IEEE for editing this volume.

The committee would also like to thank the following people for their help in reviewing the papers:

E. Allender, V. Arvind, M. Ajtai, A. Ambainis, G. Barequet, S. Baumer, A. Berthiaume, S. Biswas, A. Broder, N. Bshouty, H. Buhrman, G. Buntrock, J. Buss, C. Calude, S. Cook, A. Dekhtyar, I. Dinur, J. Feigenbaum, M. Goldmann, J. Goldsmith, A. Gupta, E. Hemaspaandra, H. Hempel, U. Hertrampf, T. Hofmeister, S. Homer, R. Impagliazzo, G. Istrate, R. Kannan, R. Khardon, G. Kindler, P. Koiran, S. Kosub, S.R. Kumar, S. Laplante, M. Li, W. Lindner, M. Mahajan, E.M. Camara, K. McCurley, D. van Melkebeek, J. Messner, A. Naik, A. Nayak, M. Ogihara, C. Pollett, S. Radziszowski, V. Raghavan, D. Randall, D. Ranjan, K. Regan, S. Roy, M. Schaefer, R. Schuler, J. Sgall, D. Sieling, F. Stephan, H. Straubing, K.V. Subrahmanyam, P.R. Subramanya, A. Szanto, R. Szelepcsenyi, L. Sellie, A. Selman, J. Simon, Y. Stamatiu, E. Tardos, P. Tesson, S. Toda, J. Toran, L. Torenvliet, C. Umans, V. Vinay, P. Vitanyi, H. Vollmer, K. Wagner, J. Watrous and M. Zimand.

Welcome to Complexity!

Lance Fortnow
Program Chair

Manindra Agrawal
Paul Beame
Richard Chang
Frederic Green
Lane A. Hemaspaandra
Pierre McKenzie
Ronitt Rubinfeld
Amnon Ta-Shma
Thomas Thierauf

此为试读，需要完整PDF请访问：www.ertongbook.com

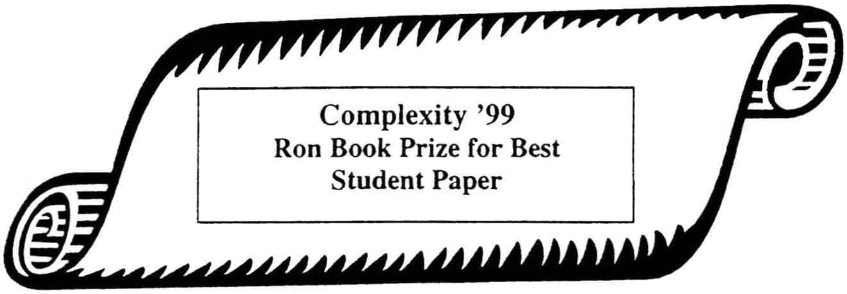
Conference Committee

Eric Allender (chair), *Rutgers University*
Richard Beigel, *University of Illinois at Chicago*
Harry Buhrman, *CWI Amsterdam*
Jin-Yi Cai, *State University of New York at Buffalo*
Russell Impagliazzo, *University of California at San Diego*
Luc Longpré, *University of Texas at El Paso*
Jacobo Torán, *Universität Ulm*
Avi Wigderson, *The Hebrew University*

Program Committee

Lance Fortnow (chair), *University of Chicago*
Manindra Agrawal, *Indian Institute of Technology, Kanpur*
Paul Beame, *University of Washington*
Richard Chang, *University of Maryland, Baltimore County*
Frederic Green, *Clark University*
Lane A. Hemaspaandra, *University of Rochester*
Pierre McKenzie, *University of Montréal*
Ronitt Rubinfeld, *IBM Almaden and Cornell University*
Amnon Ta-Shma, *International Computer Science Institute*
Thomas Thierauf, *Universität Ulm*

1999 Ron Book Prize for Best Student Paper



The Program Committee of the 1999 Conference on Computational Complexity is proud to present the Ron Book Prize for Best Student Paper to Marcus Schaefer of the University of Chicago. This award is given annually to the most outstanding paper written solely by one or more students. This year we have renamed the award in memory of Ron Book. The paper selected by the Complexity Program Committee is

Graph Ramsey Theory and the Polynomial Hierarchy

by **Marcus Schaefer**

Congratulations to the winner!

Table of Contents

Fourteenth Annual IEEE Conference on Computational Complexity

Session 7

Chair: Manindra Agrawal, Indian Institute of Technology, Kanpur

Session 8

Chair: Frederic Green, Clark University

Joint

STOC/Complexity

Session

此为试读，需要完整PDF请访问: www.ertongbook.com

Short Proofs are Narrow – Resolution made Simple *

Eli Ben-Sasson Avi Wigderson
Institute of Computer Science, Hebrew University, Jerusalem, Israel
E-mail: elli@cs.huji.ac.il, avi@cs.huji.ac.il

The *width* of a Resolution proof is defined to be the maximal number of literals in any clause of the proof. In this paper we relate proof *width* to proof *size*, in both general Resolution, and its tree-like variant. Specifically, the main observation of this paper is a relation between these two fundamental resources. Let τ be any CNF contradiction over n variables:

- If τ has a tree-like refutation of *size* S_T, then it has a refutation of maximal *width* $\log_2 S_T$.
- If τ has a *general* resolution refutation of *size* S, then it has a refutation of maximal *width* $O(\sqrt{n \log S})$.

Both the notion of width and the relations above, gradually surfaced in previous papers and we merely make them explicit. Reading through the existing lower bound proofs, it is evident that wide clauses play a central role, with the following logic: If a Resolution proof is short, then random restrictions will "kill" all wide clauses with high probability. But a separate argument shows that still they have to exist even in refutations of the restricted tautology. Thus the proof has to be long.

The first major application of our explicit width-size relations is significant simplification and unification of most known exponential lower bounds on Resolution proof length. Naturally, this understanding leads to new lower bounds as well. The main point is that now, to prove size lower bounds, it is sufficient to prove width lower bounds. It removes the need for random restrictions, and allows to concentrate on the original tautology rather than restricted forms of it.

We develop a general strategy for proving width lower bounds, which follows Haken's original proof technique but for the above reason is now simple and clear. It reveals that large width is implied by certain natural expansion properties of the clauses (axioms) of the tautology in question. We show that in the classical examples of the Pigeonhole principle, Tseitin graph tautologies, and random k-CNF's, these expansion properties are quite simple to prove.

We further illustrate the power of this approach by proving new exponential lower bounds to two different restricted versions of the pigeon-hole principle. One restriction allows the encoding of the principle to use arbitrarily many extension variables in a structured way. The second restriction allows every pigeon to choose a hole from some constant size set of holes.

The second major application of our relations is in automatization results for the Resolution proof system. This is the basic problem faced in the analysis of automatic provers searching for a proof; how long will they run, as a function of the shortest existing proof of the input tautology.

The relations beg the use of the following simple (dynamic programming) algorithm: Set $i = 1$. Start with the axioms, and try to derive all clauses of width at most i. If the empty clause is derived, we are done. If not, increase i by 1 and repeat. Clearly, the running time on any tautology τ over n variables is at most $n^{O(w)}$, when w is the minimal width of a proof of τ. By the relations above, this time is at most $S_T(\tau)^{O(\log n)}$ (namely quasi-polynomial in the minimal tree-like Resolution proof length), and at most $exp(\sqrt{n \log S(\tau)})$ (namely sub-exponential in the minimal general Resolution proof length).

Note that the relation to tree-like proofs is of particular importance, due to the fact that the most popular automated provers such as DLL procedures produce tree-like Resolution proofs. Thus our algorithm never runs much longer than these provers on any tautology.

Our final contribution is a new collection of natural tautologies, which presents the best known separation between general and tree-like Resolution systems. For these tautologies our algorithm is exponentially faster than recursive, tree-like provers, used in practice. The lower bound we present for these tautologies uses a novel connection between tree-like Resolution proofs and the classical pebble game, interesting in it's own right.

---

*The full version of this paper is published in the STOC 99 proceedings. This research was supported by grant number 69/96 of the Israel Science Foundation, founded by the Israel Academy for Sciences and Humanities

0-7695-0075-7/99 $10.00 © 1999 IEEE

On the Complexity of Diophantine Geometry in Low Dimensions

J. Maurice Rojas*

Department of Mathematics
City University of Hong Kong
83 Tat Chee Avenue
Kowloon, HONG KONG
mamrojas@math.cityu.edu.hk
http://www.cityu.edu.hk/ma/staff/rojas

Abstract

We consider the average-case complexity of some otherwise undecidable or open Diophantine problems. More precisely, we show that the following two problems can be solved within **PSPACE**:

I. Given polynomials $f_1, \ldots, f_m \in \mathbb{Z}[x_1, \ldots, x_n]$ defining a variety of dimension ≤ 0 in $\mathbb{C}^n$, find all solutions in $\mathbb{Z}^n$ of $f_1 = \cdots = f_m = 0$.

II. For a given polynomial $f \in \mathbb{Z}[v, x, y]$ defining an irreducible nonsingular non-ruled surface in $\mathbb{C}^3$, decide the sentence $\exists v \, \forall x \, \exists y \; f(v, x, y) \stackrel{?}{=} 0$, quantified over $\mathbb{N}$.

Better still, we show that the truth of the **Generalized Riemann Hypothesis (GRH)** implies that detecting roots in $\mathbb{Q}^n$ for the polynomial systems in problem (I) can be done via a two-round Arthur-Merlin protocol, i.e., well within the second level of the polynomial hierarchy. (Problem (I) is, of course, undecidable without the dimension assumption.) The decidability of problem (II) was previously unknown. Along the way, we also prove new complexity and size bounds for solving polynomial systems over $\mathbb{C}$ and $\mathbb{Z}/p\mathbb{Z}$. A practical point of interest is that the aforementioned Diophantine problems should perhaps be avoided in the construction of crypto-systems.

1 A Brief Introduction

The negative solution of Hilbert's Tenth Problem has all but dashed earlier hopes of solving large polynomial systems over the integers. However, an immediate positive consequence is the creation of a rich and diverse garden of hard problems with potential applications in complexity theory, cryptology, and logic. Even more compelling is the question of where the boundary to decidability lies.

The results mentioned in this short abstract are detailed further and proved in a more extended abstract which will appear simultaneously in the proceedings of a meeting parallel to this session [Roj99]. In closing this brief synopsis, we point out that the explicit sequential and parallel complexity bounds we give for problems (I) and (II) are the best to date. Also, we make use of two new constructions which may be of independent interest: (a) a new quantitative result on using mod p root counts for counting the rational roots of certain polynomial systems, and (b) new "output-sensitive" size and complexity bounds for equation solving over $\mathbb{C}$. Here, by output-sensitivity, we will mean bounds which are polynomial in a quantity which is the true number of complex roots with probability 1. Complexity bounds for earlier algorithms were polynomial in the Bézout number (the product of the total degrees of the equations) and such bounds are frequently much more pessimistic than our output-sensitive bounds.

References

[Roj99] Rojas, J. Maurice, *"On the Complexity of Diophantine Geometry in Low Dimensions,"* Proceedings of the 31st ACM Symposium on Theory of Computing (STOC '99), May, 1999, Atlanta, Georgia, ACM Press, to appear.

*This research was partially funded by a Hong Kong CERG Grant.

0-7695-0075-7/99 $10.00 © 1999 IEEE

Pseudorandom generators without the XOR Lemma*
[Abstract]

Madhu Sudan† Luca Trevisan‡ Salil Vadhan§

Abstract

Impagliazzo and Wigderson [IW97] have recently shown that if there exists a decision problem solvable in time $2^{O(n)}$ and having circuit complexity $2^{\Omega(n)}$ (for all but finitely many n) then P = BPP. This result is a culmination of a series of works showing connections between the existence of hard predicates and the existence of good pseudorandom generators.

The construction of Impagliazzo and Wigderson goes through three phases of "hardness amplification" (a multivariate polynomial encoding, a first derandomized XOR Lemma, and a second derandomized XOR Lemma) that are composed with the Nisan–Wigderson [NW94] generator. In this paper we present two different approaches to proving the main result of Impagliazzo and Wigderson. In developing each approach, we introduce new techniques and prove new results that could be useful in future improvements and/or applications of hardness-randomness trade-offs.

Our first result is that when (a modified version of) the Nisan-Wigderson generator construction is applied with a "mildly" hard predicate, the result is a generator that produces a distribution indistinguishable from having large min-entropy. An extractor can then be used to produce a distribution computationally indistinguishable from uniform. This is the first construction of a pseudorandom generator that works with a mildly hard predicate without doing hardness amplification.

We then show that in the Impagliazzo–Wigderson construction only the first hardness-amplification phase (encoding with multivariate polynomial) is necessary, since it already gives the required average-case hardness. We prove this result by (i) establishing a connection between the hardness-amplification problem and a list-decoding problem for error-correcting codes based on multivariate polynomials; and (ii) presenting a list-decoding algorithm that improves and simplifies a previous one by Arora and Sudan [AS97].

*The full version of this paper appears as [STV98] and an extended abstract appears as [STV99].

†Laboratory for Computer Science, 545 Technology Square, MIT, Cambridge, MA 02141. E-mail: madhu@theory.lcs.mit.edu.

‡Department of Computer Science, Columbia University, 500W 120th St., New York, NY 10027. Email: luca@cs.columbia.edu. Work done at MIT.

§Laboratory for Computer Science, 545 Technology Square, MIT, Cambridge, MA 02141. E-mail: salil@theory.lcs.mit.edu. URL: http://theory.lcs.mit.edu/~salil. Supported by a DOD/NDSEG graduate fellowship and partially by DARPA grant DABT63-96-C-0018.

References

[AS97] Sanjeev Arora and Madhu Sudan. Improved low degree testing and its applications. In *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing*, pages 485–495, El Paso, Texas, 4–6 May 1997.

[IW97] Russell Impagliazzo and Avi Wigderson. $P = BPP$ if E requires exponential circuits: Derandomizing the XOR lemma. In *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing*, pages 220–229, El Paso, Texas, 4–6 May 1997.

[NW94] Noam Nisan and Avi Wigderson. Hardness vs randomness. *Journal of Computer and System Sciences*, 49(2):149–167, October 1994.

[STV98] Madhu Sudan, Luca Trevisan, and Salil Vadhan. Pseudorandom generators without the XOR lemma. Technical Report TR98-074, Electronic Colloquium on Computational Complexity, December 1998. http://www.eccc.uni-trier.de/eccc.

[STV99] Madhu Sudan, Luca Trevisan, and Salil Vadhan. Pseudorandom generators without the XOR lemma. In *Proceedings of the Thirty-First Annual ACM Symposium on the Theory of Computing*, Atlanta, GA, May 1999.

0-7695-0075-7/99 $10.00 © 1999 IEEE

Linear Gaps Between Degrees for the Polynomial Calculus Modulo Distinct Primes
Abstract[1]

Sam Buss[2,3]
Department of Mathematics
Univ. of Calif., San Diego
La Jolla, CA 92093-0112
sbuss@ucsd.edu

Dima Grigoriev
IMR Universite Rennes-1
Beaulieu 35042
Rennes, France
dima@maths.univ-rennes1.fr

Russell Impagliazzo[2,4]
Computer Science and Engineering
Univ. of Calif., San Diego
La Jolla, CA 92093-0114
russell@cs.ucsd.edu

Toniann Pitassi[2,5]
Computer Science
University of Arizona
Tucson, AZ 85721-0077
toni@cs.arizona.edu

Two important algebraic proof systems are the Nullstellensatz system [1] and the polynomial calculus [2] (also called the Gröbner system). The Nullstellensatz system is a propositional proof system based on Hilbert's Nullstellensatz, and the polynomial calculus (PC) is a proof system which allows derivations of polynomials, over some field. The *complexity* of a proof in these systems is measured in terms of the degree of the polynomials used in the proof.

The mod p counting principle can be formulated as a set MOD_p^n of constant-degree polynomials expressing the negation of the counting principle. The Tseitin mod p principles, $TS_n(p)$, are translations of the MOD_p^n into the Fourier basis [3].

The present paper gives linear lower bounds on the degree of polynomial calculus refutations of MOD_p^n over fields of characteristic $q \neq p$ and over rings Z_q with q, p relatively prime. These are the first linear lower bounds for the polynomial calculus. As it is well-known to be easy to give constant degree polynomial calculus (and even Nullstellensatz) refutations of the MOD_p^n polynomials over F_p, our results imply that the MOD_p^n polynomials have a linear gap between proof complexity for the polynomial calculus over F_p and over F_q. We also obtain a linear gap for the polynomial calculus over rings Z_p and Z_q where p, q do not have identical prime factors.

Theorem 1 *Let F be a field of characteristic q, and let G_n be an r-regular graph with expansion ϵ. Then, for all $d < \epsilon n/8$, there is no degree d PC refutation of $TS_n(p)$ over F.*

Theorem 2 *Let $q \geq 2$ be a prime such that $q \nmid p$ and let F be a field of characteristic q. Any PC-refutation of the MOD_p^n polynomials requires degree $> \delta n$, for some constant $\delta > 0$.*

References

[1] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, and P. Pudlák. Lower bounds on Hilbert's Nullstellensatz and propositional proofs. *Proceedings of the London Mathematical Society*, 73:1–26, 1996.

[2] M. Clegg, J. Edmonds, and R. Impagliazzo. Using the Groebner basis algorithm to find proofs of unsatisfiability. In *Proceedings of the Twenty-eighth Annual ACM Symposium on the Theory of Computing*, pages 174–183, 1996.

[3] D. Grigoriev. Nullstellensatz lower bounds for Tseitin tautologies. In *Proceedings of the 39th Annual IEEE Symposium on Foundations of Computer Science*, pages 648–652. IEEE Computer Society Press, 1998.

---

[1] This paper was presented jointly to the 14th Annual IEEE Conference on Computational Complexity and the 31st Annual ACM Symposium on Theory of Computer Science. The complete version is in the latter's proceedings volume.

[2] Supported in part by international grant INT-9600919/ME-103 from the NSF (USA) and the MSMT (Czech republic)

[3] Supported in part by NSF grant DMS-9803515

[4] Supported in part by NSF grant CCR-9734911, Sloan Research Fellowship BR-3311, and US-Israel BSF grant 97-00188.

[5] Supported in part by NSF grant CCR-9457783 and US-Israel BSF grant 95-00238.

0-7695-0075-7/99 $10.00 © 1999 IEEE

Graph Ramsey Theory and the Polynomial Hierarchy

Marcus Schaefer
Department of Computer Science
University of Chicago
1100 East 58th Street
Chicago, Illinois 60637, USA
schaefer@cs.uchicago.edu

Abstract

In the Ramsey theory of graphs $F \rightarrow (G, H)$ means that for every way of coloring the edges of F red and blue F will contain either a red G or a blue H as a subgraph. The problem ARROWING of deciding whether $F \rightarrow (G, H)$ lies in $\Pi_2^p = \text{coNP}^{\text{NP}}$ and it was shown to be **coNP**-hard by Burr [1]. We prove that ARROWING is actually Π_2^p-complete, simultaneously settling a conjecture of Burr and providing a natural example of a problem complete for a higher level of the polynomial hierarchy. We also consider several specific variants of ARROWING, where G and H are restricted to particular families of graphs. We have a general completeness result for this case under the assumption that certain graphs are constructible in polynomial time.

Furthermore we show that STRONG ARROWING, the version of ARROWING for induced subgraphs, is Π_2^p-complete.

References

[1] Stefan A. Burr. On the computational complexity of ramsey-type problems. In Nešetřil & Rödl, editor, *Mathematics of Ramsey Theory*. Springer-Verlag, 1990.

0-7695-0075-7/99 $10.00 © 1999 IEEE

The communication complexity of pointer chasing
Applications of entropy and sampling[3]

Stephen J. Ponzio[1]   Jaikumar Radhakrishnan[2]   S. Venkatesh[2]

1 The problem

The following pointer chasing problem plays a central role in the study of bounded round communication complexity. There are two players A and B. There are two sets of vertices V_A and V_B of size n each. Player A is given a function $f_A : V_A \to V_B$ and player B is given a function $f_B : V_B \to V_A$. In the problem g_k the players have to determine the vertex reached by applying f_A and f_B alternately, k times starting with a fixed vertex $v_0 \in V_A$. That is, in g_1, they must determine $f_A(v_0)$, in g_2 they must determine $f_B(f_A(v_0))$, in g_3 they must determine $f_A(f_B(f_A(v_0)))$, and so on. We will use the following notation: $C^{A,k}(f)$ $[C^{B,k}(f)]$ denotes the cost of the best k-round deterministic protocol for f in which player A [B] sends the first message. It is easy to see that $C^{A,k}(g_k)= k \log n$ but proving bounds for $C^{B,k}(g_k)$ is a much harder problem.

2 Main results of this paper

The pointer game, g_k. Although, the problem g_k was the first problem studied in bounded round communication complexity, the bounds for $C^{B,k}(g_k)$ are not tight. Damm, Jukna and Sgall [1] showed that $C^{B,k}(g_k) = O(n \log^{(k-1)} n)$ for any fixed k. Nisan and Wigderson [2] proved that $C^{B,k}(g_k)= \Omega(n)$ for any fixed k. Our first result shows that the protocol of Damm, Jukna and Sgall [1] is optimal upto a constant factor.

Theorem 1 *(a)* $C^{B,k}(g_k) = \Omega(n \log^{(k-1)} n)$ *for all fixed* k.

(b) $C^{B,k}_{1/3}(g_k) = \Omega(n \log^{(k-1)} n)$ *for all fixed* k.

Here, $C^{B,k}_{\epsilon}(f)$ denotes the cost of the best k-round ϵ-error randomized protocol for f when player B sends the first message.

[1] Integrated Objects, Boston, USA, email:ponzio@erols.com

[2] Computer Science Group, Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai 400005, email: {jaikumar,venkat}@tcs.tifr.res.in.

[3] Part of this work was done while Stephen Ponzio and Jaikumar Radhakrishnan were visiting The Hebrew University, Jerusalem.

The bit game, p_k. The problem g_k demands a $\log n$ bit answer; Suppose we consider a related problem where only the most significant bit of the answer is required. Let $p_k(f_A, f_B) = [g_k(f_A, f_B)]_o$, where b_o denotes the most significant bit of the Boolean vector b.

Theorem 2 *(a)* $C^{B,k-r}(p_k) = O((k-r-2)\log n + (r+1)n)$ *for* $r \le \frac{k}{2} - 1$.

(b) $C^{B,\frac{k}{2}}(p_k) = O(n \log^{(k/2-1)} n)$ *for all fixed* k.

The protocol in part 1 of the above theorem works only if more than $k/2$ rounds are allowed and uses linear number bits of communication for constant k. What if only $k/2$ rounds or less are available? Part 2 of the above theorem gives a $k/2$-round protocol which uses superlinear number of bits. Thus there is an abrupt jump at $r = k/2$. We next show that such an abrupt jump is unavoidable.

Theorem 3 *(a)* $C^{B,\frac{k}{2}}(p_k) = \omega(n)$ *for all fixed* k.

(b) $C^{B,\frac{k}{2}}_{1/3}(p_k) = \omega(n)$ *for all fixed* k.

The proof of Theorem 3(a) and 3(b) uses a *transfer lemma*, based on ideas that connect entropy and sampling. We believe that the techniques developed here are an important contribution of this work, and that this method will find other applications.

We also prove an upper bound for the s-pointer game, a generalization of the pointer game. We also mention some applications to circuit complexity.

References

[1] C. Damm, S. Jukna, J. Sgall: Some bounds on multiparty communication complexity of pointer jumping, *proceedings of the 13th STACS*, LNCS 1046, 1996, 643-654.

[2] N. Nisan, A. Wigderson: Rounds in communication complexity revisited, *SIAM journal of computing*, 22, 1993, 211-219.

0-7695-0075-7/99 $10.00 © 1999 IEEE

此为试读，需要完整PDF请访问：www.ertongbook.com