Univariate matrices for faster polynomial system solving

Master internship in Computer Algebra

Équipe PoLSys, LIP6, Sorbonne Université, 4 place Jussieu, 75005 Paris, France

Environment

Advisors: Jérémy Berthomieu[1], Vincent Neiger[2].

This internship will take place in LIP6, a joint lab between Sorbonne Université and CNRS in Paris. The intern will join a dynamic and scientifically ambitious team which advises and co-advises Ph.D. students and postdoctoral researchers from France and many other countries (currently and recently: China, Germany, The Netherlands, Spain, UK, USA, Vietnam). The intern will have access to office space, to all the necessary software, and to computing servers owned by the team.

This internship is particularly appropriate for students willing to pursue a Ph.D. after obtaining their Master degree.

Context, scientific positioning

Many problems, for example from biology, coding theory, robotics, or aerospace engineering, boil down to solving a system of multivariate polynomial equations of the form

$$f_1(x_1, \ldots, x_n) = \cdots = f_m(x_1, \ldots, x_n) = 0,$$

where $f_1, \ldots, f_m$ are known n-variate polynomials over some field $\mathbb{K}$. Here, solving the system means finding the common roots in $\mathbb{K}^n$ of these polynomials.

The fastest known methods for solving such systems, with finitely many solutions, are based on two steps (2002; 2017):

1. find a basis of the ideal $\langle f_1, \ldots, f_m \rangle$ which has useful properties, called a *Gröbner basis*;
2. use this basis to better understand the algebraic structure of the quotient $\mathbb{K}[x_1, \ldots, x_n]/\langle f_1, \ldots, f_m \rangle$, and from there find the solutions of the system.

Whereas the second step is better understood than the first in terms of complexity, after numerous recent advances in algorithms and implementations for the first step, there are now many types of instances for which the second step takes most of the computational time.

The classical approach for the second step models the problem as one of $\mathbb{K}$-linear algebra and relies on fast arithmetic for matrices over $\mathbb{K}$. However, since the problem comes from a multivariate polynomial setting, it has an algebraic structure which is ignored by this linear algebra viewpoint.

Internship objectives, requirements

This internship aims at exploring a new algorithmic approach to accelerate the second step, and at writing implementations to make the obtained improvements available in state-of-the-art software libraries (2021). Depending on the intern's interests and skills, the balance between algorithm design and software implementation might slightly lean towards one side or the other. In all cases, basic knowledge on the following topics is required:

- $\mathbb{K}$-linear algebra and matrices over $\mathbb{K}$, univariate and multivariate polynomials over $\mathbb{K}$;
- design and complexity of algorithms, implementations in C/C++ or a similar language.

The idea of the new approach is to use, instead of $\mathbb{K}$-linear algebra and matrices over $\mathbb{K}$, operations with *matrices whose entries are univariate polynomials*. This object, intermediate between multivariate polynomials and matrices over $\mathbb{K}$, has several advantages: it has algebraic properties similar to those of univariate polynomials (principal ideal domain), and for computations it benefits from fast arithmetic for matrices over $\mathbb{K}$ and for univariate polynomials.

A lot of progress on algorithms and software for univariate polynomial matrices has been made recently (2019; 2016), and this internship will study how to exploit this progress to accelerate the second step of polynomial system solving.

References

J. Berthomieu, C. Eder, and M. Safey El Din (2021), *msolve: A Library for Solving Polynomial Systems*, https://msolve.lip6.fr/.

J.-C. Faugère (2002), "A New Efficient Algorithm for Computing Gröbner Bases Without Reduction to Zero (F5)", in *Proceedings ISSAC '02*.

J.-C. Faugère and C. Mou (2017), "Sparse FGLM algorithms", in *Journal of Symbolic Computation* 80.3, pp. 538–569.

S. Hyun, V. Neiger, and É. Schost (2019), "Implementations of Efficient Univariate Polynomial Matrix Algorithms and Application to Bivariate Resultants", in *Proceedings ISSAC '19*, pp. 235–242.

V. Neiger (2016), "Bases of relations in one or several variables: fast algorithms and applications", PhD thesis, É.N.S. de Lyon, France.

[1]Sorbonne Université, jeremy.berthomieu@lip6.fr, https://www-polsys.lip6.fr/~berthomieu

[2]Sorbonne Université, vincent.neiger@lip6.fr, https://vincent.neiger.science