Master 2 Internships
Gröbner bases, the MinRank problem and algebraic cryptanalysis

We are seeking top candidates willing to prepare a PhD at the interface of computational mathematics, algebra, and their application areas.

Scientific context and positioning. Polynomial systems arise in many areas of engineering and computer science such as robotics, computer vision or cryptology. Solving such algebraic systems is known to be $\mathcal{NP}$-hard (even when the ground field has finite characteristic). Despite this intrinsic computational difficulty, many algorithms have been developed to solve polynomial systems with a flavour of algebraic methods (a.k.a. *computer algebra* methods), in order to circumvent numerical issues which are amplified by the non-linearity of these systems.

In this setting, Gröbner bases play a fundamental role. They are systems equivalent to the ones one wants to solve, but also provide greater ability to compute modulo the input equations (algebraically, this solves the ideal membership problem). Hence, the scientific community spent significant effort to obtain efficient Gröbner bases algorithms and implementations such as F4 and F5 [3, 4]. These reduce Gröbner bases computations to successive computations of row echelon forms of some well-chosen matrices. Analyzing the complexity of Gröbner bases algorithms is usually done with some suitable (but common) algebraic assumptions (such as regularity assumptions) by bounding the number of considered matrices and their sizes. These rough complexity analyses do not take into account amortized phenomena and the sparsity structure of those matrices.

One exception is [1] which accurately analyzes a variant of the F5 algorithm taking into account the sparsity structure of the matrices appearing during the computation and other properties derived from the so-called Hilbert series associated to some polynomial ideals (these provide some knowledge of their combinatorial properties). Still such an analysis is valid for polynomial systems satisfying regularity properties and cannot be applied to many of them which come from applications because of their specific structure.

Objectives of the internship. Such accurate complexity analysis of Gröbner bases is important not only from a theoretical point of view and for algorithmic purpose but also for areas such as cryptography where Gröbner bases can be used to assess the security of crypto-ciphers through *algebraic cryptanalysis*. In this framework, a family of polynomial systems which is of special interest is the so-called *MinRank* family. Such polynomial systems are the conjunctions of polynomial equations encoding the fact that some matrix, with polynomial entries, has maximum prescribed rank. For example, given a $p \times q$ matrix M with entries in $\mathbb{K}[x_1, \ldots, x_n]$ (where $\mathbb{K}$ is a field)

and $r < \min(p, q)$, we consider the simultaneous vanishing of the determinants of all $(r+1) \times (r+1)$ submatrices of M.

Note that systems with such determinantal structures can be used to encode critical points of some polynomial maps. Hence, they actually arise in a wider range of areas than cryptanalysis since critical points appear in optimization problems in robotics, biology and many other engineering sciences.

Solving determinantal systems through Gröbner bases has been studied in [5]. Results provided there allow one to bound the number of matrices and their sizes involved in the Gröbner basis computation through the identification of the so-called degree of regularity of determinantal ideals. More recently, the combinatorial structure of Gröbner bases of generic determinantal systems has been identified in [2]. Such results can be considered as a complexity analysis providing upper bounds on the number of arithmetic operations performed by all reasonable Gröbner basis algorithm for solving determinantal ideals. However, at the moment, there is no available analysis of the behaviour of the F5 algorithm. Indeed, assumptions needed to apply the results in [1] are not satisfied by generic determinantal systems. The main (and challenging) goal of this internship is to investigate the behaviour of the F5 algorithm for computing Gröbner bases on determinantal ideals and provide accurate complexity results.

First cases that will be studied are the easiest ones, i.e. those where determinantal ideals under consideration define a finite algebraic set which will be the basis of a more general analysis that can be applied to the so-called over-determined case which is of interest in algebraic cryptanalysis.

The case under consideration will require good knowledge of basic commutative algebra notions and their effective counterpart such as Gröbner bases (the internship will need to study properties of the syzygy module of determinantal ideals), combined with a taste for algorithms.

Scientific environment. This internship will be co-supervised by Vincent Neiger[1] and Mohab Safey El Din[2]. It will take place at Sorbonne University, in the computer science lab LIP6, which is located on the Pierre and Marie Curie campus, at the heart of Paris. The intern will be welcome in the PolSys team which develops and implements fast computer algebra algorithms for polynomial system solving and their applications. The intern will work in a kind and international environment gathering PhD students and Post-Docs representing 6 nationalities and animated with several working groups and a monthly seminar. All computing facilities will be provided.

How to apply. All interested applicants should send a full CV, a letter of motivation and the grades obtained during the last two years to

vincent.neiger@lip6.fr, mohab.safey@lip6.fr

References

[1] M. Bardet, J.-Ch. Faugère, and B. Salvy. On the complexity of the f5 gröbner basis algorithm. *Journal of Symbolic Computation*, 70:49–70, 2015.

[1] Sorbonne Université, vincent.neiger@lip6.fr
[2] Sorbonne Université, mohab.safey@lip6.fr

[2] J. Berthomieu, A. Bostan, A. Ferguson, and M. Safey El Din. Gröbner bases and critical values: The asymptotic combinatorics of determinantal systems. working paper or preprint, Apr. 2021.

[3] J.-Ch. Faugère. A New Efficient Algorithm for Computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139(1):61 – 88, 1999.

[4] J.-Ch. Faugère. A New Efficient Algorithm for Computing Gröbner Bases Without Reduction to Zero (F5). In *Proceedings ISSAC '02*, 2002.

[5] J.-Ch. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. On the complexity of the generalized minrank problem. *Journal of Symbolic Computation*, 55:30–58, 2013.