Logical Foundations of Proof Complexity

This book treats bounded arithmetic and propositional proof complexity from the point of view of computational complexity. The first seven chapters include the necessary logical background for the material and are suitable for a graduate course.

Associated with each of many complexity classes are both a two-sorted predicate calculus theory, with induction restricted to concepts in the class, and a propositional proof system. The complexity classes range from AC^0 for the weakest theory up to the polynomial hierarchy. Each bounded theorem in a theory translates into a family of (quantified) propositional tautologies with polynomial size proofs in the corresponding proof system. The theory proves the soundness of the associated proof system.

The result is a uniform treatment of many systems in the literature, including Buss's theories for the polynomial hierarchy and many disparate systems for complexity classes such as AC^0, $AC^0(m)$, TC^0, NC^1, L, NL, NC, and P.

Stephen Cook is a professor at the University of Toronto. He is author of many research papers, including his famous 1971 paper "The Complexity of Theorem Proving Procedures," and the 1982 recipient of the Turing Award. He was awarded a Steacie Fellowship in 1977 and a Killam Research Fellowship in 1982 and received the CRM/Fields Institute Prize in 1999. He is a Fellow of the Royal Society of London and the Royal Society of Canada and was elected to membership in the National Academy of Sciences (United States) and the American Academy of Arts and Sciences.

Phuong Nguyen is a postdoctoral researcher at McGill University. He received his MSc and PhD degrees from University of Toronto in 2004 and 2008, respectively. He has been awarded postdoctoral fellowships by the Eduard Čech Center for Algebra and Geometry (the Czech Republic) and by the Natural Sciences and Engineering Research Council of Canada (NSERC).

PERSPECTIVES IN LOGIC

The *Perspectives in Logic* series publishes substantial, high-quality books whose central theme lies in any area or aspect of logic. Books that present new material not now available in book form are particularly welcome. The series ranges from introductory texts suitable for beginning graduate courses to specialized monographs at the frontiers of research. Each book offers an illuminating perspective for its intended audience.

The series has its origins in the old *Perspectives in Mathematical Logic* series edited by the Ω-Group for "Mathematische Logik" of the Heidelberger Akademie der Wissenchaften, whose beginnings date back to the 1960s. The Association for Symbolic Logic has assumed editorial responsibility for the series and changed its name to reflect its interest in books that span the full range of disciplines in which logic plays an important role.

For more information, see http://www.aslonline.org/books_perspectives.html

PERSPECTIVES IN LOGIC

Logical Foundations of Proof Complexity

STEPHEN COOK
University of Toronto

PHUONG NGUYEN
McGill University

ASSOCIATION FOR SYMBOLIC LOGIC

CAMBRIDGE UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore,
São Paulo, Delhi, Dubai, Tokyo

Cambridge University Press
32 Avenue of the Americas, New York, NY 10013-2473, USA

www.cambridge.org
Information on this title: www.cambridge.org/9780521517294

Association for Symbolic Logic
Richard A. Shore, Publisher
Department of Mathematics, Cornell University, Ithaca NY 14853
http://www.aslonline.org

First published 2010

Printed in the United States of America

A catalog record for this publication is available from the British Library.

Library of Congress Cataloging in Publication data

ISBN 978-0-521-51729-4 Hardback

CONTENTS

PREFACE

"Proof complexity" as used here has two related aspects: (i) the complexity of proofs of propositional formulas, and (ii) the study of weak (i.e., "bounded") theories of arithmetic. Aspect (i) goes back at least to Tseitin [109], who proved an exponential lower bound on the lengths of proofs in the weak system known as regular resolution. Later Cook and Reckhow [46] introduced a general definition of propositional proof system and related it to mainstream complexity theory by pointing out that such a system exists in which all tautologies have polynomial length proofs iff the two complexity classes ***NP*** and *co*-***NP*** coincide.

Aspect (ii) goes back to Parikh [88], who introduced the theory known as $\boldsymbol{I}\Delta_0$, which is Peano Arithmetic with induction restricted to bounded formulas. Paris and Wilkie advanced the study of $\boldsymbol{I}\Delta_0$ and extensions in a series of papers (including [90, 89]) which relate them to complexity theory. Buss's seminal book [20] introduced the much-studied interleaved hierarchies $\boldsymbol{S}_2^i$ and $\boldsymbol{T}_2^i$ of theories related to the complexity classes Σ_i^p making up the polynomial hierarchy. Clote and Takeuti [38] and others introduced a host of theories related to other complexity classes.

The notion of propositional translation, which relates aspects (i) and (ii), goes back to [39], which introduced the equational theory ***PV*** for polynomial time functions and showed how theorems of ***PV*** can be translated into families of tautologies which have polynomial length proofs in the extended Frege proof system. Later (and independently) Paris and Wilkie [90] gave an elegant translation of bounded theorems in the relativized theory $\boldsymbol{I}\Delta_0(R)$ to polynomial length families of proofs in the weak propositional system bounded-depth Frege. Krajíček and Pudlák [73] introduced a hierarchy of proof systems $\langle \boldsymbol{G}_i \rangle$ for the quantified propositional calculus and showed how bounded theorems in Buss's theory $\boldsymbol{T}_2^i$ translate into polynomial length proofs in $\boldsymbol{G}_i$.

The aim of the present book is, first of all, to provide a sufficient background in logic for students in computer science and mathematics to understand our treatment of bounded arithmetic, and then to give an original treatment of the subject which emphasizes the three-way relationship among complexity classes, weak theories, and propositional proof systems.

Our treatment is unusual in that after Chapters 2 and 3 (which present Gentzen's sequent calculus $\boldsymbol{LK}$ and the bounded theory $\boldsymbol{I}\Delta_0$) we present our theories using the two-sorted vocabulary of Zambella [112]: one sort for natural numbers and the other for binary strings (i.e., finite sets of natural numbers). Our point of view is that the objects of interest are the binary strings: they are the natural inputs to the computing devices (Turing machines and Boolean circuits) studied by complexity theorists. The numbers are there as auxiliary variables, for example, to index the bits in the strings and measure their length. One reason for using this vocabulary is that the weakest complexity classes (such as $\boldsymbol{AC}^0$) that we study do not contain integer multiplication as a function, and since standard theories of arithmetic include multiplication as a primitive function, it is awkward to turn them into theories for these weak classes. In fact, our theories are simpler than many of the usual single-sorted theories in bounded arithmetic, because there is only one primitive function $|X|$ (the length of X) for strings X, while the axioms for the number sort are just those for $\boldsymbol{I}\Delta_0$.

Another advantage of using the two-sorted systems is that our propositional translations are especially simple: they are based on the Paris-Wilkie method [90]. The propositional atoms in the translation of a bounded formula $\varphi(X)$ with a free string variable X simply represent the bits of X.

Chapter 5 introduces our base theory $\boldsymbol{V}^0$, which corresponds to the smallest complexity class $\boldsymbol{AC}^0$ which we consider. All two-sorted theories we consider are extensions of $\boldsymbol{V}^0$. Chapter 6 studies $\boldsymbol{V}^1$, which is a two-sorted version of Buss's theory $\boldsymbol{S}^1_2$ and is related to the complexity class $\boldsymbol{P}$ (polynomial time). Chapter 7 introduces propositional translations for some theories. These translate bounded predicate formulas to families of quantified Boolean formulas. Chapter 8 introduces "minimal" theories for polynomial time by a method which is used extensively in Chapter 9. Chapter 8 also presents standard results concerning Buss's theories $\boldsymbol{S}^i_2$ and $\boldsymbol{T}^i_2$, but in the form of the two-sorted versions $\boldsymbol{V}^i$ and $\boldsymbol{TV}^i$ of these theories. Chapter 9 is based on the second author's PhD thesis, and uses an original uniform method to introduce minimal theories for many complexity classes between $\boldsymbol{AC}^0$ and $\boldsymbol{P}$. Some of these are related to single-sorted theories in the literature. Chapter 10 gives more examples of propositional translations and gives evidence for the thesis that each theory has a corresponding propositional proof system which serves as a kind of nonuniform version of the theory.

One purpose of this book is to serve as a basis for a program we call "Bounded Reverse Mathematics". This is inspired by the Friedman/Simpson program Reverse Mathematics [101], where now "Bounded" refers to bounded arithmetic. The goal is to find the weakest theory capable of proving a given theorem. The theorems in question are those of interest in computer science, and in general these can be proved in weak

theories. From the complexity theory point of view, the idea is to find the smallest complexity class such that the theorem can be proved using concepts in that class. This activity not only sheds light on the role of complexity classes in proofs, it can also lead to simplified proofs. A good example is Razborov's [96] greatly simplified proof of Hastad's Switching Lemma, which grew out of his attempt to formalize the lemma using only polynomial time concepts. His new proof led to important new results in propositional proof complexity. Throughout the book we give examples of theorems provable in the theories we describe.

The first seven chapters of this book grew out of notes for a graduate course taught several times beginning in 1998 at the University of Toronto by the first author. The prerequisites for the course and the book are some knowledge of both mathematical logic and complexity theory. However, Chapters 2 and 3 give a complete treatment of the necessary logic, and the Appendix together with material scattered throughout should provide sufficient background in complexity theory. There are exercises sprinkled throughout the text, which are intended both to supplement the material presented and to help the reader master the material. The more difficult exercises are marked with an asterisk.

Two sources have been invaluable to the authors in writing this book. The first is Krajíček's monograph [72], which is an essential possession for anyone working in this field. The second source is Buss's chapters [27, 28] in the *Handbook of Proof Theory*. His chapter I provides an excellent introduction to the proof theory of $\boldsymbol{LK}$, and his chapter II provides a thorough introduction to the first-order theories of bounded arithmetic. And of course Buss's monograph [20] *Bounded Arithmetic* was the origin of much of the material in our book.

We are grateful to Sam Buss and Jan Krajíček not only for their books but also for their considerable encouragement and help during the lengthy process of writing our book.

This book includes valuable input from several students of the first author as well as material from their PhD theses. The students include (besides the second author) Antonina Kolokolova, Tsuyoshi Morioka, Steven Perron, and Michael Soltys.

We are indebted to many others who have provided us with feedback on earlier versions of the book. These include Noriko Arai, Toshi Arai, Anton Belov, Mark Braverman, Timothy Chow, Lila Fontes, Kaveh Ghasemloo, Remo Goetschi, Daniel Ivan, Emil Jeřábek, Akitoshi Kawamura, Markus Latte, Dai Tri Man Le, Leonid Libkin, Dieter van Melkebeek, Toni Pitassi, Francois Pitt, Pavel Pudlák, Alan Skelley, Robert Solovay, Neil Thapen, Alasdair Urquhart, and Daniel Weller.

Stephen Cook
Phuong Nguyen