LOGICAL FOUNDATIONS OF PROOF COMPLEXITY

STEPHEN COOK AND PHUONG NGUYEN

September 3, 2008

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 [83], who proved an exponential lower bound on the lengths of proofs in the weak system known as regular resolution. Later Cook and Reckhow [34] introduced a general definition of propositional proof system and related it to main-stream 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 [67] who introduced the theory known as $\mathbf{I}\Delta_0$, which is Peano Arithmetic with induction restricted to bounded formulas. Paris and Wilkie advanced the study of $\mathbf{I}\Delta_0$ and extensions in a series of papers (including [68, 69]) which relate them to complexity theory. Buss's seminal book [12] introduced the much-studied interleaved hierarchies $\mathbf{S}_2^i$ and $\mathbf{T}_2^i$ of theories related to the complexity classes Σ_i^p making up the polynomial hierarchy. Clote and Takeuti [27] 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 [28], 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 [68] gave an elegant translation of bounded theorems in the relativized theory $\mathbf{I}\Delta_0(R)$ to polynomial length families of proofs in the weak propositional system bounded-depth Frege. Krajíček and Pudlák [56] introduced a hierarchy of proof systems $\langle \mathbf{G}_i \rangle$ for the quantified propositional calculus and showed how bounded theorems in Buss's theory $\mathbf{T}_2^i$ translate into polynomial length proofs in $\mathbf{G}_i$.

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 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 $\mathbf{I}\Delta_0$) we present our theories using the two-sorted vocabulary of Zambella [85]: 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 $\mathbf{AC}^0$) 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 $\mathbf{I}\Delta_0$.

Another advantage of using the two-sorted systems is that our propositional translations are especially simple: they are based on the Paris-Wilkie method [68]. 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 $\mathbf{V}^0$, which corresponds to the smallest complexity class $\mathbf{AC}^0$ which we consider. All two-sorted theories we consider are extensions of $\mathbf{V}^0$. Chapter 6 studies $\mathbf{V}^1$, which is a two-sorted version of Buss's theory $\mathbf{S}^1_2$ and is related to the complexity class $\mathbf{P}$ (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 $\mathbf{S}^i_2$ and $\mathbf{T}^i_2$, but in the form of the two-sorted versions $\mathbf{V}^i$ and $\mathbf{TV}^i$ 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 $\mathbf{AC}^0$ and $\mathbf{P}$. Some of these are related to single-sorted theories in the literature. Chapter 10 gives more examples of propositional translations and 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 [77], 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 [75] 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 lead 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.

Two sources have been invaluable for writing this book. The first is Krajíček's monograph [55], which is an essential possession for anyone working in this field. The second source is Buss's chapters [19, 20] in *Handbook of Proof Theory*. Chapter I provides an excellent introduction to the proof theory of **LK**, and Chapter II provides a thorough introduction to the first-order theories of bounded arithmetic.

The authors would like to thank the many students and colleagues who have provided us with feedback on earlier versions of this book.

CONTENTS

Chapter 1

INTRODUCTION

This book studies logical systems which use restricted reasoning based on concepts from computational complexity. One underlying motivation is to determine the complexity of the concepts needed to prove theorems of interest in computer science. The complexity classes of interest lie mainly between the basic class $\mathbf{AC}^0$(whose members are computed by polynomial-size families of bounded-depth circuits), and the polynomial hierarchy **PH**, and includes the sequence

$$\mathbf{AC}^0 \subset \mathbf{TC}^0 \subseteq \mathbf{NC}^1 \subseteq \mathbf{P} \subseteq \mathbf{PH} \tag{1}$$

where **P** is polynomial time. We associate with each of these classes a logical theory and a propositional proof system, where the proof system can be considered a nonuniform version of the universal (or sometimes the bounded) fragment of the theory. The functions definable in the logical theory are those associated with the complexity class, and (in some cases) the lines in a polynomial size proof in the propositional system express concepts in the complexity class. This three-way association for the above classes is depicted as follows:

	class	$\mathbf{AC}^0$	$\mathbf{TC}^0$	$\mathbf{NC}^1$	**P**	**PH**
(2)	theory	$\mathbf{V}^0$	$\mathbf{VTC}^0$	$\mathbf{VNC}^1$	**VP**	$\mathbf{V}^\infty$
	system	$\mathbf{AC}^0$**-Frege**	$\mathbf{TC}^0$**-Frege**	**Frege**	**eFrege**	$\langle \mathbf{G}_i \rangle$

Consider, for example, the class $\mathbf{NC}^1$. The uniform version is **ALogTime**, the class of problems solvable by an alternating Turing machine in time $O(\log n)$. The definable functions in the associated theory $\mathbf{VNC}^1$ are the $\mathbf{NC}^1$ functions, i.e., those functions whose bit graphs are $\mathbf{NC}^1$ relations. A problem in nonuniform $\mathbf{NC}^1$ is defined by a polynomial-size family of log-depth Boolean circuits, or equivalently a polynomial-size family of propositional formulas. The corresponding propositional proof systems are called **Frege** systems, and are described in standard logic textbooks: a **Frege** proof of a tautology A consists of a sequence of propositional formulas ending in A, where each formula is either an axiom or follows from earlier formulas by a rule of inference. Universal theorems of $\mathbf{VNC}^1$ translate into polynomial-size families of **Frege** proofs. Finally, $\mathbf{VNC}^1$ proves the soundness of **Frege** systems, but not of any more powerful propositional proof system.

The famous open question in complexity theory is whether the conjecture that $\mathbf{P}$ is a proper subset of $\mathbf{NP}$ is in fact true (we know $\mathbf{P} \subseteq \mathbf{NP} \subseteq \mathbf{PH}$). If $\mathbf{P} = \mathbf{NP}$ then the polynomial hierarchy $\mathbf{PH}$ collapses to $\mathbf{P}$, but it is possible that $\mathbf{PH}$ collapses only to $\mathbf{NP}$ and still $\mathbf{P} \neq \mathbf{NP}$. What may be less well known is that not only is it possible that $\mathbf{PH} = \mathbf{P}$, but it is consistent with our present knowledge that $\mathbf{PH} = \mathbf{TC}^0$, so that all classes in (1) might be equal except $\mathbf{AC}^0$, which is known to be a proper subset of $\mathbf{TC}^0$. This is one motivation for studying the theories associated with these complexity classes, since it ought to be easier to separate the theories corresponding to the complexity classes than to separate the classes themselves (but so far the theories in (2) have not been separated, except for $\mathbf{V}^0$).

A common example used to illustrate the complexity of the concepts needed to prove a theorem is the Pigeonhole Principle (PHP). Our version states that if $n+1$ pigeons are placed in n holes, then some hole has two or more pigeons. We can present an instance of the PHP using a Boolean array $\langle P(i,j)\rangle$ $(0 \le i \le n,\ 0 \le j < n)$, where $P(i,j)$ asserts that pigeon i is placed in hole j. Then the PHP can be formulated in the theory $\mathbf{V}^0$ by the formula

(3)
$$\forall i \le n\, \exists j < n\, P(i,j) \supset \exists i_1, i_2 \le n\, \exists j < n\, (i_1 \neq i_2 \wedge P(i_1,j) \wedge P(i_2,j))$$

Ajtai [3] proved that this formula is not a theorem of $\mathbf{V}^0$, and also that the propositional version (which uses atoms p_{ij} to represent $P(i,j)$ and finite conjunctions and disjunctions to express the bounded universal and existential number quantifiers) does not have polynomial size $\mathbf{AC}^0$-**Frege** proofs. The intuitive reason for this is that a counting argument seems to be required to prove the PHP, but the complexity class $\mathbf{AC}^0$ cannot count the number of ones in a string of bits. On the other hand, the class $\mathbf{NC}^1$ can count, and indeed Buss proved that the propositional PHP does have polynomial size **Frege** proofs, and his method shows that (3) is a theorem of the theory $\mathbf{VNC}^1$. (In fact it is a theorem of the weaker theory $\mathbf{VTC}^0$.)

A second example comes from linear algebra. If A and B are $n \times n$ matrices over some field, then

$$AB = I \supset BA = I \qquad (4)$$

A standard proof of this uses Gaussian elimination, which is a polynomial-time process. Indeed Soltys showed that (4) is a theorem of the theory $\mathbf{VP}$ corresponding to polynomial-time reasoning, and its propositional translation (say over the field of two elements) has polynomial-size **eFrege** proofs. It is an open question whether (4) over $\mathbf{GF(2)}$ (or any field) can be proved in $\mathbf{VNC}^1$, or whether the propositional version has polynomial-size **Frege** proofs.

The preceding example (4) is a universal theorem, in the sense that its statement has no existential quantifier. Another class of examples comes from existential theorems. From linear algebra, a natural example about $n \times n$ matrices is

$$\forall A \exists B \neq 0 (AB = I \vee AB = 0) \tag{5}$$

The complexity of finding B for a given A, even over $\mathbf{GF(2)}$, is thought not to be in $\mathbf{NC}^1$ (it is hard for log space). Assuming that this is the case, it follows that (5) is not a theorem of $\mathbf{VNC}^1$, since only $\mathbf{NC}^1$ functions are definable in that theory. This conclusion is the result of a general witnessing theorem, which states that if the formula $\forall x \exists y \varphi(x, y)$ (for suitable formulas φ) is provable in the theory associated with complexity class $\mathbf{C}$, then there is a Skolem function $f(x)$ whose complexity is in $\mathbf{C}$ and which satisfies $\forall x \varphi(x, f(x))$.

The theory $\mathbf{VNC}^1$ proves that (4) follows from (5), and both (4) and (5) are theorems of the theory $\mathbf{VP}$ associated with polynomial time.

Another example of an existential theorem is "Fermat's Little Theorem", which states that if n is a prime number and $1 \leq a < n$, then $a^{n-1} \equiv 1 \pmod{n}$. Its existential content is captured by its contrapositive form

$$(1 \leq a < n) \wedge (a^{n-1} \not\equiv 1 \pmod{n}) \supset \exists d (1 < d < n \wedge d | n) \tag{6}$$

It is not hard to see that the function $a^{n-1} \bmod n$ can be computed in time polynomial in the lengths of a and n, using repeated squaring. If (6) is provable in $\mathbf{VP}$, then by the witnessing theorem mentioned above it would follow that there is a polynomial time function $f(a, n)$ whose value $d = f(a, n)$ provides a proper divisor of n whenever a, n satisfy the hypothesis in (6). With the exception of the so-called Carmichael numbers, which can be factored in polynomial time, every composite n satisfies the hypothesis of (6) for at least half of the values of a, $1 \leq a < n$. Hence $f(a, n)$ would provide a probabilistic polynomial time algorithm for integer factoring. Such an algorithm is thought unlikely to exist, and would provide a method for breaking the RSA public-key encryption scheme.

Thus Fermat's Little Theorem is not provable in $\mathbf{VP}$, assuming that there is no probabilistic polynomial time factoring algorithm.

Propositional tautologies can be used to express universal theorems such as (3) (in which the Predicate P is implicitly universally quantified and the bounded number quantifiers can be expanded in translation) and (4), but are not well suited to express existential theorems such as (5) and (6). However the latter can be expressed using formulas in the quantified propositional calculus (QPC), which extends the propositional calculus by allowing quantifiers $\forall P$ and $\exists P$ over propositional variables P. Each of the complexity classes in (2) has an associated QPC system, and in fact the systems $\langle \mathbf{G}_i \rangle$ mentioned for $\mathbf{PH}$ form a hierarchy of QPC systems.

Most of the theories presented in this book, including those in (2), have the same "second-order" underlying language $\mathcal{L}_A^2$, introduced by

Zambella. The language $\mathcal{L}_A^2$ is actually a language for the two-sorted first-order predicate calculus, where one sort is for numbers in $\mathbb{N}$ and the second sort is for finite sets of numbers. Here we regard an object of the second sort as a finite string over the alphabet $\{0, 1\}$ (the i-th bit in the string is 1 iff i is in the set). The strings are the objects of interest for the complexity classes, and serve as the main inputs for the machines or circuits that determine the class. The numbers serve a useful purpose as indices for the strings when describing properties of the strings. When they are used as machine or circuit inputs, they are presented in unary notation.

In the more common single-sorted theories such as Buss's hierarchies $\mathbf{S}_2^i$ and $\mathbf{T}_2^i$ the underlying objects are numbers which are presented in binary notation as inputs to Turing machines. Our two-sorted treatment has the advantage that the underlying language has no primitive operations on strings except the length function $|X|$ and the bit predicate $X(i)$ (meaning $i \in X$). This is especially important for studying weak complexity classes such as $\mathbf{AC}^0$. The standard language for single-sorted theories includes number multiplication, which is not an $\mathbf{AC}^0$ function on binary strings.

Chapter 2 provides a sufficient background in first-order logic for the rest of the book, including Gentzen's proof system **LK**. An unusual feature is our treatment of anchored (or "free-cut-free") **LK**-proofs. The completeness of these restricted systems is proved directly by a simple term-model construction as opposed to the usual syntactic cut-elimination method. The second form of the Herbrand Theorem proved here has many applications in later chapters for witnessing theorems.

Chapter 3 presents the necessary background on Peano Arithmetic and its subsystems, including the bounded theory $\mathbf{I}\Delta_0$. The functions definable in $\mathbf{I}\Delta_0$ are precisely those in the complexity class known as **LTH** (the Linear Time Hierarchy). An important theorem needed for this result is that the predicate $y = 2^x$ is definable in the language of arithmetic using a bounded formula (Subsection 3C.3). The universal theory $\overline{\mathbf{I}\Delta_0}$ has function symbols for each function in the Linear Time Hierarchy, and forms a conservative extension of $\mathbf{I}\Delta_0$. This theory serves as a prototype for universal theories defined in later chapters for other complexity classes.

Chapter 4 introduces the syntax and intended semantics for the two-sorted theories, which will be used throughout the remaining chapters. Here Σ_0^B is defined to be the class of formulas with no string quantifiers, and with all number quantifiers bounded. The Σ_1^B-formulas begin with zero or more bounded existential string quantifiers followed by a Σ_0^B-formula, and more generally Σ_i^B-formulas begin with at most i alternating blocks of bounded string quantifiers $\exists\forall\exists\ldots$. Representation theorems are proved which state that formulas in the syntactic class Σ_0^B

represent precisely the (two-sorted) $\mathbf{AC}^0$ relations, and for $i \geq 1$, formulas in Σ_i^B represent the relations in the i-th level of the polynomial hierarchy.

Chapter 5 introduces the hierarchy of two-sorted theories $\mathbf{V}^0 \subset \mathbf{V}^1 \subseteq \mathbf{V}^2 \subseteq \ldots$. For $\imath \geq 1$, $\mathbf{V}^i$ is the two-sorted version of Buss's single-sorted theory $\mathbf{S}_2^i$, which is associated with the ith level of the polynomial hierarchy. In this chapter we concentrate on $\mathbf{V}^0$, which is associated with the complexity class $\mathbf{AC}^0$. All two-sorted theories considered in later chapters are extensions of $\mathbf{V}^0$. A Buss-style witnessing theorem is proved for $\mathbf{V}^0$, showing that the existential string quantifiers in a Σ_1^B-theorem of $\mathbf{V}^0$ can be witnessed by $\mathbf{AC}^0$-functions. Since Σ_1^B-formulas have all string quantifiers in front, the proof is easier than for the usual Buss-style witnessing theorems. (The same applies to the witnessing theorems proved in later chapters.) The final section proves that $\mathbf{V}^0$ is finitely axiomatizable.

Chapter 6 concentrates on the theory $\mathbf{V}^1$, which is associated with the complexity class $\mathbf{P}$. All (and only) polynomial time functions are Σ_1^B-definable in $\mathbf{V}^1$. The positive direction is shown in two ways: by analyzing Turing machine computations and by using Cobham's characterization of these functions. The witnessing theorem for $\mathbf{V}^1$ is shown using (two-sorted versions of) the anchored proofs described in Chapter 2, and implies that only polynomial time functions are Σ_1^B-definable in $\mathbf{V}^1$.

Chapter 7 gives a general definition of propositional proof system. The goal is to associate a proof system with each theory so that each Σ_0^B-theorem of the theory translates into a polynomial size family of proofs in the proof system. Further the theory should prove the soundness of the proof system. In this chapter, translations are defined from $\mathbf{V}^0$ to bounded-depth $\mathbf{PK}$-proofs (i.e. bounded-depth Frege proofs), and also from $\mathbf{V}^1$ to extended Frege proofs. Systems $\mathbf{G}_i$ and $\mathbf{G}_i^\star$ for the quantified propositional calculus are defined, and for $i \geq 1$ we show how to translate bounded theorems of $\mathbf{V}^i$ to polynomial size families of proofs in the system $\mathbf{G}_i^\star$. The two-sorted treatment makes these translations simple and natural.

Chapter 8 begins by introducing other two-sorted theories associated with polynomial time. The finitely axiomatized theory $\mathbf{VP}$ and its universal conservative extension $\mathbf{VPV}$ both appear to be weaker than $\mathbf{V}^1$, although they have the same Σ_1^B theorems as $\mathbf{V}^1$. $\mathbf{VP} = \mathbf{TV}^0$ is the base of the hierarchy of theories $\mathbf{TV}^0 \subseteq \mathbf{TV}^1 \subseteq \ldots$, where for $i \geq 1$, $\mathbf{TV}^i$ is isomorphic to Buss's single-sorted theory $\mathbf{T}_2^i$. The definable problems in $\mathbf{TV}^1$ have the complexity of Polynomial Local Search. A form of the Herbrand Theorem known as KPT Witnessing is proved and applied to show independence of the Replacement axiom scheme from some theories, and to relating the collapse of the $\mathbf{V}^\infty$ hierarchy with the provable collapse of the polynomial hierarchy. The

Σ_j^B-definable search problems in $\mathbf{V}^i$ and $\mathbf{TV}^i$ are characterized for many i and j. The RSUV isomorphism theorem between $\mathbf{S}_2^i$ and $\mathbf{V}^i$ is proved.

See Table 1 page 239 for a summary of which search problems are definable in $\mathbf{V}^i$ and $\mathbf{TV}^i$.

Chapter 9 gives a uniform way of introducing minimal canonical theories for many complexity classes between $\mathbf{AC}^0$ and $\mathbf{P}$, including those mentioned earlier in (1). Each finitely axiomatized theory is defined as an extension of $\mathbf{V}^0$ obtained by adding a single axiom stating the existence of a computation solving a complete problem for the associated complexity class. The "minimality" of each theory is established by defining a universal theory whose axioms are simply the defining axioms for all the functions in the associated complexity class. These functions are defined as the function $\mathbf{AC}^0$-closure of the complexity class, or (as is the case for $\mathbf{P}$) using a recursion-theoretic characterization of the function class. The main theorem in each case is that the universal theory is a conservative extension of the finitely axiomatized theory.

Chapter 10 extends Chapter 7 by presenting quantified propositional proof systems associated with various complexity classes, and defining translations from the bounded theorems of the theories introduced in Chapter 9 to the appropriate proof system. The theories prove the (restricted) soundness of the associated proof system (this is the *reflection principle*).