Edward Hirsch Technion

(Semi)algebraic proof complexity

Abstract:

A propositional proof system is roughly a polynomial-time procedure that checks certificates (proofs) for propositional tautologies (or another co-NP-complete language); thus, the existence of a proof system possessing polynomial-size proofs is equivalent to NP=co-NP. "Steve Cook's program" suggests considering more and more powerful specific proof systems and proving exponential lower bounds for them. An algebraic proof system proves that a system of polynomials $f_1,...,f_m$ has no common roots. For example, Hilbert's Nullstellensatz provides a certificate consisting of polynomials $g_1,...,g_m$ such that $\sum_i f_i g_i = 1$. A semialgebraic proof system can provide proofs of the infeasibility for a system of polynomial inequalities. Such proofs have been brought to proof complexity in the late 90s by Pavel Pudlak, who suggested a proof system based on the Lovasz--Schrijver optimization procedure, and by Dima Grigoriev and Nicolai Vorobjev, who suggested to use the Positivstellensatz theorem. After a short introduction to the field, I will show how close we are to converting semialgebraic proofs into algebraic proofs and prove an exponential lower bound conditioned on the Shub and Smale conjecture about computing $n!$. I will also speak on the latest developments. Main reference: 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? Proceedings of STOC'20.