On the Computation of the Topology of a Non-Reduced Implicit Space Curve

Daouda Diatta, Bernard Mourrain, Olivier Ruatta

On the Computation of the Topology of a Non-Reduced Implicit Space Curve

Daouda Niang Diatta
University of Limoges, XLIM,
INRIA Sophia-Antipolis,
France.
dndiatta@sophia.inria.fr

Bernard Mourrain
INRIA Sophia-Antipolis,
France.
mourrain@sophia.inria.fr

Olivier Ruatta
University of Limoges, XLIM,
France.
olivier.ruatta@unilim.fr

ABSTRACT

An algorithm is presented for the computation of the topology of a non-reduced space curve defined as the intersection of two implicit algebraic surfaces. It computes a Piecewise Linear Structure (PLS) isotopic to the original space curve.

The algorithm is designed to provide the exact result for all inputs. It's a symbolic-numeric algorithm based on subresultant computation. Simple algebraic criteria are given to certify the output of the algorithm.

The algorithm uses only one projection of the non-reduced space curve augmented with adjacency information around some "particular points" of the space curve.

The algorithm is implemented with the Mathemagix Computer Algebra System (CAS) using the SYNAPS library as a backend.

Categories and Subject Descriptors

I.1.4 [**Symbolic and Algebraic Manipulation**]: Applications; I.3.5 [**Computer Methodologies**]: Computer Graphics, Computational Geometry and Object Modeling-Geometric Algorithms

General Terms

Algorithms

Keywords

Algebraic Curves, Subresultants Sequence, Generic Conditions, Topology Computation, Sturm-Habicht Sequence, Exact Geometric Computation

Introduction

The problem of computing the topological graph of algebraic curves plays an important role in many applications such as plotting [13] and sectioning in Computer Aided Geometric Design [15], [16]. A wide literature exists on the computation of the topology of plane curves ([8], [7], [10], [11], [12], [6] and [14]). The problem of computing the topology of space curves has been less investigated. In [1], Alcázar and Sendra give a symbolic-numeric algorithm for **reduced** space curves using subresultant and GCD computations of approximated polynomials. If their approach gives good practical results however it doesn't give a rigorous proof that a sufficient precision is selected for all inputs in the computation of GCD of approximated polynomials. In [11], Owen, Rockwood and Alyn give a numerical algorithm for **reduced** space curve using subdivision method. Their algorithm has a good complexity but the topology around the singularities of the space curve is not certified. We also mention the work in [7], where two projections of a **reduced** space curve are used, and where the connection algorithm is valid under genericity conditions.

To our knowledge, the general problem of computing the topology of **non-reduced** space curves is not investigated in the algorithmic point of view despite its significance in the problem of computing the topology of a real algebraic surface.

We present a certified algorithm that computes the topology of **non-reduced** algebraic space curves. We compute the topology of a plane projection of the space curve and then we lift the computed topology on the space. The topology of the projected curve is computed using a classical sweeping algorithm (see [10], [8]). For the computation of the topology of a plane algebraic curve, we present an **efficient generic test** that certifies the output of the algorithm in [8] .

For space curves, we introduce the notion of pseudo-generic position. A space curve is said to be in pseudo-generic position with respect to the (x, y)-plane if and only if almost every point of its projection on the (x, y)-plane has only one geometric inverse-image. A simple algebraic criterion is given to certify the pseudo-genericity of the position of a space curve. From a theoretical point of view, the use of the notion of curve in **pseudo-generic position gives us a rational parametrization of the space curve**. The use of this rational parametrization allows us to lift the topology computed after projection without any supplementary effort. From a practical point of view, the use of the rational parametrization of the space curve makes the lifting faster, avoiding numerical problems.

We need to distinguish two kinds of singularities on the projected curve. A **certified** algorithm is given to do so. Unlike previous approaches, our algorithm uses **only one projection** of the space curve and works for **non-reduced space curves.** We therefore avoid the cost of the second

ISSAC '08 Hagenberg, Austria

projection used by previous approaches.
In the next section we describe the fundamental algebraic tools that we use in this paper. In Section 2, we present our contribution to certify the algorithm for computing the topology of a plane algebraic curve. Our algorithm itself is introduced in Section 3. We report on our implementation and experiments in section 4.

1. SUBRESULTANTS

Let $P_1, P_2 \in \mathbb{Q}[X,Y,Z]$ and $\mathcal{C}_{\mathbb{R}} := \{(x,y,z) \in \mathbb{R}^3 | P_1(x,y,z) = P_2(x,y,z) = 0\}$ be the intersection of the vanishing sets of P_1 and P_2. Our curve analysis needs to compute a plane projection of $\mathcal{C}_{\mathbb{R}}$. Subresultant sequences are a suitable tool to do it. For the reader's convenience, we recall their definition and relevant properties. For all the results of this section, we refer to [3], for proofs.

Let $\mathbb{A}$ be a integral domain. Let $P = \sum_{i=0}^{p} a_i X^i$ and $Q = \sum_{i=0}^{q} b_i X^i$ be two polynomials with coefficients in $\mathbb{A}$. We shall always assume $a_p \neq 0$, $b_q \neq 0$ and $p \geqslant q$.

Let $\mathbb{P}_r(\mathbb{A})$ be the set of polynomials in $\mathbb{A}[X]$ of degree not exceeding r, always, with the basis (as an $\mathbb{A}$-module) $1, X, \ldots, X^r$. If $r < 0$, we set $\mathbb{P}_r(\mathbb{A}) = 0$ by convention, and we will identify an element $S = s_0 + \ldots + s_r X^r$ of $\mathbb{P}_r(\mathbb{A})$ with the row vector $(s_0, \ldots, s_r)$.

Let k be an integer such that $0 \leqslant k \leqslant q$, and let Ψ_k:

$$\mathbb{P}_{q-k-1}(\mathbb{A}) \times \mathbb{P}_{p-k-1}(\mathbb{A}) \to \mathbb{P}_{p+q-k-1}(\mathbb{A})$$

be the $\mathbb{A}$-linear map defined by $\Psi_k(\boldsymbol{U}, \boldsymbol{V}) = P\boldsymbol{U} + Q\boldsymbol{V}$, with $M_k(P,Q)$ the $(p+q-k) \times (p+q-k)$ matrix of Ψ_k. As we write vectors as row vectors, we have

$$M_k(P,Q) = \begin{pmatrix} a_0 & \ldots & a_p & & \\ & \ddots & & \ddots & \\ & & a_0 & \ldots & a_p \\ b_0 & \ldots & b_q & & \\ & \ddots & & \ddots & \\ & & b_0 & \ldots & b_q \end{pmatrix}$$

That is $M_0(P,Q)$ is the classical Sylvester matrix associated to P, Q. To be coherent with the degree of polynomials, we will attach index $i-1$ to the i^{th} column of $M_k(P,Q)$, so the indices of the columns go from 0 to $p+q-k-1$.

Definition 1 *For $j \leqslant p+q-k-1$ and $0 \leqslant k \leqslant q$, let $\mathrm{sr}_{k,j}$ be the determinant of the submatrix of $M_k(P,Q)$ formed by the last $p+q-2k-1$ columns, the column of index j and all the $(p+q-2k)$ rows. The polynomial $\mathrm{Sr}_k(P,Q) = \mathrm{sr}_{k,0} + \ldots + \mathrm{sr}_{k,k} X^k$ is the k^{th} sub-GCD of P and Q, and its leading term $\mathrm{sr}_{k,k}$ (sometimes noted sr_k) is the k^{th} subresultant of P and Q. So, it follows that $\mathrm{Sr}_0(P,Q) = \mathrm{sr}_0$ is the usual resultant of P and Q.*

Remark 1

1. For $k < j \leqslant p+q-k-1$, we have $\mathrm{sr}_{k,j} = 0$, because it is the determinant of a matrix with two equal columns.
2. If $q < p$, we have $\mathrm{Sr}_q = (b_q)^{p-q-1} Q$ and $\mathrm{sr}_q = (b_q)^{p-q}$.

The following proposition will justify the name of sub-GCD given to the polynomial Sr_k.

Proposition 1 *Let d be the degree of the GCD of P and Q (d is defined because $\mathbb{A}$ is an integral domain, so we may compute the GCD over the quotient field of $\mathbb{A}$). Let k be an integer such that $k \leqslant d$.*

1. *The following assertions are equivalent:*
   a) $k < d$;
   b) $\mathrm{Sr}_k = 0$;
   c) $\mathrm{sr}_k = 0$.
2. *$\mathrm{sr}_d \neq 0$ and Sr_d is the GCD of P and Q.*

Theorem 1 ***Fundamental property of subresultants*** *The first polynomial Sr_k associated to P and Q with $\mathrm{sr}_k \neq 0$ is the greatest common divisor of P and Q.*

We will often call $(\mathrm{Sr}_i)_i$ the subresultant sequence associated to P and Q and $(\mathrm{sr}_{i,j})_{i,j}$ the sequence of their subresultants coefficients. We will denote by $\mathrm{lcoef}_X(f)$ the leading coefficient of the polynomial f with respect to the variable X.

Theorem 2 ***Specialization property of subresultants*** *Let $P_1, P_2 \in \mathbb{A}[Y,Z]$ and $(\mathrm{Sr}_i(Y,Z))_i$ be their subresultant sequence with respect to Z. Then for any $\alpha \in \mathbb{A}$ with:*
$deg_Z(P(Y,Z)) = deg_Z(P(\alpha,Z))$;
$deg_Z(Q(Y,Z)) = deg_Z(Q(\alpha,Z))$,
$(\mathrm{Sr}_i(\alpha,Z))_i$ is the subresultant sequence of the polynomials $P(\alpha,Z)$ and $Q(\alpha,Z)$.

2. TOPOLOGY OF A PLANE ALGEBRAIC CURVE

Let $f \in \mathbb{Q}[X,Y]$ be a square free polynomial and

$$\mathcal{C}(f) := \{(\alpha,\beta) \in \mathbb{R}^2, f(\alpha,\beta) = 0\} \quad (1)$$

be the real algebraic curve associated to f. We want to compute the topology of $\mathcal{C}(f)$.

For curves in generic position, computing its critical fibers and one regular fiber between two critical ones is sufficient to obtain the topology using a sweeping algorithm (see [8]). But for a good computational behaviour, it is essential to certify the genericity of the position of the curve.

We propose an effective test allowing to certify the computation and connection, in a deterministic way. This is an important tool in order to address the case of space curves.

Now, let us introduce the definitions of generic position, critical, singular and regular points.

Definition 2 *Let $f \in \mathbb{Q}[X,Y]$ be a square free polynomial and $\mathcal{C}(f) = \{(\alpha,\beta) \in \mathbb{R}^2 : f(\alpha,\beta) = 0\}$ be the curve defined by f. A point $(\alpha,\beta) \in \mathcal{C}(f)$ is called:*

- *a x-critical point if $\partial_Y f(\alpha,\beta) = 0$,*
- *a singular point if $\partial_X f(\alpha,\beta) = \partial_Y f(\alpha,\beta) = 0$,*
- *a regular point if $\partial_X f(\alpha,\beta) \neq 0$ or $\partial_Y f(\alpha,\beta) \neq 0$.*

With these definitions we can describe the generic conditions required for plane curves.

Definition 3 *Let $f \in \mathbb{Q}[X,Y]$ be a square free polynomial and $\mathcal{C}(f) = \{(\alpha,\beta) \in \mathbb{R}^2 : f(\alpha,\beta) = 0\}$ be the curve defined by f. Let $\mathcal{N}_x(\alpha) := \#\{\beta \in \mathbb{R}$, such that (α,β) is a x-critical point of $\mathcal{C}(f)\}$. $\mathcal{C}(f)$ is in generic position for the x-direction, if:*

1. $\forall \alpha \in \mathbb{C}, \mathcal{N}_x(\alpha) \leqslant 1$,
2. *There is no asymptotic direction of $\mathcal{C}(f)$ parallel to the y-axis.*

This notion of genericity also appears in [12] and in a slightly more restrictive form in [6]. Previous approaches succeed if genericity conditions are satisfied, but they do **not guarantee to reject the curve** if they are not; i.e, it does **not decide genericity**. So for some input curves the computed topology might not be exact.

A change of coordinates such that $\mathrm{lcoef}_Y(f) \in \mathbb{Q}^*$ is sufficient to place $\mathcal{C}(f)$ in a position such that any asymptotic direction is not parallel to the y-axis. It remains to find an efficient way to verify the first condition. This follows from the next propositions. We refer to [8], for proofs.

Proposition 2 *Let $f \in \mathbb{Q}[X,Y]$ be a square free polynomial with $\mathrm{lcoef}_Y(f) \in \mathbb{Q}^*$, $\mathrm{Res}_Y(f, \partial_Y f)$ be the resultant with respect to Y of the polynomials f, $\partial_Y f$ and $\{\alpha_1, \ldots, \alpha_l\}$ be the set of the roots of $\mathrm{Res}_Y(f, \partial_Y f)$ in $\mathbb{C}$.*

Then $\mathcal{C}(f)$ is in generic position if and only if $\forall i \in \{1, \ldots, l\}, \gcd(f(\alpha_i, Y), \partial_Y f(\alpha_i, Y))$ has at most one root.

Let $f \in \mathbb{Q}[X,Y]$ be a square free polynomial with $\mathrm{lcoef}_Y(f) \in \mathbb{Q}^*$ and $d := \deg_Y(f)$. We denote by $\mathrm{Sr}_i(X,Y)$ the i^{th} subresultant polynomial of f and $\partial_Y f$ and $\mathrm{sr}_{i,j}(X)$ the coefficient of Y^j in $\mathrm{Sr}_i(X,Y)$. We define inductively the following polynomials:

$$\Phi_0(X) = \frac{\mathrm{sr}_{0,0}(X)}{\gcd(\mathrm{sr}_{0,0}(X), \mathrm{sr}'_{0,0}(X))};$$

$\forall i \in \{1, \ldots, d-1\}$, $\Phi_i(X) = \gcd(\Phi_{i-1}(X), \mathrm{sr}_{i,i}(X))$ and $\Gamma_i(X) = \frac{\Phi_{i-1}(X)}{\Phi_i(X)}$.

Proposition 3

1. $\Phi_0(X) = \prod_{i=1}^{d-1} \Gamma_i(X)$ *and* $\forall i, j \in \{1, \ldots, d-1\}, i \neq j \Longrightarrow \gcd(\Gamma_i(X), \Gamma_j(X)) = 1$;
2. *Let $k \in \{1, \ldots, d-1\}$, $\alpha \in \mathbb{C}$. $\Gamma_k(\alpha) = 0$ if and only if $\gcd(f(\alpha, Y), \partial_Y f(\alpha, Y)) = \mathrm{Sr}_k(\alpha, Y)$;*
3. $\{(\alpha,\beta) \in \mathbb{R}^2 : f(\alpha,\beta) = \partial_Y f(\alpha,\beta) = 0\} = \bigcup_{k=1}^{d-1} \{(\alpha,\beta) \in \mathbb{R}^2 : \Gamma_k(\alpha) = \mathrm{Sr}_k(\alpha,\beta) = 0\}$.

In the following theorem, we give an effective and efficient algebraic test to certify the genericity of the position of a curve with respect to a given direction.

Theorem 3 *Let $f \in \mathbb{Q}[X,Y]$ be a square free polynomial such that $deg_Y(f) = d$, $lcoef_Y(f) \in \mathbb{Q}^*$. Then $\mathcal{C}(f)$ is in generic position for the projection on the x axis if and only if $\forall k \in \{1, \ldots, d-1\}$, $\forall i \in \{0, \ldots, k-1\}$,* $k(k-i)\,\mathrm{sr}_{k,i}(X)\,\mathrm{sr}_{k,k}(X) - (i+1)\,\mathrm{sr}_{k,k-1}(X)\,\mathrm{sr}_{k,i+1}(X) = 0 \bmod \Gamma_k(X)$.

Proof. Assume that $\mathcal{C}(f)$ is in generic position and let $\alpha \in \mathbb{C}$ be a root of $\Gamma_k(X)$. According to Proposition 3 (2.) $\gcd(f(\alpha,Y), \partial_Y f(\alpha,Y)) = \mathrm{Sr}_k(\alpha,Y) = \sum_{j=0}^{k} \mathrm{sr}_{k,j}(\alpha) Y^j$. According to Proposition 2, $\mathrm{Sr}_k(\alpha,Y)$ has an only root $\beta(\alpha) = -\frac{\mathrm{sr}_{k,k}(\alpha)}{k\,\mathrm{sr}_{k,k-1}(\alpha)}$, so $\mathrm{Sr}_k(\alpha,Y) = \mathrm{sr}_{k,k}(\alpha)(Y-\beta)^k$. Binomial Newton formula gives $\mathrm{Sr}_k(\alpha,Y) = \mathrm{sr}_{k,k}(\alpha)(Y-\beta)^k = \mathrm{sr}_{k,k}(\alpha) \sum_{i=0}^{k} \binom{k}{i} (-\beta)^{k-i} Y^i$. So by identification $\forall k \in \{1, \ldots, d-1\}, \forall i \in \{0, \ldots, k-1\}$ and $\forall \alpha \in \mathbb{C}$ such that $\Gamma_k(\alpha) = 0$,

$$k(k-i)\,\mathrm{sr}_{k,i}(\alpha)\,\mathrm{sr}_{k,k}(\alpha) - (i+1)\,\mathrm{sr}_{k,k-1}(\alpha)\,\mathrm{sr}_{k,i+1}(\alpha) = 0.$$

It is to say that $\forall k \in \{1, \ldots, d-1\}, \forall i \in \{0, \ldots, k-1\}$, $k(k-i)\,\mathrm{sr}_{k,i}(X)\,\mathrm{sr}_{k,k}(X) - (i+1)\,\mathrm{sr}_{k,k-1}(X)\,\mathrm{sr}_{k,i+1}(X) = 0 \bmod \Gamma_k(X)$.
Conversely, let α be a root of $\Gamma_k(X)$ such that

$$k(k-i)\,\mathrm{sr}_{k,i}(\alpha)\,\mathrm{sr}_{k,k}(\alpha) - (i+1)\,\mathrm{sr}_{k,k-1}(\alpha)\,\mathrm{sr}_{k,i+1}(\alpha) = 0.$$

With the same argument used in the first part of this proof we obtain

$$\begin{aligned} \gcd\left(f(\alpha,Y), \partial_Y f(\alpha,Y)\right) &= \mathrm{Sr}_k(\alpha,Y) \\ &= \textstyle\sum_{j=0}^{k} \mathrm{sr}_{k,j}(\alpha) Y^j \\ &= \mathrm{sr}_{k,k}(\alpha)(Y-\beta)^k \end{aligned} \tag{2}$$

with

$$\beta = -\frac{\mathrm{sr}_{k,k-1(\alpha)}}{k\,\mathrm{sr}_{k,k(\alpha)}}. \tag{3}$$

Then we conclude that $\gcd(f(\alpha,Y), \partial_Y f(\alpha,Y))$ has only one distinct root and, according to Proposition 2, $\mathcal{C}(f)$ is in generic position. □

Remark 2 Theorem 3 shows that it is possible to check with certainty if a plane algebraic curve is in generic position or not. If not, we can put it in generic position by a basis change.
In fact, it is well known that there is only a finite number of bad changes of coordinates of the form $X := X + \lambda Y$, $Y := Y$, such that if $\mathcal{C}(f)$ is not in generic position then the transformed curve remains in a non-generic position. This number of bad cases is bounded by $\binom{c}{2}$, where c is the number of distinct x-critical points of $\mathcal{C}(f)$ [8].

3. TOPOLOGY OF IMPLICIT THREE DIMENSIONAL ALGEBRAIC CURVES

3.1 Description of the problem

Let $P_1, P_2 \in \mathbb{Q}[X,Y,Z]$ and

$$\mathcal{C}_{\mathbb{R}} := \{(x,y,z) \in \mathbb{R}^3 : P_1(x,y,z) = P_2(x,y,z) = 0\} \tag{4}$$

be the intersection of the surfaces defined by $P_1 = 0$ and $P_2 = 0$. We assume that $\gcd(P_1, P_2) = 1$ so that $\mathcal{C}_{\mathbb{R}}$ is a space curve. Our goal is to analyze the geometry of $\mathcal{C}_{\mathbb{R}}$ in the following sense: We want to compute a piecewise linear graph of $\mathbb{R}^3$ isotopic to the original space curve.
Our method allows to use a new sweeping algorithm using only one projection of the space curve.
To make the lifting possible using only one projection, a new definition of generic position for space curves and an algebraic characterization of it are given. We will also need to distinguish the "apparent singularities" and the "real singularities". A **certified** algorithm is given to **distinguish**

these two kinds of **singularities**.
For the lifting phase, using the new notion of curve in **pseudo-generic position**, we give an algorithm that computes a rational parametrization of the space curve. The use of this rational parametrization allows us to lift the topology of the projected curve without any supplementary computation.

3.2 Genericity conditions for space curves

Let $\Pi_z : (x,y,z) \in \mathbb{R}^3 \mapsto (x,y) \in \mathbb{R}^2$. We still denote $\Pi_z = \Pi_z|_{\mathcal{C}_\mathbb{R}}$. Let $\mathcal{D} = \Pi_z(\mathcal{C}_\mathbb{R}) \subset \mathbb{R}^2$ be the curve obtained by projection of $\mathcal{C}_\mathbb{R}$.

We assume that $\deg_Z(P_1) = \deg(P_1)$ and $\deg_Z(P_2) = \deg(P_2)$ (by a basis change, these conditions are always satisfied). Let $h(X,Y)$ be **the squarefree** part of $\mathrm{Res}_Z(P_1,P_2) \in \mathbb{Q}[X,Y]$. With the above notation and assumptions we have the following "geometric" equality, $\Pi_z(\mathcal{C}_\mathbb{R}) = \mathcal{C}(h)$.

Definition 4 *[Pseudo-generic position]*
Let $\mathcal{C}_\mathbb{C} := \{(x,y,z) \in \mathbb{C}^3 | P_1(x,y,z) = P_2(x,y,z) = 0\}$. *The curve* $\mathcal{C}_\mathbb{R}$ *is in pseudo-generic position with respect to the* (x,y)*-plane if and only if almost every point of* $\Pi_z(\mathcal{C}_\mathbb{C})$ *has only one geometric inverse-image, i.e. generically, if* $(\alpha,\beta) \in \Pi_z(\mathcal{C}_\mathbb{C})$, *then* $\Pi_z^{-1}(\alpha,\beta)$ *consists in one point possibly multiple.*

Let m be the minimum of $\deg_Z(P_1)$ and $\deg_Z(P_2)$.
The following theorems give us an effective way to test if a curve is in pseudo-generic position or not.

Theorem 4 *Let* $(\mathrm{Sr}_j(X,Y,Z))_{j\in\{0,\ldots,m\}}$ *be the subresultant sequence and* $(\mathrm{sr}_j(X,Y))_{j\in\{0,\ldots m\}}$ *be the principal subresultant coefficient sequence. Let* $(\Delta_i(X,Y))_{i\in\{1,\ldots,m\}}$ *be the sequence of* $\mathbb{Q}[X,Y]$ *defined by the following relations*

- $\Delta_0(X,Y) = 1; \Theta_0(X,Y) = h(X,Y)$;
- *For* $i \in \{1,...,m\}$,
  $\Theta_i(X,Y) = \gcd(\Theta_{i-1}(X,Y), \mathrm{sr}_i(X,Y))$,
  $\Delta_i(X,Y) = \frac{\Theta_{i-1}(X,Y)}{\Theta_i(X,Y)}$.

For $i \in \{1,\ldots,m\}$, *let* $\mathcal{C}(\Delta_i) := \{(x,y) \in \mathbb{R}^2 | \Delta_i(x,y) = 0\}$ *and* $\mathcal{C}(h) := \{(x,y) \in \mathbb{R}^2 | h(x,y) = 0\}$ *then*

1. $h(X,Y) = \prod_{i=1}^{m} \Delta_i(X,Y)$,
2. $\mathcal{C}(h) = \bigcup_{i=1}^{m} \mathcal{C}(\Delta_i)$,
3. $\mathcal{C}_\mathbb{R}$ *is in pseudo-generic position with respect to the* (x,y)*-plane if and only if* $\forall i \in \{1,\ldots,m\}, \forall (x,y) \in \mathbb{C}^2$ *such that* $\mathrm{sr}_i(x,y) \neq 0$ *and* $\Delta_i(x,y) = 0$, *we have* $\mathrm{Sr}_i(x,y,Z) = \mathrm{sr}_{i,i}(x,y)\left(Z + \frac{\mathrm{sr}_{i,i-1}(x,y)}{i\,\mathrm{sr}_{i,i}(x,y)}\right)^i$.

Proof. 1. By definition, $\forall i \in \{1,\ldots,m\}$, $\Delta_i(X,Y) = \frac{\Theta_{i-1}(X,Y)}{\Theta_i(X,Y)}$. So by a trivial induction

$$\prod_{i=1}^{m} \Delta_i(X,Y) = \frac{\Theta_0(X,Y)}{\Theta_m(X,Y)}.$$

$\deg_Z(P_1) = \deg(P_1)$ and $\deg_Z(P_2) = \deg(P_2)$ imply $\mathrm{sr}_m(X,Y) \in \mathbb{Q}^*$ (see Remark 1).
So $\Theta_m(X,Y) = \gcd(\Theta_{m-1}(X,Y), \mathrm{sr}_m(X,Y)) = 1$, then $\prod_{i=1}^{m} \Delta_i(X,Y) = \Theta_0(X,Y) = h(X,Y)$.

2. Knowing that $h(X,Y) = \prod_{i=1}^{m} \Delta_i(X,Y)$, so it is clear that $\mathcal{C}(h) = \bigcup_{i=1}^{m} \mathcal{C}(\Delta_i)$.

3. Assume that $\mathcal{C}_\mathbb{R}$ is in pseudo-generic position with respect to the (x,y)-plane. Let $i \in \{1,\ldots,m\}$ and $(\alpha,\beta) \in \mathbb{C}^2$ such that $\mathrm{sr}_i(\alpha,\beta) \neq 0$ and $\Delta_i(\alpha,\beta) = 0$. Then $\Delta_i(X,Y) = \frac{\Theta_{i-1}(X,Y)}{\Theta_i(X,Y)} \Longrightarrow \Theta_{i-1}(\alpha,\beta) = 0$. Knowing that $\Theta_{i-1}(X,Y) = \gcd(\Theta_{i-2}(X,Y), \mathrm{sr}_{i-1}(X,Y))$, so it exists $d_1, d_2 \in \mathbb{Q}[X,Y]$ such that
$\Theta_{i-2}(X,Y) = d_1(X,Y)\Theta_{i-1}(X,Y)$ and
$\mathrm{sr}_{i-1}(X,Y) = d_2(X,Y)\Theta_{i-1}(X,Y)$. In this way,
$\Theta_{i-1}(\alpha,\beta) = 0 \Longrightarrow \Theta_{i-2}(\alpha,\beta) = 0$ and $\mathrm{sr}_{i-1}(\alpha,\beta) = 0$. By using the same arguments, $\Theta_{i-2}(\alpha,\beta) = 0 \Longrightarrow \Theta_{i-3}(\alpha,\beta) = 0$ and $\mathrm{sr}_{i-2}(\alpha,\beta) = 0$. By repeating the same argument, we show $\mathrm{sr}_{i-1}(\alpha,\beta) = \ldots = \mathrm{sr}_0(\alpha,\beta) = 0$. Because $\mathrm{sr}_i(\alpha,\beta) \neq 0$, then the fundamental theorem of subresultant gives
$\gcd((P_1(\alpha,\beta,Z), P_2(\alpha,\beta,Z)) = \mathrm{Sr}_i(\alpha,\beta,Z) = \sum_{j=0}^{i} \mathrm{sr}_{i,i-j}(\alpha,\beta)Z^{i-j}$. Knowing that $\mathcal{C}_\mathbb{R}$ is in pseudo-generic position with respect to the (x,y)-plane and $\Delta_i(\alpha,\beta) = 0$ then the polynomial $\mathrm{Sr}_i(\alpha,\beta,Z)$ has only one distinct root which can be written $-\frac{\mathrm{sr}_{i,i-1}(\alpha,\beta)}{i\,\mathrm{sr}_{i,i-1}(\alpha,\beta)}$ depending on the relation between coefficients and roots of a polynomial. So $\mathrm{Sr}_i(\alpha,\beta,Z) = \sum_{j=0}^{m} \mathrm{sr}_{,i,i-j}(\alpha,\beta)Z^{i-j} = \mathrm{sr}_{i,i}(\alpha,\beta)\left(Z + \frac{\mathrm{sr}_{i,i-1}(\alpha,\beta)}{i\,\mathrm{sr}_{i,i-1}(\alpha,\beta)}\right)^i$.
Conversely, assume that $\forall i \in \{1,\ldots,m\}$, $\forall (x,y) \in \mathbb{C}^2$ such that $\mathrm{sr}_i(x,y) \neq 0$ and $\Delta_i(x,y) = 0$, we have $\mathrm{Sr}_i(x,y,Z) = \sum_{j=0}^{m} \mathrm{sr}_{,i,i-j}(x,y)Z^{i-j} = \mathrm{sr}_{i,i}(x,y)\left(Z + \frac{\mathrm{sr}_{i,i-1}(x,y)}{i\,\mathrm{sr}_{i,i-1}(x,y)}\right)^i$. Let $\mathcal{O}$ be an irreductible component of $\Pi_z(\mathcal{C}_\mathbb{C})$. Then there exists $i \in \{1,\ldots,m\}$ such that $\mathcal{O} \subset \mathcal{C}(\Delta_i)$. Let (α,β) be a point of $\mathcal{O}$, such that $\Delta_i(\alpha,\beta) = 0$ and $\mathrm{sr}_i(\alpha,\beta) \neq 0$. Now if we define $\gamma := -\frac{\mathrm{sr}_{i,i-1}(\alpha,\beta)}{i\,\mathrm{sr}_{i,i}(\alpha,\beta)}$, we obtain that $\mathrm{Sr}_i(\alpha,\beta,\gamma) = 0$, then (α,β,γ) is the only point of $\mathcal{C}_\mathbb{C}$ with (α,β) as projection. So $\mathcal{C}_\mathbb{R}$ is in pseudo-generic position with respect to the (x,y)-plane.

□

The following proposition is a corollary of the third result of the previous theorem. If $\mathcal{C}_\mathbb{R}$ is in pseudo-generic position with respect to the (x,y)-plane, it gives a rational parametrization for the regular points of $\mathcal{C}_\mathbb{R}$.

Proposition 4 *Assume that* $\mathcal{C}_\mathbb{R}$ *is in pseudo-generic position with respect to the* (x,y)*-plane and let* $(\alpha,\beta,\gamma) \in \mathcal{C}_\mathbb{R}$ *such that* $\mathrm{sr}_i(\alpha,\beta) \neq 0$ *and* $\Delta_i(\alpha,\beta) = 0$. *Then,*

$$\gamma := -\frac{\mathrm{sr}_{i,i-1}(\alpha,\beta)}{i\,\mathrm{sr}_{i,i}(\alpha,\beta)}. \tag{5}$$

Remark 3 By construction, the parametrization given in Proposition 4 is valid when $\mathrm{sr}_{i,i}(\alpha,\beta) \neq 0$. If $\mathrm{sr}_{i,i}(\alpha,\beta) = 0$ then either $\Delta_j(\alpha,\beta) = 0$ for some $j > i$ or (α,β) is a x-critical point of $\mathcal{C}(\Delta_i)$ (see section 3.3).

The following theorem gives an algebraic test to certify the pseudo-genericity of the position of a space curve with respect to a given plane.

Theorem 5 *Let $(\mathrm{Sr}_j(X,Y,Z))_{j\in\{0,\ldots,m\}}$ be the subresultants sequence associated to $P_1(X,Y,Z)$ and $P_2(X,Y,Z)$ and $(\Delta_i(X,Y))_{i\in\{1,\ldots,m\}}$ be the sequence of $\mathbb{Q}[X,Y]$ previously defined. The curve $\mathcal{C}_{\mathbb{R}}$ is in pseudo-generic position with respect to the (x,y)-plane if and only if*

$$\forall i \in \{1,\ldots,m-1\}, \forall j \in \{0,\ldots,i-1\},$$

$$i(i-j)\,\mathrm{sr}_{i,j}(X,Y)\,\mathrm{sr}_{i,i}(X,Y) - (j+1)\,\mathrm{sr}_{i,i-1}(X,Y)\,\mathrm{sr}_{i,j+1}(X,Y) = 0 \bmod \Delta_i(X,Y).$$

Proof. Assume $\mathcal{C}_{\mathbb{R}}$ be in pseudo-generic position. Let $i \in \{1,\ldots,m-1\}$, $j \in \{0,\ldots,i-1\}$, $(\alpha,\beta) \in \mathbb{R}^2$ such that $\Delta_i(\alpha,\beta) = 0$.
If $\mathrm{sr}_{i,i}(\alpha,\beta) = 0$, then $\mathrm{sr}_{i,i-1}(\alpha,\beta) = 0$, consequently $i(j+1)\,\mathrm{sr}_{i,j+1}(\alpha,\beta)\,\mathrm{sr}_{i,i}(\alpha,\beta) - (i-j)\,\mathrm{sr}_{i,i-1}(\alpha,\beta)\,\mathrm{sr}_{i,j}(\alpha,\beta) = 0$.
If $\mathrm{sr}_{i,i}(\alpha,\beta) \neq 0$, then according to Theorem 4 (3.)
$\mathrm{Sr}_i(\alpha,\beta,Z) = \sum_{j=0}^{i} \mathrm{sr}_{,i,i-j}(\alpha,\beta)Z^{i-j} =$
$\mathrm{sr}_{i,i}(\alpha,\beta)\left(Z + \frac{\mathrm{sr}_{i,i-1}(\alpha,\beta)}{i\,\mathrm{sr}_{i,i-1}(\alpha,\beta)}\right)^i$. Let $\gamma := -\frac{\mathrm{sr}_{i,i-1}(\alpha,\beta)}{i\,\mathrm{sr}_{i,i-1}(\alpha,\beta)}$, then $\mathrm{Sr}_i(\alpha,\beta,Z) = \sum_{j=0}^{i} \mathrm{sr}_{,i,i-j}(\alpha,\beta)Z^{i-j} = \mathrm{sr}_{i,i}(\alpha,\beta)\,(Z-\gamma)^i$.
Using the binomial Newton formula we obtain $\mathrm{Sr}_i(\alpha,\beta,Z) = \sum_{j=0}^{i} \mathrm{sr}_{,i,i-j}(\alpha,\beta)Z^{i-j} = \mathrm{sr}_{i,i}(\alpha,\beta)\sum_{j=0}^{i}\binom{i}{j}(-\gamma)^{i-j}Z^j$. So by identification, it comes that

$$\forall i \in \{1,\ldots,m-1\}, \forall j \in \{0,\ldots,i-1\},$$

$i(i-j)\,\mathrm{sr}_{i,j}(\alpha,\beta)\,\mathrm{sr}_{i,i}(\alpha,\beta) - (i+j)\,\mathrm{sr}_{i,i-1}(\alpha,\beta)\,\mathrm{sr}_{i,j+1}(\alpha,\beta) = 0$, $\forall(\alpha,\beta), \Delta_i(\alpha,\beta) = 0$. The reciprocal uses the same arguments. □

Remark 4 Theorem 5 shows that it is possible to check with certainty if a space algebraic curve is in pseudo-generic position or not. If it is not, we can put it in pseudo-generic position by a change of coordinates. In fact, there is only a finite number of bad changes of coordinates of the form
$X := X + \lambda Z$; $Y := Y + \mu Z$; $Z := Z$,
with $\lambda, \mu \in \mathbb{Q}^*$ such that if $\mathcal{C}_{\mathbb{R}}$ is not in pseudo-generic position then the transformed curve remains in a non-pseudo-generic position [1].

Let us introduce the definitions of generic position, critical, singular, regular points, apparent singularity and real singularity for a space algebraic curve.

Definition 5 *Let $M(X,Y,Z)$ be the 2×3 Jacobian matrix with rows $(\partial_X P_1, \partial_Y P_1, \partial_Z P_1)$ and $(\partial_X P_2, \partial_Y P_2, \partial_Z P_2)$.*

- *A point $p \in \mathcal{C}_{\mathbb{R}}$ is regular (or smooth) if the rank of $M(p)$ is 2.*
- *A point $p \in \mathcal{C}_{\mathbb{R}}$ which is not regular is called singular.*
- *A point $p = (\alpha,\beta,\gamma) \in \mathcal{C}_{\mathbb{R}}$ is x-critical (or critical for the projection on the x-axis) if the curve $\mathcal{C}_{\mathbb{R}}$ is tangent at this point to a plane parallel to the (y,z)-plane. The corresponding α is called a x-critical value.*

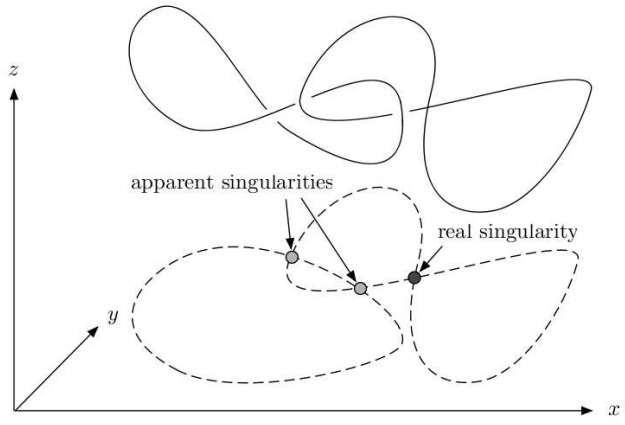

Figure 1: Apparent and real singularities.

Definition 6 ***[Apparent singularity, Real singularity]*** *We call:*

1. *Apparent singularities: the singularities of the projected curve $\mathcal{D} = \Pi_z(\mathcal{C}_{\mathbb{R}})$ with at least two points as inverse-images (see figure 1).*
2. *Real singularities: the singularities of the projected curve $\mathcal{D} = \Pi_z(\mathcal{C}_{\mathbb{R}})$ with exactly one point as inverse-image (see figure 1).*

Definition 7 ***[Generic position]***
The curve $\mathcal{C}_{\mathbb{R}}$ is in generic position with respect to the (x,y)-plane if and only if

1. *$\mathcal{C}_{\mathbb{R}}$ is in pseudo-generic position with respect to the (x,y)-plane,*
2. *$\mathcal{D} = \Pi_z(\mathcal{C}_{\mathbb{R}})$ is in generic position (as a plane algebraic curve) with respect to the x-direction,*
3. *any apparent singularity of $\mathcal{D} = \Pi_z(\mathcal{C}_{\mathbb{R}})$ is a node.*

This notion of genericity also appears in a slightly more restrictive form in [1].

The aim of the next section is to give an algorithm to certify the third point of the previous definition of generic position. We give also in this section an effective way to distinguish the real singularities from the apparent ones.

3.3 Distinguish real singularities and apparent singularities

In this section, we suppose that $\mathcal{C}_{\mathbb{R}}$ is in **pseudo-generic position** and $\mathcal{D} = \Pi_z(\mathcal{C}_{\mathbb{R}})$ is in **generic position as a plane** algebraic curve.

Let $(\Gamma_j(X))_{j\in\{1,\ldots,n\}}$ be the sequence of Γ polynomials associated to the plane curve $\mathcal{D}$ and $(\beta_j(X))_{j\in\{1,\ldots,n\}}$ be the sequence of associated rational parametrization (see (3)). Let $(\mathrm{Sr}_j(X,Y,Z))_{j\in\{0,\ldots,m\}}$ be the subresultant sequence associated to $P_1, P_2 \in \mathbb{Q}[X,Y,Z]$. For any $(k,i) \in \{1,\ldots,m\}\times\{0,\ldots,k-1\}$ let, $R_{k,i}(X,Y)$ be the polynomial

$k(k-i)\,\mathrm{sr}_{k,i}(X,Y)\,\mathrm{sr}_{k,k}(X,Y) - (i+1)\,\mathrm{sr}_{k,k-1}(X,Y)\,\mathrm{sr}_{k,i+1}(X,Y)$.

Lemma 1 *Let $(a,b) \in \mathbb{R}^2$ such that $\mathrm{sr}_{k,k}(a,b) \neq 0$, the polynomial $\mathrm{Sr}_k(a,b,Z) = \sum_{i=0}^{k} \mathrm{sr}_{k,i}(a,b)Z^i \in \mathbb{R}[Z]$ has one and only one root if and only if $\forall i \in \{0,\ldots,k-1\}$ $R_{k,i}(a,b) = 0$.*

For any $j \in \{1,\ldots,n\}$ we define the sequences $(u_k(X))_{k\in\{1,\ldots,j\}}$ and $(v_k(X))_{k\in\{2,\ldots,j\}}$ by
$u_1(X) := \gcd(\Gamma_j(X), \mathrm{sr}_{1,1}(X,\beta_j(X)))$,
$u_k(X) := \gcd(\mathrm{sr}_{k,k}(X,\beta_j(X)), u_{k-1}(X))$
$v_k(X) := \mathrm{quo}(u_{k-1}(X), u_k(X))$.
For $k \in \{2,\ldots,j\}$ and $i \in \{0,k-1\}$, we define $(w_{k,i}(X))$ by
$w_{k,0}(X) := v_k(X)$,
$w_{k,i+1}(X) := \gcd(R_{k,i}(X,\beta_j(X)), w_{k,i}(X))$.

Theorem 6 *For any $j \in \{1,\ldots,n\}$, let $(\Gamma_{j,k}(X))_{k\in\{1,\ldots,j\}}$ and $(\chi_{j,k}(X))$ be the sequences defined by the following relations*

$\Gamma_{j,1}(X) = \mathrm{quo}(\Gamma_j(X), u_1(X))$ *and* $\Gamma_{j,k}(X) := w_{k,k}(X)$. $\chi_{j,k}(X) := \mathrm{quo}(w_{k,0}(X), \Gamma_{j,k}(X))$.

1. *For any root α of $\Gamma_{j,k}(X)$, the x-critical fiber $(\alpha, \beta_j(\alpha))$ contain only the point $(\alpha,\beta_j(\alpha),\gamma_j(\alpha))$ with $\gamma_j(\alpha) := -\frac{\mathrm{sr}_{k,k-1}(\alpha,\beta_j(\alpha))}{k\,\mathrm{sr}_{k,k}(\alpha,\beta_j(\alpha))}$, so $(\alpha,\beta_j(\alpha))$ is a real singularity.*

2. *For any root α of $\chi_{j,k}(X)$, $(\alpha,\beta_j(\alpha))$ is an apparent singularity.*

3. *$\mathcal{C}_\mathbb{R}$ is in generic position if and only if for any $(j,k) \in \{2,\ldots,n\} \times \{2,\ldots j\}$ $\chi_{j,k}(X) = 1$.*

PROOF. 1. Let α be a root of $\Gamma_{j,k}(X) := w_{k,k}(X) = \gcd(R_{k,k-1}(X,\beta_j(X)), w_{k,k-1}(X))$. Then $w_{k,k-1}(\alpha) = R_{k,k-1}(\alpha,\beta_j(\alpha)) = 0$.
$w_{k,k-1}(X) := \gcd(R_{k,k-2}(X,\beta_j(X)), w_{k,k-2}(X))$, so $w_{k,k-2}(\alpha) = R_{k,k-2}(\alpha,\beta_j(\alpha)) = 0$.
By induction, using the same argument, it comes that for i from 0 to $(k-1)$, $w_{k,i}(\alpha) = R_{k,i}(\alpha,\beta_j(\alpha)) = 0$.
$w_{k,0}(X) := v_k(X)$, so $v_k(\alpha) = 0$. Knowing that $v_k(X) := \mathrm{quo}(u_{k-1}(X), u_k(X))$; $u_k(X)$ and $u_{k-1}(X)$ are square free, then $u_{k-1}(\alpha) = 0$ and $u_k(\alpha) \neq 0$. Knowing that $u_k(X) = \gcd(\mathrm{sr}_{k,k}(X,\beta_j(X)), u_{k-1}(X))$, then $\mathrm{sr}_{k,k}(\alpha,\beta_j(\alpha)) \neq 0$.
$u_{k-1}(X) = \gcd(\mathrm{sr}_{k-1,k-1}(X,\beta_j(X)), u_{k-2}(X))$ and $u_{k-1}(\alpha) = 0$, so $\mathrm{sr}_{k-1,k-1}(\alpha,\beta_j(\alpha)) = u_{k-2}(\alpha) = 0$.
By induction, using the same argument, it comes that for i from 0 to $k-1$ $\mathrm{sr}_{i,i}(\alpha,\beta_j(\alpha)) = 0$.
For i from 0 to $k-1$ $\mathrm{sr}_{i,i}(\alpha,\beta_j(\alpha)) = 0$ and $\mathrm{sr}_{k,k}(\alpha,\beta_j(\alpha)) \neq 0$, so by the fundamental theorem of subresultants,
$\gcd(P_1(\alpha,\beta_j(\alpha),Z), P_2(\alpha,\beta_j(\alpha),Z)) = \mathrm{Sr}_k(\alpha,\beta_j(\alpha),Z) = \sum_{i=0}^{k} \mathrm{sr}_{k,i}(\alpha,\beta_j(\alpha))Z^i$. Knowing that $\gcd(P_1(\alpha,\beta_j(\alpha),Z), P_2(\alpha,\beta_j(\alpha),Z)) = \mathrm{Sr}_k(\alpha,\beta_j(\alpha),Z) = \sum_{i=0}^{k} \mathrm{sr}_{k,i}(\alpha,\beta_j(\alpha))Z^i$ and for i from 0 to $(k-1)$, $R_{k,i}(\alpha,\beta_j(\alpha)) = 0$ then by the previous lemma the polynomial $\gcd(P_1(\alpha,\beta_j(\alpha),Z), P_2(\alpha,\beta_j(\alpha),Z)$ have only one root $\gamma_j(\alpha) := -\frac{\mathrm{sr}_{k,k-1}(\alpha,\beta_j(\alpha))}{k\times\mathrm{sr}_{k,k}(\alpha,\beta_j(\alpha))}$.

2. Let α be a root of the polynomial $\chi_{j,k}(X) := \mathrm{quo}(w_{k,0}(X), \Gamma_{j,k}(X))$. Then $w_{k,0}(\alpha) = 0$ and $\Gamma_{j,k}(\alpha) = w_{k,k}(\alpha) \neq 0$ because $w_{k,0}(X)$ and $\Gamma_{j,k}(X)$ are square free. For i from 0 to $k-1$, knowing that $w_{k,i+1}(X) := \gcd(R_{k,i}(X,\beta_j(X)), w_{k,i}(X))$, $w_{k,0}(\alpha) = 0$ and $w_{k,k}(\alpha) \neq 0$, then it exist $i \in \{0,\ldots,k-1\}$ such that $R_{k,i}(\alpha,\beta_j(\alpha)) \neq 0$. So by the previous lemma the polynomial $\mathrm{Sr}_k(\alpha,\beta_j(\alpha),Z) = \sum_{i=0}^{k} \mathrm{sr}_{k,i}(\alpha,\beta_j(\alpha))Z^i$ has at least two distinct roots.
By definition $w_{k,0}(X) := v_k(X)$, so $v_k(\alpha) = 0$. Knowing that $v_k(X) := \mathrm{quo}(u_{k-1}(X), u_k(X))$; $u_k(X)$ and $u_{k-1}(X)$ are squarefree, then $u_{k-1}(\alpha) = 0$ and $u_k(\alpha) \neq 0$.
$u_{k-1}(\alpha) = 0$, $u_k(\alpha) \neq 0$ and $u_k(X) = \gcd(\mathrm{sr}_{k,k}(X,\beta_j(X)), u_{k-1}(X))$ imply $\mathrm{sr}_{k,k}(\alpha,\beta_j(\alpha)) \neq 0$.
$u_{k-1}(X) = \gcd(\mathrm{sr}_{k-1,k-1}(X,\beta_j(X)), u_{k-2}(X))$ and $u_{k-1}(\alpha) = 0$ imply $\mathrm{sr}_{k-1,k-1}(\alpha,\beta_j(\alpha)) = u_{k-2}(\alpha) = 0$.
By induction, using the same argument it comes that for i from 0 to $(k-1)$ $\mathrm{sr}_{i,i}(\alpha,\beta_j(\alpha)) = 0$.
For i from 0 to $(k-1)$ $\mathrm{sr}_{i,i}(\alpha,\beta_j(\alpha)) = 0$ and $\mathrm{sr}_{k,k}(\alpha,\beta_j(\alpha)) \neq 0$, so by the fundamental theorem of subresultants
$\gcd(P_1(\alpha,\beta_j(\alpha),Z), P_2(\alpha,\beta_j(\alpha),Z)) = \mathrm{Sr}_k(\alpha,\beta_j(\alpha),Z) = \sum_{i=0}^{k} \mathrm{sr}_{k,i}(\alpha,\beta_j(\alpha))Z^i$.
$\gcd(P_1(\alpha,\beta_j(\alpha),Z), P_2(\alpha,\beta_j(\alpha),Z)) = \mathrm{Sr}_k(\alpha,\beta_j(\alpha),Z)$ and $\mathrm{Sr}_k(\alpha,\beta_j(\alpha),Z)$ has at least two distinct roots imply that $(\alpha,\beta_j(\alpha))$ is an apparent singularity.

3. $\mathcal{C}_\mathbb{R}$ is in generic position if and only if any apparent singularity of $\mathcal{D} = \Pi_z(\mathcal{C}_\mathbb{R})$ is a node. Knowing that the apparent singularities of $\mathcal{D}$ which are nodes are exactly those with a root of $\chi_{1,2}(X)$ as x-coordinate, so $\mathcal{C}_\mathbb{R}$ is in generic position if and only if for any $(j,k) \in \{2,\ldots,n\} \times \{2,\ldots,j\}$, $\chi_{j,k}(X) = 1$.

□

3.4 Lifting and connection phase

In this section, we suppose that $\mathcal{C}_\mathbb{R}$ is in **generic position** that means that $\mathcal{C}_\mathbb{R}$ is in **pseudo-generic position**, $\mathcal{D} = \Pi_z(\mathcal{C}_\mathbb{R})$ is in **generic position as a plane** algebraic curve and any **apparent singularity** of $\mathcal{D} = \Pi_z(\mathcal{C}_\mathbb{R})$ is a **node**.
To compute the topology of $\mathcal{C}_\mathbb{R}$ we first compute the topology of its projection on the (x,y)-plane and in second we lift the computed topology.

As mentioned in section 2, to compute the topology of a plane algebraic curve in generic position, we need to compute its critical fibers and one regular fiber between two critical ones. So to obtain the topology of $\mathcal{C}_\mathbb{R}$ we just need to lift the critical and regular fibers of $\mathcal{D} = \Pi_z(\mathcal{C}_\mathbb{R})$.

Here after we explain how this lifting can be done without any supplementary computation for the regular fibers and the real critical fibers. And for the special case of the apparent singular fibers, we present a new approach for the lifting and the connections.

3.4.1 *Lifting of the regular points of $\mathcal{D} = \Pi_z(\mathcal{C}_\mathbb{R})$*

The lifting of the regular fibers of $\mathcal{D} = \Pi_z(\mathcal{C}_\mathbb{R})$ is done by using the rational parametrizations given in Proposition 4.

3.4.2 *Lifting of the real singularities of $\mathcal{D} = \Pi_z(\mathcal{C}_\mathbb{R})$*

The lifting of the real singularities of $\mathcal{D} = \Pi_z(\mathcal{C}_\mathbb{R})$ is done by using the rational parametrizations given by 1. of Theorem 6.

3.4.3 *Connection between real singularities and regular points*

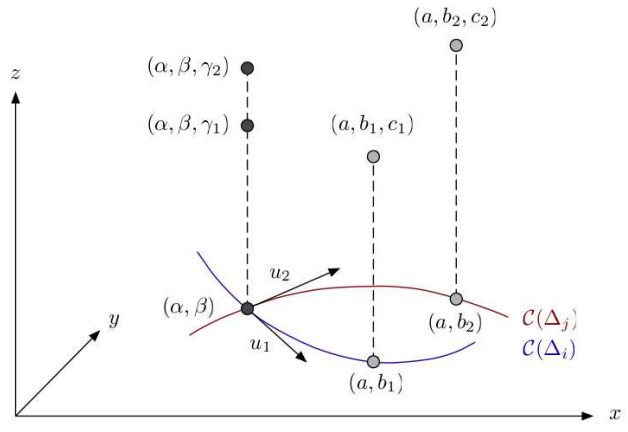

Figure 2: Connection between real singularities and regular points.

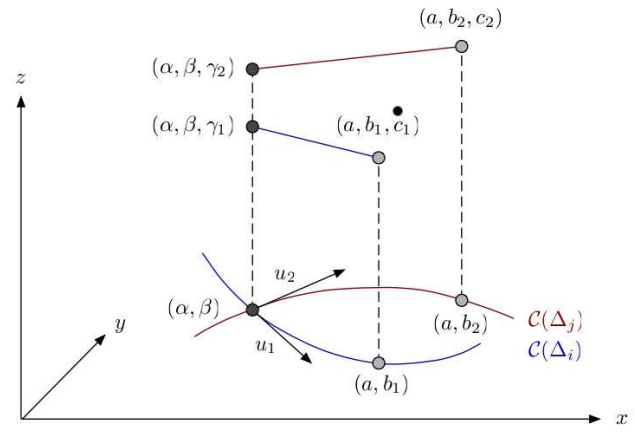

Figure 3: Lifting of an apparent singularity.

For a space curve in pseudo-generic position, the connections between real singularities and regular points are exactly those obtained on the projected curve using Grandine's sweeping algorithm [8] (see figure 2).

3.4.4 *Lifting of the apparent singularities*

The lifting of the topology around an apparent singularity is a little more complex. Above an apparent singularity of $\mathcal{D} = \Pi_z(\mathcal{C}_\mathbb{R})$ we have firstly to compute the z-coordinates and secondly to decide which of the two branches pass over the other (see figure 3). We solve these problems by analyzing the situation at an apparent singularity.

According to Theorem 4 (2.), $\mathcal{D} = \Pi_z(\mathcal{C}_\mathbb{R}) = \bigcup_{i=1}^{m} \mathcal{C}(\Delta_i)$, so an apparent singularity is a cross point of a branch of $\mathcal{C}(\Delta_i)$ and a branch of $\mathcal{C}(\Delta_j)$ with $i, j \in \{1, \ldots, m\}$. So we have the following proposition.

Proposition 5 *If (α, β) is an apparent singularity of $\mathcal{D}$ such that $\Delta_i(\alpha, \beta) = \Delta_j(\alpha, \beta) = 0$, then the degree of the polynomial $\gcd(P_1(\alpha, \beta, Z), P_2(\alpha, \beta, Z)) \in \mathbb{R}[Z]$ will be $(i + j)$.*

Let (α, β) be an apparent singularity of $\mathcal{D}$ such that $\Delta_i(\alpha, \beta) = \Delta_j(\alpha, \beta) = 0$ and γ_1, γ_2 the corresponding z-coordinates. So by Proposition 5 and Proposition 1 $\mathrm{sr}_{0,0}(\alpha, \beta) = \ldots = \mathrm{sr}_{i,i}(\alpha, \beta) = \ldots = \mathrm{sr}_{j,j}(\alpha, \beta) = \ldots = \mathrm{sr}_{i+j-1,i+j-1}(\alpha, \beta) = 0$.
By Proposition 4, for any $(a, b, c) \in \mathcal{C}_\mathbb{R}$ such that $\Delta_i(a, b) = 0$ and $\mathrm{sr}_{i,i}(a, b) \neq 0$ we have $c = -\frac{\mathrm{sr}_{i,i-1}(a,b)}{i\,\mathrm{sr}_{i,i}(a,b)}$. So the function $(x, y) \longmapsto Z_i := -\frac{\mathrm{sr}_{i,i-1}(x,y)}{i\,\mathrm{sr}_{i,i}(x,y)}$ gives the z-coordinate of any $(a, b, c) \in \mathcal{C}_\mathbb{R}$ such that $\Delta_i(a, b) = 0$ and $\mathrm{sr}_{i,i}(a, b) \neq 0$. $\Delta_i(\alpha, \beta) = 0$ but $\mathrm{sr}_{i,i}(\alpha, \beta) = 0$, so the function Z_i is not defined on (α, β). The solution comes from the fact that the function Z_i is continuously extensible on (α, β). Let u_1 be the slope of the tangent line of $\mathcal{C}(\Delta_i)$ at (α, β) and $t \in \mathbb{R}^*$. Let $\gamma_i(t) := Z_i(\alpha, \beta + tu_1) = -\frac{\mathrm{sr}_{i,i-1}(\alpha,\beta+tu_1)}{i\,\mathrm{sr}_{i,i}(\alpha,\beta+tu_1)}$. Knowing that the algebraic curve $\mathcal{C}_\mathbb{R}$ hasn't any discontinuity, it comes $\lim_{t\to 0^+} \gamma_i(t) = \lim_{t\to 0^-} \gamma_i(t) = \gamma_1$. By the same arguments, if we denote u_2 the slope of the tangent line of $\mathcal{C}(\Delta_j)$ at (α, β) and $\gamma_j(t) := Z_j(\alpha, \beta + tu_2) = -\frac{\mathrm{sr}_{j,j-1}(\alpha,\beta+tu_2)}{j\,\mathrm{sr}_{j,j}(\alpha,\beta+tu_2)}$, then $\lim_{t\to 0^+} \gamma_j(t) = \lim_{t\to 0^-} \gamma_j(t) = \gamma_2$. The values u_1, u_2, γ_1 and γ_2 are computed using Taylor formulas and certified numerical approximations.

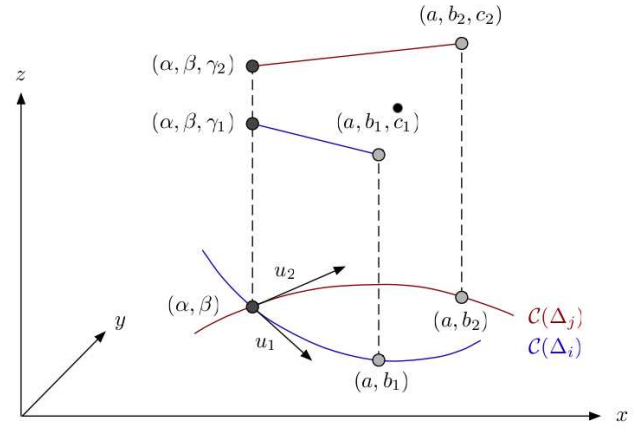

Figure 4: Connection above an apparent singularity.

Now it remains to decide which of the two branches pass over the other. This problem is equivalent to the problem of deciding the connection around an apparent singularity. Let (a, b_1, c_1) and (a, b_2, c_2) the regular points that we have to connect to $(\alpha, \beta, \gamma_1)$ and $(\alpha, \beta, \gamma_2)$. The question is which of the points (a, b_1, c_1) and (a, b_2, c_2) will be connected to $(\alpha, \beta, \gamma_1)$ and the other to $(\alpha, \beta, \gamma_2)$ (see figure 3)? In [1] Alcázar and Sendra give a solution using a second projection of the space curve but it costs a computation of a Sturm Habicht sequence of P_1 and P_2. Our solution does not use any supplementary computation. It comes from the fact that γ_1 is associated to u_1 and γ_2 to u_2. Knowing that u_1 is the slope of the tangent line of $\mathcal{C}(\Delta_i)$ at (α, β) and u_2 the slope of the tangent line of $\mathcal{C}(\Delta_j)$ at (α, β), so $(\alpha, \beta, \gamma_1)$ will be connected to (a, b_1, c_1) if (a, b_1) is on the branch associated to u_1. If (a, b_1) is not on the branch associated to u_1, then (a, b_1) is on the branch associated to u_2, so $(\alpha, \beta, \gamma_2)$ will be connected to (a, b_1, c_1) (see figure 4).

Remark 5 For a curve in generic position any apparent singularity is a node, so the slopes at an apparent singularity

Curve	$P_1(x,y,z)$	$P_2(x,y,z)$	Time (s)
1	$x^2+y^2+z^2-1$	x^2-y^2-z+1	0.032
2	$x^2+y^2+z^2-1$	$x^3+3x^2z+3xz^2+z^3+y^3-xyz-yz^2$	0.659
3	$(x-2y+2z)^2+y^2+z-1$	$z^3-z-(x-2y+2z)^3+3(x-2y+2z)y^2$	2.125
4	$(x-2y+2z)^2+y^2+z^2-1$	$y^3-(x-2y+2z)^3-(x-2y+2z)yz$	1.031
5	$(x-y+z)^2+y^2+z^2-1$	$y^2-(x-y+z)^2-(x-y+z)z)^2-z^2((x-y+z)^2+y^2)$	1.6963
6	$(x-y+z)^2+y^2+z^2-1$	$((x-y+z)^2+y^2+z^2)^2-4((x-y+z)^2+y^2)$	2.228
7	$(x-y+z)^2+y^2-2(x-y+z)$	$((x-y+z)^2+y^2+z^2)^2-4((x-y+z)^2+y^2)$	2.875

Figure 5: Running time of experimentations.

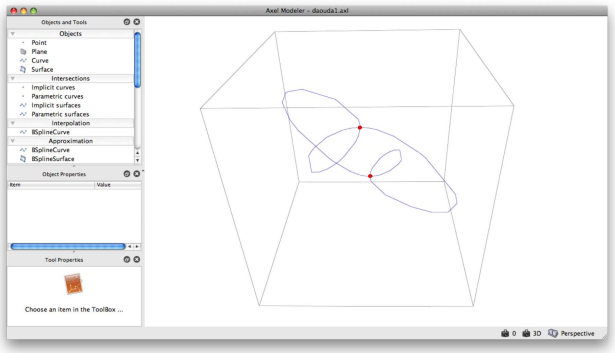

Figure 6: Computed topology of curve 2 of table 5.

are always distinct that is to say $u_1 \neq u_2$.

4. IMPLEMENTATION, EXPERIMENTS

A preliminary implementation of our method has been written using the Computer Algebra System Mathemagix. Results are visualized using the Axel[1] algebraic geometric modeler which allows the manipulation of geometric objects with algebraic representation such as implicit or parametric curves or surfaces.

Since existing methods have no publicly available implementations, table 5 only reports our experiments, performed on an Intel(R) Core machine clocked at 2GHz with 1GB RAM.

5. REFERENCES

[1] J.G. Alcazár, and J.R Sendra. *Computation of the Topology of Algebraic Space Curves. J. Symbolic Comput.*, vol. 39, no. 6, 719–744, 2005.

[2] S. Basu, R. Pollack and M.F. Roy. *Algorithms in real algebraic geometry*, Algorithms and Computation in Mathematics, vol. 10, second edition, Springer-Verlag, Berlin, 2006.

[3] R. Benedetti and J.J Risler. *Real algebraic and semi-algebraic sets*, Actualités Mathématiques. [Current Mathematical Topics], Hermann, Paris, 1990.

[4] G.E. Collins. *Subresultants and reduced polynomial remainder sequences.* J. ACM, 14 :128-142, 1967.

[5] D. Cox, J. Little, and D. O'Shea. *Ideals Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Undergraduate Texts in Mathematics. Springer Verlag, New-York, 1992.

[1] `http://axel.inria.fr`

[6] M. El Kahoui. *Topology of real algebraic space curves.* Preprint 2007.

[7] G. Gatellier, A. Labrouzy, B. Mourrain, and J.P. Técourt. *Computing the topology of three-dimensional algebraic curves.* In *Computational methods for algebraic spline surfaces*, p. 27–43, Springer, Berlin, 2005.

[8] L. Gonzalez-Vega, I. Necula. *Efficient topology determination of implicitly defined algebraic plane curves.* In *Comput. Aided Geom. Design*, vol. 19, no. 9, 719-743, 2002.

[9] T.A Grandine. *Applications of contouring.* In *SIAM Rev.*, Vol. 42, no. 2, 297-316, 2000.

[10] T.A Grandine, F.W Klein. *A new approach to the surface intersection problem.* In *Comput. Aided Geom. Design*, Vol. 14, no. 2, 111–134, 1997.

[11] J.C. Owen, and A.P. Rockwood. *Intersection of general implicit surfaces.* In *Geometric modeling*, *SIAM*, 335–345, 1987.

[12] A. Eigenwillig, M. Kerber and N. Wolpert. *Fast and Exact Geometric Analysis of Real Algebraic Plane Curves. In Proc. of the 2007 Int. Symp. on Symb. and Alg. Comp.* (ISSAC 2007).

[13] C. Mittermaier, W. Schreiner and F. Winkler. *Plotting Algebraic Space Curves by Cluter Computing. In Proc. of ASCM 2000.pp. 49-58* .

[14] H. Hong. *An Efficient Method for Analyzing The Topology of Plane Real Algebraic Curves . Math. and Comp. Sim.* 42 (1996) 541-582.

[15] C. Bajaj, C.M. Hoffmann. *Tracing Surfaces Intersection. 1988 Comput. Aided. Geom. Design 5, 285-307.*

[16] J. Keyser, T. Culver., D. Manocha, S. Krishnan *Efficient and Exact Manipulation of Algebraic Points and Curves 2000 Comput. Aided. Geom. Design 32(11), 649-662.*

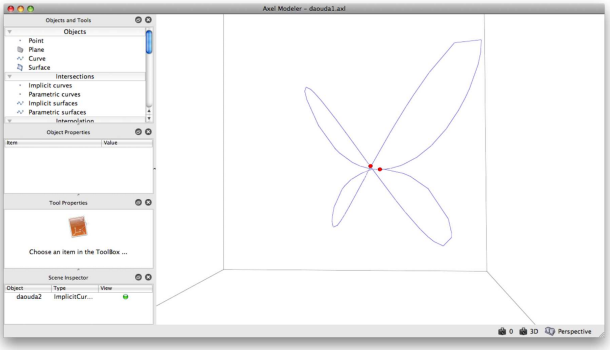

Figure 7: Computed topology of curve 7 of table 5.