From Classical Proof Theory to P versus NP: a Guide to Bounded Theories

Iddo Tzameret
Royal Holloway, University of London, UK
http://www.cs.rhul.ac.uk/home/tzameret
Iddo.Tzameret@rhul.ac.uk

Abstract

This talk explores the question of what does logic and specifically proof theory can tell us about the fundamental hardness questions in computational complexity. We start with a brief description of the main concepts behind *bounded arithmetic* which is a family of weak formal theories of arithmetic that mirror in a precise manner the world of propositional proofs: if a statement of a given form is provable in a given bounded arithmetic theory then the same statement is suitably translated to a family of propositional formulas with short (polynomial-size) proofs in a corresponding propositional proof system.

We will proceed to describe the motivations behind the study of bounded arithmetic theories, their corresponding propositional proof systems, and how they relate to the fundamental complexity class separations and circuit lower bounds questions in computational complexity. We provide a collage of results and recent developments showing how bounded arithmetic and propositional proof complexity form a cohesive framework in which both concrete combinatorial questions about complexity as well as meta-mathematical questions about provability of statements of complexity theory itself, are studied.

Specific topics we shall mention are: (i) *The bounded reverse mathematics program* [2]: studying the weakest possible axiomatic assumptions that can prove important results in mathematics and computing (cf. [8, 4]), and the correspondence between circuit classes and theories. (ii) *The meta-mathematics of computational complexity*: what kind of reasoning power do we need in order to prove major results in complexity theory itself, and applications to complexity lower bounds (cf. [6, 7]). (iii) *Proof complexity*: the systematic treatment of propositional proofs as combinatorial and algebraic objects and their algorithmic applications (cf. [1, 5, 3]).

2012 ACM Subject Classification Theory of computation → Proof complexity; Theory of computation → Complexity theory and logic; Theory of computation → Circuit complexity; Theory of computation → Proof theory; Theory of computation → Algebraic complexity theory

Keywords and phrases Bounded arithmetic, complexity class separations, circuit complexity, proof complexity, weak theories of arithmetic, feasible mathematics

Digital Object Identifier 10.4230/LIPIcs.CSL.2020.5

Category Invited Talk

References

1 Samuel Buss. Towards NP-P via Proof Complexity and Search. *Annals of Pure and Applied Logic*, 163(7):906–917, 2012.

2 Stephen Cook and Phuong Nguyen. *Logical Foundations of Proof Complexity*. ASL Perspectives in Logic. Cambridge University Press, 2010.

3 Noah Fleming, Pravesh Kothari, and Toniann Pitassi. Semialgebraic Proofs and Efficient Algorithm Design. *Electronic Colloquium on Computational Complexity (ECCC)*, 26:106, 2019. URL: https://eccc.weizmann.ac.il/report/2019/106.

4 Pavel Hrubeš and Iddo Tzameret. Short Proofs for the Determinant Identities. *SIAM J. Comput.*, 44(2):340–383, 2015. (A preliminary version appeared in Proceedings of the 44th Annual ACM Symposium on the Theory of Computing (STOC'12)). doi:10.1137/130917788.

5 Tonnian Pitassi and Iddo Tzameret. Algebraic Proof Complexity: Progress, Frontiers and Challenges. *ACM SIGLOG News*, 3(3), 2016.

6 Alexander A. Razborov. Unprovability of lower bounds on circuit size in certain fragments of bounded arithmetic. *Izv. Ross. Akad. Nauk Ser. Mat.*, 59(1):201–224, 1995.

7 Rahul Santhanam and Jan Pich. Why are proof complexity lower bounds hard? In *60th Annual IEEE Symposium on Foundations of Computer Science FOCS 2019, November 9-12, 2019, Baltimore, Maryland USA*, 2019.

8 Iddo Tzameret and Stephen A. Cook. Uniform, integral and efficient proofs for the determinant identities. In *32nd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2017, Reykjavik, Iceland, June 20-23, 2017*, pages 1–12, 2017. doi:10.1109/LICS.2017.8005099.