Complexity, Proofs and Algebra

Iddo Tzameret

August 2, 2018

Abstract

This is a very short summary of some of my work.

My research lies broadly in the ***theory of computing***, where I am interested in all aspects of the foundations of computer science: from algorithms and complexity to provability and semantics. The overarching theme of my research is the phenomenon of computational intractability and the ways in which it can be leveraged. In particular, I work in *Computational Complexity* with an emphasis on satisfiability, proof complexity, the interplay between algebra and computation, applications of logic in computer science, and the theory (with direct connection to the practice) of SAT-solving.

My most notable contributions are in the study of *proof complexity*. Proof complexity is an interdisciplinary endeavor aiming to understand the computational resources required to prove statements. The general goal is to better understand which problems possess solutions with short correctness proofs and which do not. Central questions in this field are: *what is the most efficient way to prove the unsatisfiability of SAT instances*? *Or the insolvability of a collections of polynomial equations*? *Or the fact that the nodes of a given graph cannot be coloured with three colours, such that each edge connects two nodes with different colours*? Since the transcript of any complete algorithm for these problems also provides a proof of unsatisfiability (or insolvability, or non-3-colourability, resp.) in the case that the input instances are unsatisfiable, answering these or similar questions allows us, for example, to understand which families of algorithms can quickly solve routine engineering problems, for example problems that are central to software and hardware verification.

In that respect, some of my major contributions are in an area which I termed *Algebraic Proof Complexity* in my survey with T. Pitassi [PT16] appearing in the July 2016 ACM SIGLOG News' complexity column (*ed.* Neil Immerman). These contributions are: (**i**) Introducing (together with my students Li and Wang) the non-commutative characterisation of propositional proofs [CCC'15; invited to a special journal issue (declined in favour of SIAM Journal of Computing [LTW18]); see also Forbes-Shpilka-Tzameret-Wigderson CCC'16 [FSTW16]]—showing that any standard propositional proof is in fact a "disguised" straight-line parallel program for computing certain non-commutative functions. This seemingly surprising result is important since such straight-line programs are well understood, in contrast to standard (general) propositional proofs, on which almost no non-trivial complexity result is known to date. (**ii**) The development (with Hrubeš) of proof systems for polynomial identities with connections to derandomization theory [CCC'09, [HT09]]. The importance of this result is in identifying and analysing specific nondeterministic symbolic algorithms for testing polynomial identities. (**iii**) The solution (together with Hrubeš) of a longstanding open problem posed originally by Stephen Cook and Charles Rackoff about the proof complexity of the multiplicativity of the determinant function [STOC'12, [HT15]]. (**iv**) Considered a breakthrough in the field, this latter contribution has triggered a recent collaboration with Cook [LICS'17 [TC17]], in which we have essentially obtained the most constructive proof possible for basic statements of linear algebra.

In my aforementioned survey with Pitassi, I have laid out a detailed vision of the emerging Algebraic Proof Complexity programme. This programme is aimed to achieve (and partially already has achieved) a unified theory of proof complexity and algebraic complexity in which breakthroughs in our understanding of proof-length lower bounds can be obtained. This includes connections to major aspects of contemporary computational complexity: hardness results and connections to the complexity of the permanent function, connections to different algebraic computational models, derandomization theory (through polynomial identity testing) and feasible mathematics. The pathway towards this goal is to transfer the technology of algebraic circuit complexity into the area of proof complexity. The latter area is dominated by techniques from (probabilistic) combinatorics and Boolean circuits, and the goal is to complement this by using predominantly algebraic techniques.

In a different collection of works I have contributed to the study of *random k-SAT phenomena*, and its connection to refutation algorithms. For example, together with Müller [MT14] (see also Tzameret [Tza14, DT10]) I have identified *the weakest known* propositional proof system that can certify the unsatisfiability of almost all random 3-SAT formulas with sufficiently many clauses ("constraints"). This shows, for example, that resolution refutations—which form the basis for many contemporary industrial-level SAT-solvers—could be outperformed on almost all (randomly generated) instances by slightly stronger refutation systems.

Other research directions I am pursuing (or have pursued in the past) are constructive mathematics, provability and complexity in the framework of weak theories of arithmetic, Kolmogorov complexity and infinite combinatorics [ADF+13, RT08, DT03a, DT03b, Tza11, LT18, PT18].

References

[ADF+13] Eric Allender, George Davie, Luke Friedman, Sam Hopkins, and Iddo Tzameret. Kolmogorov complexity, circuits, and the strength of formal theories of arithmetic. *Chicago Journal of Theoretical Computer Science*, (5):1–15, 2013.

[DT03a] Nachum Dershowitz and Iddo Tzameret. Gap embedding for well-quasi-orderings. In Elaine Pimentel Ruy de Queiroz and Lucilia Figueiredo, editors, *Proceedings of the 10th Workshop on Logic, Language, Information and Computation (Wollic'03)*, volume 84 of *Electronic Notes in Theoretical Computer Science*. Elsevier, 2003.

[DT03b] Nachum Dershowitz and Iddo Tzameret. Gap embedding for well-quasi-orderings. *Electr. Notes Theor. Comput. Sci.*, 84:80–90, 2003.

[DT10] Nachum Dershowitz and Iddo Tzameret. Complexity of propositional proofs under a promise. *ACM Transactions on Computational Logic*, 11(3):1–30, 2010. Preliminary version appeared in *ICALP* '07, pp. 291–302.

[FSTW16] Michael A. Forbes, Amir Shpilka, Iddo Tzameret, and Avi Wigderson. Proof complexity lower bounds from algebraic circuit complexity. In *31st Conference on Computational Complexity, CCC 2016, May 29 to June 1, 2016, Tokyo, Japan*, pages 32:1–32:17, 2016.

[HT09] Pavel Hrubeš and Iddo Tzameret. The proof complexity of polynomial identities. In *Proceedings of the 24th Annual IEEE Conference on Computational Complexity, CCC 2009, Paris, France, 15-18 July 2009*, pages 41–51, 2009.

[HT15] 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)).

[LT18] Fu Li and Iddo Tzameret. Witnessing matrix identities and proof complexity. *International Journal of Algebra and Computation*, 28(2):217–256, 2018.

[LTW18] Fu Li, Iddo Tzameret, and Zhengyu Wang. Characterizing propositional proofs as noncommutative formulas. In *SIAM Journal on Computing*, volume 47, pages 1424–1462, 2018. Full Version: `http://arxiv.org/abs/1412.8746`.

[MT14] Sebastian Müller and Iddo Tzameret. Short propositional refutations for dense random 3CNF formulas. *Annals of Pure and Applied Logic*, 165:1864–1918, 2014. Extended abstract in Proceedings of the 27th Annual ACM-IEEE Symposium on Logic In Computer Science (LICS), 2012.

[PT16] Tonnian Pitassi and Iddo Tzameret. Algebraic proof complexity: Progress, frontiers and challenges. *ACM SIGLOG News*, 3(3), 2016.

[PT18] Fedor Part and Iddo Tzameret. Resolution with counting: Lower bounds over different moduli. *Electronic Colloquium on Computational Complexity (ECCC)*, 25:117, 2018.

[RT08] Ran Raz and Iddo Tzameret. The strength of multilinear proofs. *Computational Complexity*, 17(3):407–457, 2008.

[TC17] 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.

[Tza11] Iddo Tzameret. Algebraic proofs over noncommutative formulas. *Inf. Comput.*, 209(10):1269–1292, 2011.

[Tza14] Iddo Tzameret. Sparser random 3-SAT refutation algorithms and the interpolation problem - (extended abstract). In *Proceedings of the 41st International Colloquium on Automata, Languages and Programming (ICALP), track A*, pages 1015–1026, 2014.