



**HAL**  
open science

# Numeric certified algorithm for the topology of resultant and discriminant curves

Guillaume Moroz, Marc Pouget

## ► To cite this version:

Guillaume Moroz, Marc Pouget. Numeric certified algorithm for the topology of resultant and discriminant curves. [Research Report] RR-8653, Inria. 2014. hal-01093040v2

**HAL Id: hal-01093040**

**<https://inria.hal.science/hal-01093040v2>**

Submitted on 7 Jan 2015 (v2), last revised 27 Apr 2015 (v3)

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



# Numeric certified algorithm for the topology of resultant and discriminant curves

Guillaume Moroz, Marc Pouget

**RESEARCH  
REPORT**

**N° 8653**

Decembre 2014

Project-Team Vegas





## Numeric certified algorithm for the topology of resultant and discriminant curves

Guillaume Moroz, Marc Pouget

Project-Team Vegas

Research Report n° 8653 — Decembre 2014 — 16 pages

**Abstract:** Let  $\mathcal{C}$  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 cusp). State-of-the-art numerical algorithms cannot handle the computation of its topology. The main challenge is to find 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  $\mathcal{C}$ . We solve this problem by providing a square deflation system that can be used to certify numerically whether  $B$  contains a singularity  $p$ . Then we introduce a numeric adaptive separation criterion based on interval arithmetic to ensure that the topology of  $\mathcal{C}$  in  $B$  is homeomorphic to the local topology at  $p$ .

**Key-words:** Topology of algebraic curves, resultant, discriminant, subresultant, numerical algorithm, singularities, interval arithmetic, node and cusp singularities

RESEARCH CENTRE  
NANCY – GRAND EST

615 rue du Jardin Botanique  
CS20101  
54603 Villers-lès-Nancy Cedex

## Algorithmes numériques certifiés pour la topologie d'une courbe résultante ou discriminante

**Résumé :** Bien que francophones et très attachés à notre langue maternelle, nous avons pensé et rédigé ce travail en anglais comme la grande majorité de la production scientifique mondiale. Dans ce contexte, il est clair que cette version française de l' "abstract" n'a aucun intérêt pour notre communauté, et nous avons peu d'espoir qu'il puisse en être autrement même en dehors de notre communauté. Nous proposons néanmoins quelques pistes en français pour cet improbable lecteur et serions comblés si celui-ci en venait à apprendre l'anglais pour pouvoir lire notre prose.

Nous étudions la topologie d'une courbe plane issue de la projection d'une courbe lisse dans l'espace. Génériquement, la projection présente des singularités de type noeud et cusp (dans le cas d'un discriminant seulement). Les algorithmes numériques de l'état de l'art ne calculent la topologie que dans le cas de courbes lisses. L'enjeu est donc de concevoir des critères numériques garantissant l'existence et l'unicité d'une singularité dans une boîte donnée, tout en assurant que cette boîte ne contienne pas d'autre partie de la courbe non connectée à ce point dans la boîte. Nous proposons une déflation basée sur les sous-résultants pour le premier problème ainsi qu'un critère de séparation basée sur de l'arithmétique d'intervalles pour le second problème.

**Mots-clés :** Topologie de courbes algébriques, résultant, discriminant, sous-résultant, algorithmes numériques, singularités, arithmétique d'intervalles, noeuds et cusps

## 1 Introduction

Given a bivariate polynomial  $f$  with rational coefficients, a classical problem is the computation of the topology of the real plane curve  $\mathcal{C} = \{(x, y) \in \mathbb{R}^2 \mid f(x, y) = 0\}$ . 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  $\mathcal{C}$ . 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 but can only handle non-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.

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 graphs connecting the boxes.

The third step can be done using existing certified numerical algorithms (e.g. [GG10, vdH11, BL13]). For the first step, numerical algorithms cannot certify singularities of a curve defined by  $f$  in the general case.

**Contribution and overview** 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  $Q$ :  $f = \text{Resultant}_z(P, Q)$ . We show that it is possible to certify its singularities and compute its local topology with adaptive numerical algorithms. More precisely, Section 2 presents a numerical algorithm to isolate and certify nodes and ordinary cusp points of  $f$ . Section 3.1 describes how to compute the local topology of nodes of  $f$ . Finally, when  $Q = \frac{\partial P}{\partial z}$ , Section 3.2 describes how to compute the local topology of nodes and ordinary cusps of  $f$ .

**Notations** Let  $f$  be a bivariate polynomial and  $\mathcal{C}$  its 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  $\det(\text{Hessian}(f)) = f_{xy}^2 - f_{xx}f_{yy} \neq 0$ . 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.

Given an interval box  $B \subset \mathbb{R}^2$ , we denote by  $\square f(B)$  the interval of  $\mathbb{R}$  defined by replacing the arithmetic operations  $+$ ,  $-$ ,  $\times$  by the corresponding interval operations (note that due to the non-distributivity of interval operations, different evaluation schemes of the same function  $f$  give different interval functions). By abuse of notation, we often simply denote  $\square f(B)$  by  $\square f$ . The Krawczyk operator of a mapping  $F$  defined in Lemma 2 is denoted by  $K_F$ .

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  $i^{\text{th}}$  subresultant polynomial is of degree at most  $i$  (see e.g. [Kah03, §3]), we denote it  $S_i(z) = s_{ii}z^i + s_{i,i-1}z^{i-1} + \dots + s_{i0}$ . The resultant is thus  $S_0(z) = s_{00}$  in  $\mathbb{D}$  and we also denote it more classically as  $\text{Res}_z(P, Q)$ . Finally,  $\mathbb{V}(f_1, \dots, f_n)$  denotes the solutions of the system  $f_1 = \dots = f_n = 0$ .

**Previous and related work** There are many works addressing the topology computation via symbolic methods, see for instance the book chapter [MPS<sup>+</sup>06] and references therein. Most of them use subresultant theory, but there are also some alternatives using only resultants (e.g. [SW05, ES11]) or Gröbner bases and rational univariate representations [CLP<sup>+</sup>10]. For the restricted case of non-singular curves, numerical methods are usually faster and can in addition reduce the computation to a user defined bounding box. One can mention certified homotopy methods [vdH11] or ad hoc interval analysis methods [GG10], both being based on the Krawczyk operator [Rum83]. Another well-studied numerical approach is via recursive subdivision of the plane. Indeed, the initial idea of the marching cube algorithm [LC87] can be further improved with interval arithmetic to certify the topology of smooth curves [Sny92, PV04, LMP08]. 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 [Neu90].

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 is to combine its equations in the form  $f_{1x_i}f_1 + \dots + f_{m_{x_i}}f_m = 0$  for each variable  $x_i$ , to transform it into a square system [Ded06], but this introduces spurious solutions. Singular solutions can be handled through deflation [GLSY07, OWM83, LVZ06, MM11], 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 don't have the same local structure. Thus, this cannot be used to separate solutions with different multiplicity structures. When the curve we consider is a resultant, its singular locus can be related to the coefficients of the first subresultant [Jou79]. 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 define the set of points for which the polynomials  $P$  and  $Q$  have two solutions. This approach was considered in [DL13] 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 [Sza88, AMW08, MM11] or with the fiber multiplicity together with isolation on the box boundary [SW05].

Finally, certifying the topology inside a box requires the detection of loops near a singularity. It is usually solved in the literature by isolating of the  $x$ -extreme points, which reduces the problem to a univariate polynomial that is computed with resultants ([SW05, MPS<sup>+</sup>06] for example).

## 2 Subresultant based deflation

In this section, we exhibit a square polynomial system  $g = h = 0$  and two polynomials  $u$  and  $v$  such that the singularities of  $f$  are exactly the solutions of the system  $g = h = u = 0$  and of the system  $g = h = 0$  and  $v \neq 0$ . Moreover, they are regular solution of  $g = h = 0$ , such that we can use numerical method to certify if a box contains or not a singularity.

### 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. In addition, we define the assumptions:

- (A<sub>1</sub>) The intersection of the surfaces  $P(x, y, z) = 0$  and  $Q(x, y, z) = 0$  is a smooth space curve denoted  $\mathcal{C}_{P \cap Q}$ , i.e. the tangent vector  $\mathbf{t} = \nabla P \times \nabla Q$  is nowhere null on  $\mathcal{C}_{P \cap Q}$  (where  $\nabla P$  is the gradient vector  $(P_x, P_y, P_z)$ ).
- (A<sub>2</sub>) Above any point  $(\alpha, \beta)$  in the  $(x, y)$ -plane, there are at most two points of  $\mathcal{C}_{P \cap Q}$  counted with multiplicities, or in other words, the polynomial  $\gcd(P(\alpha, \beta, z), Q(\alpha, \beta, z))$  has degree at most two.
- (A<sub>3</sub>) 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.

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.

**Theorem 1 ([Rec13])** *Let  $f$  be the resultant of the polynomials  $P$  and  $Q$  in  $\mathbb{Q}[x, y, z]$  with respect the variable  $z$ . Then  $S_{sres} \subset S_{sing}$  and if the assumptions (A<sub>1</sub>) to (A<sub>3</sub>) 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 [Kah03, 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,  $\partial(s_{22}^2 f) = 3s_{22}^2 f \partial s_{22} + s_{22}^3 \partial f$  hence  $s_{22}^3 \partial f = \partial(s_{22}^2 f) - 3s_{22}^2 f \partial s_{22}$  with both terms in  $\langle s_{11}, s_{10} \rangle$ , thus  $\partial(s_{22}^3 f)$  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  $(\alpha, \beta)$  be a singular point of  $f$ , so that  $f(\alpha, \beta) = 0$ . According to the generic condition (A<sub>2</sub>),  $\gcd(P(\alpha, \beta, z), Q(\alpha, \beta, z))$  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. [Kah03, Corollary 5.1]) and assumption (A<sub>3</sub>): (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  $(\alpha, \beta)$  is in  $S_{sres}$ .

Otherwise, let  $\gamma$  be a simple root of  $\gcd(P(\alpha, \beta, z), Q(\alpha, \beta, z))$ , the generic condition (A<sub>1</sub>) yields that the tangent vector  $\mathbf{t}(p)$  to  $\mathcal{C}_{P \cap Q}$  at the point  $p = (\alpha, \beta, \gamma)$  is well defined and not vertical. Indeed, the multiplicity of  $\gamma$  in  $\gcd(P(\alpha, \beta, z), Q(\alpha, \beta, z))$  is 1, so it is also one 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<sub>1</sub>)). Without loss of generality we may assume that the  $x$ -coordinate of  $\mathbf{t}(p)$  is not null:  $x_{\mathbf{t}(p)} = P_y(p)Q_z(p) - P_z(p)Q_y(p) \neq 0$ .



We now apply [BM09, 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:  $f_y(\alpha, \beta) = \pm x_{t(p)} s_{11}(\alpha, \beta)$ . Since  $(\alpha, \beta)$  is a singular point of  $f$ ,  $f_y(\alpha, \beta) = 0$ , and together with  $x_{t(p)} \neq 0$  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 two. Together with the generic condition  $(A_2)$ , this degree is exactly two and so is the degree of the second subresultant  $S_2$  evaluated at  $(\alpha, \beta)$ , thus  $s_{22}(\alpha, \beta) \neq 0$ . We then conclude that in this case too  $(\alpha, \beta)$  is in  $S_{sres}$ .

## 2.2 Checking assumptions

As opposed to symbolic methods, our numerical approach requires assumptions on the input. To be complete it is desirable to be able to check that the assumptions are fulfilled using also only numerical methods. We design Algorithm 1 that will terminate iff the assumptions  $(A_1)$ ,  $(A_2)$  and  $(A_3)$  are satisfied.

**Proof of correctness of Algorithm 1.** We first show that if the algorithm terminates then  $(A_1)$ ,  $(A_2)$  and  $(A_3)$  are satisfied. Indeed, for any box of the subdivision, (a) Lines 5 and 6 ensures that the leadings of  $P$  and  $Q$  have no common solutions  $(A_3)$ ; (b) Lines 7, 9 and 15 ensures that  $f, s_{11}$  and  $s_{22}$  do not vanish simultaneously, hence there is at most two points of the curve  $\mathcal{C}_{P \cap Q}$  above each point of  $B_0$ ,  $(A_2)$  is satisfied; (c) Lines 11 and 17 ensures that the curve  $\mathcal{C}_{P \cap Q}$  is smooth  $(A_1)$ .

Conversely, it is easy to see that when the assumptions  $(A_1)$ ,  $(A_2)$  and  $(A_3)$  are satisfied 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.

## 2.3 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 solutions of a 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 [Kea96] 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 Section 2.1. Note that even if the assumptions  $(A_1)$ ,  $(A_2)$  and  $(A_3)$  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  $\varepsilon$ -inflation of a box when using the Krawczyk test and cluster neighboring boxes of the subdivision. For simplicity we do not detail this issue and refer for instance to [Kea97, SN05].

Remark also that this algorithm does not necessary need to be run from the global input box  $B_0$ . The idea is that it may be more efficient in practice to avoid the global subdivision from a large input box. An heuristic alternative is to first compute numerical approximations of the singular points with a non-certified algorithm, for instance using homotopy. Algorithm 2 can then be run on boxes enclosing these approximations. Finally, the certification may be recovered globally on the box  $B_0$  if a post-processing is able to check that there is no solution in the complement of the certified boxes found so far.

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  $F = (0, 0)$ . For simplicity, we state the following lemma on  $\mathbb{R}^2$  but this result holds in any dimension.

---

**Algorithm 1** Subdivision based checking of assumptions  $(A_1)$ ,  $(A_2)$  and  $(A_3)$

---

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

**Output:** The algorithm terminates iff the assumptions  $(A_1)$ ,  $(A_2)$  and  $(A_3)$  are satisfied.

```

1: Let  $f$  be the resultant and  $s_{22}, s_{11}, s_{10}$  be the subresultant coefficients of  $P$  and  $Q$  wrt  $z$ .
2:  $L := \{B_0\}$ 
3: repeat
4:    $B := L.pop$ 
5:   if  $0 \in \square L_P(B)$  and  $0 \in \square L_Q(B)$  then
6:     Subdivide  $B$  and insert its children in  $L$ , continue
7:   else if  $0 \notin \square f(B)$  then
8:     continue
9:   else if  $0 \notin \square s_{11}(B)$  then
10:     $I_z := -\square s_{10}(B) / \square s_{11}(B)$ 
11:    if  $0 \in \square P(B \times I_z)$  and  $0 \in \square Q(B \times I_z)$ 
        and  $(0, 0, 0) \in \square \mathbf{t}(B \times I_z)$  then
12:      Subdivide  $B$  and insert its children in  $L$ , continue
13:    else
14:      continue
15:    else if  $0 \notin \square s_{22}(B)$  then
16:       $I_z :=$  the union of the real intervals or complex boxes  $I_{z_1}$  and  $I_{z_2}$  solutions of the degree
        2 interval polynomial  $\square S_2(B, z)$ 
17:      if  $0 \in \square P(B \times I_z)$  and  $0 \in \square Q(B \times I_z)$ 
        and  $(0, 0, 0) \in \square \mathbf{t}(B \times I_z)$  then
18:        Subdivide  $B$  and insert its children in  $L$ , continue
19:      else
20:        continue
21: until  $L = \emptyset$ 
22: return Assumptions  $(A_1)$ ,  $(A_2)$  and  $(A_3)$  are satisfied.

```

---

**Lemma 2** (*Krawczyk [Kra69][Rum83, §7]*) Let  $B$  be a box in  $\mathbb{R}^2$ ,  $(x_0, y_0)$  the center point of  $B$  and  $\Delta B = \begin{pmatrix} B_x - x_0 \\ B_y - y_0 \end{pmatrix}$ . Let  $N$  be the mapping:

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

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  $F = (0, 0)$  has a unique solution in  $B$ .

In addition, for a small enough box enclosing a regular solution, the previous criterion will eventually succeed to prove the unicity. In the next section, we study sufficient conditions for the system  $s_{11} = s_{10} = 0$  to have regular solutions.

## 2.4 Termination in the case of node and ordinary cusp points

In this section, we assume that  $f$  is a resultant satisfying the assumptions  $(A_1)$ ,  $(A_2)$  and  $(A_3)$ . We show that if furthermore the singularities of  $f$  are either node or ordinary cusp points, then they are regular solutions of the system  $s_{11} = s_{10} = 0$ . This implies that Algorithm 2 will always terminate in those cases.

**Algorithm 2** Subdivision based isolation of singularities

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

**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  $L_{Sing}$ .

```

1: Let  $f$  be the resultant and  $s_{22}, s_{11}, s_{10}$  be the subresultant coefficients of  $P$  and  $Q$  wrt  $z$ .
2:  $L := \{B_0\}$ 
3: repeat
4:    $B := L.pop$ 
5:   if  $0 \notin \square f(B)$  or  $0 \notin \square s_{11}(B)$  or  $0 \notin \square s_{10}(B)$  then
6:     Discard  $B$ 
7:   else
8:     if  $K_{(s_{11}, s_{10})}(B) \subset int(B)$  and  $0 \notin \square s_{22}(B)$  then
9:       Insert  $B$  in  $L_{Sing}$ 
10:    else
11:      Subdivide  $B$  and insert its children in  $L$ 
12: until  $L = \emptyset$ 
13: return  $L_{Sing}$ 

```

**Lemma 3 ([Rec13])** *Let  $p$  be a node of  $f$ . Then  $p$  is a regular point of the system  $s_{11} = s_{10} = 0$ .*

**Proof 4** *We saw in the proof of Theorem 1 that  $S_{res} \subset S_{sing}$  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 particular, this 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 one in  $\langle s_{11}, s_{10} \rangle$ .*

**Lemma 5** *Let  $p$  be an ordinary cusp point of  $f$ . Then  $p$  is a regular point of the system  $s_{11} = s_{10} = 0$ .*

**Proof 6** *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 ([Kah03, 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 the contradiction.*

### 3 Local topology at singularities

Once a singularity is isolated in a box, we want to recover the local topology. More precisely, given a box containing a singularity  $p$ , we need to:

1. Compute the number of real branches connected to  $p$ .
2. Reduce the size of the box until it contains no closed loop.

### 3.1 Resultant

In this case, we cannot distinguish between nodes and other types of 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 or any other type of singularity.

In this section, we show how to recover the topology around nodes. Our algorithm always returns a correct answer if it terminates, and guarantees in this case that all the singularities are nodes.

#### 3.1.1 Number of real branches

For a node, the local topology is easily deduced from the topological degree of the mapping  $(f_x, f_y)$ .

**Lemma 7** [AMW08, 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, Algorithm 3 will always terminate and compute the number of real branches connected to  $p$ .

---

#### 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:    $B := B \cap K_{(s_{11}, s_{10})}(B)$
  - 4: **if**  $\square \det(\text{Hessian}(f))(B) > 0$  **then**
  - 5:   **return** 0
  - 6: **else**
  - 7:   **return** 4
- 

#### 3.1.2 Loop detection

Now that we know the number of branches  $n_p$  connected to  $p$  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 check that the number of branches crossing the boundary of  $B$  matches  $n_p$ . But this is not enough, since  $B$  could contain closed loops of  $f$ . This case can be discarded by ensuring that  $B$  contains a unique solution of the system  $f_x = f_y = 0$ .

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 the 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  $f_x = f_y = 0$ .

**Lemma 8 (Node near loops)** *Let  $K_{f_x, f_y}$  be the Krawczyk operator defined in Lemma 2 with respect to the system  $f_x = f_y = 0$ , and  $B$  be a box containing a singularity  $p$  of  $f$ . If  $K_{f_x, f_y}(B) \subset \text{int}(B)$  then  $B$  contains no closed loop of  $f$ .*

**Proof 9** *Lemma 2 ensures that  $p$  is the only solution of  $f$  in  $B$ . If  $B$  contains a closed loop included in  $\text{int}(B)$ , then a connected subset of  $B$  has its boundary included in the curve defined by  $f$ . Thus it contains an point  $q$  where  $f$  reaches a local extrema and such that  $f(q) \neq 0$ . In particular,  $f_x(q) = f_y(q) = 0$  and  $q \neq p$ , hence the contradiction.*

**Remark 10** *Alternatively, using tools from the next section, denoting by  $\square f$  the 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  $f_x = f_y = 0$ .*

### 3.2 Discriminant

In this section we focus on the discriminant curve. Let  $f$  be the resultant of  $P$  and  $Q := P_z$  satisfying the assumptions  $(A_1)$ ,  $(A_2)$  and  $(A_3)$ . Note that  $\text{Res}_z(P, P_z) = LT_z(P) \text{Disc}_z(P)$ , in particular, 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  $P$ .

In this case, we can detect not only nodes but also singularities  $p = (\alpha, \beta)$  of higher multiplicity if they are the projection of a triple root of the polynomial  $P(\alpha, \beta, z)$ . Notably, in the generic case, these are the only kind of singularities of the discriminant.

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 the projection of a triple point of  $P(\alpha, \beta, z)$ . In this case, the determinant of the Hessian is 0 ([LM09, Proposition 10]), and Lemma 15 shows that in this case, the singularity is an ordinary cusp.

First we show how we can certify that a box  $B$  contains the projection of a triple root of  $P$ .

**Lemma 11 (triple points)** *Let  $B$  be a box containing the singular point  $p$  of  $f$ . Assume that  $0 \notin \square s_{22}$  and let  $I_z$  be the interval  $\frac{-\square s_{21}}{2\square s_{22}}$ . Finally let  $K_{P, P_z, P_{zz}}$  be the Krawczyk operator associated to the system  $P = P_z = P_{zz} = 0$ . If  $K_{P, P_z, P_{zz}}(B \times I_z) \subset \text{int}(B \times I_z)$  then,  $p$  is the projection of a triple point of  $P$ .*

**Proof 12** *If  $P(\alpha, \beta, z)$  has a triple root  $z_0$  for  $(\alpha, \beta) \in B$ , then it has a multiplicity 2 in  $\text{gcd}(P(\alpha, \beta, z), P_z(\alpha, \beta, z))$ . 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  $z_0 = -\frac{s_{21}(\alpha, \beta)}{2s_{22}(\alpha, \beta)} \in I_z$ . Thus if  $(\alpha, \beta)$  is the projection of a triple point of  $P$ , then this point is necessarily in the box  $B \times I_z$ . Finally if the Krawczyk criterion  $K_{P, P_z, P_{zz}}$  is satisfied on  $B \times I_z$ , then we can conclude that the 3d box contains a unique triple point of  $P$ .*

**Remark 13** *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 14 (of Remark 13)** *At the triple point  $q$ , the Jacobian of the system  $P = P_z = P_{zz} = 0$  is  $P_{zz}(q) \begin{vmatrix} P_x(q) & P_{xz}(q) \\ P_y(q) & P_{yz}(q) \end{vmatrix}$ . By assumption,  $P_{zz}(q) \neq 0$ . 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.*

In the following, we focus on the case where the considered box  $B$  contains a singularity that is the projection of a triple point of  $P$ , and we show how to compute its local topology and how to guarantee that  $B$  contains no closed loop.

### 3.2.1 Number of real branches

An ordinary cusp is connected to exactly 2 real branches. The following lemma shows that the projection of a triple root of  $P$  is an ordinary cusp.

**Lemma 15 (cusp and triple points)** *Let  $f$  be the resultant of  $P$  and  $P_z$ . Assume that  $p = (\alpha, \beta)$  is a triple root of  $P(\alpha, \beta, z)$ . Then, under hypotheses  $(A_1), (A_2), (A_3)$ ,  $p$  is an ordinary cusp point of  $f$ .*

**Proof 16** *Without restriction of generality, we can assume that the common root of  $P$  and  $P_z$  at  $p$  is 0. Thus  $P$  is of the form  $P = \sum a_i(x, y)z^i$ , such that  $a_0(p) = a_1(p) = a_2(p) = 0$ . Our assumptions also imply that  $a_3(p) \neq 0$ . The authors of [LM09, Proposition] showed that in this case,  $p$  is a singular point of  $f$ . Using the same kind of arguments, we will show that for any non trivial direction  $d = (u, v)$ , the polynomial  $f(\alpha + ut, \beta + vt)$  vanishes on 0 with multiplicity at most 3. The multiplicity associated to a direction is denoted in the following by  $\mu_d$ . Let  $S$  be the Sylvester matrix of  $P$  and  $P_z$ :*

$$S = \begin{pmatrix} 1 & 2 & \dots & & & & n & n+1 & n+2 & \dots \\ a_0 & & & & & & a_1 & & & & \\ a_1 & a_0 & & & & & 2a_2 & a_1 & & & \\ a_2 & a_1 & a_0 & & & & 3a_3 & 2a_2 & a_1 & & \\ a_3 & a_2 & a_1 & a_0 & & & 4a_4 & 3a_3 & 2a_2 & a_1 & \\ a_4 & a_3 & a_2 & a_1 & a_0 & & 5a_5 & 4a_4 & 3a_3 & 2a_2 & a_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}$$

Proposition 10 of [LM09] shows that the quadratic part of  $f$  is  $a_0^2 a_3 D_3$ , where  $D_3(p) \neq 0$  if the gcd of  $P(\alpha, \beta, z)$  and  $P_z(\alpha, \beta, z)$  is reduced to  $z^2$ , which is our case. Thus for any direction  $d$  that is not parallel to the tangent of  $a_0(x, y) = 0$  at  $p$ , we have  $\mu_d = 2$ . Otherwise, let  $d$  be a non trivial direction orthogonal to  $\nabla a_0$ . On the other hand, expanding the determinant of  $S$  along the 5 first rows and the columns 1, 2, and  $n, n+1, n+2$ , we observe that the resultant is of the form  $f = 4a_1^3 a_3^2 \sigma + a_0(a_0 U + a_1^2 V + a_1 a_2 W)$ , where  $\sigma$  is the second subresultant of the polynomials  $\frac{P - a_0}{z}$  and  $P_z$ . In particular,  $\sigma(p) \neq 0$  since  $a_0(p) = 0$  and  $P(p)$  and  $P_z(p)$  have at most 2 common solutions in  $z$ .

It remains to show that  $d$  cuts  $a_1 = 0$  transversally at  $p$ . If it were not the case, then the gradients of  $a_0$  and  $a_1$  would be collinear. In particular,  $\begin{vmatrix} P_x(p) & P_{xx}(p) \\ P_y(p) & P_{zy}(p) \end{vmatrix}$  would be zero, all the maximal minor of the Jacobian matrix of  $P, P_z$  would be zero and the curve  $P = P_z = 0$  would not be smooth, hence the contradiction.

Thus, Algorithm 4 classifies the singularities between nodes and ordinary cusps, and compute the number of real branches connected to them. It always terminates when the discriminant singularity is a node or the projection of a triple root of  $P$ .

### 3.2.2 Loop detection

Finally, once we know that a box contains an ordinary cusp, we want to ensure that it does not contain any closed loop. This is ensured by the following lemma.

**Lemma 17 (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:*

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

**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).

```

1: 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
    $z$ .
2: while true do
3:   if  $\square \det(\text{Hessian}(f))(B) > 0$  then
4:     return (0, node)
5:   if  $\square \det(\text{Hessian}(f))(B) < 0$  then
6:     return (4, node)
7:    $I_z := -\frac{\square s_{2,1}(B)}{2\square s_{2,2}(B)}$ 
8:   if  $K_{(P, P_z, P_{zz})}(B \times I_z) \subset \text{int}(B \times I_z)$  then
9:     return (2, ordinary cusp)
10:   $B := B \cap K_{(s_{11}, s_{10})}(B)$ 

```

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

**Remark 18** 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 ([VH94] for example). In our case, this would amount to solve a system of two polynomials of degree lower than 3 and check if these 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 17 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 17, we define the notion of separation polynomial that we will use.

### Separation polynomial

**Definition 19** 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  $q$  be a polynomial such that  $q(x, y)(x - \alpha)^k \in I_S$  and  $q(p) \neq 0$ . Then we say that  $q$  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  $q(x)(x - \alpha)$  where  $q(\alpha) \neq 0$ . However we do not restrict  $q$  to be a univariate polynomial.

**Lemma 20** Let  $q$  be a separation polynomial and  $B$  be a box. If  $0 \notin \square q$ , 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 21** Let  $(x_0, y_0) \in B$  such that  $x_0 \neq 0$ . If  $q(x_0, y_0) \neq 0$ , then  $q(x_0, y_0)(x_0 - \alpha)^k \neq 0$ . 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  $(\alpha, y_0)$  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 17** Consider the system  $f_x = f_y = 0$ . Any closed loop of  $f$  contains a solution of this system. The cusp point  $p$  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:  $f_{xy}(p) = f_{x^2}(p)f_{y^2}(p)$ . And 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  $f_{y^2}(p) \neq 0$ . And let  $X, Y$  be two new variables such that  $\begin{pmatrix} x \\ y \end{pmatrix} = M \cdot \begin{pmatrix} X \\ Y \end{pmatrix}$  where:

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

Differentiating  $f$  along the new variables, we have:

$$\begin{pmatrix} f_{XX} & f_{XY} \\ f_{XY} & f_{YY} \end{pmatrix} = M^T \begin{pmatrix} f_{xx} & f_{xy} \\ f_{xy} & f_{yy} \end{pmatrix} M$$

In particular, we have:

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

Observe that  $f_{XY}(p) = 0$  and  $f_{XX}(p) = f_{yy}(p)(f_{xx}(p)f_{yy}(p) - f_{xy}(p)^2) = 0$ . Thus, the polynomial system  $f_X, f_Y$  has the form:

$$\begin{aligned} f_X &= a(X)\Delta X^2 + b(X, Y)\Delta Y \\ f_Y &= c(X)\Delta X^2 + d(X, Y)\Delta Y \end{aligned}$$

Eliminating  $\Delta Y$ , we get the polynomial  $\Delta X^2(ad - cb)$  in the ideal generated by  $f_x$  and  $f_y$ . Letting  $q = ad - cb$ , we can verify that  $q(p) \neq 0$ . Indeed we have  $2q(p) = f_{XXX}(p)f_{YY}(p) - f_{XXY}(p)f_{XY}(p) = f_{XXX}(p)f_{YY}(p)$ . By assumption,  $f_{YY}(p) = f_{yy}(p) \neq 0$  and since  $p$  is an ordinary cusp, it cannot have a triple root in  $X$  and  $f_{XXX}(p) \neq 0$ . Thus  $q$  is a separation polynomial.

Then, we can observe that  $a(X) = \frac{f_X(X, \beta)}{\Delta X^2}$ ,  $c(X) = \frac{f_Y(X, \beta)}{\Delta X^2}$ , and  $b(X, Y) = \frac{f_X - a\Delta X^2}{\Delta Y}$ ,  $d(X, Y) = \frac{f_Y - c\Delta X^2}{\Delta Y}$ . Thus, using Taylor-Lagrange theorem, we can deduce that if  $B$  is a box containing  $(\alpha, \beta)$ :

$$\begin{aligned} a(B) &\subset \frac{\square f_{XXX}}{2} & c(B) &\subset \frac{\square f_{XXY}}{2} \\ b(B) &\subset \square f_{XY} & d(B) &\subset \square f_{YY} \end{aligned}$$



Finally, evaluating  $2q$  on a box containing  $p$ , we get:

$$\begin{aligned}
2\Box q &\subset \Box f_{XXX}\Box f_{YY} - \Box f_{XXY}\Box f_{XY} \\
&\subset f_{yy}(p)(f_{yy}(p))^2\Box f_{xxx} - 3f_{yy}(p)f_{xy}(p)\Box f_{xxy} + 3f_{xy}(p)^2\Box f_{xyy} - f_{xy}(p)f_{xx}(p)\Box f_{yyy})\Box f_{yy} \\
&\quad - f_{yy}(p)(f_{yy}(p)\Box f_{xxy} + f_{xx}(p)\Box f_{yyy} - 2f_{xy}(p)\Box f_{xyy})(f_{yy}(p)\Box f_{xy} - f_{xy}(p)\Box f_{yy}) \\
&\subset I(IJ - KL)
\end{aligned}$$

Thus if  $0 \notin I(IJ - KL)$  then,  $0 \notin \Box q$  and  $0 \notin f_{YY}$ , thus  $B$  contains no other solution of  $f_x = f_y = 0$  than  $p$ .

### 3.3 Loop detection in the general case

Gathering Lemma 8 and 17 for loop detection, Algorithm 5 returns a refined box of a singular point that avoids closed loops of the curve, as soon as we know in advance if the singularity is a node or an ordinary cusp. Note that this algorithm always terminates if the singularity is a node or an ordinary cusp, and works for any algebraic curve.

---

**Algorithm 5** Avoid curve loops in a singularity box

---

**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.

**Output:** A box that avoids closed loops of the curve.

- 1: 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  $z$ .
  - 2: **while** true **do**
  - 3:   **if**  $B$ -type = node **and**  $K_{(f_x, f_y)}(B) \subset \text{int}(B)$  **then**
  - 4:     **return**  $B$
  - 5:   **if**  $B$ -type = cusp **then**
  - 6:     Compute  $I$  and  $I'$  as defined in Lemma 17
  - 7:     **if**  $0 \notin I$  **or**  $0 \notin I'$  **then**
  - 8:       **return**  $B$
  - 9:      $B := B \cap K_{(s_{11}, s_{10})}(B)$
- 

## Acknowledgments

The authors would like to thank Laurent Busé and Éric Schost for fruitful discussions.

## References

- [AMW08] L. Alberti, B. Mourrain, and J. Wintz. Topology and arrangement computation of semi-algebraic planar curves. *Comput. Aided Geom. Des.*, 25(8):631–651, 2008.
- [BL13] Carlos Beltrán and Anton Leykin. Robust certified numerical homotopy tracking. *Foundations of Computational Mathematics*, pages 1–43, 2013.
- [BM09] Laurent Busé and Bernard Mourrain. Explicit factors of some iterated resultants and discriminants. *Mathematics of Computation*, 78(265):345–386, 2009.

- [CLP<sup>+</sup>10] J. Cheng, S. Lazard, L. Penaranda, M. Pouget, F. Rouillier, and E. Tsigaridas. On the topology of real algebraic plane curves. *Mathematics in Computer Science*, 4:113–137, 2010.
- [Ded06] J.P. Dedieu. *Points fixes, zéros et la méthode de Newton*. Mathématiques et Applications. Springer, 2006.
- [DL13] Nicolas Delanoue and Sébastien Lagrange. A numerical approach to compute the topology of the apparent contour of a smooth mapping from  $R^2$  to  $R^2$ . *submitted to Journal of Computational and Applied Mathematics*, 2013.
- [ES11] Pavel Emeliyanenko and Michael Sagraloff. On the complexity of solving a bivariate polynomial system. *CoRR*, abs/1104.4954, 2011.
- [GG10] Alexandre Goldsztejn and Laurent Granvilliers. A new framework for sharp and efficient resolution of ncsp with manifolds of solutions. *Constraints*, 15(2):190–212, April 2010.
- [GLSY07] M. Giusti, G. Lecerf, B. Salvy, and J.-C. Yakoubsohn. On location and approximation of clusters of zeros: Case of embedding dimension one. *Found. Comput. Math.*, 7(1):1–58, February 2007.
- [Jou79] J. P. Jouanolou. Singularités rationnelles du résultant. In *Algebraic geometry (Proc. Summer Meeting, Univ. Copenhagen, Copenhagen, 1978)*, volume 732 of *Lecture Notes in Math.*, pages 183–213. Springer, Berlin, 1979.
- [Kah03] M’hammed El Kahoui. An elementary approach to subresultants theory. *J. Symb. Comput.*, 35(3):281–292, 2003.
- [Kea96] R. Baker Kearfott. *Rigorous global search : continuous problems*. Nonconvex optimization and its applications. Kluwer Academic Publishers, Dordrecht, Boston, 1996.
- [Kea97] R Baker Kearfott. Empirical evaluation of innovations in interval branch and bound algorithms for nonlinear systems. *SIAM Journal on Scientific Computing*, 18(2):574–594, 1997.
- [Kra69] R. Krawczyk. Newton-Algorithmen zur Bestimmung von Nullstellen mit Fehler-schranken. *Computing (Arch. Elektron. Rechnen)*, 4:187–201, 1969.
- [LC87] W. E. Lorensen and H. E. Cline. Marching cubes: A high resolution 3d surface construction algorithm. *SIGGRAPH Comput. Graph.*, 21:163–169, August 1987.
- [LM09] Daniel Lazard and Scott McCallum. Iterated discriminants. *J. Symb. Comput.*, 44(9):1176–1193, 2009.
- [LMP08] C. Liang, B. Mourrain, and J. Pavone. Subdivision methods for 2d and 3d implicit curves. In *Geometric modeling and algebraic geometry*, pages 171–186. Springer, 2008. RR INRIA in 2005.
- [LVZ06] Anton Leykin, Jan Verschelde, and Ailing Zhao. Newton’s method with deflation for isolated singularities of polynomial systems. *Theoretical Computer Science*, 359(13):111 – 122, 2006.

- [MM11] Angelos Mantzaflaris and Bernard Mourrain. Deflation and certified isolation of singular zeros of polynomial systems. In *Proceedings of the 36th international symposium on Symbolic and algebraic computation*, ISSAC '11, pages 249–256, New York, NY, USA, 2011. ACM.
- [MPS<sup>+</sup>06] Bernard Mourrain, Sylvain Pion, Susan Schmitt, Jean-Pierre T  court, Elias P. Tsigaridas, and Nicola Wolpert. Algebraic issues in Computational Geometry. In J.-D. Boissonnat and M. Teillaud, editors, *Effective Computational Geometry for Curves and Surfaces*, Mathematics and Visualization, chapter 3, pages 117–155. Springer, 2006.
- [Neu90] A. Neumaier. *Interval methods for systems of equations / Arnold Neumaier*. Cambridge University Press, Cambridge [England] ; New York :, 1990.
- [OWM83] Takeo Ojika, Satoshi Watanabe, and Taketomo Mitsui. Deflation algorithm for the multiple roots of a system of nonlinear equations. *Journal of Mathematical Analysis and Applications*, 96(2):463 – 479, 1983.
- [PV04] S. Plantinga and G. Vegter. Isotopic approximation of implicit curves and surfaces. In *SGP '04: Eurographics/ACM SIGGRAPH Symposium on Geometry Processing*, pages 245–254, 2004.
- [Rec13] Judit Recknagel. Topology of planar singular curves resultant of two trivariate polynomials, August 2013. Bachelor’s Thesis.
- [Rum83] Siegfried M. Rump. Solving algebraic problems with high accuracy. In *Proc. of the symposium on A new approach to scientific computation*, pages 51–120, San Diego, CA, USA, 1983. Academic Press Professional, Inc.
- [SN05] Hermann Schichl and Arnold Neumaier. Exclusion regions for systems of equations. *SIAM Journal on Numerical Analysis*, 42(1):pp. 383–408, 2005.
- [Sny92] John M. Snyder. Interval analysis for computer graphics. In *Proceedings of the 19th annual conference on Computer graphics and interactive techniques*, SIGGRAPH '92, pages 121–130, New York, NY, USA, 1992. ACM.
- [SW05] R. Seidel and N. Wolpert. On the exact computation of the topology of real algebraic curves. In *Proc 21st ACM Symposium on Computational Geometry*, pages 107–115, 2005.
- [Sza88] Zbigniew Szafraniec. On the number of branches of a 1-dimensional semianalytic set. *Kodai Math. J.*, 11(1):78–85, 1988.
- [vdH11] J. van der Hoeven. Reliable homotopy continuation. Technical report, HAL, 2011. <http://hal.archives-ouvertes.fr/hal-00589948/fr/>.
- [VH94] Jan Verschelde and Ann Haegemans. Homotopies for solving polynomial systems within a bounded domain. *Theor. Comput. Sci.*, 133(1):165–185, October 1994.



**RESEARCH CENTRE  
NANCY – GRAND EST**

615 rue du Jardin Botanique  
CS20101  
54603 Villers-lès-Nancy Cedex

Publisher  
Inria  
Domaine de Voluceau - Rocquencourt  
BP 105 - 78153 Le Chesnay Cedex  
[inria.fr](http://inria.fr)

ISSN 0249-6399