Connecting Complexity Classes, Weak Formal Theories, and Propositional Proof Systems

Stephen A. Cook

University of Toronto
sacook@cs.toronto.edu

Abstract

This is a survey talk explaining the connection between the three items mentioned in the title.

1998 ACM Subject Classification F.1.3, F.4.1

Keywords and phrases Complexity Classes, Weak Formal Theories, Propositional Proof Systems

Digital Object Identifier 10.4230/LIPIcs.CSL.2012.9

Category Invited Talk

1 Overview

I've been interested in this three-way connection since my 1975 paper [7] in which I introduced the formal theory PV to capture polynomial time reasoning, and showed how each of its theorems can be translated into a polynomial size family of Extended Resolution proofs. The corresponding triple is $(\mathsf{P}, PV, \mathsf{ERes})$. I originally defined PV as an equational theory in which the function symbols range over all polynomial time functions on $\mathbb{N}$. The axioms consist of equations defining the polynomial time functions, based on Cobham's Theorem [6], and a rule giving "induction on notation"; i.e. induction based on binary notation for numbers. (Later Martin Dowd and others pointed out that ordinary induction on $\mathbb{N}$ can be derived from this rule, using binary search.) My idea for PV came from Skolem's 1923 equational theory based on function symbols for all primitive recursive functions.

The Extended Resolution proof system ERes was introduced by Tseitin [16], and is equivalent to Extended Frege systems [10]. ERes can be characterized roughly as the strongest propositional proof system whose soundness can be proved in PV. See [13] for much more on these ideas.

The theory PV can formalize the proofs of many theorems useful in computer science, such as the Pigeonhole Principle, Extended Euclidean Algorithm, Hall's Theorem, Menger's Theorem, and properties of integer (or rational) determinants. Each of these corresponds to a family of tautologies with polynomial size Extended Frege proofs. However it follows from the witnessing theorem for PV that no polynomial time algorithm for prime recognition (such as [1]) can be proved correct in PV unless there is a polynomial time algorithm for integer factorization.

Buss's influential 1986 book *Bounded Arithmetic* [4] introduced a hierarchy of first-order theories S^i_2 corresponding to the polynomial hierarchy. The functions Σ^b_1-definable in the base theory S^1_2 are the polynomial time functions, and Buss proved that $\mathsf{S}^1_2(PV)$ is Σ^b_1-conservative over PV (where now PV is regarded as a first-order theory axiomatized by the theorems of the original equational theory). Later [12] proved that (first-order) PV is properly included in $\mathsf{S}^1_2(PV)$, unless the polynomial hierarchy collapses. In particular $\mathsf{S}^1_2(PV)$ proves that integers can be factored as a product of primes, which is unlikely to be a consequence of PV.

Computer Science Logic 2012 (CSL'12).
Editors: Patrick Cégielski, Arnaud Durand; pp. 9–11

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

There are plenty of interesting complexity classes included in P which have been studied extensively, including

$$\mathsf{AC}^0 \subset \mathsf{AC}^0(2) \subset \mathsf{AC}^0(6) \subseteq \mathsf{TC}^0 \subseteq \mathsf{NC}^1 \subseteq \mathsf{LogSpace} \subseteq \mathsf{NL} \subseteq \mathsf{P}$$

The famous open question in complexity theory is $\mathsf{P} =?\mathsf{NP}$, but a more embarrassing open question is whether

$$\mathsf{NP} = \mathsf{P} = \mathsf{NL} = \mathsf{LogSpace} = \mathsf{NC}^1 = \mathsf{TC}^0 = \mathsf{AC}^0(6),$$

where as far as we know, the smallest class $\mathsf{AC}^0(6)$ cannot count the number of 1-bits in an input bit string. This is one motivation for studying small complexity classes: we need to separate them from NP before separating P from NP.

In [9] Phuong Nguyen and I develop a uniform way of associating each of these classes C with a theory VC and a suitable propositional proof system, which are connected like $(\mathsf{P}, PV, \mathsf{ERes})$ mentioned above. (The design of the propositional translation is inspired by [15].) The triple connecting NC^1 is especially interesting here since the associated propositional proof system is a 'Frege system'; i.e. a standard Hilbert style proof system for the propositional calculus. (Earlier Arai [3] connected NC^1 to Frege systems in a similar way, using a theory AID which is syntactically very different but logically equivalent to our theory VNC^1 [8].)

The theories in [9] use the two-sorted vocabulary developed by Zambella [17], in which variables of the number sort $x, y, z, \ldots$ range over $\mathbb{N}$, and those of the string sort $X, Y, Z, \ldots$ range over finite subsets of $\mathbb{N}$, interpreted as binary bit strings. The base theory V^0 corresponds to the complexity class AC^0. The two-sorted setting is ideal here, because (using the descriptive complexity characterization $\mathsf{AC}^0 = \mathsf{FO}$ [11]) we have the convenient fact that the bounded two-sorted Σ^B_0 formulas represent precisely the AC^0 relations. Part of the interest here is that of 'bounded reverse mathematics' [14], where the goal is to find the smallest complexity class C such that the corresponding theory VC proves a given combinatorial theorem. The standard example here is the Pigeonhole Principle, which can be proved in VTC^0 (and in VNC^1) but not in V^0, and in fact the corresponding tautology family does not have polynomial size proofs in the corresponding propositional proof system Bounded-Depth Frege [2] (but does have polynomial size Frege proofs [5]). There are many other interesting examples, but in most cases the lower bounds remain conjectures.

References

1 Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. *Annals of Mathematics*, 160(2):781–793, 2004.

2 Ajtai. The complexity of the pigeonhole principle. *Combinatorical*, 14(4):417–433, 1994.

3 Toshiyasu Arai. A bounded arithmetic AID for Frege systems. *Annals of Pure and Applied Logic*, 103(1–3):155–199, 2000.

4 Samuel Buss. *Bounded Arithmetic*. Bibliopolis, 1986.

5 Samuel Buss. Polynomial size proofs of the propositional pigeonhole principle. *Journal of Symbolic Logic*, 52:916–927, 1987.

6 A. Cobham. The intrinsic computational difficulty of functions. In Y. Bar-Hillel, editor, *Proceedings of the International Congress Logic, Methodology, and Philosophy of Science*, pages 24–30. North Holland, 1965.

7 Stephen Cook. Feasibly constructive proofs and the propositional calculus. *Proceedings of the 7th Annual ACM Symposium on Theory of computing*, pages 83–97, 1975.

8 Stephen Cook and Tsuyoshi Morioka. Quantified Propositional Calculus and a Second-Order Theory for NC^1. *Archive for Mathematical Logic*, 44(6):711–749, 2005.

9 Stephen Cook and Phuong Nguyen. *Logical Foundations of Proof Complexity*. Cambridge University Press, 2010. Draft available from URL `http://www.cs.toronto.edu/~sacook`.

10 Stephen Cook and Robert Reckhow. The relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44(1):36–50, 1979.

11 Neil Immerman. *Descriptive Complexity*. Springer, 1999.

12 J. Krajíček, P. Pudlák, and G. Takeuti. Bounded arithmetic and the polynomial hierarchy. *Annals of Pure and Applied Logic*, 52:143–153, 1991.

13 Jan Krajíček. *Bounded Arithmetic, Propositional Logic and Computational Complexity*. Cambridge University Press, 1995.

14 Phuong Nguyen. *Bounded Reverse Mathematics*. PhD thesis, University of Toronto, 2008. `http://www.cs.toronto.edu/~pnguyen/`.

15 Jeff B. Paris and Alex J. Wilkie. Counting problems in bounded arithmetic. In *Methods in Mathematical Logic*, number 1130 in Lecture Notes in Mathematics, pages 317–340. Springer, 1985.

16 G. S. Tseitin. On the complexity of derivation in propositional calculus. In A. O. Slisenko (Translated from Russian), editor, *Studies in Constructive Mathematics and Mathematical Logic, Part 2*, pages 115–125. Consultants Bureau, New Yor, London, 1970.

17 D. Zambella. Notes on polynomially bounded arithmetic. *Journal of Symbolic Logic*, 61(3):942–966, 1996.