A certified numerical algorithm for the topology of resultant and discriminant curves

Rémi Imbach, Guillaume Moroz, Marc Pouget

A certified numerical algorithm for the topology of resultant and discriminant curves

Rémi Imbach[a,b], Guillaume Moroz[a,b], Marc Pouget[a,b]

[a]*Inria, France.*
[b]*LORIA laboratory, Nancy, France.*

Abstract

Let C be a real plane algebraic curve defined by the resultant of two polynomials (resp. by the discriminant of a polynomial). Geometrically such a curve is the projection of the intersection of the surfaces $P(x, y, z) = Q(x, y, z) = 0$ (resp. $P(x, y, z) = \frac{\partial P}{\partial z}(x, y, z) = 0$), and generically its singularities are nodes (resp. nodes and ordinary cusps). State-of-the-art numerical algorithms compute the topology of smooth curves but usually fail to certify the topology of singular ones. The main challenge is to find practical numerical criteria that guarantee the existence and the uniqueness of a singularity inside a given box B, while ensuring that B does not contain any closed loop of C. We solve this problem by first providing a square deflation system, based on subresultants, that can be used to certify numerically whether B contains a unique singularity p or not. Then we introduce a numeric adaptive separation criterion based on interval arithmetic to ensure that the topology of C in B is homeomorphic to the local topology at p. Our algorithms are implemented and experiments show their efficiency compared to state-of-the-art symbolic or homotopic methods.

1. Introduction

Given a bivariate polynomial f with rational coefficients, a classical problem is the computation of the topology of the real plane curve $C = \{(x, y) \in \mathbb{R}^2 | f(x, y) = 0\}$. One may ask for the topology in the whole plane or restricted to some bounding box. In both cases, the topology is output as an embedded piecewise-linear graph that has the same topology as the curve C. For a smooth curve, the graph is hence a collection of topological circles or lines; for a singular curve, the graph must report all the singularities: isolated points and self-intersections.

Symbolic methods based on the cylindrical algebraic decomposition can guarantee the topology of any curve. However, the high complexity of these purely algebraic methods prevents them to be applied in practice on difficult instances. On the other hand, purely numerical methods such as curve tracking with interval arithmetic or subdivision are efficient in practice for smooth curves but typically fail to certify the topology of singular curves. A long-standing challenge is to extend numerical methods to compute efficiently the topology of singular curves.

Computing the topology of a singular curve can be done in three steps.

Email addresses: Remi.Imbach@inria.fr (Rémi Imbach), Guillaume.Moroz@inria.fr (Guillaume Moroz), Marc.Pouget@inria.fr (Marc Pouget)

1. Enclose the singularities in isolating boxes.
2. Compute the local topology in each box, that is *i*) compute the number of real branches connected to the singularity, *ii*) ensure that it contains no other branches.
3. Compute the graph connecting the boxes.

Up to homeomorphisms, the local topology at a point of a curve is characterized by the number of real (half-) branches of the curve connected to the point. This number is two for a regular point, and can be any even number at a singular point. We define a *witness box* of a singular point as a box containing the singular point such that the topology of the curve inside the box is the one of the graph connecting the singularity to the crossings of the curve with the box boundary. The topology of the curve in a witness box is thus completely determined by its number of crossings with the box boundary. In this article, we only focus on the first two steps of the above-mentioned topology algorithm, that is computing witness boxes. The third step can be seen as reporting the topology of a smooth curve in the complement of the witness boxes of the singular points. There already exist certified algorithms for this task using subdivision (Plantinga and Vegter (2004); Lin and Yap (2011)). Another option is to use certified path tracking (e.g. Martin et al. (2013); Van Der Hoeven (2011); Beltrán and Leykin (2013)) starting at the crossings of the curve with the boundary of singularity boxes, note that to report the closed loops without singularity, at least one point on such components must be provided.

Contribution and overview.. The specificity of the resultant or the discriminant curves computed from generic surfaces is that their singularities are stable, this is a classical result of singularity theory due to Whitney. The key idea of our work is to show that, in this specific case, the over-determined system defining the curve singularities can be transformed into a regular well-constrained system of a transverse intersection of two curves defined by subresultants. This new formulation can be seen as a specific deflation system that does not contain spurious solutions.

Our contribution focuses on the first two steps of the above mentioned topology algorithm for a curve defined by the resultant of two trivariate polynomials P and Q: $f = \text{Resultant}_z(P, Q)$, see Figure 1 for an illustration of the discriminant curve of a torus.

In Section 2, the main results are Theorems 1 and 2 that characterize the singularities of the resultant or discriminant curve in terms of subresultants under generic assumptions. A semi-algorithm 1 is proposed to check these generic assumptions, i.e. it terminates if and only if the assumptions are satisfied (note that this is the best one can hope for when using a purely numerical method). Based on the characterization of Theorems 1 and 2, Algorithm 2, using subdivision and interval evaluation, isolates the node and cusp singularities with an adaptive certification.

Sections 3 and 4 address the second step on the above-mentioned topology algorithm. Algorithms 3 and 4 in Section 3 distinguish nodes from cusps and compute the number of branches. Then in Section 4, Algorithm 5 refines an isolating box of a singular point such that it becomes a witness box.

In Section 5, experiments are detailed showing that our specialized certified numerical method outperforms state-of-the-art implemented methods for polynomials of degree greater or equal to 5. Moreover, the performance of our method is also improved when we restrict the problem to a box.

Notations.. Let f be a bivariate polynomial and C it associated curve. We denote by $f_{x^i y^j}$ the partial derivative $\frac{\partial^{i+j} f}{(\partial x)^i (\partial y)^j}$. A point $p = (\alpha, \beta)$ in $\mathbb{C}^2$ is *singular* for f if $f(p) = f_x(p) = f_y(p) = 0$,

and *regular* otherwise. A *node* is a singular point with $\det(\text{Hessian}(f)) = f_{xy}^2 - f_{x^2} f_{y^2} \neq 0$. An *ordinary cusp* is a singular point such that $\det(\text{Hessian}(f)) = 0$ and for all non trivial direction (u, v), $f(\alpha + ut, \beta + vt)$ vanishes at $t = 0$ with multiplicity at most 3.

We denote by $\square f$ any convergent interval extension of f, that is for any box B, $\{f(x, y) | (x, y) \in B\} \subset \square f(B)$, and for any decreasing sequence of boxes B_i converging to a point p, the sequence $\square f(B_i)$ converges to $f(p)$. By abuse of notation, we often denote $\square f(B)$ by $\square_B f$ or simply $\square f$. The Krawczyk operator of a mapping F defined in Lemma 7 is denoted by K_F. The topological interior of a box B is denoted $int(B)$.

For two polynomials P and Q in $\mathbb{D}[z]$ with $\mathbb{D}$ a unique factorization domain (in this article $\mathbb{D}$ will be $\mathbb{Q}[x, y]$), recall that the i^{th} subresultant polynomial is of degree at most i (see e.g. (Kahoui, 2003, §3)), we denote it $S_i(z) = s_{ii} z^i + s_{i,i-1} z^{i-1} + \cdots + s_{i0}$. The resultant is thus $S_0(z) = s_{00}$ in $\mathbb{D}$ and we also denote it more classically as $Res_z(P, Q)$. Finally, $\mathbb{V}(f_1, \ldots, f_n)$ denotes the solutions of the system $f_1 = \cdots = f_n = 0$.

Previous and related work.. There are many works addressing the topology computation via symbolic methods, see for instance the book chapter by Mourrain et al. (2006) and references therein. Most of them use subresultant theory, but there are also some alternatives using only resultants (e.g. Seidel and Wolpert (2005); Emeliyanenko and Sagraloff (2012)) or Gröbner bases and rational univariate representations (Cheng et al. (2010)). An alternative by Akoglu et al. (2014) even computes a rational univariate representation numerically if all approximate solutions are known. For the restricted case of computing the topology of non-singular curves, certified numerical methods are usually faster and can in addition reduce the computation to a user defined bounding box. One can mention interval analysis methods (Martin et al. (2013)) or more generally certified homotopy methods (Beltrán and Leykin (2013); Van Der Hoeven (2011)). These methods are based on the fact that the regular solutions of a square system can be certified and approximated with quadratic convergence with the interval Newton-Krawczyk operator (Rump (1983); Neumaier (1990)). Another well-studied numerical approach is via recursive subdivision of the plane. Indeed, the initial idea of the marching cube algorithm by Lorensen and Cline (1987) can be further improved with interval arithmetic to certify the topology of smooth curves (Snyder (1992); Plantinga and Vegter (2004); Liang et al. (2008)).

For singular curves, isolating the singular points is already a challenge from a numerical point of view. Indeed, singular points are defined by an over-determined system $f = f_x = f_y = 0$ and are not necessarily regular solutions of this system. A classical approach to handle an over-determined system $\{f_1, \ldots, f_m\}$ is to combine its equations in the form $f_{1 x_i} f_1 + \cdots + f_{m x_i} f_m = 0$ for each variable $\{x_i\}_{1 \leq i \leq n < m}$, to transform it into a square system (Dedieu (2006)), but this introduces spurious solutions. Singular solutions can be handled through deflation (Giusti et al. (2007); Ojika et al. (1983); Leykin et al. (2006); Mantzaflaris and Mourrain (2011)), roughly speaking, the idea is to compute partially the local structure of a non-regular solution, and use this information to create a new system where this solution is regular. However this system is usually still overdetermined, and it does not vanish on the solutions of the original system that do not have the same local structure. Thus, this cannot be directly used to separate solutions with different multiplicity structures. It is important to mention that the certification of solutions of over-determined systems is theoretically out of reach of numerical methods in the general case. In the polynomial case, non-adaptive lower bounds can be used but they are too pessimistic to be practical, see (Hauenstein and Sottile, 2012, Remark 7) or Burr et al. (2012).

When the curve we consider is a resultant, its singular locus can be related to the first subresultant (see (Jouanolou, 1979, §4.3) and (Busé and Mourrain, 2009, §5) for examples). In

Section 2, we use this structure to exhibit a square deflation system. Another approach would be to exhibit a square system in higher dimension that defines the set of points for which the polynomials P and Q have two solutions. This approach was considered by Delanoue and Lagrange (2014) to compute the topology of the apparent contour of a smooth mapping from $\mathbb{R}^2$ to $\mathbb{R}^2$.

The number of real branches connected to the singularity can be computed with the topological degree of a suitable mapping (Szafraniec (1988); Alberti et al. (2008); Mantzaflaris and Mourrain (2011)) or with the fiber multiplicity together with isolation on the box boundary (Seidel and Wolpert (2005)). Certifying the topology inside a box requires the detection of loops near a singularity. It is usually solved in the literature by isolating the x-extreme points, which reduces the problem to a univariate polynomial computed with resultants (Seidel and Wolpert (2005); Mourrain et al. (2006) for example).

We are not aware of numerical algorithms that can certify in practice the computation of the topology of singular curves, but several promising approaches have been presented. Relying on global non-adaptive separation bounds for algebraic systems, the subdivision approach presented by Burr et al. (2012) can theoretically certify the topology of any singular curve. Due to these worst-case bounds, this algorithm cannot be practical. A numerical algebraic geometric approach is presented by Lu et al. (2007) using irreducible decomposition, generic projection and plane sweep, deflation and homotopy to compute the topology of a singular curve in any codimension. Even if this work has been implemented by Bates et al. (2013)[1], the certification of all the algorithm steps appears as a challenge. The numerical approach by Corless et al. (2013), based on Bezoutian and eigenvalue computation, can handle singular curves but even if multiprecision gives accurate results no certification is provided.

2. Subresultant based deflation

The input of algorithms in this section are two trivariate polynomials P, Q and a box B_0 in $\mathbb{R}^2$. Our goal is to isolate the singularities of the plane curve $f = 0$ defined by the resultant of P and Q with respect to z. In this section, we exhibit a square polynomial system $g = h = 0$ and a polynomial u such that the singularities of f are exactly the solutions of the constrained system $g = h = 0$ and $u \neq 0$. Moreover, the singularities are regular solutions of $g = h = 0$, such that numerical methods can certify whether a box contains or not a singularity. In Section 2.1, the constrained system is constructed using subresultants. In Section 2.2, the regularity of this system is translated in terms of types of singularities. Generic assumptions are required so that these characterizations of the singularities of f hold. Section 2.3 presents a semi-algorithm for checking the assumptions that we now define. Given two trivariate polynomials P, Q in $\mathbb{Q}[x, y, z]$ and a two-dimensional box B_0, we define the generic assumptions:

(A_1) Above the box B_0 for the x and y-coordinates, the intersection of the surfaces $P(x, y, z) = 0$ and $Q(x, y, z) = 0$ is a smooth space curve denoted $C_{P\cap Q}$, i.e. the tangent vector $\mathbf{t} = \nabla P \times \nabla Q$ is nowhere null on $C_{P\cap Q}$ (where ∇P is the gradient vector (P_x, P_y, P_z)).

(A_2) Above any point (α, β) in B_0, there are at most two points of $C_{P\cap Q}$ counted with multiplicities, or in other words, the polynomial $\gcd(P(\alpha, \beta, z), Q(\alpha, \beta, z))$ has degree at most two. In addition, there are finitely many (α, β) in B_0 such that this degree is two.

[1] See also `www.bertinireal.com` and Myszka et al. (2013) for an application to real curves arising in engineering.

(A_3) The leading coefficients $L_P(x,y)$ and $L_Q(x,y)$ of P and Q seen as polynomials in z have no common solutions in B_0.

(A_4) The singularities of the resultant or discriminant curve are only nodes or ordinary cusps.

Note that these assumptions are satisfied for almost all pairs of polynomials in $\mathbb{Q}[x,y,z]$.

2.1. Singularities via subresultants

Let f be the resultant polynomial (with respect to the variable z) of two polynomials P and Q in $\mathbb{Q}[x,y,z]$. We always assume that f is square-free and thus its singularities are isolated. Let $S_{sing} = \mathbb{V}(f, f_x, f_y)$ be the set of singular points of f and $S_{sres} = \mathbb{V}(s_{11}, s_{10}) - \mathbb{V}(s_{22})$. We prove in this section that, under our assumptions, these two sets coincide. Figure 2 illustrates Theorem 1 for the discriminant curve of a torus.

Theorem 1 (Recknagel (2013))**.** *Let f be the resultant of the polynomials P and Q in $\mathbb{Q}[x,y,z]$ with respect to the variable z. Then $S_{sres} \subset S_{sing}$ and if the assumptions (A_1) to (A_3) are satisfied then $S_{sing} \subset S_{sres}$.*

Proof of the inclusion $S_{sres} \subset S_{sing}$.. Let $I = \langle f, f_x, f_y\rangle$ and $J = \langle s_{11}, s_{10}\rangle : \langle s_{22}\rangle^\infty$, then $S_{sing} = \mathbb{V}(I)$ and $\mathbb{V}(J) = \overline{\mathbb{V}(s_{11}, s_{10}) - \mathbb{V}(s_{22})} = \overline{S_{sres}} \supset S_{sres}$. It is thus sufficient to prove that $I \subset J$, or in other words that there exists a positive integer m such that $\langle f, f_x, f_y\rangle \cdot \langle s_{22}\rangle^m = \langle s_{22}^m f, s_{22}^m f_x, s_{22}^m f_y\rangle \subset \langle s_{11}, s_{10}\rangle$.

The generic chain rule of subresultant (see for instance (Kahoui, 2003, Theorem 4.1)) yields $s_{22}^2 f = Res(S_2, S_1)$. On the other hand, $Res(S_2, S_1) = \begin{vmatrix} s_{22} & s_{11} & \\ s_{21} & s_{10} & s_{11} \\ s_{20} & & s_{10} \end{vmatrix} = s_{10}^2 s_{22} + s_{11}^2 s_{20} - s_{10} s_{11} s_{21}$. Hence $s_{22}^2 f \in \langle s_{11}, s_{10}\rangle$.

The previous identity expresses $s_{22}^2 f$ as a quadratic form in s_{11} and s_{10}, differentiating with respect to x (or y) yields a sum with s_{11} or s_{10} as a factor in each term, thus $\partial(s_{22}^2 f)$ is in $\langle s_{11}, s_{10}\rangle$. This implies that $\partial(s_{22}^3 f)$ is also in $\langle s_{11}, s_{10}\rangle$. In addition, $\partial(s_{22}^3 f) = 3 s_{22}^2 f \partial s_{22} + s_{22}^3 \partial f$ hence $s_{22}^3 \partial f = \partial(s_{22}^3 f) - 3 s_{22}^2 f \partial s_{22}$ with both terms in $\langle s_{11}, s_{10}\rangle$, thus $s_{22}^3 \partial f$ is in $\langle s_{11}, s_{10}\rangle$. We conclude that $\langle s_{22}^3 f, s_{22}^3 f_x, s_{22}^3 f_y\rangle \subset \langle s_{11}, s_{10}\rangle$, hence $I \subset J$ and $S_{sres} \subset S_{sing}$.

Proof of the inclusion $S_{sing} \subset S_{sres}$.. Let (α,β) be a singular point of f, so that $f(\alpha,\beta) = 0$. According to the generic condition (A_2), $\gcd(P(\alpha,\beta,z), Q(\alpha,\beta,z))$ has at most two simple roots or one double root.

For the case of a double root, $\gcd(P(\alpha,\beta,z), Q(\alpha,\beta,z))$ has degree 2 and by the gap structure theorem (more precisely its corollary showing the link between the gcd and the last non-vanishing subresultant, see e.g. (Kahoui, 2003, Corollary 5.1)) and assumption (A_3): (a) this gcd is the subresultant $S_2(\alpha,\beta)$, hence $s_{22}(\alpha,\beta) \neq 0$, and (b) the subresultants of lower indices are vanishing, in particular $s_{11}(\alpha,\beta) = 0$ and $s_{10}(\alpha,\beta) = 0$. Hence (α,β) is in S_{sres}.

Otherwise, let γ be a simple root of $\gcd(P(\alpha,\beta,z), Q(\alpha,\beta,z))$, the generic condition (A_1) yields that the tangent vector $\mathbf{t}(p)$ to $C_{P\cap Q}$ at the point $p = (\alpha,\beta,\gamma)$ is well defined and not vertical. Indeed, the multiplicity of γ in $\gcd(P(\alpha,\beta,z), Q(\alpha,\beta,z))$ is 1, so it is also 1 in at least one of the polynomials $P(\alpha,\beta,z)$ or $Q(\alpha,\beta,z)$. In other words, $P_z(p) \neq 0$ or $Q_z(p) \neq 0$ which implies that the x and y-coordinates of $\mathbf{t}(p)$ cannot both vanish (otherwise, $\mathbf{t}(p)$ would be the null vector contradicting assumption (A_1)). Without loss of generality we may assume that the x-coordinate of $\mathbf{t}(p)$ is not null: $x_{\mathbf{t}(p)} = P_y(p)Q_z(p) - P_z(p)Q_y(p) \neq 0$.

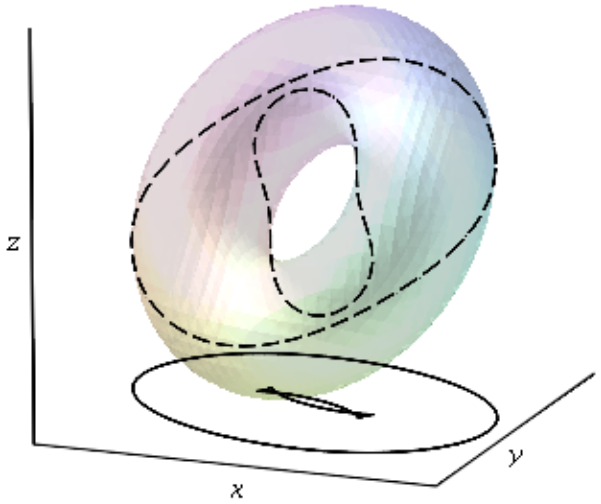

Figure 1: A torus defined by $P = 0$, in dashed line the curve $P = P_z = 0$ and in solid line the discriminant curve of the torus defined by $Res_z(P, P_z) = 0$.

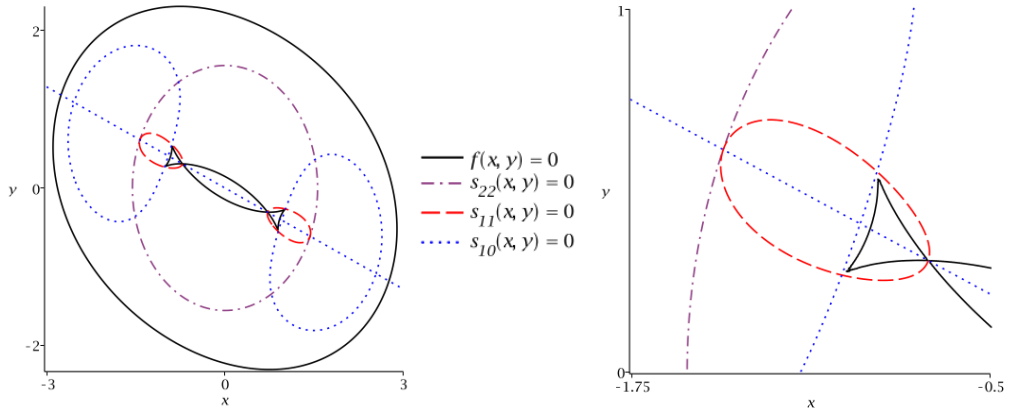

Figure 2: Illustration of Theorem 1. Two views of the discriminant curve $f = 0$ of the torus of Figure 1 and curves defined by the coefficients s_{10}, s_{11}, s_{22} of the sub-resultants chain of P and P_z. The singularities of the discriminant curve are the solutions of the system $s_{11} = s_{10} = 0$ such that s_{22} does not vanish.

We now apply (Busé and Mourrain, 2009, Theorem 5.1) rephrased in the affine setting to P and Q:

$$f_y = \pm \begin{vmatrix} P_y & P_z \\ Q_y & Q_z \end{vmatrix} s_{11} + uP + vQ$$

with u, v in $\mathbb{Q}[x, y]$. Evaluated at p, P and Q vanish and we obtain: $f_y(\alpha,\beta) = \pm x_{\mathfrak{t}(p)} s_{11}(\alpha,\beta)$. Since (α,β) is a singular point of f, $f_y(\alpha,\beta) = 0$, and together with $x_{\mathfrak{t}(p)} \neq 0$ this gives $s_{11}(\alpha,\beta) = 0$. The gap structure theorem and $f(\alpha,\beta) = 0$ then implies that (a) $s_{10}(\alpha,\beta) = 0$, and (b) the degree of $\gcd(P(\alpha,\beta,z), Q(\alpha,\beta,z))$ is at least 2. Together with the generic condition (A_2), this degree is exactly 2 and so is the degree of the second subresultant S_2 evaluated at (α,β), thus $s_{22}(\alpha,\beta) \neq 0$. We then conclude that in this case too (α,β) is in S_{sres}. □

2.2. Regularity conditions

The main theorem of this section is the relation between the types of singularities of f and the regularity of the solutions of the system $s_{11} = s_{10} = 0$. We assume for this section that the assumptions (A_1), (A_2) and (A_3) hold.

Theorem 2. *Let f be the resultant of the polynomials P and Q in $Q[x, y, z]$ with respect to the variable z. If the assumptions (A_1), (A_2) and (A_3) hold then the following propositions are equivalent:*

i. p is a regular solution of $s_{11} = s_{10} = 0$ and $s_{22}(p) \neq 0$
ii. p is a node or an ordinary cusp of the curve $f = 0$

Furthermore in this case, p is an ordinary cusp point if and only if $C_{P\cap Q}$ has a vertical tangent above p.

The proof of this theorem is decomposed with the following lemmas.

Lemma 3 (Recknagel (2013))**.** *Let p be a node of f. Then p is a regular point of the system $s_{11} = s_{10} = 0$.*

Proof. Since p is a node, it is a singular point of $f = 0$ and Theorem 1 implies that p is a solution of the system $s_{11} = s_{10} = 0$. Moreover, we saw in the proof of Theorem 1 that $S_{sres} \subset S_{sing}$ but more precisely that $\langle s_{22}^3 f, s_{22}^3 f_x, s_{22}^3 f_y\rangle \subset \langle s_{11}, s_{10}\rangle$. In the following, we use the notion of multiplicity of a point in an ideal sometimes called the intersection multiplicity as defined for instance in (Cox et al., 2005, §4.2, Definition 2.1). In particular, the latter inclusion implies that the multiplicity of p in $\langle s_{11}, s_{10}\rangle$ is lower or equal to its multiplicity in $\langle s_{22}^3 f, s_{22}^3 f_x, s_{22}^3 f_y\rangle$. Since p is a node of f, the determinant of the Hessian of f is non-zero and p is a regular point of $\langle f, f_x, f_y\rangle$. And since $s_{22}(p) \neq 0$, we can conclude that the multiplicity of p in $\langle s_{22}^3 f, s_{22}^3 f_x, s_{22}^3 f_y\rangle$ is 1. Thus p has also a multiplicity 1 in $\langle s_{11}, s_{10}\rangle$. □

Lemma 4. *Let p be an ordinary cusp point of f. Then p is a regular point of the system $s_{11} = s_{10} = 0$.*

Proof. Let $p = (\alpha,\beta)$ be an ordinary cusp point of f. Suppose by contradiction that p is a singular solution of $s_{11} = s_{10} = 0$. Then the determinant of the Jacobian matrix $\begin{pmatrix} s_{11x} & s_{10x} \\ s_{11y} & s_{10y} \end{pmatrix}$ is 0 and there exists a vector $(u, v) \in \mathbb{R}^2 \setminus \{(0, 0)\}$ orthogonal simultaneously to the gradient of s_{11} and to the gradient of s_{10}. In particular, $s_{11}(\alpha + ut, \beta + vt)$ (resp. $s_{10}(\alpha + ut, \beta + vt)$) vanishes at 0 in

t with multiplicity at least 2. Using standard formula on the resultants ((Kahoui, 2003, Theorem 4.1) for example) we have $s_{22}^2 f = Res(S_1, S_2)$. Developing the right hand side we get:

$$s_{22}^2 f = s_{22}s_{10}^2 - s_{21}s_{11}s_{10} + s_{20}s_{11}^2.$$

Thus, evaluating the right hand side on $(\alpha + ut, \beta + vt)$, we observe that it vanishes at 0 in t with multiplicity at least 4.

On the other hand, p being an ordinary cusp of f, the polynomial $f(\alpha + ut, \beta + vt)$ vanishes at 0 in t with multiplicity at most 3. In addition, under the assumptions (A_2) and (A_3), we have $s_{22}(p) \neq 0$ and the left hand side vanishes at 0 in t with multiplicity at most 3, hence a contradiction follows. □

Lemma 5. *Let $q = (\alpha, \beta, \gamma)$ be a regular point of the curve $C_{P\cap Q}$ such that $s_{22}(p) \neq 0$ with $p = (\alpha, \beta)$. Then q is a regular point of the curve $S_2(x, y, z) = S_1(x, y, z) = 0$. Moreover, the vectors $\nabla P(q), \nabla Q(q)$ generate the same vector space as $\nabla S_2(q)$ and $\nabla S_1(q)$.*

Proof. Using the identities of (Kahoui, 2003, Theorem 4.2), there exists U, V, U', V' such that:

$$s_{22}^2 P = US_2 + VS_1$$
$$s_{22}^2 Q = U'S_2 + V'S_1$$

Since $s_{22}(p) \neq 0$, we have:

$$\nabla P(q) = \frac{U(q)}{s_{22}(p)^2}\nabla S_2(q) + \frac{V(q)}{s_{22}(p)^2}\nabla S_1(q) \qquad \nabla Q(q) = \frac{U'(q)}{s_{22}(p)^2}\nabla S_2(q) + \frac{V'(q)}{s_{22}(p)^2}\nabla S_1(q)$$

Since q is a regular point of $P = Q = 0$, $\nabla P(q)$ and $\nabla Q(q)$ generate a dimension 2 vector space. Thus $\nabla S_2(q)$ and $\nabla S_1(q)$ also generate the same dimension 2 vector space and q is a regular point of the curve $S_2 = S_1 = 0$. □

Proof of Theorem 2. The implication ii. $\implies$ i. is a direct corollary of Lemma 3 and 4.

For the reciprocal, we know that $s_{22}(p) \neq 0$, thus

$$f = \frac{1}{s_{22}}s_{10}^2 + \frac{1}{s_{22}^2}s_{20}s_{11}^2 - \frac{1}{s_{22}^2}s_{21}s_{10}s_{11}$$

Let us denote by A, J and V the matrices and the vector

$$A = \begin{pmatrix} 2s_{22} & -s_{21} \\ -s_{21} & 2s_{20} \end{pmatrix} \qquad J = \begin{pmatrix} s_{10x} & s_{10y} \\ s_{11x} & s_{11cy} \end{pmatrix} \qquad V = \begin{pmatrix} s_{10} \\ s_{11} \end{pmatrix}$$

The resultant satisfies $f = \frac{1}{2s_{22}^2} V^t \cdot A \cdot V$. Let p be a singular point of the curve $f = 0$. According to Theorem 1, $s_{11}(p) = s_{10}(p) = 0$. Moreover, without restriction of generality, we can assume that $(\alpha, \beta, 0)$ satisfy $P(\alpha, \beta, 0) = Q(\alpha, \beta, 0) = 0$ using the property that the resultant is invariant by translation of z in P and Q. In this case, we have also $s_{20}(p) = 0$.

With abuse of notations, we denote by $O_k(x, y)$ a polynomial that is in the ideal $\langle x, y\rangle^k$ where k is a positive integer. In particular we have:

$$O_{k_1}(x, y) \cdot O_{k_2}(x, y) = O_{k_1+k_2}(x, y)$$
$$O_{k_1}(x, y) + O_{k_2}(x, y) = O_{min(k_1,k_2)}(x, y)$$
$$\delta O_k(x, y) = O_{k-1}(x, y) \text{ for } \delta = \partial/\partial_x \text{ or } \partial/\partial_y$$

With this notation, the taylor expansion of V at p gives

$$V(p+(x,y)) = J(p)\begin{pmatrix} x \\ y \end{pmatrix} + O_2(x,y)$$

such that :

$$f(p+(x,y)) = \frac{1}{2s_{22}(p)^2}\begin{pmatrix} x & y \end{pmatrix} J(p)^t \cdot A(p) \cdot J(p)\begin{pmatrix} x \\ y \end{pmatrix} + O_3(x,y)$$

This implies that the Hessian of f at p is the matrix $\frac{1}{s_{22}(p)} J(p)^t \cdot A(p) \cdot J(p)$. If the determinant of the Hessian is not zero, then p is a node. Otherwise we have $\det(A(p))\det(J(p))^2 = 0$. Let us prove in this case that p is an ordinary cusp in f. For that, we need to prove that for every direction $(u,v) \neq (0,0)$, the valuation of t in $f(p+t(u,v))$ is lower or equal to 3. By hypothesis *i.*, $\det(J) \neq 0$, thus $\det(A(p)) = 4s_{22}(p)s_{20}(p) - s_{21}(p)^2 = 0$. In particular, this means that $s_{21}(p) = 0$. In particular recalling that:

$$f = \frac{1}{s_{22}} s_{10}^2 + \frac{1}{s_{22}^2} s_{20} s_{11}^2 - \frac{1}{s_{22}^2} s_{21} s_{10} s_{11}$$

we have for (u,v) such that $a := us_{10_x}(p) + vs_{10_y}(p) \neq 0$:

$$\begin{aligned} s_{10}^2(\alpha+ut,\beta+vt) &= a^2t^2 + O_3(t) \\ s_{20}s_{11}^2(\alpha+ut,\beta+vt) &= O_3(t) \\ s_{21}s_{10}s_{11}(\alpha+ut,\beta+vt) &= O_3(t) \end{aligned}$$

This implies:

$$f(\alpha+ut,\beta+vt) = \frac{1}{s_{22}(p)} a^2t^2 + O_3(t)$$

and for (u,v) such that $us_{10_x}(p) + vs_{10_y}(p) = 0$ there exists a constant $c \neq 0$ such that $(u,v) = (cs_{10_y}, -cs_{10_x})$ and we have:

$$\begin{aligned} f(\alpha+ut,\beta+vt) &= \frac{c^3}{s_{22}(p)^2}(s_{20_x}(p)s_{10_y}(p) - s_{20_y}(p)s_{10_x}(p))(s_{11_x}(p)s_{10_y}(p) - s_{11_y}(p)s_{10_x}(p))^2t^3 \\ &\quad + O_4(t) \\ &= \frac{c^3}{s_{22}(p)^2}\det(G(p))\det(J(p))^2t^3 + O_4(t) \end{aligned}$$

where

$$G := \begin{pmatrix} s_{20_x} & s_{20_y} \\ s_{10_x} & s_{10_y} \end{pmatrix}$$

Lemma 5 implies that $(\alpha,\beta,0)$ is a regular point of $S_2(x,y,z) = S_1(x,y,z) = 0$. On the other hand,

$$\begin{aligned} \nabla S_1(\alpha,\beta,0) &= \begin{pmatrix} s_{10_x}(p) & s_{10_y}(p) & s_{11}(p) \end{pmatrix} \\ \nabla S_2(\alpha,\beta,0) &= \begin{pmatrix} s_{20_x}(p) & s_{20_y}(p) & s_{21}(p) \end{pmatrix} \end{aligned}$$

Since $s_{11}(p) = s_{21}(p) = 0$, the point $(\alpha, \beta, 0)$ is regular in $S_2(x, y, z) = S_1(x, y, z) = 0$ only if the determinant of the matrix $G(p)$ is different from zero. In addition, hypothesis *i.* implies $\det(J(p)) \neq 0$. We thus conclude that for every $(u, v) \neq (0, 0)$, the valuation of t in $f(ut, vt)$ is lower or equal to 3, and p is an ordinary cusp.

Finally, we prove that p is an ordinary cusp if and only if $C_{P\cap Q}$ has a vertical tangent above p at $q = (\alpha, \beta, 0)$. First, if p is an ordinary cusp, then the Hessian of f is zero at p and $\det(A(p)) = 0$. In this case we saw that $s_{21}(p) = 0$ and since $s_{11}(p) = 0$, this implies that $\frac{\partial S_2}{\partial z}(q) = s_{21}(p) = 0$ and $\frac{\partial S_1}{\partial z}(q) = s_{11}(p) = 0$. Using Lemma 5 this implies that $\frac{\partial P}{\partial z}(q) = \frac{\partial Q}{\partial z}(q) = 0$ such that the tangent vector of $C_{P\cap Q}$ at q is vertical. Reciprocally, if the tangent vector of $C_{P\cap Q}$ at q is vertical, then $\frac{\partial P}{\partial z}(q) = \frac{\partial Q}{\partial z}(q) = 0$ and Lemma 5 implies that $\frac{\partial S_2}{\partial z}(q) = 0$, thus S_2 has a double root in z and $\det(A(p)) = 0$. Thus the Hessian of f is vanishing at p and p is an ordinary cusp of f. □

2.3. Checking the assumptions

As opposed to symbolic methods, our numerical approach requires assumptions on the input. To be complete we provide a way to check that the assumptions are fulfilled using only numerical methods. Note that we only provide a semi-algorithm, when it halts one is sure that the assumptions are satisfied. On the other hand, if it is stopped at an arbitrary time threshold, no result is provided. In addition, when the assumptions are satisfied the running time could be considered as a measure of how near the input is from the degenerate ones, that is the set of inputs that do not satisfy the assumptions.

Lemma 6. *The semi-algorithm 1 terminates if and only if the assumptions* (A_1)*,* (A_2)*,* (A_3) *and* (A_4) *are satisfied.*

Proof. We first show that if the semi-algorithm terminates then (A_1), (A_2), (A_3) and (A_4) are satisfied. Indeed, for any box of the subdivision, (a) Lines 5 ensures that the leading coefficients L_P and L_Q of P and Q have no common solutions so that (A_3) holds; (b) Lines 7, 9 and 15 ensure that f, s_{11} and s_{22} do not vanish simultaneously, hence there is at most two points of the curve $C_{P\cap Q}$ above each point of B_0, (A_2) is satisfied; (c) Lines 11 and 17 ensure that the curve $C_{P\cap Q}$ is smooth so that (A_1) holds; Line 19 finally ensures the regularity assumption (A_4).

Conversely, it is easy to see that when the assumptions (A_1), (A_2), (A_3) and (A_4) are satisfied Semi-algorithm 1 will terminate due to the convergence of the interval functions to the actual value of the corresponding function when the diameter of a box tends to 0. □

2.4. Numerical certified isolation

There is no new result in this section, but for the reader's convenience, we recall a classical numerical method to isolate regular solutions of a square system within a given domain via recursive subdivision and show how it applies in our case. Such a subdivision method is often called branch and bound method (Kearfott (1996)) and uses the Krawczyk operator or Kantorovich theorem to certify existence and unicity of solutions. We recall the properties of the Krawczyk operator and propose the naive Algorithm 2 for the isolation of the singularities of a resultant using the characterization of these points proved in Theorem 2. Note that even if the assumptions (A_1) to (A_4) are satisfied, this naive algorithm may fail if a singularity lies on (or near) the boundary of a box during the subdivision. Indeed, for this algorithm to be certified, there is a need to use ε-inflation of a box when using the Krawczyk test and cluster neighboring boxes of

Semi-algorithm 1 Subdivision based checking of assumptions (A_1), (A_2), (A_3) and (A_4)

Input: A box B_0 in $\mathbb{R}^2$ and two polynomials P and Q in $\mathbb{Q}[x, y, z]$.

Output: The semi-algorithm terminates if and only if the assumptions (A_1), (A_2), (A_3) and (A_4) are satisfied.

Let f be the resultant and s_{22}, s_{11}, s_{10} be the subresultant coefficients of P and Q wrt z.
$L := \{B_0\}$
repeat
  $B := L.pop$
  if $0 \in \square L_P(B)$ **and** $0 \in \square L_Q(B)$ **then** ▷ Checking (A_3)
    Subdivide B and insert its children in L, **continue**
  else if $0 \notin \square f(B)$ **then** ▷ Checking if P and Q have no common solution (A_2)
    continue
  else if $0 \notin \square s_{11}(B)$ **then** ▷ Checking if P and Q have at most 1 common solution (A_2)
    $I_z := -\square s_{10}(B)/\square s_{11}(B)$
    if $(0, 0, 0) \in \square \mathbf{t}(B \times I_z)$ **then** ▷ Checking (A_1)
      Subdivide B and insert its children in L, **continue**
    else
      continue
  else if $0 \notin \square s_{22}(B)$ **then** ▷ Checking if P and Q have at most 2 common solutions (A_2)
    $I_z :=$ union of the complex boxes solution of: $\square s_{22}(B)z^2 + \square s_{21}(B)z + \square s_{20}(B) = 0$
    if $(0, 0, 0) \in \square \mathbf{t}(B \times I_z)$ **then** ▷ Checking (A_1)
      Subdivide B and insert its children in L, **continue**
    else if $0 \in \square Jacobian(s_{11}, s_{10})(B)$ **then** ▷ Checking (A_4)
      Subdivide B and insert its children in L, **continue**
    else
      continue
  else
    Subdivide B and insert its children in L, **continue**
until $L = \emptyset$
return true

the subdivision. For simplicity we do not detail this issue and refer for instance to (Stahl, 1995, §5.9),Kearfott (1997); Schichl and Neumaier (2005).

Let F be a mapping from $\mathbb{R}^2$ to $\mathbb{R}^2$ and denote J_F its Jacobian matrix. The following lemma is a classical tool to certify existence and uniqueness of regular solutions of the system $F = \binom{0}{0}$. For simplicity, we state the following lemma on $\mathbb{R}^2$ but this result holds in any dimension.

Lemma 7. *(Krawczyk Krawczyk (1969)(Rump, 1983, §7)) Let B_x, B_y be real intervals, $B = (B_x, B_y)$ be a box in $\mathbb{R}^2$, (x_0, y_0) be the center point of B and $\Delta B = \binom{B_x - x_0}{B_y - y_0}$. Let N be the mapping:*

$$N(x, y) = \binom{x}{y} - J_F(x_0, y_0)^{-1} \cdot F(x, y)$$

and K_F the Krawczyk operator defined by:

$$K_F(B) := N(x_0, y_0) + \square J_N(B) \cdot \Delta B.$$

If $K_F(B)$ is contained in the interior of B then $F = \binom{0}{0}$ has a unique solution in B.

Algorithm 2 Subdivision based isolation of singularities

Input: A box B_0 in $\mathbb{R}^2$ and two polynomials P and Q in $\mathbb{Q}[x, y, z]$ such that the assumptions (A_1), (A_2), (A_3) and (A_4) are satisfied.

Output: A list L_{Sing} of boxes such that each box isolates a singularity of the curve defined by $f = Res_z(P, Q)$, and each singularity in B_0 is in a box of L_{Sing}.

```
Let f be the resultant and s22, s11, s10 be the subresultant coefficients of P and Q wrt z.
L := {B0}
repeat
    B := L.pop
    if 0 ∉ □f(B) or 0 ∉ □s11(B) or 0 ∉ □s10(B) then
        Discard B
    else
        if K(s11,s10)(B) ⊂ int(B) and 0 ∉ □s22(B) then
            Insert B in L_Sing
        else
            Subdivide B and insert its children in L
until L = ∅
return L_Sing
```

The Krawczyk operator can be seen as the mean value evaluation of the Newton mapping. This implies that the refinement, by recursively applying the Krawczyk operator, of a box containing a unique solution is quadratically convergent (Moore and Jones (1977)). We use such a refinement in Algorithms 3, 4 and 5.

Termination of Algorithm 2.. We assume that P, Q satisfy the assumptions $(A_1), (A_2), (A_3)$ and (A_4). Since in this case the singularities of f are either nodes or ordinary cusp points, Theorem 2 implies that they are regular solutions of the system $s_{11} = s_{10} = 0$. This implies that Algorithm 2 will always terminate.

3. Number of real branches at singularities

Algorithm 2 isolates singularities in boxes. The next step is to identify the singularity type, node or ordinary cusp, and compute its local topology i.e. the number of real branches of the curve connected to the singular point.

3.1. Resultant

For a resultant curve, recall that nodes are stable singularities whereas cusps are not, thus a purely numerical method cannot distinguish between node and cusp singularities. In particular, given a box B containing a singularity, let I be a box evaluation of the determinant of the Hessian. If I does not vanish in the considered box, it is a node, but if it contains 0, it can still be a node, but also a cusp. For a node, the local topology is easily deduced from the topological degree of the mapping (f_x, f_y).

Lemma 8. *(Alberti et al., 2008, Theorem 4.15) Let B be a box containing a singularity p of f such that $I := \square \det(H)(B) \neq 0$, then if $I < 0$ then p is connected to 4 real branches, otherwise if $I > 0$, then p is an isolated real point.*

Conversely, if p is a node, then for a small enough box containing p, the determinant of the Hessian does not contain 0 and the number of branches connected to p can be recovered. Thus, when B contains a node singularity of the resultant, Semi-algorithm 3 will always terminate and compute the number of real branches connected to p. Note that in the case when the singularity is an ordinary cusp, Semi-algorithm 3 will not terminate.

Semi-algorithm 3 Number of branches at a resultant singularity

Input: A box B in $\mathbb{R}^2$ output by Algorithm 2 containing a unique singular point p.
Output: The number of branches connected to p.

1: Let f be the resultant and s_{11}, s_{10} be the subresultant coefficients of P and Q wrt z.
2: **while** $0 \in \square \det(\text{Hessian}(f))(B)$ **do**
3: $\quad B := B \cap K_{(s_{11},s_{10})}(B)$
4: **if** $\square \det(\text{Hessian}(f))(B) > 0$ **then return** 0
5: **else return** 4

3.2. Discriminant

In this section we focus on a discriminant curve. Let f be the resultant of P and $Q := P_z$ satisfying the assumptions $(A_1), (A_2), (A_3)$ and (A_4).

The discriminant of P is equal to the resultant of P and P_z divided by the leading term of P in z. Assumption (A_3) implies that the leading coefficient of P in z is constant, such that the curve defined by f is the same as the one defined by the discriminant of P.

As for the resultant, the singularities of the curve $f = 0$ are either nodes or ordinary cusps. Furthermore, for the discriminant curve, the ordinary cusps are stable and we can identify them numerically. Node singularities can be detected and their local topology computed with the same algorithm as in the previous section for the resultant. We will now focus on the case where the singular point is an ordinary cusp. First we show that above an ordinary cusp, the polynomial P has a triple root in z.

Lemma 9. *Under the assumptions $(A_1), (A_2), (A_3), (A_4)$ the point $p = (\alpha, \beta)$ is an ordinary cusp of the discriminant curve $f = 0$ if and only if $P(\alpha, \beta, z)$ has a triple root in z.*

Proof. Under our assumptions, Theorem 2 states that $p = (\alpha, \beta)$ is an ordinary cusp of the discriminant curve $f = 0$ if and only if the curve $C_{P \cap P_z}$ has a vertical tangent above p. This is the case if and only if there exists γ such that $P_z(\alpha, \beta, \gamma) = P_{zz}(\alpha, \beta, \gamma) = 0$. Moreover, (A_2) implies that $P_{zzz}(\alpha, \beta, \gamma) \neq 0$, such that γ is a triple root of $P(\alpha, \beta, z)$. □

It is thus desirable to identify cusps via triple points, the following lemma states the regularity of these points which is a necessary condition to use numerical methods for their isolation.

Lemma 10. *If P has a triple point, and the curve $P = P_z = 0$ is smooth then the point is a regular solution of $P = P_z = P_{zz} = 0$.*

Proof. At the triple point q, the Jacobian of the system $P = P_z = P_{zz} = 0$ is $P_{zzz}(q) \begin{vmatrix} P_x(q) & P_{xz}(q) \\ P_y(q) & P_{yz}(q) \end{vmatrix}$. By assumption, $P_{zzz}(q) \neq 0$. Moreover, since the curve $P = P_z = 0$ is regular, at least one minor of its jacobian matrix is not zero. Since $P_z(q) = 0$ and $P_{zz}(q) = 0$, this means that $\begin{vmatrix} P_x(q) & P_{xz}(q) \\ P_y(q) & P_{yz}(q) \end{vmatrix} \neq 0$. Thus the Jacobian is not zero and q is regular. □

The following more effective version of this Lemma delimits the box containing the triple root.

Lemma 11 (triple points)**.** *Let B be a box containing a unique singular point p of f and assume that $0 \notin \square s_{22}$. The polynomial P has a triple point in z above p if and only if the system $P = P_z = P_{zz} = 0$ has a regular solution in the box $B \times I_z$ where I_z is the interval $\frac{-\square s_{21}}{2\square s_{22}}$.*

Proof. If $P(\alpha, \beta, z)$ has a triple root z_0 for $(\alpha, \beta) \in B$, then it has a multiplicity 2 in $\gcd(P(\alpha, \beta, z), P_z(\alpha, \beta, z))$. In particular z_0 is a double root of the second polynomial subresultant $S_2 = s_{22}z^2 + s_{21}z + s_{20}$, and $z_0 = -\frac{s_{21}(\alpha,\beta)}{2s_{22}(\alpha,\beta)} \subset I_z$. Thus if (α, β) is the projection of a triple point of P, then this point is necessarily in the box $B \times I_z$. Finally if the system $P = P_z = P_{zz} = 0$ has a regular solution in $B \times I_z$, then we can conclude that the $3d$ box contains a triple point of P and that its projection is p. □

An ordinary cusp is connected to exactly 2 real branches. Using Lemma 11, Algorithm 4 classifies the singularities between nodes and ordinary cusps, and compute the number of real branches connected to them. It always terminates since the diameter of the box converges toward 0 such that eventually either $\det(\text{Hessian}(f))(B) \neq 0$ or $K_{(P,P_z,P_{zz})}(B \times I_z) \subset int(B \times I_z)$.

Algorithm 4 Number of branches at a discriminant singularity

Input: A box B in $\mathbb{R}^2$ output by Algorithm 2 containing a unique singular point p.
Output: The number of branches connected to p and its singularity type (node or ordinary cusp).

Let f be the resultant and $s_{2,2}, s_{2,1}, s_{11}, s_{10}$ be the subresultant coefficients of P and P_z wrt z.
while true **do**
  if $\square \det(\text{Hessian}(f))(B) > 0$ **then return** (0, node)
  if $\square \det(\text{Hessian}(f))(B) < 0$ **then return** (4, node)
  $I_z := -\frac{\square s_{21}(B)}{2\square s_{22}(B)}$
  if $K_{(P,P_z,P_{zz})}(B \times I_z) \subset int(B \times I_z)$ **then return** (2, ordinary cusp)
  $B := B \cap K_{(s_{11},s_{10})}(B)$

4. Loop detection near singularities

Now that we know the number of branches n_p connected to a singularity p, we need to ensure that the enclosing box B computed so far does not contain any other branches not connected to p. First we can refine B until the number of branches crossing the boundary of B matches n_p. But this is not enough, since B could contain closed loops of f, see Figure 3. This case can be discarded for a node by ensuring that B contains a unique solution of the system $f_x = f_y = 0$ (Lemma 12), for a cusp we define a specific interval test (Lemma 14).

4.1. Resultant

In the case of nodes, p is a regular solution of the system $f_x = f_y = 0$ since the determinant of the Jacobian of this system is the determinant of the Hessian of f and is not zero at p. Thus we can use standard tools from interval analysis to guarantee that p is the only root in B of the system $f_x = f_y = 0$.

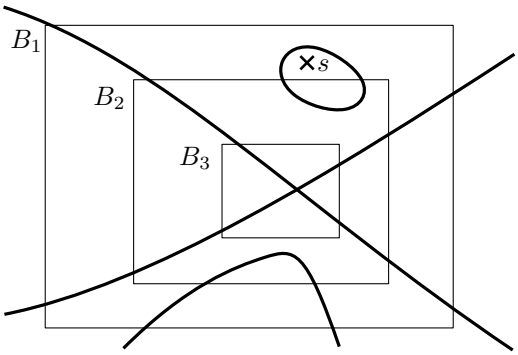

Figure 3: Illustration for Algorithm 5. As input, B_1 is an isolating box of a node that contains a closed loop of the resultant curve $f = 0$. The first refinement of Algorithm 5 yields a box B_2 that avoids the point s solution of the system $f_x = f_y = 0$. B_2 no longer contains the closed loop but is still intersected by branches not connected to the node. The second refinement of Algorithm 5 yields the witness box B_3.

Lemma 12 (Node near loops)**.** *Let $K_{(f_x,f_y)}$ be the Krawczyk operator defined in Lemma 7 with respect to the system $f_x = f_y = 0$, and B be a box containing a node p of f. If $K_{(f_x,f_y)}(B) \subset int(B)$ then B contains no closed loop of f.*

Proof. Lemma 7 ensures that p is the only solution of $f_x = f_y = 0$ in B. If B contains a closed loop included in $int(B)$, then a connected subset of B has its boundary included in the curve defined by f. Thus it contains a point q where f reaches a local extremum and such that $f(q) \neq 0$. In particular, $f_x(q) = f_y(q) = 0$ and $q \neq p$, hence the contradiction. □

Remark 13. *Alternatively, using tools from the next section, denoting by $\square f$ an evaluation of f on the box B, we let $I := \square f_{xx}\square f_{yy} - \square f_{xy}\square f_{xy}$. Then we claim that if I does not contain 0 then B contains at most 1 solution of the system $f_x = f_y = 0$.*

4.2. Discriminant

For the discriminant, the loops near the nodes can be handled as for the resultant. However, the same approach cannot handle ordinary cusps. The problem is that ordinary cusps are singular solutions of the system $f_x = f_y = 0$. We need the following lemma to handle ordinary cusps.

Lemma 14 (Ordinary cusp near loops)**.** *Let p be an ordinary cusp point of f in a box B. Let J, K, L, M be the intervals:*

$$\begin{aligned} J &= \square f_{yy} \\ K &= \square f_{yy}^2\square f_{xxx} - 3\square f_{yy}\square f_{xy}\square f_{xxy} + 3\square f_{xy}^2\square f_{xyy} - \square f_{xy}\square f_{xx}\square f_{yyy} \\ L &= \square f_{yy}\square f_{xxy} + \square f_{xx}\square f_{yyy} - 2\square f_{xy}\square f_{xyy} \\ M &= \square f_{yy}\square f_{xy} - \square f_{xy}\square f_{yy} \end{aligned}$$

and let J', K', L', M' be the intervals obtained by the same formula with x and y swapped. Let $I = JK - LM$ and $I' = J'K' - L'M'$. If (J and I) or (J' and I') do not contain 0, then B does not contain any closed loop of the curve defined by f.

Remark 15. *If B is small enough, then either I or I' does not contain zero.*

When a solution of a system S is singular, there are several ways to check that a box B does not contain any other solutions of S. One way is to compute a univariate polynomial r vanishing on the projection of the solutions of S (with resultant or Gröbner bases), and check that the projection of B contains only one solution of the square-free part of r. Another way is to use a multivariate version of the Rouché theorem (see for instance Verschelde and Haegemans (1994)). In our case, this would amount to solve a system of two polynomials of degree lower than 3 and check if its solutions are within a suitable complex box containing B.

The method we propose is easy to implement and can potentially be extended to other kinds of functions than polynomials. The main idea behind the proof of Lemma 14 is to compute a pseudo-resultant of f_x and f_y in the ring localized at p. Then using the fact that the evaluation on a box of the coefficients of the Taylor expansion of a polynomial f is included in the evaluation of the corresponding derivative of f, we can compute the evaluation of the local elimination polynomial on B using only derivatives of the polynomials f_x and f_y.

Before proving Lemma 14, we define the notion of separation polynomial that we will use.

Definition 16. *Let S be a bivariate polynomial system vanishing on $p = (\alpha, \beta)$, and I_S the ideal generated by its polynomials. Let k be an integer and h be a polynomial such that $h(x, y)(x-\alpha)^k \in I_S$ and $h(p) \neq 0$. Then we say that h is a* separation polynomial.

A classical separation polynomial is obtained by computing the resultant of f and g seen as univariate polynomials in y with coefficients in $K[x]$. We get a polynomial $r(x)$ that can be factorized in $h(x)(x-\alpha)^k$ where $h(\alpha) \neq 0$. However we do not restrict h to be a univariate polynomial.

Lemma 17. *Let h be a separation polynomial and B be a box containing a solution $p = (\alpha, \beta)$ of S. If $0 \notin \square h$, then the solutions of S in B all have the same x-coordinate. Moreover, if there is a polynomial r in I_S such that $0 \notin \square r_y$, then S has only one solution in B.*

Proof. Let $(x_0, y_0) \in B$ such that $x_0 \neq \alpha$. If $h(x_0, y_0) \neq 0$, then $h(x_0, y_0)(x_0 - \alpha)^k \neq 0$. Thus there is a polynomial in I_S that does not vanish on (x_0, y_0) and this point is not a solution of S. Moreover, if (α, y_0) is solution of S with $y_0 \neq \beta$, then $r(\alpha, \beta) = r(\alpha, y_0) = 0$ and r_y has a solution in B which contradicts the second part of the lemma. □

Proof of Lemma 14. Consider the system $f_x = f_y = 0$. Any closed loop of f contains a solution of this system. The cusp point $p = (\alpha, \beta)$ is also solution of this system and if B contains no other solution than p, then B cannot contain a loop. By hypothesis, p is a cusp, hence a singular solution of the system $f_x = f_y = 0$, thus the determinant of the Hessian vanishes and we have: $f_{xy}(p)^2 = f_{x^2}(p) f_{y^2}(p)$. In addition, since p is an ordinary cusp, we know that either $f_{x^2}(p)$ or $f_{y^2}(p)$ is not zero (otherwise the multiplicity would be 4 or more in one direction). Assume without restriction of generality that $f_{y^2}(p) \neq 0$. Let X, Y be two new variables such that $\binom{x}{y} = M \cdot \binom{X}{Y}$ where:

$$M = \begin{pmatrix} f_{yy}(p) & 0 \\ -f_{xy}(p) & 1 \end{pmatrix}$$

In the following, we denote by F the function $f \circ M$, and by $P = (\gamma, \delta)$ the point $M^{-1} \cdot p$. Let H_f be the Hessian of f and H_F be the Hessian of F. Using standard calculus formulas or a computer algebra system, denoting (F_X, F_Y) and (f_x, f_y) by ∇_F and ∇f respectively, we have:

$$\nabla_F \binom{X}{Y} = \nabla_f \binom{x}{y} \cdot M$$
$$H_F = M^T \cdot H_f \cdot M$$

In particular, we have:

$$F_{XY}(P) = f_{yy}(p)f_{xy}(p) - f_{xy}(p)f_{yy}(p) = 0$$
$$F_{XX}(P) = 2f_{yy}(p)(f_{xx}(p)f_{yy}(p) - f_{xy}(p)^2) = 0$$

Thus, letting $\Delta x = x - \alpha$ and $\Delta y = y - \beta$, we can write F_X and F_Y as:

$$F_X(X,Y) = \frac{F_X(X,\delta)}{\Delta x^2}\Delta x^2 + \frac{F_X(X,Y) - F_X(X,\delta)}{\Delta y}\Delta y$$
$$F_Y(X,Y) = \frac{F_Y(X,\delta)}{\Delta x^2}\Delta x^2 + \frac{F_Y(X,Y) - F_Y(X,\delta)}{\Delta y}\Delta y$$

In the following we let $a(x) = \frac{F_X(X,\delta)}{\Delta x^2}$, $b(x,y) = \frac{F_X(X,Y)-F_X(X,\delta)}{\Delta y}$, $c(x) = \frac{F_Y(X,\delta)}{\Delta x^2}$, and $d(x,y) = \frac{F_Y(X,Y)-F_Y(X,\delta)}{\Delta y}$. Using Taylor-Lagrange theorem, we know that if I is an interval, x_0 is a real in I and $g : I \to \mathbb{R}$ is a function satisfying $g(x_0) = 0$, then for any $x \in I$, there exists $x_1 \in I$ such that $g(x) = g'(x_1)(x - x_0)$. In particular, $\frac{g(x)}{x-x_0} \in \square g'$. Moreover, if $g'(x_0) = 0$ as well, then there exists $x_2 \in I$ such that $g(x) = \frac{1}{2}g''(x_2)(x - x_0)^2$. In particular, in this case we have $\frac{g(x)}{(x-x_0)^2} \in \frac{\square g''}{2}$. Applying this theorem on the univariate functions $g_1 : x \mapsto F_X(X,\delta), g_2 : y \mapsto F_X(X,Y) - F_X(X,\delta), g_3 : x \mapsto F_Y(X,\delta)$, and $g_4 : y \mapsto F_Y(X,Y) - F_Y(X,\delta)$, remark that:

$$g_1''(x) = \frac{1}{f_{yy}^2}F_{XXX}(X,\delta) \qquad g_2'(y) = F_{XY}(X,Y)$$
$$g_3''(x) = \frac{1}{f_{yy}^2}F_{XXY}(X,\delta) \qquad g_4'(y) = F_{YY}(X,Y)$$

This allows us to conclude:

$$a(B) \subset \frac{1}{f_{yy}^2}\frac{\square_B F_{XXX}}{2} \qquad b(B) \subset \square_B F_{XY}$$
$$c(B) \subset \frac{1}{f_{yy}^2}\frac{\square_B F_{XXY}}{2} \qquad d(B) \subset \square_B F_{YY}$$

Finally, let letting $h = ad - cb$. Eliminating Δy from F_X and F_Y, we get the polynomial $dF_X - bF_Y = \Delta x^2(ad - cb) = h\Delta x^2$ in the ideal generated by F_X and F_Y. Since F_X and F_Y are an invertible linear combination of f_x and f_y, the polynomial h is in $\left\langle f_x, f_y \right\rangle$. Furthermore we have $h(p) \neq 0$ since $2h(p) = F_{XXX}(P)F_{YY}(P) - F_{XXY}(P)F_{XY}(P) = F_{XXX}(P)F_{YY}(P)$. By assumption, $F_{YY}(P) = f_{yy}(p) \neq 0$ and since p is an ordinary cusp, F vanishes at P in the X direction with a multiplicity at mot 3 by definition, thus $F_{XXX}(P) \neq 0$. Thus h is a separation polynomial. Moreover, using the inclusion given by Taylor-Lagrange theorem, we have:

$$2\square h \subset \frac{1}{f_{yy}(p)^2}\left(\square_B F_{XXX}\square_B F_{YY} - \square_B F_{XXY}\square_B F_{XY}\right)$$

Using standard calculus and the relation $f_{xy}(p)^2 = f_{x^2}(p)f_{y^2}(p)$, we can expand the formula with respect to f:

$$\begin{aligned}
F_{XY} &= f_{yy}(p)f_{xy} - f_{xy}(p)f_{yy} \\
F_{YY} &= f_{yy} \\
F_{XX} &= f_{yy}(p)^2 f_{x^2} - 2f_{y^2}(p)f_{xy}(p)f_{xy} + f_{xy}(p)^2 f_{yy} \\
&= f_{yy}(p)(f_{yy}(p)f_{xx} + f_{xx}(p)f_{yy} - 2f_{xy}(p)f_{xy}) \\
F_{XXY} &= f_{yy}(p)(f_{yy}(p)f_{xxy} + f_{xx}(p)f_{yyy} - 2f_{xy}(p)f_{xyy}) \\
F_{XXX} &= f_{yy}(p)^3 f_{xxx} - 3f_{yy}(p)^2 f_{xy}(p)f_{xxy} + 3f_{yy}(p)f_{xy}(p)^2 f_{xyy} - f_{xy}(p)^3 f_{yyy} \\
&= f_{yy}(p)(f_{yy}(p)^2 f_{xxx} - 3f_{yy}(p)f_{xy}(p)f_{xxy} + 3f_{xy}(p)^2 f_{xyy} - f_{xy}(p)f_{xx}(p)f_{yyy})
\end{aligned}$$

$$\begin{aligned}
2\square h \subset\ & \frac{1}{f_{yy}(p)}\left(f_{yy}(p)^2\square f_{xxx} - 3f_{yy}(p)f_{xy}(p)\square f_{xxy} + 3f_{xy}(p)^2\square f_{xyy} - f_{xy}(p)f_{xx}(p)\square f_{yyy}\right)\square f_{yy} \\
& - \frac{1}{f_{yy}(p)}\left(f_{yy}(p)\square f_{xxy} + f_{xx}(p)\square f_{yyy} - 2f_{xy}(p)\square f_{xyy}\right)(f_{yy}(p)\square f_{xy} - f_{xy}(p)\square f_{yy}) \\
\subset\ & \frac{JK - LM}{J}
\end{aligned}$$

Thus if $0 \notin J$ and $0 \notin JK - LM$ then, $0 \notin \square h$ and $0 \notin \square f_{yy}$, thus, according to Lemma 17, B contains no other solution of $f_x = f_y = 0$ than p.

4.3. Algorithm for the resultant and the discriminant curves

As illustrated on Figure 3, a box output by Algorithms 3 or 4 may contain a closed loop of the curve. Algorithm 5 first refines this box to avoid such closed loops using the interval criteria of Lemmas 12 or 14. The box can still be crossed by branches of the curve not connected to the singular point. Then a second refinement is performed to ensure that the number of crossings of the curve with the box boundary matches the known value given as input: the output box is thus a witness box of the singularity. Note that, in Line 8 of Algorithm 5, computing the intersections of the curve with the box boundary boils down to univariate polynomial isolation for which many certified numerical algorithms exist, see for instance Rouillier and Zimmermann (2003).

5. Experiments

As recalled in introduction, the topology of a curve can be recovered through three steps, computing successively: (1) the singularities, (2) the local topology at the singularities and (3) the global isotopic graph. Even though this is not always clearly reported in previous software experiments, the computation time of steps (1) and (2) usually dominates the one of step (3). For example, in the software Isotop (see (Peñaranda, 2010, § A.1.3) and Cheng et al. (2010)), based on a symbolical approach, step (3) uses at most 5% of the total computation time on resultant curves. The connection step (3) could be done by the subdivision method of Lin and Yap (2011) that computes the topology of non-singular curves. The experiments reported in Lin and Yap (2011) show that this step should not be dominating in our proposed algorithm. We thus focus our experimental comparisons on the steps (1) and (2).

One of the main advantage of our approach is that the singularities are the regular solutions of a square system and step (1) consists in isolating those solutions. This allows us to use a certified

Algorithm 5 Witness box of a singularity

Input: A box B in $\mathbb{R}^2$ output by Algorithm 3 or Algorithm 4 containing a unique singular point p with its type: node or cusp and n_p its number of branches.
Output: A witness box of the singularity p.

Let f be the resultant and s_{11}, s_{10} be the subresultant coefficients of P and Q wrt z.
while true **do**
  if B-type = node **and** $K_{(f_x,f_y)}(B) \subset int(B)$ **then break**
  if B-type = cusp **then**
    Compute I and I' as defined in Lemma 14
    if $0 \notin I$ **or** $0 \notin I'$ **then break**
  $B := B \cap K_{(s_{11},s_{10})}(B)$
while $n_p \neq$ (number of crossings of $f = 0$ with the boundary of B) **do**
  $B := B \cap K_{(s_{11},s_{10})}(B)$
return B

subdivision-based solver to isolate and certify the solutions (Algorithm 2). In Section 5.2, we compare this approach with the methods used to isolate singularities in state-of-the-art algorithms to computing the topology of a curve.

For step (2), we need to refine the boxes around each singularity until the local topology is trivial inside the box (Algorithms 3, 4 and 5). We observe experimentally in section 5.3 that the number of evaluations required to refine the boxes is small and that multiprecision arithmetic is needed for the certification.

All softwares were tested on a Intel(R) Xeon(R) CPU L5640 @ 2.27GHz machine with Linux. Running times given here have to be understood as sequential times in seconds.

Data for Tables 1, 2 and 3.. Random dense polynomials P, Q are generated with given degree d and bitsize σ, that is the coefficients are integers chosen uniformly at random with absolute values smaller than 2^σ. Unless explicitly stated, the given running times are averages over five instances for each pair (d, σ).

5.1. Details of implementations

Symbolic methods.. We tested `RS4`, developed by F. Rouillier, that is specialized for bivariate systems and uses triangular decompositions and Rational Univariate Representations(RUR); it is shown in Bouzidi et al. (2011); Bouzidi (2014) that it is one of the best bivariate solvers. Roughly speaking, it performs two steps: the first one, purely symbolic, computes the RUR of the system. The second one is the numeric isolation of the solutions. A more stable but less efficient version, called `RSCube`[2], can be found as a package for the software `Maple`.

The first column of Tables 1 and 2 reports running times in seconds for `RS4` for isolating the real solutions of the system $\{s_{11}, s_{10}\}$. Recall that solutions of this system are singularities of the curve only if they also are solutions of the resultant $f = \text{Resultant}_z(P, Q)$.

We did also test the routine `Isolate` of the package `RootFinding` natively available within `Maple`. Since it deals with over-determined systems, it has been used to isolate solutions of $\{s_{11}, s_{10}, f\}$. Obtained results are not reported in Tables 1 and 2 because they are outperformed by `RS4` in every cases.

[2] available at https://gforge.inria.fr/projects/rsdev/

Homotopy methods.. We tested two homotopy solvers, `HOM4PS` Lee et al. (2008) and `Bertini` Bates et al. (2013). These methods do not accept constraints, thus the isolation of the system $\{s_{11}, s_{10}\}$ is performed. Note that the path tracking of these software is not certified and solutions can be missed when the path tracker jumps from one path to another. We measure the reliability of a resolution by comparing the number of obtained complex solutions to the Bézout bound of the system, which is the actual number of solutions since our systems are dense and regular. In Tables 1 and 2, this measure is reported in the column nsol/deg. Notice that we tackled the problem of overflows that can arise when representing large integers by normalizing coefficients of input polynomials.

Subdivision method.. We have implemented Algorithms 2, 3, 4 and 5 within the mathematical software `sage`. The critical sub-algorithms are the evaluation of polynomials and the Krawczyk operator. Since the subresultant polynomials s_{10} and s_{11} have a large number of monomials with very large coefficients, an important issue lies in both efficiency and sharpness of their interval evaluation. We used the `fast_polynomial` library Moroz (2013) that allows to compile polynomial evaluations using Horner scheme. The double precision interval arithmetic of the `C++ boost` library is used for Tables 1 and 2. For Table 3, we used the quadruple precision interval arithmetic of MPFI Revol and Rouillier (2005). We used the centered form at order two evaluation of polynomials that requires to compute symbolically partial derivatives up to order two of polynomials. Precisely, for a box B with center c, $\square f(B) = f(c) + J_f(c)(B - c) + \frac{1}{2}H_f(B)(B - c)^2$ where J_f is the Jacobian and H_f the Hessian of f. This evaluation form is studied in (Neumaier, 1990, §2.4) and proved to be quadratically convergent. It happened to be more efficient in our experiments than the classical mean value form. In the Krawczyk operator, derivatives of s_{10} and s_{11} are evaluated at order 1.

Algorithm 2 performs the isolation in a bounded box. To extend the isolation to all real solutions, we use a method introduced by (Neumaier, 1990, p. 210) (see also (Stahl, 1995, §5.10) for a two dimensional example). By changes of variables, this method transforms the isolation problem in $\mathbb{R}^2$ to three isolations in the bounded box $[-1, 1] \times [-1, 1]$. The running times of Algorithm 2 are given for the input box $[-1, 1] \times [-1, 1]$ and for the global isolation in $\mathbb{R}^2$. Concerning the isolation in $[-1, 1] \times [-1, 1]$, the column diam of Tables 1 and 2 gives the minimum value of $\log_{10}(diam(B))$ for all boxes B either discarded or inserted in the list of results L_{sing} in Algorithm 2, and $diam(B)$ stands for the diameter of B.

5.2. *Singularities isolation: Tables 1 and 2*

We analyze the results obtained with different approaches to isolate singularities of a plane curve defined by $\text{Resultant}_z(P, Q) = 0$. Table 1 reports results for a constant bitsize $\sigma = 8$ and a variable degree d while in Table 2 the degree is a constant $d = 4$ and the bitsize σ is the variable. Note that for input polynomials P and Q of total degree d, the total degree of the resultant curve is d^2.

- For all methods, the running times increases significantly with the degree of the input polynomials.
- Only the symbolic method has a significant increase of running time with the bitsize of the input polynomials.

- HOM4PS performs computation in double precision. Notice that it fails to parse input polynomials with large numbers of monomials. For instance, for P, Q of degree 8, the subresultant polynomial s_{10} has 1326 monomials. In addition, as reported by the column nsol/deg, HOM4PS fails to find all solutions.

  Bertini allows to use adaptive multi-precision and this has two consequences. First, Bertini was almost always able to isolate all solutions, thus we did not add the column nsol/deg as for HOM4PS. It only failed once in our experiments for a pair of input polynomials of degree 7 with bitsize 8, where the maximum precision of 1024 bits has been reached. Note also that for a degree larger than 7, we only computed a subset of the solutions so we cannot report on this reliability measure. Second, the multi-precision arithmetic has a heavy cost.

  Bertini is thus more reliable but also slower than HOM4PS.

- The isolation by subdivision in $\mathbb{R}^2$ is roughly three times more expensive than in the bounded box $[-1,1] \times [-1,1]$. This is consistent with the fact that the isolation in $\mathbb{R}^2$ involves three isolations of systems of roughly the same complexity on this bounded box.

- With constant values of (d, σ), running times of the subdivision approach have a high variance. For instance, when $(d, \sigma) = (5, 4)$ running times for the isolation in $\mathbb{R}^2$ are, for the five instances, $(229, 4.56, 3.03, 1.67, 2.08)$.

- Our approach is certified and more efficient than both homotopic and symbolic tested methods when $d > 6$ for all the tests we did perform.

5.3. Topology around singularities

We focus here on the computation of the topology around singularities of resultant and discriminant curves by applying successively Algorithms 3 or 4, and 5.

Table 3 reports the results for different degrees d and constant bitsize $\sigma = 8$ input polynomials. Algorithms 3 or 4, and 5 are applied on all boxes containing singularities given by our global subdivision method. Table 3 gives, for each type of curve and each pair (d, σ) the minimum, median and maximum of values $\log_{10}(diam(B))$ where B are the output witness boxes for which the topology is computed and certified. The large range of sizes for local topology certified boxes is due to the diversity of the local geometry of the curve around a singular point: a singular point may be near to another or near to a branch of the curve not connected to it locally. The sizes are smaller for certifying singularities of a discriminant curve since the test involves higher degrees polynomials to be evaluated. Due to the quadratic convergence of the Krawczyk iteration used for the refinement of boxes, the cost of Algorithms 3, 4 and 5 is small compared to the initial isolation. As an example, even for the smallest box of width $\sim 10^{-17}$ for a discriminant curve, only 6 iterations were performed from the isolating box which was of width $\sim 10^{-4}$.

We finally propose to appreciate the quality of different tests presented in this paper on an example with a cusp and a nearby loop. Consider the polynomial P_{cusp} defined as follows

$$P_{\text{cusp}} = (z^3 + zx - y)((x - \delta')^2 + (z-1)^2 + y^2) - (\delta'/3)^2$$

Its discriminant curve with respect to z is schematically drawn in the left part of Figure 4. This curve has a cusp point near $(0, 0)$ and a loop at a distance $\delta \simeq \delta'$ of this cusp point. The radius of the loop is approximately δ. While the value of δ' decreases, we compute

- the largest diameter τ_K of a box B centered at the cusp point such that $K_{(s_{11},s_{10})}(B) \subset B$,
- the largest diameter τ_C of a box B centered at the cusp point such that Algorithm 4 detects that the singularity in B is a cusp,
- the largest diameter τ_L of a box B centered at the cusp point such that the test of Lemma 14 is satisfied.

The right part of figure 4 displays the values of $\log_{10}(\frac{\tau_K}{\delta})$, $\log_{10}(\frac{\tau_C}{\delta})$, $\log_{10}(\frac{\tau_L}{\delta})$ when $\log_{10}(\delta)$ varies in $[-0.5, -6]$. For instance, when $\delta' = 2^{-16} \simeq 1.5 * 10^{-5}$, we obtain $\delta \simeq 10^{-5}$, $\tau_L \simeq 3.9 * 10^{-9}$, $\tau_K \simeq 3 * 10^{-11}$ and $\tau_C \simeq 1.7 * 10^{-21}$. In this very precise case, the isolation of the singularities in the initial box $[-1, 1]\times[-1, 1]$ together with the computation of the local topology with our certified numerical method takes 2.94 seconds.

Notice that once a singularity has been isolated in a box B by the subdivision process, the box B' allowing to certify the nature of the singularity is obtained by contracting B with the Krawczyk operator, which is known to be quadratically convergent. In the above example, when $\delta' = 2^{-16}$, three iterations of the Krawczyk operator are needed to obtain the suitable box. As a consequence, rather than having an incidence on the computation time, the high gradient of τ_C with respect to δ leads to the need of a multi-precision arithmetic to carry out the topology certification.

Finally one can remark that in this example the test to avoid loops presented in Lemma 14 do not require to contract the box obtained by the subdivision process to be fulfilled.

Acknowledgments

The authors would like to thank Laurent Busé and Éric Schost for fruitful discussions. This research was supported by the ANR JCJC SingCAST (ANR-13-JS02-0006).

Akoglu, T. A., Hauenstein, J. D., Szántó, Á., 2014. Certifying solutions to overdetermined and singular polynomial systems over Q. CoRR abs/1408.2721.
URL http://arxiv.org/abs/1408.2721

Alberti, L., Mourrain, B., Wintz, J., 2008. Topology and arrangement computation of semi-algebraic planar curves. Comput. Aided Geom. Des. 25 (8), 631–651.

Bates, D. J., Hauenstein, J. D., Sommese, A. J., Wampler, C. W., 2013. Bertini: Software for numerical algebraic geometry. Available at bertini.nd.edu with permanent doi: dx.doi.org/10.7274/R0H41PB5.

Beltrán, C., Leykin, A., 2013. Robust certified numerical homotopy tracking. Foundations of Computational Mathematics, 1–43.

Bouzidi, Y., Mar. 2014. Solving bivariate algebraic systems and topology of plane curves. Theses, Université de Lorraine.
URL https://tel.archives-ouvertes.fr/tel-00979707

Bouzidi, Y., Lazard, S., Pouget, M., Rouillier, F., 2011. New bivariate system solver and topology of algebraic curves. In: 27th European Workshop on Computational Geometry - EuroCG.
URL http://hal.inria.fr/inria-00580431/en

Burr, M., Choi, S. W., Galehouse, B., Yap, C. K., 2012. Complete subdivision algorithms ii: Isotopic meshing of singular algebraic curves. Journal of Symbolic Computation 47 (2), 131 – 152.
URL http://www.sciencedirect.com/science/article/pii/S0747717111001337

Busé, L., Mourrain, B., 2009. Explicit factors of some iterated resultants and discriminants. Mathematics of Computation 78 (265), 345–386.

Cheng, J., Lazard, S., Peñaranda, L., Pouget, M., Rouillier, F., Tsigaridas, E., 2010. On the topology of real algebraic plane curves. Mathematics in Computer Science 4, 113–137.
URL http://dx.doi.org/10.1007/s11786-010-0044-3

Corless, R. M., Diaz-Toca, G. M., Fioravanti, M., Gonzalez-Vega, L., Rua, I. F., Shakoori, A., 2013. Computing the topology of a real algebraic plane curve whose defining equations are available only "by values". Comput. Aided Geom. Design 30 (7), 675–706.
URL http://dx.doi.org/10.1016/j.cagd.2013.04.003

Table 1: Isolating singularities of $\text{Resultant}_z(P, Q) = 0$, with P and Q of degree d and coefficients of constant bitsize $\sigma = 8$. The running times are in seconds, the value diam is the minimum value of $\log_{10}(diam(B))$ for all boxes B considered in Algorithm 2, where $diam(B)$ is the diameter of the box.

	RS4	HOM4PS		Bertini	Subdivision		
domain	$\mathbb{R}^2$	$\mathbb{C}^2$		$\mathbb{C}^2$	$[-1,1]\times[-1,1]$		$\mathbb{R}^2$
d, σ	t	t	nsol/deg	t	t	diam	t
4, 8	0.214	0.078	98.6%	3.256	0.435	-3.2	1.071
5, 8	2.845	1.543	96.3%	124.774	0.682	-3.0	2.678
6, 8	23.90	15.18	90.3%	1604 (2)	3.067	-3.8	9.630
7, 8	137.9	97.95	75.5%	83120 (2)	8.469	-4.4	27.43
8, 8	725.7	(1)	(1)	382200 (2,3)	43.47	-5.0	82.98
9, 8	2720 (2)	(1)	(1)	2766400 (2,3)	47.25	-4.8	273.2

(1) Fails with segmentation false (does not support polynomials with large number of terms)
(2) Has been run on a unique example
(3) Time has been obtained by interpolating the time spent for tracking a unique path

Table 2: Isolating singularities of $\text{Resultant}_z(P, Q) = 0$, with P and Q of constant degree $d = 5$ and coefficients of bitsize σ. The running times are in seconds, the value diam is the minimum value of $\log_{10}(diam(B))$ for all boxes B considered in Algorithm 2, where $diam(B)$ is the diameter of the box.

	RS4	HOM4PS		Bertini	Subdivision		
domain	$\mathbb{R}^2$	$\mathbb{C}^2$		$\mathbb{C}^2$	$[-1,1]\times[-1,1]$		$\mathbb{R}^2$
d, σ	t	t	nsol/deg	t	t	diam	t
5, 4	1.788	1.532	94.63%	263.4	0.755	-3.2	48.13
5, 8	2.845	1.543	96.32%	124.7	0.682	-3.0	2.678
5, 16	4.687	1.431	93.60%	300.2	7.052	-4.2	19.22
5, 32	7.468	1.817	94.48%	264.2	2.439	-3.6	7.173
5, 64	13.33	1.728	96.98%	233.7	1.906	-3.4	4.676

Table 3: Computing topology around singularities of discriminant (resp. resultant) curves when P (resp. P, Q) has degree d and constant bit-size $\sigma = 8$. The values min, med and max are the minimum, median and maximum values of $\log_{10}(diam(B))$ where B are the witness boxes computed by Algorithms 3 or 4, and 5 and $diam(B)$ is the diameter of the box.

	Resultant			Discriminant		
d, σ	min	med	max	min	med	max
4, 8	−5	−4	−2	−12	−5	−3
5, 8	−6	−4	−2	−9	−4	−3
6, 8	−8	−5	−3	−17	−5	−2
7, 8	−9	−4	−3	−15	−6	−3
8, 8	−12	−5	−3	−12	−6	−2
9, 8	−9	−5	−3	−15	−6	−3

Cox, D., Little, J., O'Shea, D., 2005. Using Algebraic Geometry, 2nd Edition. No. 185 in Graduate Texts in Mathematics. Springer, New York.

Dedieu, J., 2006. Points fixes, zéros et la méthode de Newton. Mathématiques et Applications. Springer.

Delanoue, N., Lagrange, S., 2014. A numerical approach to compute the topology of the apparent contour of a smooth mapping from R^2 to R^2. Journal of Computational and Applied Mathematics 271, 267–284.
URL http://www.sciencedirect.com/science/article/pii/S0377042714001812

Emeliyanenko, P., Sagraloff, M., 2012. On the complexity of solving a bivariate polynomial system. In: Proceedings of the 37th international symposium on Symbolic and algebraic computation. ISSAC '12. pp. 154–161.

Giusti, M., Lecerf, G., Salvy, B., Yakoubsohn, J.-C., Feb. 2007. On location and approximation of clusters of zeros: Case of embedding dimension one. Found. Comput. Math. 7 (1), 1–58.
URL http://dx.doi.org/10.1007/s10208-004-0159-5

Hauenstein, J. D., Sottile, F., Aug. 2012. Algorithm 921: alphacertified: Certifying solutions to polynomial systems. ACM Trans. Math. Softw. 38 (4), 28:1–28:20.
URL http://doi.acm.org/10.1145/2331130.2331136

Jouanolou, J. P., 1979. Singularités rationnelles du résultant. In: Algebraic geometry (Proc. Summer Meeting, Univ. Copenhagen, Copenhagen, 1978). Vol. 732 of Lecture Notes in Math. Springer, Berlin, pp. 183–213.

Kahoui, M. E., 2003. An elementary approach to subresultants theory. J. Symb. Comput. 35 (3), 281–292.

Kearfott, R. B., 1996. Rigorous global search: continuous problems. Nonconvex optimization and its applications. Kluwer Academic Publishers, Dordrecht, Boston.
URL http://opac.inria.fr/record=b1092397

Kearfott, R. B., 1997. Empirical evaluation of innovations in interval branch and bound algorithms for nonlinear systems. SIAM Journal on Scientific Computing 18 (2), 574–594.

Krawczyk, R., 1969. Newton-Algorithmen zur Bestimmung von Nullstellen mit Fehlerschranken. Computing (Arch. Elektron. Rechnen) 4, 187–201.

Lee, T., Li, T., Tsai, C., 2008. Hom4ps-2.0: a software package for solving polynomial systems by the polyhedral homotopy continuation method. Computing 83 (2-3), 109–133.
URL http://dx.doi.org/10.1007/s00607-008-0015-6

Leykin, A., Verschelde, J., Zhao, A., 2006. Newton's method with deflation for isolated singularities of polynomial systems. Theoretical Computer Science 359 (13), 111 – 122.
URL http://www.sciencedirect.com/science/article/pii/S030439750600168X

Liang, C., Mourrain, B., Pavone, J., 2008. Subdivision methods for 2d and 3d implicit curves. In: Geometric modeling and algebraic geometry. Springer, pp. 171–186.

Lin, L., Yap, C., 2011. Adaptive isotopic approximation of nonsingular curves: the parameterizability and nonlocal isotopy approach. Discrete & Computational Geometry 45 (4), 760–795.
URL http://dx.doi.org/10.1007/s00454-011-9345-9

Lorensen, W. E., Cline, H. E., August 1987. Marching cubes: A high resolution 3d surface construction algorithm. SIGGRAPH Comput. Graph. 21, 163–169.
URL http://doi.acm.org/10.1145/37402.37422

Lu, Y., Bates, D. J., Sommese, A. J., Wampler, C. W., 2007. Finding all real points of a complex curve. In: Algebra, geometry and their interactions. Vol. 448 of Contemp. Math. Amer. Math. Soc., Providence, RI, pp. 183–205.
URL http://dx.doi.org/10.1090/conm/448/08665

Mantzaflaris, A., Mourrain, B., 2011. Deflation and certified isolation of singular zeros of polynomial systems. In: Proceedings of the 36th international symposium on Symbolic and algebraic computation. ISSAC '11. ACM, New York, NY, USA, pp. 249–256.
URL http://doi.acm.org/10.1145/1993886.1993925

Martin, B., Goldsztejn, A., Granvilliers, L., Jermann, C., 2013. Certified parallelotope continuation for one-manifolds. SIAM J. Numerical Analysis 51 (6), 3373–3401.

Moore, R. E., Jones, S. T., 1977. Safe starting regions for iterative methods. SIAM Journal on Numerical Analysis 14 (6), 1051–1065.
URL http://dx.doi.org/10.1137/0714072

Moroz, G., Jul. 2013. Fast polynomial evaluation and composition. Technical Report RT-0453, Inria Nancy - Grand Est (Villers-lès-Nancy, France).
URL https://hal.archives-ouvertes.fr/hal-00846961

Mourrain, B., Pion, S., Schmitt, S., Técourt, J.-P., Tsigaridas, E. P., Wolpert, N., 2006. Algebraic issues in Computational Geometry. In: Boissonnat, J.-D., Teillaud, M. (Eds.), Effective Computational Geometry for Curves and Surfaces. Mathematics and Visualization. Springer, Ch. 3, pp. 117–155.

Myszka, D. H., Murray, A. P., Wampler, C. W., 2013. Computing the branches, singularity trace, and critical points of single degree-of-freedom, closed-loop linkages. Journal of Mechanisms and Robotics 6 (1).
URL http://dx.doi.org/10.1115/1.4025752y

Neumaier, A., 1990. Interval methods for systems of equations. Cambridge University Press.
URL http://www.loc.gov/catdir/toc/cam041/89070812.html

Ojika, T., Watanabe, S., Mitsui, T., 1983. Deflation algorithm for the multiple roots of a system of nonlinear equations. Journal of Mathematical Analysis and Applications 96 (2), 463 – 479.
URL http://www.sciencedirect.com/science/article/pii/0022247X83900550

Peñaranda, L. M., Dec. 2010. Non-linear computational geometry for planar algebraic curves. Theses, Université Nancy II.
URL https://tel.archives-ouvertes.fr/tel-00547829

Plantinga, S., Vegter, G., 2004. Isotopic approximation of implicit curves and surfaces. In: SGP '04: Eurographics/ACM SIGGRAPH Symposium on Geometry Processing. pp. 245–254.

Recknagel, J., Aug. 2013. Topology of planar singular curves resultant of two trivariate polynomials. Bachelor's Thesis.
URL http://hal.inria.fr/hal-00927768

Revol, N., Rouillier, F., 2005. Motivations for an arbitrary precision interval arithmetic and the mpfi library. Reliable Computing 11, 1–16.

Rouillier, F., Zimmermann, P., 2003. Efficient isolation of polynomial real roots. J. of Computational and Applied Mathematics 162 (1), 33–50.

Rump, S. M., 1983. Solving algebraic problems with high accuracy. In: Proc. of the symposium on A new approach to scientific computation. Academic Press Professional, Inc., San Diego, CA, USA, pp. 51–120.
URL http://dl.acm.org/citation.cfm?id=312.316

Schichl, H., Neumaier, A., 2005. Exclusion regions for systems of equations. SIAM Journal on Numerical Analysis 42 (1), pp. 383–408.
URL http://www.jstor.org/stable/4101140

Seidel, R., Wolpert, N., 2005. On the exact computation of the topology of real algebraic curves. In: Proc 21st ACM Symposium on Computational Geometry. pp. 107–115.

Snyder, J. M., 1992. Interval analysis for computer graphics. In: Proceedings of the 19th annual conference on Computer graphics and interactive techniques. SIGGRAPH '92. ACM, New York, NY, USA, pp. 121–130.
URL http://doi.acm.org/10.1145/133994.134024

Stahl, V., 1995. Interval methods for bounding the range of polynomials and solving systems of nonlinear equations. Ph.D. thesis, Johannes Kepler University, Linz, Austria.

Szafraniec, Z., 1988. On the number of branches of a 1-dimensional semianalytic set. Kodai Math. J. 11 (1), 78–85.
URL http://dx.doi.org/10.2996/kmj/1138038822

Van Der Hoeven, J., May 2011. Reliable homotopy continuation. Tech. rep., LIX, École Polytechnique.
URL http://hal.archives-ouvertes.fr/hal-00589948

Verschelde, J., Haegemans, A., Oct. 1994. Homotopies for solving polynomial systems within a bounded domain. Theor. Comput. Sci. 133 (1), 165–185.
URL http://dx.doi.org/10.1016/0304-3975(94)00064-6

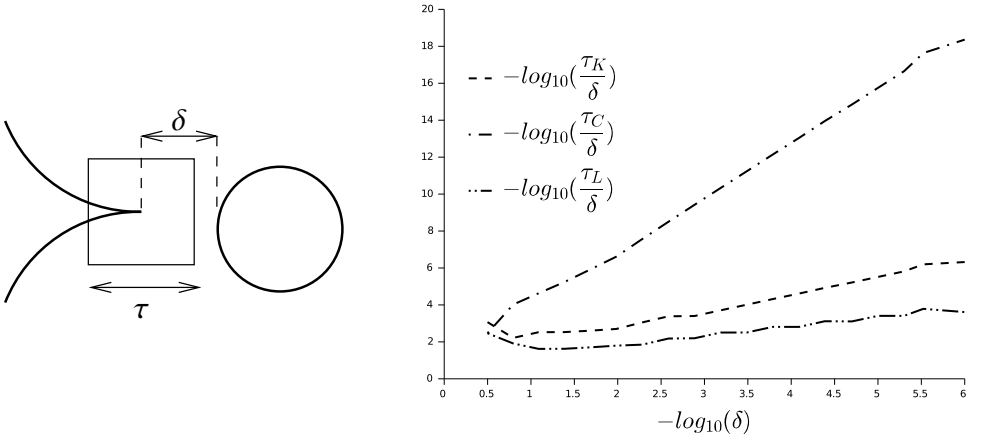

Figure 4: Left: a schematic representation of the discriminant of the polynomial P_{cusp}. Right: largest diameters τ_K, τ_C, τ_L of a certified box as a function of the parameter δ.