Citations
From References: 3
From Reviews: 0

MR2775706 (2012c:03174) 03F30 03D15 03F20 68Q15

Kołodziejczyk, Leszek Aleksander (PL-WASW-IM);
Nguyen, Phuong [Nguyen, Phuong The] (CZ-AOS); **Thapen, Neil** (CZ-AOS)

The provably total NP search problems of weak second order bounded arithmetic. (English summary)

Ann. Pure Appl. Logic **162** (2011), *no. 6,* 419–446.

From the introduction: "An NP search problem is the problem of finding, given the parameter x, a witness y for a true $\forall\Sigma^b_1$ sentence, that is, a sentence of the form $\forall x \exists y < 2^{|x|^k} R(x,y)$, where R is decidable in polynomial time. If such a sentence is provable in a theory T, we would like to be able to extract from the proof an algorithm to solve the problem. In this way, we think of the set of NP search problems provably total in a theory, which we identify with the set of such sentences, as characterizing the algorithmic strength of the theory. This is analogous with the classification of classical fragments of PA by their provably recursive functions.

"A more satisfying characterization would be to classify the strength of the theories of the hierarchies [of bounded arithmetic] and beyond by describing, in a non-logical way, the class of algorithms needed to solve their provably total NP search problems, perhaps in terms of some class of machines built up out of polynomial time 'atoms' and based on a simple combinatorial principle. Again a guiding analogy here is the characterization of the provably recursive functions of fragments of PA in terms of primitive recursive functions and countable ordinals. . . .

"Our characterizations involve a 'local improvement' principle, LI, which is about labellings of a directed, acyclic, bounded-generated graph. We are given a scoring function that computes a 'score' for every node in the graph from the labels given to that node and its neighbours; an initial labelling which scores 0 everywhere; and an improvement function which allows us to increase the score of a node x by 1 if the score s of x under the current labelling is even and all predecessors of x already score $s+1$, or if the current score s is odd and successors already score $s+1$. The principle says that under these conditions, we can find labellings that give arbitrarily high scores.

"The principle can be thought of as an exponentially blown-up version of PLS: the solution space is the set of (exponential-sized) total labellings, and the cost of a labelling is the (exponential-sized) total assignment of scores to nodes that it generates. The improvement functions change a labelling to give you a 'better' cost. However, all functions work locally, on a finite part of a labelling at a time; this is what allows the principle to be written in a $\forall\Sigma^b_1$ way.

"In its full strength, LI captures the $\forall\Sigma^b_1$ consequences of V^1_2. If we restrict the score to be of at most polylogarithmic size in our parameters, and fix the graph to an interval $[0,a)$ with the usual ordering on it, the principle captures the $\forall\Sigma^b_1$ consequences of U^1_2. If we restrict the maximum score to a finite number k, and keep the graph as an interval, it corresponds to the game induction principle [. . .] and thus to the $\forall\Sigma^b_1$ consequences of T^k_2 (equivalently, of S^{k+1}_2); in particular for $k=1$ it can be seen to correspond to the 'exponentially long iteration' version of PLS.

"In this way we give new algorithmic/combinatorial characterizations of the strength of a large range of bounded arithmetic theories, in a uniform way (except, unfortunately, for the change in the topology of the underlying graph), over PV, a relatively weak base theory.

"The results mentioned above concern bounded arithmetic theories with the smash function, corresponding to the polynomial hierarchy and its extensions. But by a similar construction we can show that the principle LI captures precisely the Σ^B_0 consequences of V^1 over V^0, where V^1 is a 'linear' version of V^1_2 and V_0 has essentially the strength of $I\Delta_0$ . . . . Via the RSUV translation between one-sorted theories with the smash function and two-sorted theories without it, this can be seen as a new characterization of the '$\forall\Pi^b_1$ consequences of S^1_2' (previously known characterizations have usually been based on consistency statements for extended Frege and related propositional proof systems, although these can have an elegant combinatorial nature. . .). We would suggest that questions about the $\forall\Pi^b_1$ consequences of S^1_2 are more naturally studied in the second-order setting. This is because using the first-order setting leads to issues about finding a suitable language (for example, a language containing all polynomial time functions is too strong) and a suitable base theory (BASIC is too weak and PV too strong). V^0 provides a robust base theory which is substantially weaker than V^1, and studying the strength of V^1 over V^0 is analogous to studying complexity classes below P using AC^0-reductions."

Saeed Salehi

References

1. J. Avigad, Plausibly hard combinatorial tautologies, in: P. Beame, S. Buss (Eds.), Proof Complexity and Feasible Arithmetics, AMS, 1997, pp. 1–12. MR1486611 (99c:03081)
2. P. Beame, S. Cook, J. Edmonds, R. Impagliazzo, T. Pitassi, The relative complexity of NP search problems, Journal of Computer and System Sciences 57 (1) (1998) 3–19. MR1649804 (2000g:68045)
3. A. Beckmann, S. Buss, Polynomial local search in the polynomial hierarchy and witnessing in fragments of bounded arithmetic. Preprint, 2008. cf. MR 2011i:03064
4. J. Buresh-Oppenheim, T. Morioka, Relativized NP search problems and propositional proof systems, in: IEEE Conference on Computational Complexity, 2004, pp. 54–67.
5. S. Buss, Bounded Arithmetic, Bibliopolis, 1986. MR0880863 (89h:03104)
6. S. Buss, Chapter 1: An introduction to proof theory & Chapter 2: First-order proof theory of arithmetic, in: S. Buss (Ed.), Handbook of Proof Theory, Elsevier, 1998. MR1640325 (2000b:03200)
7. S. Buss, J. Krajíček, An application of Boolean complexity to separation problems in bounded arithmetic, Proceedings of the London Mathematical Society 69 (1994) 1–21. MR1272418 (96b:03074)
8. S. Cook, Feasibly constructive proofs and the propositional calculus, in: Proceedings of the 7th Annual ACM Symposium on Theory of computing, 1975, pp. 83–97. MR0502226 (58 #19341)
9. S. Cook, Bounded reverse mathematics, Plenary Lecture for CiE, 2007.
10. S. Cook, P. Nguyen, Logical Foundations of Proof Complexity, Cambridge University Press, 2010. MR2589550 (2011g:03001)
11. M. Fairtlough, S. Wainer, Hierarchies of provably recursive functions, in: S. Buss (Ed.), Handbook of Proof Theory, Elsevier, 1998. MR1640327 (2000a:03063)
12. F. Ferreira, What are the $\forall\sum^b_1$-consequences of T^1_2 and T^2_2? Annals of Pure and Applied Logic 75 (1) (1995) 79–88. MR1357472 (96j:03079)
13. E. Jeřábek, On theories of bounded arithmetic for NC^1, Annals of Pure and Applied Logic 162 (4) (2011) 322–340. MR2747052
14. D. Johnson, C. Papadimitriou, M. Yannakakis, How easy is local search?, Journal of Computer and System Sciences 37 (1) (1988) 79–100. MR0973658 (90d:68032)
15. J. Krajíček, Bounded Arithmetic, Propositional Logic and Computational Com-

plexity, Cambridge University Press, 1995. MR1366417 (97c:03003)

16. J. Krajíĉcek, On Frege and extended Frege proof systems, in: P. Clote, J. Remmel (Eds.), Feasible Mathematics II, Birkhäuser, 1995, pp. 284–319. MR1322280 (96a:03066b)
17. J. Krajíček, A. Skelley, N. Thapen, NP search problems in low fragments of bounded arithmetic, Journal of Symbolic Logic 72 (2) (2007) 649–672. MR2320295 (2008i:03068)
18. P. Nguyen, Bounded Reverse Mathematics, Ph.D. Thesis, University of Toronto, 2008. http://www.cs.toronto.edu/∼pnguyen/.
19. P. Pudlák, Fragments of bounded arithmetic and the lengths of proofs, Journal of Symbolic Logic 73 (4) (2008) 1389–1406. MR2467225 (2010b:03078)
20. A. Skelley, N. Thapen, The provably total search problems of bounded arithmetic, Preprint, 2007.
21. D. Zambella, Notes on polynomially bounded arithmetic, Journal of Symbolic Logic 61 (3) (1996) 942–966. MR1412519 (98b:03080)

Note: This list reflects references listed in the original paper as accurately as possible with no attempt to correct errors.