Complexity of expander-based reasoning and the power of monotone proofs

Antonina Kolokolova*

May 29, 2018

Abstract

Some of the main successes in circuit complexity are the proofs of strong lower bounds on the complexity of monotone circuits. By analogy, one might expect that studying monotone reasoning would lead to similar lower bounds in proof complexity. Yet surprisingly, Atserias, Galesi and Pudlak have given a general quasipolynomial simulation of sequent calculus LK by its monotone fragment MLK. Moreover, their techniques give a polynomial simulation, provided properties of AKS sorting networks can be formalized inside LK. Such formalization was obtained in 2011 by Jerabek, assuming that the existence of certain expander graphs is provable in LK.

Several major results in complexity theory such as undirected graph reachability in logspace (Reingold, Rozenman-Vadhan) and monotone formulas for sorting (Ajtai-Komlos-Szemeredi sorting networks) are based on the properties of expander graphs. But what is the complexity such proofs? Many existing expander constructions rely on computationally non-trivial algebraic concepts for their analysis, such as spectral gap, even when constructions themselves are combinatorial.

In this work, we show that the existence of expanders of arbitrary size can be proven using NC^1 reasoning. We give a fully combinatorial analysis of an iterative construction of expanders using replacement product, powering and tensoring, and formalize this analysis in the bounded arithmetic system VNC^1. Combined with Atserias, Galesi, Pudlak'2002 and Jerabek'2011, this completes the proof that monotone LK is as powerful as LK for proving monotone sequents.

Based on joint work with Sam Buss, Valentine Kabanets and Michal Koucký.

Some of the greatest successes in proving lower bounds in complexity theory lie in the monotone world. From Razborov's classical monotone circuit lower bound for the CLIQUE problem [Raz85] to the recent exponential lower bound for a host of monotone models by Pitassi and Robere [PR17], strong monotone bounds are now known for numerous models and problems, both in the exact and approximate settings. It is natural to ask whether there is a similar phenomenon for suitably defined monotone proof systems. In 1994, Buss and Pudlák presented a monotone version of Frege system [PB94] and asked whether it can polynomially simulate the general Frege system on monotone sequents, proposing to use this framework to try to prove lower bounds. More specifically, they defined a monotone version of the sequent calculus LK, MLK: only a trivial monotone formula would be a tautology, but sequents $A \longrightarrow B$, even restricted to only monotone formulas on both sides, can represent a variety of interesting tautologies including the PigeonHolePrinciple (PHP).

However, subsequent results have chipped away at the hope of lower bounds in this model. First, Atserias, Galesi and Gavaldá [AGG01] have shown that the PHP and Clique-CoCLique have quasipolynomial size monotone sequent calculus proofs (thus giving exponential separation of MLK from Resolution, bounded-depth Frege and Cutting Planes restricted to polynomial coefficients). Building upon the machinery from this paper, Atserias, Galesi and Pudlák [AGP02] have shown that any proof of a monotone sequent in LK, no matter how non-monotone, can be turned into a monotone proof of size quasipolynomial in the original LK proof (they also gave a polynomial proof of the PHP, answering a question from [Pud99]). Moreover, the only part that required quasipolynomial blow-up was the proof of the properties of threshold formulas. To make the simulation of LK by MLK fully polynomial, they needed polynomial-size monotone threshold formulas with properties provable in LK; just non-monotone LK were sufficient.

*Department of Computer Science, Memorial University of Newfoundland, St. John's, NL, Canada, kol@mun.ca.

A construction of monotone threshold formulas of polynomial size has been known since 1983: the AKS sorting networks of Ajtai, Komlós, and Szemerédi [AKS83]. Already Pudlák [Pud99] wondered whether AKS sorting networks could be used to prove counting-based upper bounds in monotone sequent calculus. However, proving properties of AKS sorting networks in systems of low complexity was a daunting task. The construction of AKS sorting networks is highly non-trivial, with the added complexity from the use of expander graphs (essentially for derandomization). Yet in 2010 Jeřábek has shown that the properties of AKS sorting networks can, after all, be proven in LK (more specifically, in a corresponding theory of bounded arithmetic) – provided there is an LK proof of the existence of expander graphs with right parameters.

For most constructions of expander graphs, even when the constructions themselves are combinatorial, the proofs rely on the properties of the eigenvalues of the graph matrices – objects too complex to even talk about in LK. In this paper, we are able to show that it is possible to prove the existence of expander graphs without using algebraic concepts, by giving a fully combinatorial analysis of a variant of Reingold, Vadhan and Wigderson [RVW02]'s zig-zag construction of expanders (in particular, using arguments about mixing time of random walks instead of eigenvalues). Thus, we could show the existence of expander graphs needed for Jeřábek's AKS sorting networks in a way that is combinatorial enough to be formalizable in VNC^1, a theory of bounded arithmetic with proofs translatable to LK proofs of polynomial size.

This added the last piece of the puzzle, completing the proof that monotone sequent calculus is as powerful as full LK on monotone sequents: any LK proofs can be simulated in MLK with only a polynomial increase in size. Thus, in contrast to Boolean circuits where the monotonicity restriction drastically reduces the power of the model, making LK monotone does not result in a weaker system. It is still open, though, whether tree-like MLK is as powerful as full MLK (and thus LK): thus the question of Buss and Pudlák [PB94] of whether tree-like MLK is a suitable candidate for lower bound proofs remains unanswered.

References

[AGG01] Albert Atserias, Nicola Galesi, and Ricard Gavaldá. Monotone proofs of the pigeon hole principle. *Mathematical Logic Quarterly*, 47(4):461–474, 2001.

[AGP02] Albert Atserias, Nicola Galesi, and Pavel Pudlák. Monotone simulations of non-monotone proofs. *Journal of Computer and System Sciences*, 65(4):626–638, 2002.

[AKS83] Miklós Ajtai, Janós Komlós, and Endre Szemerédi. An $O(n \log n)$ sorting network. In *Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing*, pages 1–9. Association for Computing Machinery, 1983.

[PB94] Pavel Pudlák and Samuel R Buss. How to lie without being (easily) convicted and the lengths of proofs in propositional calculus. In *International Workshop on Computer Science Logic*, pages 151–162. Springer, 1994.

[PR17] Toniann Pitassi and Robert Robere. Strongly exponential lower bounds for monotone computation. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 1246–1255. ACM, 2017.

[Pud99] Pavel Pudlák. On the complexity of the propositional calculus. In S. Barry Cooper and John K.Editors Truss, editors, *Sets and Proofs:*, London Mathematical Society Lecture Note Series, page 197218. Cambridge University Press, Jun 1999.

[Raz85] A. A. Razborov. Lower bounds on the monotone complexity of some boolean functions. *Sov. Math. Dokl.*, 31:354–357, 1985.

[RVW02] Omer Reingold, Salil Vadhan, and Avi Wigderson. Entropy waves, the zig-zag graph product, and new constant-degree expanders. *Annals of Mathematics*, 155(1):157–187, 2002.