Algebraic Proof Systems

Toniann Pitassi ✉
University of Toronto, Canada

Abstract

Given a set of polynomial equations over a field F, how hard is it to prove that they are simultaneously unsolvable? In the last twenty years, algebraic proof systems for refuting such systems of equations have been extensively studied, revealing close connections to both upper bounds (connections between short refutations and efficient approximation algorithms) and lower bounds (connections to fundamental questions in circuit complexity.)

The Ideal Proof System (IPS) is a simple yet powerful algebraic proof system, with very close connections to circuit lower bounds: [2] proved that lower bounds for IPS imply $VNP \neq VP$, and very recently connections in the other direction have been made, showing that circuit lower bounds imply IPS lower bounds [3, 1].

In this talk I will survey the landscape of algebraic proof systems, focusing on their connections to complexity theory, derandomization, and standard proposional proof complexity. I will discuss the state-of-the-art lower bounds, as well as the relationship between algebraic systems and textbook style propositional proof systems. Finally we end with open problems, and some recent progress towards proving superpolynomial lower bounds for bounded-depth Frege systems with modular gates (a major open problem in propositional proof complexity).

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

Keywords and phrases complexity theory, proof complexity, algebraic circuits

Digital Object Identifier 10.4230/LIPIcs.ICALP.2021.5

Category Invited Talk

References

1 Yaroslav Alekseev, Dima Grigoriev, Edward A. Hirsch, and Iddo Tzameret. Semi-algebraic proofs, IPS lower bounds, and the tau-conjecture: can a natural number be negative? In Konstantin Makarychev, Yury Makarychev, Madhur Tulsiani, Gautam Kamath, and Julia Chuzhoy, editors, *Proccedings of the 52nd Symposium on Theory of Computing, (STOC)*, pages 54–67. ACM, 2020.

2 Joshua A. Grochow and Toniann Pitassi. Circuit complexity, proof complexity, and polynomial identity testing: The ideal proof system. *J. ACM*, 65(6):37:1–37:59, 2018.

3 Rahul Santhanam and Iddo Tzameret. Iterated lower bound formulas: A diagonalization approach to proof co mplexity. In *Proceedings of the 53rd Symposium on Theory of Computing (STOC)*. ACM, 2021.

48th International Colloquium on Automata, Languages, and Programming (ICALP 2021).
Editors: Nikhil Bansal, Emanuela Merelli, and James Worrell; Article No. 5; pp. 5:1–5:1
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany