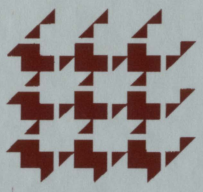


DIMACS

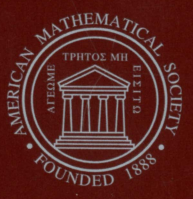
Series in Discrete Mathematics and Theoretical Computer Science

Volume 39

Proof Complexity and Feasible Arithmetics

DIMACS Workshop
April 21–24, 1996

Paul W. Beame
Samuel R. Buss
Editors



American Mathematical Society

Selected Titles in This Series

39 **Paul W. Beame and Samuel R. Buss, Editors,** Proof Complexity and Feasible Arithmetics

38 **Rebecca N. Wright and Peter G. Neumann, Editors,** Network Threats

37 **Boris Mirkin, F. R. McMorris, Fred S. Roberts, and Andrey Rzhetsky, Editors,** Mathematical Hierarchies and Biology

36 **Joseph G. Rosenstein, Deborah S. Franzblau, and Fred S. Roberts, Editors,** Discrete Mathematics in the Schools

35 **Dingzhu Du, Jun Gu, and Panos M. Pardalos, Editors,** Satisfiability Problem: Theory and Applications

34 **Nathaniel Dean, Editor,** African Americans in Mathematics

33 **Ravi B. Boppana and James F. Lynch, Editors,** Logic and random structures

32 **Jean-Charles Grégoire, Gerard J. Holzmann, and Doron A. Peled, Editors,** The SPIN verification system

31 **Neil Immerman and Phokion G. Kolaitis, Editors,** Descriptive complexity and finite models

30 **Sandeep N. Bhatt, Editor,** Parallel Algorithms: Third DIMACS Implementation Challenge

29 **Doron A. Peled, Vaughan R. Pratt, and Gerard J. Holzmann, Editors,** Partial Order Methods in Verification

28 **Larry Finkelstein and William M. Kantor, Editors,** Groups and Computation II

27 **Richard J. Lipton and Eric B. Baum, Editors,** DNA Based Computers

26 **David S. Johnson and Michael A. Trick, Editors,** Cliques, Coloring, and Satisfiability: Second DIMACS Implementation Challenge

25 **Gilbert Baumslag, David Epstein, Robert Gilman, Hamish Short, and Charles Sims, Editors,** Geometric and Computational Perspectives on Infinite Groups

24 **Louis J. Billera, Curtis Greene, Rodica Simion, and Richard P. Stanley, Editors,** Formal Power Series and Algebraic Combinatorics/Séries formelles et combinatoire algébrique, 1994

23 **Panos M. Pardalos, David I. Shalloway, and Guoliang Xue, Editors,** Global Minimization of Nonconvex Energy Functions: Molecular Conformation and Protein Folding

22 **Panos M. Pardalos, Mauricio G. C. Resende, and K. G. Ramakrishnan, Editors,** Parallel Processing of Discrete Optimization Problems

21 **D. Frank Hsu, Arnold L. Rosenberg, and Dominique Sotteau, Editors,** Interconnection Networks and Mapping and Scheduling Parallel Computations

20 **William Cook, László Lovász, and Paul Seymour, Editors,** Combinatorial Optimization

19 **Ingemar J. Cox, Pierre Hansen, and Bela Julesz, Editors,** Partitioning Data Sets

18 **Guy E. Blelloch, K. Mani Chandy, and Suresh Jagannathan, Editors,** Specification of Parallel Algorithms

17 **Eric Sven Ristad, Editor,** Language Computations

16 **Panos M. Pardalos and Henry Wolkowicz, Editors,** Quadratic Assignment and Related Problems

15 **Nathaniel Dean and Gregory E. Shannon, Editors,** Computational Support for Discrete Mathematics

14 **Robert Calderbank, G. David Forney, Jr., and Nader Moayeri, Editors,** Coding and Quantization: DIMACS/IEEE Workshop

13 **Jin-Yi Cai, Editor,** Advances in Computational Complexity Theory

12 **David S. Johnson and Catherine C. McGeoch, Editors,** Network Flows and Matching: First DIMACS Implementation Challenge

11 **Larry Finkelstein and William M. Kantor, Editors,** Groups and Computation

10 **Joel Friedman, Editor,** Expanding Graphs

9 **William T. Trotter, Editor,** Planar Graphs

(*Continued in the back of this publication*)

This page intentionally left blank

Proof Complexity and Feasible Arithmetics

This page intentionally left blank

https://doi.org/10.1090/dimacs/039

DIMACS

Series in Discrete Mathematics
and Theoretical Computer Science

Volume 39

Proof Complexity and Feasible Arithmetics

DIMACS Workshop
April 21–24, 1996

Paul W. Beame
Samuel R. Buss
Editors

NSF Science and Technology Center
in Discrete Mathematics and Theoretical Computer Science
A consortium of Rutgers University, Princeton University,
AT&T Labs, Bell Labs, and Bellcore

American Mathematical Society

This DIMACS volume contains papers from the DIMACS Workshop on Feasible Arithmetics and Length of Proofs, which was part of the DIMACS Special Year on Logic and Algorithms. The Workshop was held on April 21–24, 1996.

1991 *Mathematics Subject Classification.* Primary 03F20, 03F30, 03F50, 68Q15, 68R05, 03D15, 03–06, 68–06.

Library of Congress Cataloging-in-Publication Data

Proof complexity and feasible arithmetics : DIMACS workshop, April 21–24, 1996 / Paul W. Beame, Samuel R. Buss, editors.

p. cm. — (DIMACS series in discrete mathematics and theoretical computer science, ISSN 1052-1798 ; v. 39)

Papers from the proceedings of a workshop held in Rutgers, N. J.

Includes bibliographical references.

ISBN 0-8218-0577-0 (alk. paper)

1. Proof theory—Congresses. 2. Constructive mathematics—Congresses. 3. Computational complexity—Congresses. I. Beame, Paul W., 1959– II. Buss, Samuel R. III. Series.

QA9.54.P75 1997

511.3—dc21 97-29122

CIP

---

10 9 8 7 6 5 4 3 2 1 03 02 01 00 99 98

Contents

Foreword

The DIMACS Workshop on "Feasible Arithmetics and Length of Proofs" held in April 1996 was part of DIMACS Special Year on Logic and Algorithms. We would like to express our appreciation to Paul Beame and Sam Buss for their efforts to organize and plan this successful workshop as well as editing this volume of papers.

The workshop was part of the broader Special Year on Logic and Algorithms program which focused on computer aided verification, finite models, and proof complexity. The special year encouraged collaborations among very different research communities and this volume records one of many workshops in which this was achieved. We also extend our thanks to Eric Allender, Robert Kurshan, and Moshe Vardi for their work over many months as special year organizers.

DIMACS gratefully acknowledges the generous support that makes these programs possible. The National Science Foundation, through its Science and Technology Center program, the New Jersey Commission on Science and Technology, DIMACS partners at Rutgers, Princeton, AT&T Labs, Bell Labs, and Bellcore generously supported the special year.

Fred S. Roberts
Director

Bernard Chazelle
Co-Director for Princeton

Stephen R. Mahaney
Associate Director for Research

This page intentionally left blank

Preface

The complexity of proofs in propositional logic and the properties of feasible theories of arithmetic are closely related and give important and strong connections between logical properties and the properties of computational complexity classes.

Defining the proof complexity of logical formulas requires the specification of a particular *proof system* that determines the expressive power of and the relationships between the objects that may be used in their proofs. In addition, a proof system includes an efficient mechanism for checking the validity of proofs. Within such a proof system, the proof complexity of a formula is typically measured as the amount of space required to write down a proof. The study of proof complexity seeks to understand the complexity of proofs of formulas in specific proof systems, classify the relative complexity of proofs of formulas within different proof systems, and to develop better proof systems. For example, a major open question in proof complexity, equivalent to the NP versus co-NP problem, is whether or not there is a proof system in which all propositional tautologies have polynomial-size proofs.

Feasible theories of arithmetic are first-order theories of arithmetic designed to have proof-theoretic strength closely corresponding to low-level computational classes from the polynomial-time or NC hierarchies. The most natural feasible theories of arithmetic have the property that the functions which are provably total in the theory are precisely the functions which are computable in some given natural complexity class. Furthermore, it is frequently the case that first-order proofs in feasible theories of arithmetic can be translated directly into propositional proofs. The primary goals of the study of feasible theories of arithmetic are to understand the computational implications of various proof-theoretic constructions and use these to characterize complexity classes, and to establish connections between the logical properties of feasible theories and open problems in computational complexity. It is hoped that the study of feasible theories will ultimately yield useful new complexity results.

Over the last dozen years there has been substantial progress in proof complexity and feasible arithmetic as the two have grown together and have also benefited from a very productive cross-fertilization of techniques with Boolean circuit complexity. This progress has significantly broadened and deepened many connections of proof complexity and feasible arithmetic with computational complexity and greatly enriched both areas.

The papers in this volume represent the proceedings of a workshop on "Feasible Arithmetic and Proof Complexity" held at the DIMACS Institute at Rutgers, New Jersey on April 21-24, 1996. The principal speakers at this workshop included J. Avigad, P. Beame, S. Bellantoni, S. Buss, J.-Y. Cai, A. Carbone, P. Clote, F. Ferreira, X. Fu, R. Impagliazzo, J. Johannsen, B. Kauffmann, J. Krajíček, D. Leivant,

A.A. Razborov, K. Regan, S. Riis, T. Pitassi, P. Pudlak, S. Rudich, G. Takeuti and D. Willard, and many of these speakers submitted talks to this volume. The papers primarily cover lower bounds on the complexity of propositional proofs and meta-mathematical results on feasible theories of arithmetics. All papers in this volume are refereed.

We wish to thank the DIMACS institute for their generous support in hosting and financing the workshop and the DIMACS staff for their help in organizing the meeting. We also thank the referees for the rigorous and thorough review of the articles.

Paul Beame and Sam Buss

Selected Titles in This Series

(*Continued from the front of this publication*)

8 **Simon Gindikin, Editor,** Mathematical Methods of Analysis of Biopolymer Sequences

7 **Lyle A. McGeoch and Daniel D. Sleator, Editors,** On-Line Algorithms

6 **Jacob E. Goodman, Richard Pollack, and William Steiger, Editors,** Discrete and Computational Geometry: Papers from the DIMACS Special Year

5 **Frank Hwang, Fred Roberts, and Clyde Monma, Editors,** Reliability of Computer and Communication Networks

4 **Peter Gritzmann and Bernd Sturmfels, Editors,** Applied Geometry and Discrete Mathematics, The Victor Klee Festschrift

3 **E. M. Clarke and R. P. Kurshan, Editors,** Computer-Aided Verification '90

2 **Joan Feigenbaum and Michael Merritt, Editors,** Distributed Computing and Cryptography

1 **William Cook and Paul D. Seymour, Editors,** Polyhedral Combinatorics

ISBN 0-8218-0577-0