Lower bounds for univariate polynomials

advisors: Pascal Koiran and/or Natacha Portier
LIP*, École Normale Supérieure de Lyon, Université de Lyon

November 13, 2013

The cost of evaluating a polynomial can be measured by the number of arithmetic operations performed by an evaluation algorithm. This notion can be made precise using the model of arithmetic circuits. The internship will be devoted to the study of this arithmetic cost for univariate polynomials, and especially to lower bound techniques.

A univariate polynomial of degree d can always be evaluated with $O(d)$ arithmetic operations using Horner's rule, but some polynomials are much cheaper to evaluate. For instance, the cost of evaluating X^d is only $O(\log d)$. A polynomial (or more precisely, a family of polynomials) is sometimes called "easy to compute" if its cost is polynomial in $\log d$. Some explicit polynomials such as $\prod_{i=1}^{d}(X-i)$ are conjectured to be hard to compute, but almost no nontrivial lower bounds are known.

Given the difficulty of obtaining lower bounds for general arithmetic circuits, we will focus on a restricted class of circuits: we will try to obtain lower bounds for polynomials represented as "sums of products of sparse polynomials", i.e., as expression of the form

$$\sum_{i=1}^{k}\prod_{j=1}^{m} f_{ij}(X) \tag{1}$$

where the f_{ij} are given as sums of monomials. If t denotes the maximum number of monomials in one of the f_{ij}, the size of such an expression can be measured roughly by kmt (a more refined measure could also take into account the degrees of the f_{ij}). This representation is general enough to lead to challenging lower bound problems, but seems significantly weaker than general arithmetic circuits. For instance, the polynomial $(X+1)^d$ is easy to compute by arithmetic circuits, but it seems that it cannot be represented efficiently under form (1). This is an example of a concrete question which could be studied during the internship. More generally, the intern will try to apply existing lower bound techniques to this representation, will compare them and will possibly develop new lower bound techniques. Some promising approaches are as follows:

1. According to the "real τ-conjecture" [7], the number of real roots of a polynomial of the form (1) should be polynomially bounded in kmt. This

*UMR 5668 ENS Lyon, CNRS, UCBL, INRIA. Email: [Pascal.Koiran, Natacha.Portier]@ens-lyon.fr

suggests to deduce circuit lower bounds from upper number on the number of real roots [4].

2. Instead of bounding the number of real roots, one can try to bound the multiplicities of roots [6]. This approach seems particularly well-suited to the polynomial $(X+1)^d$. The *Wronskian determinant* seems to be an effective tool for bounding multiplicities [2] as well as real roots [8].

3. For multivariate polynomials, the method of partial derivatives is a well-established technique (see [3] for a survey); more generally, one can consider *shifted partial derivatives* [5]. One could try to adapt this method to univariate polynomials and compare it to the first two methods.

Finally, it should be pointed out that strong lower bounds for polynomials under form (1) imply strong lower bounds for the size of *general* arithmetic circuits computing the permanent polynomial [7]. This would give a solution to the algebraic version of the P versus NP problem proposed by Valiant [9] (see [1] for a book-length treatment of this topic).

References

[1] P. Bürgisser. *Completeness and Reduction in Algebraic Complexity Theory*. Number 7 in Algorithms and Computation in Mathematics. Springer, 2000.

[2] Arkadev Chattopadhyay, Bruno Grenet, Pascal Koiran, Natacha Portier, and Yann Strozecki. Computing the multilinear factors of lacunary polynomials without heights. Conference version: Factoring bivariate lacunary polynomials without heights (ISSAC 2012), 2013.

[3] Xi Chen, Neeraj Kayal, and Avi Wigderson. Partial derivatives in arithmetic complexity and beyond. *Foundations and Trends in Theoretical Computer Science*, 6(1):1–138, 2011.

[4] B. Grenet, P. Koiran, N. Portier, and Y. Strozecki. The limited power of powering: polynomial identity testing and a depth-four lower bound for the permanent. In *Proc. FSTTCS*, 2011. arxiv.org/abs/1107.1434.

[5] Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi. Approaching the chasm at depth four. In *Proceedings of the Conference on Computational Complexity (CCC)*, 2013.

[6] P. Hrubes. A note on the real τ-conjecture and the distribution of complex roots. *Theory of Computing*, 9(10):403–411, 2013. eccc.hpi-web.de/report/2012/121/.

[7] P. Koiran. Shallow circuits with high-powered inputs. In *Proc. Second Symposium on Innovations in Computer Science (ICS 2011)*, 2011. arxiv.org/abs/1004.4960.

[8] P. Koiran, N. Portier, and S. Tavenas. A Wronskian approach to the real τ-conjecture. Oral presentation at MEGA 2013. arxiv.org/abs/1205.1015, 2012.

[9] L. G. Valiant. Completeness classes in algebra. In *Proc. 11th ACM Symposium on Theory of Computing*, pages 249–261, 1979.