

Cambridge University Press
978-0-521-51729-4 - Logical Foundations of Proof Complexity
Stephen Cook and Phuong Nguyen
Frontmatter
[More information](#)

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).

Cambridge University Press
978-0-521-51729-4 - Logical Foundations of Proof Complexity
Stephen Cook and Phuong Nguyen
Frontmatter
[More information](#)

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 Wissenschaften, 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.

Pavel Pudlak, Managing Editor
Mathematical Institute of the Academy of Sciences of the Czech Republic

Editorial Board

Michael Benedikt
Department of Computing Science, University of Oxford

Michael Glanzberg
Department of Philosophy, University of California, Davis

Carl G. Jockusch, Jr.
Department of Mathematics, University of Illinois at Urbana-Champaign

Michael Rathjen
School of Mathematics, University of Leeds

Thomas Scanlon
Department of Mathematics, University of California, Berkeley

Simon Thomas
Department of Mathematics, Rutgers University

ASL Publisher
Richard A. Shore
Department of Mathematics, Cornell University

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

Cambridge University Press
978-0-521-51729-4 - Logical Foundations of Proof Complexity
Stephen Cook and Phuong Nguyen
Frontmatter
[More information](#)

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
978-0-521-51729-4 - Logical Foundations of Proof Complexity
Stephen Cook and Phuong Nguyen
Frontmatter
[More information](#)

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>

© Association for Symbolic Logic 2010

This publication is in copyright. Subject to statutory exception
and to the provisions of relevant collective licensing agreements,
no reproduction of any part may take place without the written
permission of Cambridge University Press.

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

Cambridge University Press has no responsibility for the persistence or
accuracy of URLs for external or third-party Internet Web sites referred to in
this publication and does not guarantee that any content on such Web sites is,
or will remain, accurate or appropriate.

CONTENTS

| | |
|---|------|
| PREFACE | xiii |
| CHAPTER I. INTRODUCTION | 1 |
| CHAPTER II. THE PREDICATE CALCULUS AND THE SYSTEM LK | 9 |
| II.1. Propositional Calculus | 9 |
| II.1.1. Gentzen's Propositional Proof System PK | 10 |
| II.1.2. Soundness and Completeness of PK | 12 |
| II.1.3. PK Proofs from Assumptions | 13 |
| II.1.4. Propositional Compactness | 16 |
| II.2. Predicate Calculus | 17 |
| II.2.1. Syntax of the Predicate Calculus | 17 |
| II.2.2. Semantics of Predicate Calculus | 19 |
| II.2.3. The First-Order Proof System LK | 21 |
| II.2.4. Free Variable Normal Form | 23 |
| II.2.5. Completeness of LK without Equality | 24 |
| II.3. Equality Axioms | 31 |
| II.3.1. Equality Axioms for LK | 32 |
| II.3.2. Revised Soundness and Completeness of LK | 33 |
| II.4. Major Corollaries of Completeness | 34 |
| II.5. The Herbrand Theorem | 35 |
| II.6. Notes | 38 |
| CHAPTER III. PEANO ARITHMETIC AND ITS SUBSYSTEMS | 39 |
| III.1. Peano Arithmetic | 39 |
| III.1.1. Minimization | 44 |
| III.1.2. Bounded Induction Scheme | 44 |
| III.1.3. Strong Induction Scheme | 44 |
| III.2. Parikh's Theorem | 44 |
| III.3. Conservative Extensions of $\mathbf{I}\Delta_0$ | 49 |
| III.3.1. Introducing New Function and Predicate Symbols | 50 |
| III.3.2. $\overline{\mathbf{I}\Delta_0}$: A Universal Conservative Extension of $\mathbf{I}\Delta_0$ | 54 |
| III.3.3. Defining $y = 2^x$ and $\mathbf{BIT}(i, x)$ in $\mathbf{I}\Delta_0$ | 59 |
| III.4. $\mathbf{I}\Delta_0$ and the Linear Time Hierarchy | 65 |

| | | |
|-------------|---|-----|
| III.4.1. | The Polynomial and Linear Time Hierarchies | 65 |
| III.4.2. | Representability of <i>LTH</i> Relations | 66 |
| III.4.3. | Characterizing the <i>LTH</i> by IA_0 | 69 |
| III.5. | Buss's S_2^i Hierarchy: The Road Not Taken | 70 |
| III.6. | Notes | 71 |
| CHAPTER IV. | TWO-SORTED LOGIC AND COMPLEXITY CLASSES | 73 |
| IV.1. | Basic Descriptive Complexity Theory | 74 |
| IV.2. | Two-Sorted First-Order Logic | 76 |
| IV.2.1. | Syntax | 76 |
| IV.2.2. | Semantics | 78 |
| IV.3. | Two-Sorted Complexity Classes | 80 |
| IV.3.1. | Notation for Numbers and Finite Sets | 80 |
| IV.3.2. | Representation Theorems | 81 |
| IV.3.3. | The <i>LTH</i> Revisited | 86 |
| IV.4. | The Proof System LK^2 | 87 |
| IV.4.1. | Two-Sorted Free Variable Normal Form | 90 |
| IV.5. | Single-Sorted Logic Interpretation | 91 |
| IV.6. | Notes | 93 |
| CHAPTER V. | THE THEORY V^0 AND AC^0 | 95 |
| V.1. | Definition and Basic Properties of V^i | 95 |
| V.2. | Two-Sorted Functions | 101 |
| V.3. | Parikh's Theorem for Two-Sorted Logic | 104 |
| V.4. | Definability in V^0 | 106 |
| V.4.1. | Δ_1^1 -Definable Predicates | 115 |
| V.5. | The Witnessing Theorem for V^0 | 117 |
| V.5.1. | Independence Follows from the Witnessing Theorem for V^0 | 118 |
| V.5.2. | Proof of the Witnessing Theorem for V^0 | 119 |
| V.6. | \overline{V}^0 : Universal Conservative Extension of V^0 | 124 |
| V.6.1. | Alternative Proof of the Witnessing Theorem for V^0 | 127 |
| V.7. | Finite Axiomatizability | 129 |
| V.8. | Notes | 130 |
| CHAPTER VI. | THE THEORY V^1 AND POLYNOMIAL TIME | 133 |
| VI.1. | Induction Schemes in V^i | 133 |
| VI.2. | Characterizing P by V^1 | 135 |
| VI.2.1. | The "If" Direction of Theorem VI.2.2 | 137 |
| VI.2.2. | Application of Cobham's Theorem | 140 |
| VI.3. | The Replacement Axiom Scheme | 142 |
| VI.3.1. | Extending V^1 by Polytime Functions | 145 |
| VI.4. | The Witnessing Theorem for V^1 | 147 |
| VI.4.1. | The Sequent System $LK^2\text{-}\tilde{V}^1$ | 150 |

CONTENTS

ix

| | | |
|---|--|-----|
| VI.4.2. | Proof of the Witnessing Theorem for V^1 | 154 |
| VI.5. | Notes | 156 |
| CHAPTER VII. PROPOSITIONAL TRANSLATIONS | | 159 |
| VII.1. | Propositional Proof Systems | 160 |
| VII.1.1. | Treelike vs Daglike Proof Systems | 162 |
| VII.1.2. | The Pigeonhole Principle and Bounded Depth PK | 163 |
| VII.2. | Translating V^0 to bPK | 165 |
| VII.2.1. | Translating Σ_0^B Formulas | 166 |
| VII.2.2. | \tilde{V}^0 and $LK^2\text{-}\tilde{V}^0$ | 169 |
| VII.2.3. | Proof of the Translation Theorem for V^0 | 170 |
| VII.3. | Quantified Propositional Calculus | 173 |
| VII.3.1. | QPC Proof Systems | 175 |
| VII.3.2. | The System G | 175 |
| VII.4. | The Systems G_i and G_i^* | 179 |
| VII.4.1. | Extended Frege Systems and Witnessing in G_1^* | 186 |
| VII.5. | Propositional Translations for V^i | 191 |
| VII.5.1. | Translating V^0 to Bounded Depth G_0^* | 195 |
| VII.6. | Notes | 198 |
| CHAPTER VIII. THEORIES FOR POLYNOMIAL TIME AND BEYOND | | 201 |
| VIII.1. | The Theory VP and Aggregate Functions | 201 |
| VIII.1.1. | The Theory \widehat{VP} | 207 |
| VIII.2. | The Theory VPV | 210 |
| VIII.2.1. | Comparing VPV and V^1 | 213 |
| VIII.2.2. | VPV Is Conservative over VP | 214 |
| VIII.3. | TV^0 and the TV^i Hierarchy | 217 |
| VIII.3.1. | $TV^0 \subseteq VPV$ | 220 |
| VIII.3.2. | Bit Recursion | 222 |
| VIII.4. | The Theory $V^1\text{-HORN}$ | 223 |
| VIII.5. | TV^1 and Polynomial Local Search | 228 |
| VIII.6. | KPT Witnessing and Replacement | 237 |
| VIII.6.1. | Applying KPT Witnessing | 239 |
| VIII.7. | More on V^i and TV^i | 243 |
| VIII.7.1. | Finite Axiomatizability | 243 |
| VIII.7.2. | Definability in the V^∞ Hierarchy | 245 |
| VIII.7.3. | Collapse of V^∞ vs Collapse of PH | 253 |
| VIII.8. | RSUV Isomorphism | 256 |
| VIII.8.1. | The Theories S_2^i and T_2^i | 256 |
| VIII.8.2. | RSUV Isomorphism | 258 |
| VIII.8.3. | The $\#$ Translation | 260 |
| VIII.8.4. | The b Translation | 262 |
| VIII.8.5. | The RSUV Isomorphism between S_2^i and V^i | 263 |
| VIII.9. | Notes | 266 |

| | |
|--|-----|
| CHAPTER IX. THEORIES FOR SMALL CLASSES | 267 |
| IX.1. AC^0 Reductions | 269 |
| IX.2. Theories for Subclasses of P | 272 |
| IX.2.1. The Theories \widehat{VC} | 273 |
| IX.2.2. The Theory \widehat{VC} | 274 |
| IX.2.3. The Theory \overline{VC} | 278 |
| IX.2.4. Obtaining Theories for the Classes of Interest | 280 |
| IX.3. Theories for TC^0 | 281 |
| IX.3.1. The Class TC^0 | 282 |
| IX.3.2. The Theories VTC^0 , $\widehat{VTC^0}$, and $\overline{VTC^0}$ | 283 |
| IX.3.3. Number Recursion and Number Summation | 287 |
| IX.3.4. The Theory VTC^0V | 289 |
| IX.3.5. Proving the Pigeonhole Principle in VTC^0 | 291 |
| IX.3.6. Defining String Multiplication in VTC^0 | 293 |
| IX.3.7. Proving Finite Szpilrajn's Theorem in VTC^0 | 298 |
| IX.3.8. Proving Bondy's Theorem | 299 |
| IX.4. Theories for $AC^0(m)$ and ACC | 303 |
| IX.4.1. The Classes $AC^0(m)$ and ACC | 303 |
| IX.4.2. The Theories $V^0(2)$, $\widehat{V^0(2)}$, and $\overline{V^0(2)}$ | 304 |
| IX.4.3. The "onto" PHP and Parity Principle | 306 |
| IX.4.4. The Theory $VAC^0(2)V$ | 308 |
| IX.4.5. The Jordan Curve Theorem and Related Principles | 309 |
| IX.4.6. The Theories for $AC^0(m)$ and ACC | 313 |
| IX.4.7. The Modulo m Counting Principles | 316 |
| IX.4.8. The Theory $VAC^0(6)V$ | 318 |
| IX.5. Theories for NC^1 and the NC Hierarchy | 319 |
| IX.5.1. Definitions of the Classes | 320 |
| IX.5.2. BSV P and NC^1 | 321 |
| IX.5.3. The Theories VNC^1 , $\widehat{VNC^1}$, and $\overline{VNC^1}$ | 323 |
| IX.5.4. $VTC^0 \subseteq VNC^1$ | 326 |
| IX.5.5. The Theory VNC^1V | 333 |
| IX.5.6. Theories for the NC Hierarchy | 335 |
| IX.6. Theories for NL and L | 339 |
| IX.6.1. The Theories VNL , \widehat{VNL} , and \overline{VNL} | 339 |
| IX.6.2. The Theory $V^1\text{-KROM}$ | 343 |
| IX.6.3. The Theories VL , \widehat{VL} , and \overline{VL} | 351 |
| IX.6.4. The Theory VLV | 356 |
| IX.7. Open Problems | 358 |
| IX.7.1. Proving Cayley–Hamilton in VNC^2 | 358 |
| IX.7.2. VSL and $VSL \stackrel{?}{=} VL$ | 358 |
| IX.7.3. Defining $\lfloor X/Y \rfloor$ in VTC^0 | 360 |
| IX.7.4. Proving PHP and $Count_{m'}$ in $V^0(m)$ | 360 |
| IX.8. Notes | 360 |

CONTENTS

xi

| | |
|---|-----|
| CHAPTER X. PROOF SYSTEMS AND THE REFLECTION PRINCIPLE | 363 |
| X.1. Formalizing Propositional Translations | 364 |
| X.1.1. Verifying Proofs in TC^0 | 364 |
| X.1.2. Computing Propositional Translations in TC^0 | 373 |
| X.1.3. The Propositional Translation Theorem for TV^i | 377 |
| X.2. The Reflection Principle | 382 |
| X.2.1. Truth Definitions | 383 |
| X.2.2. Truth Definitions vs Propositional Translations | 387 |
| X.2.3. RFN and Consistency for Subsystems of G | 396 |
| X.2.4. Axiomatizations Using RFN | 403 |
| X.2.5. Proving p -Simulations Using RFN | 407 |
| X.2.6. The Witnessing Problems for G | 408 |
| X.3. VNC^1 and G_0^* | 410 |
| X.3.1. Propositional Translation for VNC^1 | 410 |
| X.3.2. The Boolean Sentence Value Problem | 414 |
| X.3.3. Reflection Principle for PK | 421 |
| X.4. VTC^0 and Threshold Logic | 428 |
| X.4.1. The Sequent Calculus PTK | 428 |
| X.4.2. Reflection Principles for Bounded Depth PTK | 433 |
| X.4.3. Propositional Translation for VTC^0 | 434 |
| X.4.4. Bounded Depth GTC_0 | 441 |
| X.5. Notes | 442 |
| APPENDIX A. COMPUTATION MODELS | 445 |
| A.1. Deterministic Turing Machines | 445 |
| A.1.1. L , P , $PSPACE$, and EXP | 447 |
| A.2. Nondeterministic Turing Machines | 449 |
| A.3. Oracle Turing Machines | 451 |
| A.4. Alternating Turing Machines | 452 |
| A.5. Uniform Circuit Families | 453 |
| BIBLIOGRAPHY | 457 |
| INDEX | 465 |

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 IA_0 , which is Peano Arithmetic with induction restricted to bounded formulas. Paris and Wilkie advanced the study of IA_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 S_2^i and 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 $IA_0(R)$ to polynomial length families of proofs in the weak propositional system bounded-depth Frege. Krajíček and Pudlák [73] introduced a hierarchy of proof systems $\langle G_i \rangle$ for the quantified propositional calculus and showed how bounded theorems in Buss’s theory T_2^i translate into polynomial length proofs in 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 LK and the bounded theory IA_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 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 IA_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 V^0 , which corresponds to the smallest complexity class AC^0 which we consider. All two-sorted theories we consider are extensions of V^0 . Chapter 6 studies V^1 , which is a two-sorted version of Buss’s theory S_2^1 and is related to the complexity class 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 S_2^i and T_2^i , but in the form of the two-sorted versions V^i and 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 AC^0 and 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 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