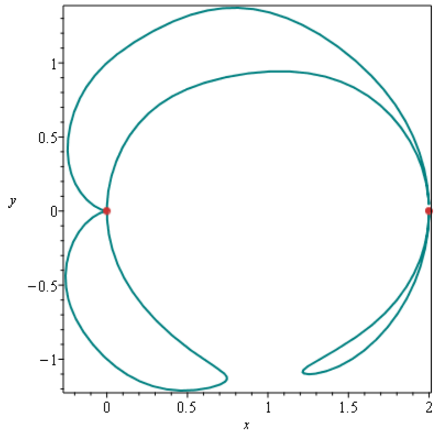
Boolean Complexity for Validated Numerical Resolution of Algebraic Curve Singularities

- **where ? CRIStAL, Université de Lille** — in the research group CFHP (Computer Algebra and HPC);
  and/or **LIP, ENS de Lyon** — in the research group Pascaline.
- **who ?** *student :* Master in CS or mathematics. *advisors :*
  - Adrien Poteaux (`adrien.poteaux@univ-lille.fr`),
  - Florent Bréhard (`florent.brehard@univ-lille.fr`),
  - Rémi Prébet (`remi.prebet@ens-lyon.fr`).
- **when ?** spring 2026 (4 – 6 months)



abstract

Isolating the roots of a univariate polynomial $p(z) \in \mathbb{C}[z]$ is a fundamental problem in computer science and numerical analysis. It raises fundamental theoretical and practical questions addressed by a rich literature, such as complexity upper bounds, rigorous error bounds or the design of efficient and reliable implementations. The goal of this internship is to extend some of these questions to a bivariate setting: Given a polynomial $P(x, y) \in \mathbb{C}[x, y]$, we want to isolate the solutions $y(x)$ called *Puiseux series* to $P(x, y(x)) = 0$ at the points called the *singularities* of the plane algebraic curve defined by P. More precisely:

- What is the complexity (in term of bit operations) to isolate a solution $y_i(x)$, i.e., to compute its coefficients in floating-point arithmetic to a sufficient accuracy and a sufficient order in x so that we can distinguish it from all other series solutions $y_j(x)$, $j \neq i$?
- Can we design an efficient validation routine, that, given a approximation $\tilde{y}_i(x)$ of $y_i(x)$ with floating-point coefficients, computes effecive, rigorous and tight error bounds for them?

Solving these questions paves the way towards improving algorithms in real and complex computational algebraic geometry used to solve challenging questions in many domains, such as robotics, theoretical physics or symbolic computation.

The first two sections provide an overview of the scientific context, the third one presents two possible objectives for the internship, and the last one details applications on a longer term, possibly during a PhD.

I. Validated numerical computation with singular algebraic curves

Algebraic curves over the reals or the complexes, are fundamental for many applications in computer science, mathematics and physics. Although they are simply defined *implicitly* by polynomial relations in their coordinates:

$$P_1(x_1, \dots, x_n) = \cdots = P_r(x_1, \dots, x_n) = 0, \qquad P_j \in \mathbb{K}[x_1, \dots, x_n] \quad \text{with } \mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C} \dots,$$

manipulating them efficiently and *explicitly* (parametrization, intersection, topology, etc.) requires sophisticated algorithms that have been continuously developed over last decades in computational algebraic geometry [9, 1], either purely symbolically or with the use of numerics [26, 14].

Singularities are the points where the curve is not similar to a line, like a pinch or a crossing of two branches (see the two red dots in the figure above). They occur in many situations like the plane projection of a space curve, or when a robot passes through a singular position. Particular care is needed at singularities since algorithms designed for regular curves may exhibit critical behavior at those points, like division by zero or numerical instability. This is a challenge for applications where maximum confidence is required, such as safety-critical engineering or computer-aided proofs in mathematics: a surgical robot is *not* safe up to erratic numerical behavior, *nor* is a geometry theorem true up to rounding errors.

Validated numerics [18, 29] aims at computing with numerical set-valued representations (real intervals, complex balls, set of functions described by a polynomial approximation and an error bound, etc.), thus exploiting the efficiency of floating-point arithmetic while guaranteeing actual mathematical statements: the solution is contained in the computed set. Such techniques have been successfully employed for critical applications and computer-assisted proofs (see, e.g., [28, 30, 6]). ***The goal of this internship is to treat singularities of algebraic curves using symbolic-numeric methods and validated numerics to combine efficiency and reliability.***

II. A validated symbolic-numeric approach to the Newton–Puiseux algorithm

The Newton–Puiseux algorithm computes parametrizations of the branches of a curve implicitly defined by $P(X,Y) = 0$ at a singularity x_0 under the form of a Puiseux series (i.e., power series with fractional exponents), with *algebraic* coefficients a_k:

$$Y(X) = \sum_{k \geqslant k_0} a_k (X - x_0)^{\frac{k}{e}}, \qquad e \in \mathbb{N}^*, \quad k_0 \in \mathbb{Z}, \quad a_k \in \mathbb{C} \quad (k \geqslant k_0). \tag{1}$$

Despite significant improvements made on Newton–Puiseux over the last years (see [23, 24] and references therein), the intrinsic representation size of the algebraic numbers a_k makes this symbolic algorithm not competitive, even for problems $P(X,Y) = 0$ of moderate degree (10 – 100). Consequently, in presence of singularities, many algorithms avoid the use of Puiseux series and prefer *turning around* such points when possible. Doing so, however, they ignore the crucial geometrical information encoded by singularities, and they increase the risk of numerical instability when working close to a singular point without exploiting it.

Yet, in many situations, computing accurate numerical approximations of the a_k together with rigorous and tight error bounds, rather than exact representations, is sufficient. Therefore, we propose to design a validated symbolic-numeric Newton–Puiseux algorithm, following strategy exposed in [21]:

1. First, reduce the equation $P(X,Y) = 0$ modulo some well-chosen prime number p and apply the Newton–Puiseux algorithm over it. Working over $\mathbb{F}_p$ (or some algebraic extension of it) allows us to avoid the problem of coefficient growth. Unfortunately, the obtained coefficients $\overline{a}_k$ cannot be lifted to $a_k \in \mathbb{C}$ in the original problem. However, under easy-to-satisfy conditions on p, the *structure* of the series (1) (i.e., its exponents) is the same over $\mathbb{F}$ and $\mathbb{C}$.

2. Now, compute the coefficients a_k numerically *following the structure* of the Puiseux series (i.e., its exponents). Note that, without this structure information, such a numerical method applied close to a singularity would be highly unstable.

3. Finally, design a validation method to compute rigorous and tight error bounds on the a_k's approximate values. This will involve techniques known as *fixed-point a posteriori validation* [5, §3.3], where error bounds are obtained afterwards from the application of a suitable fixed-point theorem.

III. Objectives of the internship

While the first step above was successfully addressed in [22], substantial work is needed to provide theoretical results, practical algorithms and efficient implementations to fully solve the problem. In particular, this internship focuses on two key aspects regarding steps 2 and 3, respectively. Each of them can be considered separately, based on the intern student's interests in the proposed topics.

Numerical isolation and Boolean complexity. A rich literature is dedicated to the case of univariate polynomials, with extensive complexity results on the number of bit operations (Boolean complexity) to approximate the roots to a given precision or to isolate them from other roots (see, e.g., [25, 19, 17] and references therein). Some complexity bounds also exist for bivariate generalizations of this problem, that is, the isolation the points (x, y) solution to:

$$\begin{cases} P(X,Y) = 0, \\ \quad R(X) = 0. \end{cases}$$

In our setting, $R(X)$ would be the resultant of $P(X,Y)$ and $\partial P(X,Y)/\partial Y$: its roots x_0 are the abscissa of the singularities and x-critical points of the curve, i.e., the x_0 for which the Puiseux series (1) are nontrivial. In [12], an algorithm requiring at most $\tilde{O}(n^6 + n^5\tau)$ bit operations is given, where n is a bound on the total degree of P and τ the bit-size of the integer coefficients of P. Our goal is to isolate not only the solutions (x_0, y_0), but the singular part of the Puiseux series at those points (the minimal part of the series that allows to distinguish this solution of $P(X,Y) = 0$ from the other ones). We believe it possible to obtain Boolean complexity bounds similar or slightly larger than those of [12] (where only *points* are isolated). This must be viewed in light of existing Boolean complexity bounds for the symbolic Newton–Puiseux algorithms (see, e.g., [31] where a bound of $\tilde{O}(n^{36}\tau^2)$ bit operations is proved for the computation of the singular part of a single Puiseux series above $x_0 = 0$).

One-step a posteriori validation. Complexity bounds for root isolation, even in the univariate case, are most of the time *asymptotic* and not fully explicit. To obtain effective and rigorous enclosures of the solutions, *a posteriori validation methods* mentioned in the third step above are often more appropriate. In opposition to a "brick by brick" validation approach where each elementary subroutine of Newton–Puiseux would be individually validated and then composed, we here propose to elaborate a global approach where error bounds for the numerical Puiseux series are derived in a single validation step. A specific difficulty is that singular equations are typical examples of ill-posed problems: naive interval approaches fail to capture the structure of the singularity, which is not stable under infinitesimal perturbations. Exploiting the structure information obtained from step 1 is thus necessary. To help us with this task, we propose to take inspiration from a previous work [7] dedicated to the singular, but univariate problem of validating multiple roots of univariate polynomials.

IV. The future: Applications to computational algebraic geometry

Beyond this internship (but possibly during a PhD afterwards), the resolution of singularities of algebraic curves using the symbolic-numeric Newton–Puiseux algorithm will be the cornerstone for improvements of algorithms in real and complex algebraic geometry. This, in turn, will help tackling computationally challenging applications in the following domains:

- *Robotics* often involves polynomial systems describing real algebraic (or semi-algebraic) varieties representing, for example, the possible configurations of a robot. *Connectivity queries* are essential for motion planning, and they can be handled by computing a *roadmap* of the algebraic variety [8, 13], thus reducing the problem to connectivity queries on real algebraic curves. A possible approach for this [16, 15] is to project the curve onto a plane and to analyze the resulting 2D singular curve [12]. Such an analysis could be improved with the use of symbolic-numeric Puiseux series.

- *Homotopy methods* are used to compute numerical roots of polynomial systems by deformation (the homotopy) from simpler systems [3]. The curves tracking the roots may cross each other, resulting in singularities that can be treated rigorously with the validated symbolic-numeric Newton–Puiseux algorithm.
- The *Abel-Jacobi map* [4, §1] links crucial information of a complex algebraic curve (a Riemann surface) to computational data, namely contour integrals along paths connecting singularities. Computing them rigorously is a major step towards proofs of existence of particular solutions to nonlinear wave equations in physics [2, 11, 10, 20]: KdV (Korteweg-de Vries), KP (Kadomtsev-Petviashvili) and NLS (nonlinear Schrödinger). This also has applications in computer algebra, e.g. integrating algebraic functions [27].

V. References

[1] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in Real Algebraic Geometry*. Springer Berlin, Heidelberg, 2003.

[2] E. D. Belokolos, A. I. Bobenko, V. Z. Enolskii, A. R. Its, and V. B. Matveev. *Algebro-geometric approach to nonlinear integrable equations*, volume 1994. Springer, 1994.

[3] C. Beltrán and A. Leykin. Robust certified numerical homotopy tracking. *Found. Comput. Math.*, 13:253–295, 2013.

[4] A. I. Bobenko and C. Klein. *Computational Approach to Riemann Surfaces*, volume 2013. Springer Science & Business Media, 2011.

[5] F. Bréhard. *Certified numerics in function spaces : polynomial approximations meet computer algebra and formal proof*. PhD thesis, University of Lyon, France, 2019.

[6] F. Bréhard, N. Brisebarre, M. Joldes, and W. Tucker. Efficient and validated numerical evaluation of Abelian integrals. *ACM Trans. Math. Softw.*, 50(1), mar 2024.

[7] F. Bréhard, A. Poteaux, and L. Soudant. Validated root enclosures for interval polynomials with multiplicities. In *Proceedings of the 2023 International Symposium on Symbolic and Algebraic Computation*, ISSAC '23, pages 90–99, New York, NY, USA, 2023. Association for Computing Machinery.

[8] J. Canny. *The complexity of robot motion planning*. PhD thesis, MIT, 1987.

[9] D. Cox, J. Little, D. O'Shea, and M. Sweedler. *Ideals, varieties, and algorithms*. Springer, 1994.

[10] B. Deconinck and M. S. Patterson. Computing the Abel map. *Physica D: Nonlinear Phenomena*, 237(24):3214–3232, 2008.

[11] B. Deconinck and H. Segur. The KP equation with quasiperiodic initial data. *Physica D: Nonlinear Phenomena*, 123(1):123–152, 1998.

[12] D. N. Diatta, S. Diatta, F. Rouillier, M.-F. Roy, and M. Sagraloff. Bounds for polynomials on algebraic numbers and application to curve topology. *Discrete & Computational Geometry*, 67(3):631–697, 2022.

[13] M. S. E. Din and E. Schost. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. *Journal of the ACM*, 63(6), 2017.

[14] J. D. Hauenstein and A. J. Sommese. What is numerical algebraic geometry? *Journal of Symbolic Computation*, 79:499–507, 2017.

[15] M. N. Islam, A. Poteaux, and R. Prébet. Algorithm for connectivity queries on real algebraic curves. In *Proceedings of the 2023 International Symposium on Symbolic and Algebraic Computation*, page 345–353. ACM, 2023.

[16] K. Jin and J. Cheng. On the complexity of computing the topology of real algebraic space curves. *Journal of Systems Science and Complexity*, 34:809–826, 2021.

[17] K. Mehlhorn, M. Sagraloff, and P. Wang. From approximate factorization to root isolation with application to cylindrical algebraic decomposition. *Journal of Symbolic Computation*, 66:34–69, 2015.

[18] R. E. Moore, R. B. Kearfott, and M. J. Cloud. *Introduction to Interval Analysis*. Society for Industrial and Applied Mathematics, 2009.

[19] V. Y. Pan. Univariate polynomials: Nearly optimal algorithms for numerical factorization and root-finding. *Journal of Symbolic Computation*, 33(5):701–733, 2002.

[20] M. S. Patterson. *Algebro-geometric algorithms for integrable systems*. PhD thesis, University of Washington, 2007.

[21] A. Poteaux. *Calcul de développements de Puiseux et application au calcul du groupe de monodromie d'une courbe algébrique plane*. PhD thesis, Université de Limoges, 2008.

[22] A. Poteaux and M. Rybowicz. Good reduction of Puiseux series and applications. *Journal of Symbolic Computation*, 47(1):32 – 63, 2012.

[23] A. Poteaux and M. Weimann. Computing Puiseux series: a fast divide and conquer algorithm. *Annales Henri Lebesgue*, 4:1061–1102, 2021.

[24] A. Poteaux and M. Weimann. Local polynomial factorisation: improving the Montes algorithm. In *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation*, ISSAC '22. ACM, 2022.

[25] A. Schönhage. The fundamental theorem of algebra in terms of computational complexity. *Manuscript. Univ. of Tübingen, Germany*, 1982.

[26] A. Sommese and C. Wampler. *The Numerical solution of systems of polynomials arising in engineering and science*. World Scientific, 2005.

[27] B. M. Trager. *Integration of Algebraic Functions*. PhD thesis, MIT, 1984.

[28] W. Tucker. A rigorous ODE solver and Smale's 14th problem. *Found. Comput. Math.*, 2:53–117, 2002.

[29] W. Tucker. *Validated Numerics: A Short Introduction to Rigorous Computations*. Princeton University Press, Princeton, 2011.

[30] J. B. van den Berg and J.-P. Lessard. Rigorous numerics in dynamics. *Notices Amer. Math. Soc.*, 62(9):1057–1061, 2015.

[31] P. Walsh. A polynomial-time complexity bound for the computation of the singular part of a Puiseux expansion of an algebraic function. *Mathematics of Computation*, 69(231):1167–1182, 2000.