PhD Research Proposal Form
China Scholarship Council (CSC)

A remplir en français ou en anglais en fonction de la langue qui sera utilisée pour la thèse

FIELD

Theoretical Computer Science

Thesis subject title: Lower bounds and reconstruction algorithms for arithmetic circuits.

Name of the French doctoral school/Ecole doctorale: InfoMaths

Name of the Research team/Equipe de recherche: research team MC2 / LIP laboratory
Website: http://www.ens-lyon.fr/LIP/MC2/

Name of the Supervisor/Directeur de thèse: Pascal Koiran
Email: pascal.koiran@ens-lyon.fr

Lab Language/ Langue de travail: English (French also suitable for day-to-day oral communication, but good written English is mandatory)

Research Proposal Abstract/Présentation du sujet: The proposed research belongs the field of algorithms and computational complexity theory. It is suitable for a computer science student with a strong background in theory, or for a math student who would like to switch to theoretical computer science.
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 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. Research on arithmetic circuits has focused in particular on reconstruction algorithms and lower bounds. The doctoral student could focus more on reconstruction, or more on lower bounds depending on his/her taste and progress of the work.

The goal of *a reconstruction algorithm* is, given an input polynomial $f(x_1,...,x_n)$, 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). The algorithm often has access to f only through function values $f(a_1,...,a_n)$ at certain sample points. This can be viewed therefore as an algebraic model of computational learning. As an introduction to this subject we recommend the reconstruction algorithm for sums of powers of linear forms in Section 5 of [4], 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 instance sections 1.2 and 1.3 of [6]); in particular reconstruction methods often yields lower bounds.

Work program: reconstruction. Most of the known reconstruction algorithms use polynomial factorization as a subroutine [1-6,8]. This is quite natural since factoring a polynomial 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 this project will be to firmly establish such bounds by taking the radical step of removing all polynomial factorization subroutines from (some) reconstruction algorithms. Along these lines, we have worked successfully on the reconstruction of sums of cubes of *linearly independent* linear forms [7], thereby removing polynomial factorization from the algorithm of [4]. In our approach, we view the reconstruction problem as a tensor decomposition problem which we solve with standard linear algebra subroutines such as simultaneous matrix diagonalization. The above model (sum of cubes of linear forms) is one of the simplest models of arithmetic circuits. In this project we will try to extend the results from [7] to more general models. One can try at first to generalize this tensor-based approach, but alternative approaches could be explored as well.

Work program: lower bounds. The set of polynomials that can be decomposed as sums of cubes of linearly independent linear forms is the orbit of the polynomial $x^3_1 + \cdots + x^3_n$ under the action of the general linear group. We plan to tackle lower bound problems by considering the closure (in the usual topological sense) of this orbit. This allows to get rid of the assumption of linear independence on the linear forms. Such orbit closures play a prominent in the Geometric Complexity Theory (GCT) program of Mulmuley and Sohoni. Their importance was already understood by Strassen in his work on the complexity of matrix multiplication. The originality of our approach is that our reconstruction algorithm gives a very explicit geometric description of the orbit. From this description one should be able to extract information about the orbit closure since an orbit completely determines its closure. A similar approach could also be pursued for more general models than sums of cubes.

References:

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.

6. 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.

7. Pascal Koiran and Mateusz Skomra. Derandomization and absolute reconstruction for sums of powers of linear forms. arXiv preprint arXiv:1912.02021, 2019.
8. Amir Shpilka. Interpolation of depth-3 arithmetic circuits with two multiplication gates. SIAM Journal on Computing, 38(6):2130–2161, 2009.

PLEASE SEND THE DOCUMENT TO
Direction des Affaires internationales : international.strategy@ens-lyon.fr