

Towards a new effective representation of polynomial systems of equations using Gröbner bases

We are seeking an excellent candidate for a 5 to 6-month research internship at the interface of computational mathematics and geometry, with the goal of opening the door towards developing new general-purpose tools in computer algebra.

The internship will be hosted by [PoLSys](#) team (Polynomial Systems) of [Sorbonne Université](#) and [CNRS](#).

Key words: Computer algebra, Gröbner bases, polynomial system solving

Gröbner bases and polynomial system solving

Polynomial systems of equations are able to model a wide variety of non-linear problems in the sciences, for example in robotics [10], in chemistry [8], in cryptography [12], and in optimization [4]. *Gröbner bases*, introduced by Buchberger in the 1960's [2], are the most widely used tool for the symbolic algorithmic treatment of polynomial systems. They form a central component of all modern computer algebra systems in this regard.

Following the view of Lazard [13], Gröbner bases can be understood as a form of *linearization* of a polynomial system: Out of a polynomial system of equations $F = 0$ one constructs several so-called *Macaulay matrices* [15], each associated to a degree d . These matrices are then echelonized, up to a certain degree D , and the rows of these echelonized matrices form the desired Gröbner basis. The central challenge in the computation of Gröbner bases comes from the fact that these Macaulay matrices rapidly grow in size with growing d and growing number of variables and that, moreover, the maximal degree D up to which these matrices need to be constructed is in the worst case doubly exponential in the number of variables of F [16]. This doubly exponential worst case bound stands in contrast to the good practical behavior of Gröbner bases which is also reflected in the fact that for “sufficiently random” systems F the maximum degree D becomes only *linear* in the number of variables and the degrees of the equations F . This striking discrepancy has as a consequence that, despite the fact that symbolic techniques are known which have a better controlled worst case complexity [14], Gröbner bases remain the practical tool of choice.

Furthermore, Macaulay matrices are usually *highly rank deficient*: During the echelonization, many rows will reduce to zero and thus not contribute to the resulting Gröbner bases. This has resulted in a significant effort to detect rows reducing to zero *before* echelonization, culminating in so-called *signature-based* Gröbner basis algorithms [6, 5].

As a consequence, several classes of polynomial systems of interest remain out of reach of a resolution via Gröbner basis computations. To give a prominent example, *matrix multiplication algorithms* for matrices of fixed size, constituting a currently highly active research field [11, 7] can be encoded as solutions of polynomial equations [1]. The number of involved variables and the high dimension of their solution sets, however, puts these techniques out of reach of state-of-the-art symbolic techniques.

Goal of the internship

The central goal of this internship is to take the first steps in the development of a new class of *probabilistic* Gröbner basis algorithms which seek to work around the two issues mentioned above. This will rely on two

ideas.

Witness sets. First, suppose that the solution set $\mathbf{V}(F)$ of $F = 0$ is *equidimensional* of positive dimension δ . This means essentially that $\mathbf{V}(F)$ does not consist of finitely many isolated points and does not have components of different dimension. For example, $\mathbf{V}(F)$ could consist of the union of two surfaces (so $\delta = 2$) but not of the union of a curve and a surface, i.e. a one- and two-dimensional component. It turns out that such a polynomial system F can be *probabilistically* represented by a so-called *witness set* W : This is a finite point sample on $\mathbf{V}(F)$ constructed by adjoining δ *random* linear equations to F , so W is a *zero-dimensional* representation of F , see also Figure 1. Such witness sets form one of the backbones of the *numerical* treatment of polynomial systems [18] and have been shown to form a desirable representation of F in symbolic computation from a complexity-theoretic point of view [9, 14]. Our first goal is to take some steps in combining such a witness set representation with Gröbner basis computations. Gröbner basis computations are better behaved in dimension zero from a complexity-theoretic point of view [13]. Ideally, their combination with witness sets could therefore yield a computational framework which retains the good practical behavior of Gröbner bases while having similarly good worst case complexity bounds as the above-mentioned [14].

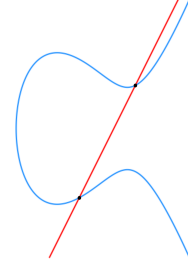


Figure 1: In cutting the curve $\mathbf{V}(y^2 - x^3 + 2x - 2)$ (in blue) with one linear constraint (in red), one obtains a witness set for X (in black).

Combining witness sets with Gröbner bases. However, only equidimensional solution sets can be represented in this manner. This will require us to combine a witness set based representation with an *equidimensional decomposition algorithm*, i.e. an algorithm that partitions $\mathbf{V}(F)$ dimension-by-dimension. For this we will use an algorithm designed by the envisioned supervisor of this internship given in [17]. This algorithm is based on the observation that the rank deficiencies of the Macaulay matrices constructed when computing a Gröbner basis of F using a signature-based algorithm contain information that can be used to effectuate a decomposition of $\mathbf{V}(F)$. Such a decomposition “simplifies” F , making further required Gröbner basis computations easier and therefore renders the rank deficiencies in the Macaulay matrices computationally useful.

We expect that combining this algorithm with the approach based on witness sets outlined above will actually simplify the decomposition procedures of [17], as adding the linear constraints turns out to automatically remove certain redundancies in the output of the decomposition that [17] needs to carefully handle. Moreover, most existing algorithms based on witness sets (be it symbolic or numerical) process the equations in F one-by-one. This turns out to necessitate the introduction of an involved *lifting procedure*, which takes a witness set W for F and lifts it to a one-dimensional representation. The fact that [17] does not rely on an incremental treatment, and instead treats all the equations in F at the same time, will allow us to circumvent the need for such a lifting procedure.

Organization of the internship

Workplan of the internship. We will realise the scientific goal of this internship outlined in the last section along the following work plan.

- Study the basic theory of the algorithmic treatment of polynomial systems of equations using Gröbner bases, e.g. along [3], as well as the decomposition algorithm of [17].
- Design new decomposition procedures for [17], combining it with a witness-set based representation,
- Implement and test the algorithm obtained in the last step in the `julia` package `AlgebraicSolving.jl` which is maintained in part by PolSys.
- if time allows, start to study complexity-theoretic questions related to the algorithm designed in the second step by using known complexity results for Gröbner basis computations in dimension zero [13].

Scientific environment. This internship will be supervised by [Rafael Mohr](#). It will take place at Sorbonne Université, in the computer science lab LIP6, which is located on the Pierre-et-Marie-Curie campus, at the heart of Paris. The intern will be welcomed in the [PolSys](#) team, which develops and implements fast computer algebra algorithms, for polynomial system solving and their applications, such as coding theory, combinatorics, cryptography, and robotics. The intern will work in a kind and international environment gathering PhD students and Post-Docs representing several nationalities, and animated with several working groups and a monthly seminar. All computing facilities will be provided.

Weekly meetings with the supervisor will be organized.

Prerequisites. We are looking for exceptional candidates who are excited about computer algebra, algorithmic design in mathematics and software implementations. A solid background in linear algebra as well as programming experience is expected. We also expect the potential candidate to be able to communicate and write in English.

We expect curiosity and openness, strong interpersonal and communicative skills, and willingness to dive into new topics, including the implementation of powerful mathematical algorithms.

How to apply. Applicants should send a full CV, a letter of motivation (in English) and the grades obtained during the last two years to

rafael.mohr@lip6.fr

References

- [1] Richard P. Brent. Algorithms for matrix multiplication. Technical Report, Stanford University, Stanford, CA, USA, February 1970.
- [2] Bruno Buchberger. *Ein Algorithmus Zum Auffinden Der Basiselemente Des Restklassenringes Nach Einem Nulldimensionalen Polynomideal*. PhD thesis, Universität Innsbruck, 1965.
- [3] David Cox, John Little, and Donal O’Shea. *Ideals, Varieties, and Algorithms*. Undergraduate Texts in Mathematics. Springer, New York, NY, 1992.
- [4] Jan Draisma, Emil Horobeț, Giorgio Ottaviani, Bernd Sturmfels, and Rekha R. Thomas. The Euclidean Distance Degree of an Algebraic Variety. *Foundations of Computational Mathematics*, 16(1):99–149, February 2016.
- [5] Christian Eder and Jean-Charles Faugère. A survey on signature-based algorithms for computing Gröbner bases. *Journal of Symbolic Computation*, 80:719–784, May 2017.
- [6] Jean Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, ISSAC ’02, pages 75–83, New York, NY, USA, July 2002. Association for Computing Machinery.
- [7] Alhussein Fawzi, Matej Balog, Aja Huang, Thomas Hubert, Bernardino Romera-Paredes, Moham-madamin Barekatin, Alexander Novikov, Francisco J. R. Ruiz, Julian Schrittwieser, Grzegorz Swirszcz, David Silver, Demis Hassabis, and Pushmeet Kohli. Discovering faster matrix multiplication algorithms with reinforcement learning. *Nature*, 610(7930):47–53, October 2022.
- [8] Elisenda Feliu and AmirHosein Sadeghimanesh. Kac-Rice formulas and the number of solutions of parametrized systems of polynomial equations. *Mathematics of Computation*, 91(338):2739–2769, November 2022.
- [9] Marc Giusti, Grégoire Lecerf, and Bruno Salvy. A Gröbner Free Alternative for Polynomial System Solving. *Journal of Complexity*, 17(1):154–211, March 2001.

- [10] Caroline Hills, Aravind Baskar, Mark Plecnik, and Jonathan D. Hauenstein. Computing complete solution sets for approximate four-bar path synthesis. *Mechanism and Machine Theory*, 196:105628, June 2024.
- [11] Manuel Kauers and Jakob Moosbauer. Flip Graphs for Matrix Multiplication. In *Proceedings of the 2023 International Symposium on Symbolic and Algebraic Computation*, ISSAC '23, pages 381–388, New York, NY, USA, July 2023. Association for Computing Machinery.
- [12] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced Oil and Vinegar Signature Schemes. In Jacques Stern, editor, *Advances in Cryptology – EUROCRYPT '99*, pages 206–222, Berlin, Heidelberg, 1999. Springer.
- [13] D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In J. A. van Hulzen, editor, *Computer Algebra*, Lecture Notes in Computer Science, pages 146–156, Berlin, Heidelberg, 1983. Springer.
- [14] Grégoire Lecerf. Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers. *Journal of Complexity*, 19(4):564–596, August 2003.
- [15] F. S. MacAulay. Some Formulæ in Elimination. *Proceedings of the London Mathematical Society*, s1-35(1):3–27, May 1902.
- [16] Ernst W Mayr and Albert R Meyer. The complexity of the word problems for commutative semigroups and polynomial ideals. *Advances in Mathematics*, 46(3):305–329, December 1982.
- [17] Rafael Mohr. A syzygial method for equidimensional decomposition. *Journal of Symbolic Computation*, 131:102455, November 2025.
- [18] Andrew J. Sommese, Jan Verschelde, and Charles W. Wampler. Introduction to numerical algebraic geometry. In Manuel Bronstein, Arjeh M. Cohen, Henri Cohen, David Eisenbud, Bernd Sturmfels, Alicia Dickenstein, and Ioannis Z. Emiris, editors, *Solving Polynomial Equations: Foundations, Algorithms, and Applications*, Algorithms and Computation in Mathematics, pages 301–337. Springer, Berlin, Heidelberg, 2005.