Reconstruction Algorithms and Combinatorial Geometry for Arithmetic Circuits

Advisor: Pascal Koiran*

November 23, 2022

The complexity of evaluating polynomials is still poorly understood even though this is one of the most studied algorithmic problems. Examples of interest include the determinant and permanent polynomials, or matrix multiplication (where the goal is to evaluate simultaneously the n^2 entries of the product of 2 matrices of size n). In the arithmetic circuit model, the complexity of an algorithm is measured by the number of arithmetic operations (additions and multiplications) performed on an input of size n. This is a very natural model for the study of polynomial evaluation. This internship proposal suggests several research problems connected to arithmetic circuit complexity. The student could work on one or several problems depending on his/her interests and the available time.

1 Reconstruction Algorithms

In recent years, a number of *reconstruction algorithms* for arithmetic circuits have been proposed. Here the goal is, given an input polynomial $f(x_1, \ldots, x_n)$, to find the smallest circuit computing f in some fixed class of circuits (usually a restricted class of circuits since the general case seems too hard given the current state of our knowledge). As an introduction to this subject we recommend reading the reconstruction algorithm for sums of powers of linear forms in Section 5 of [7], which is particularly simple and elegant. In research on *lower bounds,* the goal is to show that some explicit polynomials (such as for instance the permanent polynomial, or matrix multiplication) cannot be computed by any "small" circuit from some fixed circuit class. It turns out that the topics of lower bounds and reconstruction are closely related (see for instances sections 1.2 and 1.3 of [9]); in particular reconstruction methods often yields lower bounds.

Goal of the internship. Most of the known reconstruction algorithms use polynomial factorization as a subroutine [1, 3, 4, 6, 7, 8, 9, 15, 16]. This is quite natural since factoring f amounts to providing an arithmetic circuit for f with a multiplication gate at the top. Unfortunately, reconstruction algorithms often treat polynomial factorization as an atomic step that can be performed at unit cost. As a result, polynomial time running time bounds for these algorithms are often not available in the standard Turing machine model. One goal of the internship will be to firmly establish such bounds by taking the radical step of *removing all polynomial factorization subroutines from (some) reconstruction algorithms.* The advisor has been working successfully along these lines on the reconstruction of sums of powers of linear forms [14, 12]. In these two papers, polynomial

*Project MC2, LIP laboratory, Ecole Normale Supérieure de Lyon. Email: firstname.lastname@ens-lyon.fr.

factorization was replaced by standard linear algebra subroutines such as simultaneous matrix diagonalization. One goal for the student could be to obtain similar results for other classes of arithmetic circuits. For instance, can we handle polynomials of the form $f = g + h$ where g is a sum of powers of linearly independent linear forms (the model of [14, 12]) and h is a sum constantly many powers (the model of [1])? Or, can we remove polynomial factorization from [16]? The model for that paper is that of depth-3 arithmetic circuits with two multiplication gates, generalized in [6] to a constant number of multiplication gates,[1] and from finite fields to characteristic 0 in [17].

2 Combinatorial Geometry of Newton Polygons

Let $f(X,Y) = \sum_{i,j} c_{ij} X^i Y^j$ be a bivariate polynomial. We associate to each monomial of f with a nonzero coefficient ($c_{ij} \neq 0$) the point of the plane with coordinates (i,j). By definition, the Newton polygon $Newt(f)$ of f is the convex hull of this set of points. If f has t monomials, then its Newton polygon has at most t vertices and edges. It is known that Newton polygons behave well under product: $Newt(fg)$ is the *Minkowski sum* of $Newt(f)$ and $Newt(g)$. In particular, it has at most $2t$ vertices and edges if f and g have at most t monomials each. But what about sums of products? In the simplest version of this problem, we consider $Newt(fg+1)$ where f, g have at most t monomials each. The issue here is that adding 1 to fg might cancel the constant term of that product, thereby exposing monomials that were previously hidden inside $Newt(fg)$. Using tools from combinatorial geometry [2] we managed to obtain an $O(t^{4/3})$ upper bound [10, 18], improving significantly on the trivial quadratic upper bound. We also managed to obtain similar improvement for more general sums of products, and showed that a further improvement (the "τ-conjecture for Newton polygons") would yield very strong lower bounds for arithmetic circuits. Unfortunately, up to now this conjecture could not be proved nor refuted [5]; moreover, the $O(t^{4/3})$ upper bound for $Newt(fg+1)$ could not be improved nor proved optimal.

Goal of the internship. We will consider again simple expressions of the form $fg + 1$, assuming now that f has degree less than d and g has at most t monomials. Can the constraint on $\deg(f)$ help us obtain an upper bound for $Newt(fg+1)$? In other settings than the Newton polygon setting, similar "mixed constraints" (on the degree of f, and the number of monomials of g) have already proved fruitful [11, 13]. We will then move on to more complex expressions, for instance of the form $\sum_{i=1}^{k} f_i g_i$.

3 Student's background

For the reconstruction work, the student should be interested in algorithms and complexity and have some prior exposure to these subjects. He or she should be comfortable working with polynomials and with standard notions of linear algebra as taught for instance in "classes préparatoires" or in universities at the undergraduate level. More advanced notions could be learned as needed during the internship.

The work on Newton polygons is of a different nature. Although motivated by arithmetic circuit complexity, it is really a problem from combinatorial (convex) geometry. As such, we do not expect that a lot of algebra or experience with algorithms and complexity will be necessary.

[1] A mistake in [6] was recently corrected in [15].

References

[1] Vishwas Bhargava, Shubhangi Saraf, and Ilya Volkovich. Reconstruction Algorithms for Low-Rank Tensors and Depth-3 Multilinear Circuits. In *Proceedings of the 53rd Annual ACM Symposium on Theory of Computing*, 2021.

[2] Friedrich Eisenbrand, János Pach, Thomas Rothvoß, and Nir B. Sopher. Convexly independent subsets of the Minkowski sum of planar point sets. *Electr. J. Comb.*, 15(1), 2008.

[3] Ignacio García-Marco, Pascal Koiran, and Timothée Pecatte. Reconstruction algorithms for sums of affine powers. In *Proc. International Symposium on Symbolic and Algebraic Computation (ISSAC)*, pages 317–324, 2017.

[4] Ignacio García-Marco, Pascal Koiran, and Timothée Pecatte. Polynomial equivalence problems for sums of affine powers. In *Proc. International Symposium on Symbolic and Algebraic Computation (ISSAC)*, 2018.

[5] Pavel Hrubeš and Amir Yehudayoff. Shadows of Newton polytopes. In *36th Computational Complexity Conference (CCC 2021)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2021.

[6] Zohar Karnin and Amir Shpilka. Reconstruction of generalized depth-3 arithmetic circuits with bounded top fan-in. In *24th Annual IEEE Conference on Computational Complexity (CCC)*, pages 274–285, 2009.

[7] Neeraj Kayal. Efficient algorithms for some special cases of the polynomial equivalence problem. In *Symposium on Discrete Algorithms (SODA)*. Society for Industrial and Applied Mathematics, January 2011.

[8] Neeraj Kayal, Vineet Nair, Chandan Saha, and Sébastien Tavenas. Reconstruction of full rank algebraic branching programs. *ACM Transactions on Computation Theory (TOCT)*, 11(1):2, 2018.

[9] Neeraj Kayal and Chandan Saha. Reconstruction of non-degenerate homogeneous depth three circuits. In *Proc. 51st Annual ACM Symposium on Theory of Computing (STOC)*, pages 413–424, 2019.

[10] P. Koiran, N. Portier, S. Tavenas, and S. Thomassé. A τ-conjecture for Newton polygons. *Foundations of Computational Mathematics*, 15(1):185–197, 2015. arxiv.org/abs/1308.2286.

[11] Pascal Koiran, Natacha Portier, and Sébastien Tavenas. On the intersection of a sparse curve and a low-degree curve: A polynomial version of the lost theorem. *Discrete and Computational Geometry*, 53(1):48–63, 2015. http://arxiv.org/abs/1310.2447.

[12] Pascal Koiran and Subhayan Saha. Black Box Absolute Reconstruction for Sums of Powers of Linear Forms. In *Proceedings FSTTCS 2022. arXiv:2110.05305.*

[13] Pascal Koiran and Mateusz Skomra. Intersection multiplicity of a sparse curve and a low-degree curve. *Journal of Pure and Applied Algebra*, 224(7), 2020.

[14] Pascal Koiran and Mateusz Skomra. Derandomization and absolute reconstruction for sums of powers of linear forms. *Theoretical Computer Science*, 887, 2021. arXiv preprint arXiv:1912.02021.

[15] Shir Peleg, Amir Shpilka, and Ben Lee Volk. Tensor reconstruction beyond constant rank, 2022.

[16] Amir Shpilka. Interpolation of depth-3 arithmetic circuits with two multiplication gates. *SIAM Journal on Computing*, 38(6):2130–2161, 2009.

[17] Gaurav Sinha. Reconstruction of real depth-3 circuits with top fan-in 2. In *31st Conference on Computational Complexity*, 2016.

[18] S. Tavenas. *Bornes inférieures et supérieures dans les circuits arithmétiques*. PhD thesis, Ecole Normale Supérieure de Lyon, 2014.