Research Statement

Alan Skelley

December 2, 2006

1 Introduction

The motivation for my research is computational complexity. I am interested in many areas of theoretical computer science from algorithms to models of computation to structural complexity, but the fundamental question is always to understand the nature of computation and its complexities. This is a very broad arena, and yet has many deep interconnections; therefore, work in even the smallest area can be motivated by, and have repercussions to, the entire field.

My particular work is in the area of propositional proof complexity and bounded arithmetic. Not only are these subjects closely connected to the heart of complexity theory, they are also directly interesting in their own right: As an area of mathematics, the study of reasoning is surely as fundamental as the study of computation; and in practice, the use of automated theorem proving and other formal or mechanical forms of reasoning are becoming become more necessary to handle the vast amounts of data that mankind processes, to verify our increasingly complicated machinery and computer systems, and to assist in expanding the frontiers of mathematics. Below, I give some background into this area on the boundary of computation and logic, and discuss some past, current and future research.

2 Background and Past Work

The primary motivation for studying propositional proof systems is the theorem of Cook and Reckhow [8, 11] that NP=co-NP iff there exists a polynomially bounded proof system for propositional tautologies. Many proof systems are studied and there are some notable successes in the search for lower bounds, e.g. [13, 1], but this problem is very hard in general; nevertheless, there are many much more accessible problems than NP vs co-NP: at one end of the scale, the detailed study of weak proof systems and their interrelations, and at the other, capturing different forms of reasoning with stronger proof systems.

An alternative way of studying the power of different kinds of reasoning is through bounded arithmetic, initiated in 1971 by Parikh with his system $I\Delta_0$, similar to Peano Arithmetic, but with the important restriction of the induction scheme to Δ_0 (i.e., bounded) formulas. The first logical theory designed to reason about all "feasible," i.e. polynomial-time concepts, and only those concepts, was Cook's PV [10]. A fundamental property of PV is that its theorems translate to polynomial-size families of propositional proofs in a propositional proof system Extended Frege (EF), and the soundness of EF is provable in PV. A succession of work on this topic beginning with [17, 21, 22, 12] and especially [2] leaves us with many different theories of bounded arithmetic corresponding in interesting ways to many different complexity classes and propositional proof systems, but with the relationships intriguingly not tight.

Starting with Ignjatovic [14] and Zambella [31],[32], many authors have investigated second-order (two-sorted) arithmetic as a means to obtain theories with simpler axiomatizations; as computation is typically defined on strings, this makes bootstrapping the theory easier, and additionally allows capturing very weak complexity classes that may not even contain functions such as multiplication. Theories in this vein include V_1^1 for polynomial time [24] (later streamlined by Cook to V^1), and now many theories for classes such as V^0 for AC^0 [5], VTC^0 for TC^0 [20], V-Krom for NL [6], VNC^1 for NC^1 [7] and so on. The many analogues between first- and second-order theories are seen to be part of a pattern formalized in the RSUV isomorphism of Takeuti [30] and Razborov [23].

Some past work of mine has addressed the following topics:

- At the "high end" of the propositional proof system scale, in [25, 26] I present a new propositional proof system BPLK based on Boolean programs, a novel characterization of PSPACE due to Cook and Soltys [9]. I show that it is polynomially equivalent to G, a quantified propositional proof system for PSPACE reasoning containing levels corresponding to levels of the polynomial-time hierarchy [15, 18, 16, 4].
- Buss, Krajíček and Takeuti [3] capture strong complexity classes from levels of the EXP-time hierarchy, $\mathrm{EXP}^{\Sigma_{i-1}^p}$[wit,poly] and $\square_i^{exp}$:=$\mathrm{EXP}^{\Sigma_{i-1}^p}$, with Buss's strong theories U_2^i and V_2^i. Motivated by this work, in [27] I present a third-order theory W_1^1 for PSPACE. This theory inherits the advantages of the second-order "viewpoint" described above: namely a simpler axiomatization and direct reasoning about string-based computation, and has a higher (third) order to represent large objects such as computations of exponential-time machines. I also give a translation of certain theorems of this theory into BPLK.
- More recently in [28, 29], I describe a model of third-order computation that naturally extends ordinary (string-based) computation and give function calculi and recursion-theoretic characterizations of several large complexity classes including PSPACE and EXP. I extend the theory W_1^1 to obtain a hierarchy of theories corresponding to the levels of the EXP-time hierarchy even in the expanded sense of third-order computation. Starting with BPLK as a base, I then define propositional proof systems QBP_i by allowing quantifiers over Boolean functions, a natural extension of the notation. These systems have polynomial-sized proofs of translations of appropriate theorems of W_1^i.

3 Current Research and Future Directions

Here I briefly mention some specific problems and more general areas I look forward to working on in coming years. These problems form a nicely unified topic and are of fundamental interest on the boundary between propositional proof complexity and bounded arithmetic, yet many have been thus far been neglected by researchers.

The main question, phrased in the language of bounded arithmetic, is how the following three classes interact: the class of formulas allowed in the induction, the class of formulas used to define functions (i.e., prove totality), and the resulting complexity class of definable functions. Generally, the relationship is understood well only when the first two, namely the induction and the defining formulas, are of approximately the same class, and even then only for some specific classes. For example, in the case of Buss's hierarchy S_2, if Σ_i^b formulas are used for both then the resulting complexity class is functions from the $i-1$st level of the polynomial-time hierarchy, but if the classes of formulas differ by more than 2 levels or so, then the answer is not known. The complexity-theoretic consequences of various bounded arithmetic theories collapsing, or being distinct, are really consequences of what happens to specific fragments of those theories.

A first general problem, then, is to fill in some of the gaps in how this correspondence works, possibly by proving new witnessing theorems for existing theories, or by constructing new theories that correspond in novel ways to complexity classes, previously captured in this way or not. Another problem is to find theories that capture many complexity classes in a uniform way, for example all with Σ_1^B-definability. Also important to study is the witnessing problem for quantified propositional proof systems, which although related is different and not well studied. Work by Chiari and Krajíček has pointed to NP search problems as candidates for many witnessing problems but this is poorly understood.

Now, It is known that various fragments of bounded arithmetic theories can be axiomatized over S_2^1 by consistency statements of related subsystems of the quantified propositional calculus G. This characterization is frustrating to many researchers as it fails to give any insight into the combinatorial nature of the reasoning and computation involved. Recent work by Pudlák uses combinatorial principles related to games instead, and is an important new direction. In ongoing research, Pudlák, Neil Thapen and myself have some preliminary results directly linking Pudlák's combinatorial principles with existing results concerning search problems, in particular including a new characterization of the important class PLS, or polynomial local search. Most recently, in [19], Jan Krajíček, Neil Thapen and myself have obtained two alternative characterizations of the Σ_1^b consequences of T_2^2 and T_2^3: natural combinatorial principles related to PLS and involving colours of a directed graph, and a very different computational model of "verifiable recursion programs". These are the first combinatorial characterizations of these fragments, and we believe that both of them may generalize to the remaining theories of the bounded arithmetic hierarchy, which would be an important and long-sought characterization.

Next is the question of whether there is any complexity-theoretic consequence to collapsing the quantifier-free fragments of, say, two levels of Buss's S_2 hierarchy. Even for theories of greatly differing strength there is no reason why this could not happen. The corresponding question for propositional proof systems is whether different subsystems of the quantified propositional calculus G are equivalent for purely propositional tautologies, and there seems to be no evidence one way or the other. Possibly, existing techniques for propositional lower bounds could be adapted to this problem with the addition of a complexity assumption.

The related problem of relativized theories of bounded arithmetic and weaker propositional proof systems is well studied and there are many specific open problems concerning lower bounds and separation of theories. Although separations of the relativized hierarchy exist, one particular important problem is to obtain separations using principles of fixed quantifier complexity. Our Σ_1^b principles concerning recursive programs from [19] seem especially well suited for this as they precisely characterize the fragments of the theories in question. In ongoing research, we have some partial progress proving related propositional lower bounds for these principles.

Now a final example of problems in this area: in some cases, the propositional proof system corresponding to a complexity class has as lines in its proofs objects which are of exactly that complexity class (for example, G, EF) yet in other cases, the objects are of seemingly greater computational power (G_1, G_1^*). An interesting open problem is to find, for some of the latter type of examples, a canonical propositional proof system whose lines are exactly the appropriate complexity class. Perhaps a general technique could be devised to deal with many such classes at once, and a possible starting point is to study the systems obtained by restricting the cut rule to various classes such as $\Sigma_1^q \cup \Pi_1^q$. The more expressive formulas of the quantified propositional calculus are also a possible way to find better tautologies for some problems such as hex-reachability, previously studied by Buss, for which the current examples seem too easy to prove.

References

[1] M. Ajtai. The complexity of the pigeonhole principle. In *29th Annual Symposium on Foundations of Computer Science*, pages 346–355, White Plains, New York, 24–26 October 1988. IEEE.

[2] S. Buss. *Bounded Arithmetic*. Bibliopolis, Naples, 1986.

[3] Samuel Buss, Jan Krajíček, and Gaisi Takeuti. On provably total functions in bounded arithmetic theories R_3^i, U_2^i and V_2^i. In Peter Clote and Jan Krajíček, editors, *Arithmetic, proof theory and computational complexity*, pages 116–61. Oxford University Press, Oxford, 1993.

[4] Mario Chiari and Jan Krajíček. Witnessing functions in bounded arithmetic and search problems. *The Journal of Symbolic Logic*, 63(3):1095–1115, September 1998.

[5] S. Cook and A. Kolokolova. A second-order system for polytime reasoning using Grädel's theorem. In Joseph Halperin, editor, *16th Annual IEEE Symposium on Logic in Computer Science (LICS '01)*, pages 177–186. The IEEE Computer Society Press, June 2001.

[6] Stephen Cook and Antonina Kolokolova. A second-order theory for NL. In Harald Ganzinger, editor, *LICS04*, pages 398–407. IEEE Computer Society, July 2004.

[7] Stephen Cook and Tsuyoshi Morioka. Quantified propositional calculus and a theory for NC^1. *Archive for Mathematical Logic*, 2005. To Appear.

[8] Stephen Cook and Robert Reckhow. On the lengths of proofs in the propositional calculus (preliminary version). In *Conference Record of Sixth Annual ACM Symposium on Theory of Computing*, pages 135–148, Seattle, Washington, 30 April–2 May 1974.

[9] Stephen Cook and Michael Soltys. Boolean programs and quantified propositional proof systems. *Bulletin of the Section of Logic*, 28(3):119–129, 1999.

[10] Stephen A. Cook. Feasibly constructive proofs and the propositional calculus (preliminary version). In *Conference Record of Seventh Annual ACM Symposium on Theory of Computing*, pages 83–97, Albuquerque, New Mexico, 5–7 May 1975.

[11] Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44:36–50, 1979.

[12] Martin Dowd. *Propositional Representation of Arithmetic Proofs*. PhD thesis, University of Toronto, 1979.

[13] Armin Haken. The intractability of resolution. *Theoretical Computer Science*, 39(2–3):297–308, August 1985.

[14] Aleksandar Ignjatovic. Delineating classes of computational complexity via second order theories with weak set existence principles. I. *The Journal of Symbolic Logic*, 60(1):103–121, March 1995.

[15] Jan Krajíček and Pavel Pudlák. Propositional proof systems, the consistency of first order theories and the complexity of computations. *The Journal of Symbolic Logic*, 54(3):1063–1079, 1989.

[16] Jan Krajíček and Pavel Pudlák. Quantified propositional calculi and fragments of bounded arithmetic. *Zeitschr. f. Mathematikal Logik u. Grundlagen d. Mathematik*, 36(1):29–46, 1990.

[17] Jan Krajíček, Pavel Pudlák, and Gaisi Takeuti. Bounded arithmetic and the polynomial hierarchy. *Annals of Pure and Applied Logic*, 52(1–2):143–153, 1991.

[18] Jan Krajíček and Gaisi Takeuti. On bounded Σ^1_1 polynomial induction. In S. R. Buss and P. J. Scott, editors, *FEASMATH: Feasible Mathematics: A Mathematical Sciences Institute Workshop*, pages 259–80. Birkhauser, 1990.

[19] Jan Krajíček, Alan Skelley, and Neil Thapen. NP search problems in low fragments of bounded arithmetic. *The Journal of Symbolic Logic*. To appear.

[20] Phuong Nguyen and Stephen Cook. Theories for TC^0 and other small complexity classes. *Logical Methods in Computer Science*, 2005. To Appear.

[21] J. Paris and A. Wilkie. Counting problems in bounded arithmetic. In *Methods in Mathematical Logic*, volume 1130 of *LNM*, pages 317–40. Springer-Verlag, 1985.

[22] J. Paris and A. Wilkie. On the scheme of induction for bounded arithmetic formulas. *Annals of Pure and Applied Logic*, 35:261–302, 1987.

[23] Alexander A. Razborov. An equivalence between second order bounded domain bounded arithmetic and furst order bounded arithmetic. In Peter Clote and Jan Krajíček, editors, *Arithmetic, proof theory and computational complexity*, pages 247–77. Oxford University Press, Oxford, 1993.

[24] Alexander A. Razborov. Bounded arithmetic and lower bounds in complexity. In P. Clote and J. Remmel, editors, *Feasible Mathematics II*, pages 344–386. Birkhauser, 1995.

[25] Alan Skelley. Relating the PSPACE reasoning power of Boolean programs and quantified Boolean formulas. Master's thesis, University of Toronto, 2000. Available from ECCC in the 'theses' section.

[26] Alan Skelley. Propositional PSPACE reasoning with Boolean programs versus quantified Boolean formulas. In Josep Díaz, Juhani Karhumäki, Arto Lepistö, and Donald Sannella, editors, *ICALP04*, volume 3142 of *Lecture Notes in Computer Science*, pages 1163–1175. Springer, 2004.

[27] Alan Skelley. A third-order bounded arithmetic theory for PSPACE. In Jerzy Marcinkowski and Andrzej Tarlecki, editors, *CSL04*, volume 3210 of *Lecture Notes in Computer Science*, pages 340–354. Springer, 2004.

[28] Alan Skelley. *Theories and Proof Systems for PSPACE and the EXP-Time Hierarchy*. PhD thesis, University of Toronto, 2005. Available from ECCC in the 'theses' section.

[29] Alan Skelley. Third-order computation and bounded arithmetic. In Arnold Beckmann, Ulrich Berger, Benedikt Löwe, and John V Tucker, editors, *Logical Approaches to Computational Barriers (CiE 2006)*, Computer Science Report Series. University of Wales Swansea, 2006.

[30] Gaisi Takeuti. RSUV isomorphism. In Peter Clote and Jan Krajíček, editors, *Arithmetic, proof theory and computational complexity*, pages 364–86. Oxford University Press, Oxford, 1993.

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

[32] D. Zambella. End extensions of linearly bounded arithmetic. *Annals of Pure and Applied Logic*, 88, 1997.