From Arithmetic to Boolean Circuit Lower Bounds

Pascal Koiran, LIP, ENS Lyon

October 26, 2017

Arithmetic circuits provide a natural model for computing polynomials. They are made of arithmetic ($+$, $\times$) gates instead of Boolean gates like the probably more familiar Boolean circuits. The method of partial derivatives [3] is one of the main lower bound methods for arithmetic circuits. This method and its generalizations (to "shifted partial derivatives") have led to many new results in recent years (consult for instance the online survey [4]). It is natural to ask whether these new results shed any light on old questions from Boolean circuit complexity. With this motivation in mind, a recent paper studies the power of arithmetic circuits with inputs restricted to the Boolean hypercube $\{0,1\}^n$ [2].

The goal of this internship is to find out whether we can obtain with this approach new proofs of old results from Boolean complexity, or perhaps even new results. Special attention will be given to Boolean circuits with modular gates, which have a natural connection to arithmetic circuits over finite fields.

If we only allow modular gates for a single prime modulus p, good lower bounds for constant depth circuits have been known for 30 years thanks to Razborov and Smolensky (see e.g. [1]). If several prime moduli can be used in the same circuit, the situation is much poorly understood: we only have the celebrated NEXP lower bound obtained a few years ago by Ryan Williams with very different methods [5].

References

[1] Sanjeev Arora, Boaz Barak. Computational Complexity - A Modern Approach. Cambridge University Press 2009.

[2] Michael A. Forbes, Mrinal Kumar, Ramprasad Saptharishi. Functional Lower Bounds for Arithmetic Circuits and Connections to Boolean Circuit Complexity. Conference on Computational Complexity 2016. arXiv preprint arXiv:1605.04207.

[3] Noam Nisan, Avi Wigderson. Lower Bounds on Arithmetic Circuits Via Partial Derivatives. Computational Complexity 6(3): 217-234 (1997).

[4] R. Saptharishi. A survey of lower bounds in arithmetic circuit complexity. github.com/dasarpmar/lowerbounds-survey/releases.

[5] Ryan Williams. Nonuniform ACC Circuit Lower Bounds. J. ACM 61(1): 2:1-2:32 (2014)