Topology of real algebraic space curves

M’hammed El Kahoui

Department of Mathematics, Faculty of Sciences Semlalia, Cadi Ayyad University, P.O. Box 2390, Marrakech, Morocco

Received 26 January 2007; accepted 26 October 2007
Available online 1 November 2007

Abstract

In this paper we give a new projection-based algorithm for computing the topology of a real algebraic space curve given implicitly by a set of equations. Under some genericity conditions, which may be reached through a linear change of coordinates, we show that a plane projection of the given curve, together with a special polynomial in the ideal of the curve contains all the information needed to compute its topological shape. Our method is also designed in such a way to exploit important particular cases such as complete intersection curves or curves contained in nonsingular surfaces.

Keywords: Generic position; Topology of real algebraic curves

1. Introduction

The computation of the topology of real algebraic curves and surfaces is of fundamental interest in many areas of application such as Computer Aided Geometric Design, Robotics and Computer Vision. For real plane algebraic curves the problem is nowadays very classical, and many papers have been published so far (Arnon and McCallum, 1988; Arnborg and Feng, 1988; Coste and Roy, 1988; Roy and Szpirglas, 1990; Cucker et al., 1991; Cellini et al., 1991; Sakkalis, 1991; Hong, 1996; González-Vega and El Kahoui, 1996; Keyser et al., 2000; González-Vega and Necula, 2002; Wolpert, 2003; Eigenwillig et al., 2006; Seidel and Wolpert, 2005; Eigenwillig et al., 2007). For real space curves the problem has not been treated as extensively as for plane curves, and to our knowledge it is only recently that the certified algorithms dealing with this problem have been devised (Gatellier et al., 2005; Alcazar and Sendra, 2005; Alcazar, 2007; Eigenwillig et al., 2007).
It is worth noticing here that the method described in Alcazar (2007) applies to curves in $n$-dimensional affine space provided that they are given as the intersection of $n - 1$ hypersurfaces.

A commonly used approach to this problem is to compute several plane projections of the space curve, study their topological shape and then lift the obtained information to the space curve. Two main issues need to be addressed when opting for such an approach. The first one concerns the projection step. One needs indeed to be careful in choosing the plane projections in order to avoid the degenerate situations which cause a loss of information (it may for instance happen that complex branches of the space curve project down onto real branches of the plane projection). This means that some genericity conditions on the projections need to be imposed. The second issue concerns the lifting process in so far as when processing several projections the information we get back unavoidably overlaps, and so we need to coordinate the obtained information.

In this paper we give a new projection-based method to compute the topology of a real algebraic space curve. Contrary to the existing algorithms, our method is general in so far as it works for curves which are not necessarily complete intersection. However, it requires a generating system of the ideal of the curve to be available. Under some genericity conditions on the coordinate system $x, y, z$ we show that the projection of a given curve $C$ into the $(x, y)$-plane, together with a special polynomial in the ideal of the curve, contains all the information we need to construct a space graph $G$ such that $C$ and $G$ are semi-algebraically homeomorphic as embedded objects into the Euclidean space. In particular, the process of lifting information from the plane projection to the space curve is reduced to a simple univariate sign determination. Our method is also well designed for important situations in practice such as complete intersection and curves contained in nonsingular surfaces.

The paper is structured as follows. In Section 3 we set up notation and recall some basic concepts of algebraic curves theory. We also give a review of subresultants, which play a crucial role in our method, and recall the main properties of plane curves in generic position. In Section 4 we define the space curves in generic position and give the main result which makes working our method. An algorithm for checking generic position is given in Section 5. A description of the main steps in the computation of the topology of space curves is given in Section 6.

We have tried in this paper to keep things as elementary as possible. In particular, sophisticated concepts of algebraic geometry are avoided as much as possible at the price of lengthily but quite intuitive proofs. We should also mention that the paper contains only the theoretical principles of the algorithms and a pseudo-code description of them.

2. Outline of the algorithm

Our method for computing the topology of a real algebraic space curve is inspired from knot theory. So, let us recall some fundamental facts of this theory, see e.g., Adams (2004).

From classical knot theory we know that any knot $K \subset \mathbb{R}^3$ is equivalent to a polygonal knot, and so we may assume without loss of generality that $K$ is polygonal. Any projection of $K$ into a plane is then a plane polygonal curve with self-crossings. A generic projection of $K$ has only nodes as self-crossings.

It is clear that the information contained in a generic projection of $K$ is not enough for reconstructing the knot up to equivalence. To be able to do so we need to have at disposal, for each crossing point, additional information which says which is the overpass and which is the underpass.
Let \( \mathcal{C} \subseteq \mathbb{R}^3 \) be a real algebraic space curve. A generic projection \( \mathcal{C}_1 \) of \( \mathcal{C} \) contains only nodes as singularities caused by projection. The curve \( \mathcal{C}_1 \) contains all the topological features of \( \mathcal{C} \), but the information concerning the overpass and the underpass at the singularities caused by projection. If we are able to compute such an information then we may use a similar method as for knots to reconstruct the topology of the space curve \( \mathcal{C} \) from one of its plane projection \( \mathcal{C}_1 \).

The main contribution of this paper is a method to compute the missing information from the equations defining the ideal \( \mathcal{I} (\mathcal{C}) \) of the space curve \( \mathcal{C} \). The method works as follows.

Assume that the projection \( \mathcal{C}_1 \) of \( \mathcal{C} \) into the \((x, y)\)-plane is generic. In this case the ideal \( \mathcal{I} (\mathcal{C}) \) contains a polynomial of the form \( a(x)z - b(x, y) \) which is primitive when viewed as polynomial in terms of \( y, z \) with coefficients in \( \mathbb{R}[x] \), see Section 4. Let \((\alpha, \beta)\) be a node of \( \mathcal{C}_1 \) caused by projection and let \( y_1(x), y_2(x) \) be the branches of \( \mathcal{C}_1 \) around \((\alpha, \beta)\), with \( y_1(x) < y_2(x) \) if \( x < \alpha \).

If we let \( z_i(x) = \frac{b(x, y_i(x))}{a(x)} \) then \((y_1(x), z_1(x)), (y_2(x), z_2(x))\) are the branches of \( \mathcal{C} \) which lift \( y_1(x), y_2(x) \) and \((\alpha, \beta, z_1(\alpha)), (\alpha, \beta, z_2(\alpha))\) are the only points of \( \mathcal{C} \) above \((\alpha, \beta)\). Computing the sign of \( z_1(\alpha) - z_2(\alpha) \) is the missing information in the projection \( \mathcal{C}_1 \). Indeed, once the sign of \( z_1(\alpha) - z_2(\alpha) \) is computed we know exactly which local branch of \( \mathcal{C} \) near \( \alpha \) is above the other.

As we will show in \textbf{Theorem 4.1}, it turns out to be that \( \alpha \) is a simple root of \( a(x) \) and so we have the formula

\[
z_i(\alpha) = \frac{\partial_x b(\alpha, \beta) + \partial_y b(\alpha, \beta) y'_i(\alpha)}{a'(\alpha)}.
\]

This yields that \( a'(\alpha)(z_1(\alpha) - z_2(\alpha)) = (y'_1(\alpha) - y'_2(\alpha)) \partial_x b(\alpha, \beta) \). The fact that \((\alpha, \beta)\) is a node and \( y_1(x) - y_2(x) < 0 \) for \( x < \alpha \) implies that \( y'_1(\alpha) - y'_2(\alpha) > 0 \) and so the sign of \( z_1(\alpha) - z_2(\alpha) \) is the same as the sign of \( a'(\alpha) \partial_y b(\alpha, \beta) \).

3. Fundamental tools

Throughout this paper we let \( K \) be a commutative field of characteristic zero and \( \overline{K} \) be its algebraic closure. In case \( K \) is an ordered field we let \( \mathcal{R} \) be its real closure. All the considered algebraic sets will be defined over \( K \), i.e., defined by a finite set of equations with coefficients in \( K \).

Given an algebraic set \( \mathcal{V} \subseteq \overline{K}^n \) we let \( \mathcal{I} (\mathcal{V}) = \{ g \in K[x_1, \ldots, x_n] \; ; \; g = 0 \text{ on } \mathcal{V} \} \) be its ideal and \( K[\mathcal{V}] = K[x_1, \ldots, x_n]/\mathcal{I} (\mathcal{V}) \) be its coordinate ring.

3.1. Plane algebraic curves

Let \( f \) be a square-free polynomial in \( K[x, y] \) and \( \mathcal{C}_f \subset \overline{K}^2 \) be the affine plane algebraic curve defined by the equation \( f(x, y) = 0 \). The zeros in \( \overline{K}^2 \) of the ideal \( \mathcal{I} (f, \partial_x f) \) (resp. \( \mathcal{I} (f, \partial_y f) \)) are called the \( x \)-critical points (resp. \( y \)-critical points) of the curve \( \mathcal{C}_f \).

The multiplicity of a point \((\alpha, \beta)\) of the curve \( \mathcal{C}_f \) is defined as the largest integer \( p \) such that \( \partial_i^i y_j f(\alpha, \beta) = 0 \) for any \( i + j < p \). When \( p \geq 2 \) the point is called singular. If \((\alpha, \beta)\) is a point of multiplicity \( p \) in the curve \( \mathcal{C}_f \) then the Taylor expansion of \( f \) around \((\alpha, \beta)\) writes as

\[
f(x, y) = f_p(x - \alpha, y - \beta) + \cdots + f_d(x - \alpha, y - \beta),
\]

where the \( f_i \)'s are \( i \)-homogeneous and \( f_p \neq 0 \). Since \( f_p \) is homogeneous and bivariate it factorizes over \( \overline{K} \) into a product of linear forms. For each linear factor \( \ell(x, y) \) of \( f_p \) the equation \( \ell(x, y) = 0 \) gives a tangent line to \( \mathcal{C}_f \) at \((\alpha, \beta)\). Thus, a point of multiplicity \( p \) has \( p \) tangent lines counted with multiplicities. In case \( f_p \) is square-free the point \((\alpha, \beta)\) is called an ordinary multiple point, and in case \( p = 2 \) it is called a node.
3.2. Newton–Puiseux expansions

Let $f(x, y) \in \mathbb{K}[x, y]$ be a square-free polynomial, $(\alpha, \beta)$ be a point of $\mathcal{C}_f$ and $m$ be the multiplicity of $\beta$ as root of $f(\alpha, y)$. The classical Puiseux theorem states that there exist $n_1, \ldots, n_m \in \overline{\mathbb{K}}[[x - \alpha]]^*$ such that $\eta_i(\alpha) = \beta$ and $f(x, \eta_i) = 0$, see e.g., Walker (1978). The fractional power series $\eta_1, \ldots, \eta_m$ are called the Newton–Puiseux expansions of $\mathcal{C}_f$ at the point $(\alpha, \beta)$. The result holds true if we replace $f$ by any polynomial in $\overline{\mathbb{K}}((x - \alpha))^*[y]$, so that the field $\overline{\mathbb{K}}((x - \alpha))^*$ is algebraically closed. Notice that in case $m = 1$, i.e., $\beta$ is a simple root of $f(\alpha, y)$, the Newton–Puiseux expansion of $\mathcal{C}_f$ at $(\alpha, \beta)$ belongs to $\overline{\mathbb{K}}[[x - \alpha]]$ according to the formal implicit function theorem.

In case $(\alpha, \beta)$ is of multiplicity $p$ in the curve $\mathcal{C}_f$ and the line $x = \alpha$ is not tangent to $\mathcal{C}_f$ at $(\alpha, \beta)$, $\beta$ is a root of multiplicity $p$ of $f(\alpha, y)$ and so there are exactly $p$ Newton–Puiseux expansions of $\mathcal{C}_f$ at $(\alpha, \beta)$. If moreover $(\alpha, \beta)$ is an ordinary singular point of $\mathcal{C}_f$ then the Newton–Puiseux expansions of $\mathcal{C}_f$ at $(\alpha, \beta)$ belong to $\overline{\mathbb{K}}[[x - \alpha]]$.

3.3. Space curves

Let $\mathcal{C} \subset \overline{\mathbb{K}}^3$ be an algebraic set and $\mathcal{I}(\mathcal{C})$ be its ideal. We will say that $\mathcal{C}$ is an algebraic curve if the ideal $\mathcal{I}(\mathcal{C})$ is equi-dimensional of dimension 1. Let $G = g_1, \ldots, g_s$ be a generating system of the ideal $\mathcal{I}(\mathcal{C})$, and let $\text{Jac}(G)$ be the Jacobian matrix of $G$. This is an $s$ by 3 matrix, and at each point of the curve $\mathcal{C}$ its rank is at most 2. It is also a classical fact that the rank of $\text{Jac}(G)$ at any point of $\mathcal{C}$ does not depend on the generating system $G$.

If at a given point $(\alpha, \beta, \gamma)$ the rank of $\text{Jac}(G)$ is 2 the point is called nonsingular, otherwise it is called singular. In case $(\alpha, \beta, \gamma)$ is singular and the rank of the Jacobian matrix is 1 we will say that $\mathcal{C}$ has a plane singularity at this point. This means that the curve $\mathcal{C}$ is contained in a surface $\mathcal{S}$ which is nonsingular at the point $(\alpha, \beta, \gamma)$. It turns out to be that all the nonsingular surfaces at $(\alpha, \beta, \gamma)$ which contain $\mathcal{C}$ have the same tangent plane given by the linear system $\text{Jac}(G)(\alpha, \beta, \gamma). (x - \alpha, y - \beta, z - \gamma)^t = 0$. By abuse, we will call this plane the tangent plane to $\mathcal{C}$ at $(\alpha, \beta, \gamma)$.

A given point $(\alpha, \beta, \gamma)$ of $\mathcal{C}$ is called x-critical if the rows $(\partial_y g_1, \ldots, \partial_y g_s)_{(\alpha, \beta, \gamma)}$ and $(\partial_z g_1, \ldots, \partial_z g_s)_{(\alpha, \beta, \gamma)}$ are linearly dependent. An x-critical point is either singular or it is nonsingular and its tangent line belongs to the affine plane $x = \alpha$. In a similar way we define y-critical and z-critical points. In all the rest of this paper we will mainly consider x-critical points, and so we will simply call them critical.

Let $(\alpha, \beta, \gamma) \in \mathcal{C}$ be a nonsingular point. Then the line $x = \alpha, y = \beta$ is tangent to $\mathcal{C}$ at this point if and only if $(\partial_z g_1, \ldots, \partial_z g_s)_{(\alpha, \beta, \gamma)} = 0$. Indeed, assume that the line $x = \alpha, y = \beta$ is tangent to $\mathcal{C}$ at this point. Then $(\alpha, \beta, \gamma)$ is both $x$-critical and $y$-critical. Thus, the rows $(\partial_y g_1, \ldots, \partial_y g_s)_{(\alpha, \beta, \gamma)}$ and $(\partial_z g_1, \ldots, \partial_z g_s)_{(\alpha, \beta, \gamma)}$ and the rows $(\partial_y g_1, \ldots, \partial_y g_s)_{(\alpha, \beta, \gamma)}$ and $(\partial_z g_1, \ldots, \partial_z g_s)_{(\alpha, \beta, \gamma)}$ are linearly dependent. If $(\partial_z g_1, \ldots, \partial_z g_s)_{(\alpha, \beta, \gamma)} \neq 0$ then $(\partial_z g_1, \ldots, \partial_z g_s)_{(\alpha, \beta, \gamma)}$ and $(\partial_y g_1, \ldots, \partial_y g_s)_{(\alpha, \beta, \gamma)}$ must be linearly dependent. Therefore, rank$(\text{Jac}(G)(\alpha, \beta, \gamma)) \leq 1$ and this contradicts the fact that $(\alpha, \beta, \gamma)$ is nonsingular. Conversely, if $(\partial_z g_1, \ldots, \partial_z g_s)_{(\alpha, \beta, \gamma)} = 0$ then clearly the tangent to $\mathcal{C}$ at $(\alpha, \beta, \gamma)$ is the line given by $x = \alpha, y = \beta$.

Let us also recall that if $(\alpha, \beta, \gamma)$ is a nonsingular point of $\mathcal{C}$ then the ideal $\mathcal{I}(\mathcal{C})$ is generated in the local ring $\mathcal{K}[x, y, z]_{(\alpha, \beta, \gamma)}$ by two polynomials. More precisely, if $g_1, g_2 \in \mathcal{I}(\mathcal{C})$ are such that the Jacobian matrix $\text{Jac}(g_1, g_2)(\alpha, \beta)$ is of rank two then $g_1, g_2$ generate the ideal $\mathcal{I}(\mathcal{C})$ in the local ring $\mathcal{K}[x, y, z]_{(\alpha, \beta, \gamma)}$. 


3.4. Review on subresultants

Subresultants will play a crucial role in what follows. So we give here a short review of this theory, and refer to Basu et al. (2003) and the references therein for more details.

Let $\mathcal{A}$ be a commutative ring with unit and $m \leq n$ be two positive integers. We denote by $\mathcal{M}_{m,n}(\mathcal{A})$ the $\mathcal{A}$-module of $m \times n$ matrices with coefficients in $\mathcal{A}$. Consider the free $\mathcal{A}$-module $\mathcal{P}_n$ of polynomials with coefficients in $\mathcal{A}$ of degree at most $n - 1$ equipped with the basis $B_n = [y^n, \ldots, y, 1]$. A sequence of polynomials $[P_1, \ldots, P_n]$ in $\mathcal{P}_n$ will be identified to the $m \times n$ matrix whose row’s coefficients are the coordinates of the $P_i$’s in $B_n$.

**Definition 3.1.** Let $m \leq n$ be positive integers and $M = (a_{i,j})$ be a matrix in $\mathcal{M}_{m,n}(\mathcal{A})$. For $0 \leq j \leq n - m$ let $d_j$ be the $m \times m$ minor of $M$ extracted on the columns $1, \ldots, m - 1, n - j$. The polynomial $\text{DetPol}(M) = \sum_j d_j y^j$ is called the polynomial determinant of $M$.

Let $p, q$ be positive integers and $P, Q \in \mathcal{A}[y]$ be such that $\deg(P) = p$ and $\deg(Q) = q$. To simplify we assume that $p > q > 0$. For $i \leq q$ we let $\text{Sylv}_i(P, Q) = [y^{q-i-1}P, \ldots, P, y^{p-i-1}Q, \ldots, Q]$ be the $i$th Sylvester matrix of $P$ and $Q$.

**Definition 3.2.** Let $P, Q \in \mathcal{A}[y]$, with $\deg(P) = p$ and $\deg(Q) = q$. For any $i \leq q$ the polynomial determinant of $\text{Sylv}_i(P, Q)$, denoted by $\text{Sr}_i(P, Q)$, is called the $i$th subresultant of $P$ and $Q$. The coefficient of degree $i$ of $\text{Sr}_i(P, Q)$, denoted by $\text{sr}_i(P, Q)$, is called the $i$th principal subresultant coefficient of $P$ and $Q$.

The polynomial $\text{Sr}_i(P, Q)$ is of degree at most $i$ and belongs to the ideal $\mathcal{I}(P, Q)$. In particular $\text{Sr}_0(P, Q)$ is nothing but the resultant of $P$ and $Q$. The following specialization property of subresultants stands to reason.

**Proposition 3.1.** Let $\psi : \mathcal{A} \longrightarrow \mathcal{B}$ be a ring homomorphism and $P, Q \in \mathcal{A}[y]$ be two polynomials with $\deg(P) = p$ and $\deg(Q) = q$. If $\deg(\psi(P)) = p$ and $\deg(\psi(Q)) = q$ then for any $i \leq q$ we have:

$$\text{Sr}_i(\psi(P), \psi(Q)) = \psi(\text{Sr}_i(P, Q)).$$

The following theorem is the most important property which the subresultants satisfy.

**Theorem 3.1.** Let $\mathcal{A}$ be a domain and $P, Q \in \mathcal{A}[y]$ be two polynomials with $\deg(P) = p$ and $\deg(Q) = q$. Then the following assertions are equivalent.

(i) $P$ and $Q$ have a gcd of degree $k$ over the fractions field of $\mathcal{A}$,

(ii) $\text{sr}_0(P, Q) = \cdots = \text{sr}_{k-1}(P, Q) = 0$, $\text{sr}_k(P, Q) \neq 0$.

In this case, $\text{Sr}_k(P, Q)$ is a gcd of $P$ and $Q$ over the fractions field of $\mathcal{A}$.

The properties of subresultants listed above will be ubiquitous in what follows, so we will make use of them without explicit reference.

3.5. Plane curves in generic position

The concept of curves in generic position is cooked up exactly so that no overlapping of the critical points occurs in the projections with respect to the coordinate axes. Such a concept is widely used to come up with efficient algorithms to compute the topology of arrangements.
of real plane algebraic curves (González-Vega and El Kahoui, 1996; Eigenwillig et al., 2006; Wolpert, 2003; González-Vega and Necula, 2002; Seidel and Wolpert, 2005). For a systematic study of plane curves in generic position we refer to El Kahoui (1997) where proofs of the results we state in this subsection may be found.

**Definition 3.3.** An affine plane algebraic curve \( C_f \), defined by a square-free polynomial \( f \), is called in generic position with respect to the projection on the \( x \)-axis if the following conditions hold.

(i) \( \deg(f) = \deg_y(f) \),
(ii) two distinct \( x \)-critical points of \( C_f \) have distinct \( x \)-coordinates,
(iii) the curve \( C_f \) has no vertical tangent line at its singular points,
(iv) the curve \( C_f \) has no inflexion point with vertical tangent line.

The definition of generic position given in González-Vega and El Kahoui (1996), Eigenwillig et al. (2006), Wolpert (2003), González-Vega and Necula (2002) and Seidel and Wolpert (2005) differs from the one we recall here, see El Kahoui (1997). The two more conditions (iii) and (iv) do not provide any substantial improvement concerning the computation of the topology of a plane curve. The reason behind introducing these two conditions will become clear when we will study space algebraic curves (cf. Lemma 4.2). In fact, our method for extracting information from a plane projection cannot work without these two more conditions.

Let \( f \) be a square-free polynomial of degree \( d \) with respect to \( y \), and let \( S_0, \ldots, S_{d-1} \) be the subresultant sequence of \( f \) and \( \partial_y f \) with respect to \( y \), and write

\[
S_r = s_r(x)y^j + s_{r,j-1}(x)y^{j-1} + \cdots + s_{r,0}(x).
\]

**Proposition 3.2.** Let \( C_f \) be a plane algebraic curve in generic position given by a square-free polynomial \( f \in K[x, y] \) and \((\alpha, \beta)\) be a critical point of \( C_f \). Then we have the following properties.

(i) \((\alpha, \beta)\) is singular if and only if \( \alpha \) is a multiple root of \( s_0(\alpha) \). In this case the multiplicity \( p \) of \((\alpha, \beta)\) is equal to the multiplicity of \( \beta \) as root of \( f(\alpha, y) \) and the multiplicity of \( \alpha \) as root of \( s_0(\alpha) \) is at least \( p(p-1) \),
(ii) \((\alpha, \beta)\) is an ordinary singular point of \( C_f \) if and only if \((\alpha, \beta)\) is of multiplicity \( p \) in \( C_f \) and \( \alpha \) is a multiplicity \( p(p-1) \) root of \( s_0(\alpha) \).

As a straightforward consequence of Proposition 3.2, a point \((\alpha, \beta)\) of \( C_f \) is a node if and only if \( \alpha \) is a double root of \( s_0(\alpha) \). We turn now to one of the main features of generic position, namely the rational univariate representation of the critical points of an algebraic curve.

**Proposition 3.3.** Let \( C_f \) be a plane algebraic curve in generic position given by a square-free polynomial \( f \in K[x, y] \). If \((\alpha, \beta)\) is a critical point of \( C_f \) then there exists a unique \( k \) such that

\[
s_0(\alpha) = \cdots = s_{k-1}(\alpha) = 0, \quad s_k(\alpha) \neq 0,
\]

\[
\beta = -\frac{s_{k-1}(\alpha)}{k.s_k(\alpha)}.
\]

If \((\alpha, \beta)\) is singular of multiplicity \( p \) then \( k = p - 1 \), otherwise \( k = 2 \).
Let $\delta(x)$ be a square-free factor of $s_{r0}$ and let us perform the following gcd computation:

$$
\phi_1 = \gcd(\delta, s_{r1}), \quad \delta_1 = \frac{\delta}{\phi_1} \\
\phi_2 = \gcd(\phi_1, s_{r2}), \quad \delta_2 = \frac{\delta_1}{\phi_2} \\
\vdots \quad \vdots
$$

After deleting the $\delta_i$'s which are constant and relabelling we get a factorization $\delta = \delta_1 \cdots \delta_r$ such that for any root $\alpha$ of $\delta_i$ the degree of the polynomial $\gcd(f(\alpha, y), \partial_y f(\alpha, y))$ is the same, say $p_i$, and $p_1 < p_2 < \cdots < p_r$. In what follows, we will call such a process a factorization with respect to gcd degree.

By Proposition 3.3, we get for each $p_i$ a rational representation in the following form.

$$
\delta_i(x) = 0, \\
y = -(p_i s_{r1}(x))^{-1} s_{r1, p_i - 1}(x).
$$

This representation is more suited for numerical computations. For algebraic computations we need to get rid of the denominator in the expression of $y$ in terms of $x$. This may be achieved by computing a Bézout identity

$$
r_i \delta_i + s_i s_{r1, p_i - 1} = 1
$$

of $\delta_i$ and $s_{r1, p_i}$, and then replacing the expression of $y$ by

$$
\sigma_{i, y} = -p_i^{-1} s_{i, s_{r1, p_i - 1}}.
$$

In doing so we get a new rational representation in which the expression of $y$ in terms of $x$ is a polynomial instead of a rational function. In what follows, all the considered rational representations will be of a polynomial kind as in formula (1).

The following algorithm describes the main steps to be performed in order to obtain rational representations of the critical points of a curve in generic position.

**Algorithm 1** Rational representations.

**Input:** A square-free polynomial $f \in K[x, y]$ such that $\mathcal{C}_f$ is in generic position.

A square-free polynomial $\delta$ which divides $s_{r0}$.

**Output:** A list $L = [L_1, \ldots, L_r]$, where $L_i = [\delta_i(x), \sigma_{i,y}(x)]$ is such that $\delta = \delta_1 \cdots \delta_r$ and $L_i$ is a rational representation of the critical points of $\mathcal{C}_f$ whose $x$-coordinates are roots of $\delta_i$.

1. Factorize $\delta$ with respect to gcd degree, and write $\delta = \delta_1 \cdots \delta_r$.
2. for $i = 1$ to $r$
   3. Compute $\sigma_{i,y}$ according to formula (1), and add $[\delta_i, \sigma_{i,y}]$ to the list $L$.
4. end for

Let $f(x, y) \in K[x, y]$ be a square-free polynomial, $u$ be a new variable and let $g_u(x, y) = f(x + u y, y)$. Let $D(u, x)$ be the discriminant of $g_u(x, y)$ with respect to $y$ and let $S(u, x)$ be the maximal square-free factor of $D(u, x)$. Let $R(u)$ be the discriminant of $S(u, x)$ with respect
to \( x \). Then for \( \mu \in K \) the curve \( \mathcal{C}_{\mathcal{C}_g} \) is in generic position if and only if \( R(\mu) \neq 0 \), see El Kahoui (1997). Since \( S(u, x) \) is square-free we have \( R(u) \neq 0 \), and so almost all the curves \( \mathcal{C}_{\mathcal{C}_g} \) are in generic position. An efficient algorithm to put curves in generic position is given in Bouziane and El Kahoui (2002).

4. Space curves in generic position

Our method for computing the topology of real algebraic space curves is projection-based. In this section we state and study the genericity conditions on the coordinate axes we need to make it working.

4.1. Generic position conditions

**Definition 4.1.** Let \( \mathcal{C} \subset \overline{K}^3 \) be a space algebraic curve and \( \mathcal{I}(\mathcal{C}) \subset K[x, y, z] \) be its ideal. We will say that \( \mathcal{C} \) is in generic position with respect to the projection on the \((x, y)\)-plane if the following conditions hold.

(i) \( \mathcal{I}(\mathcal{C}) \cap K[x, y] = \mathcal{I}(f) \), the curve \( \mathcal{C}_f \) is in generic position and the projection \( \pi_z : (\alpha, \beta, \gamma) \in \mathcal{C} \mapsto (\alpha, \beta) \in \mathcal{C}_f \) is birational,

(ii) \( K[\mathcal{C}] \) is integral over \( K[\mathcal{C}_f] \),

(iii) if \((\alpha, \beta, \gamma)\) is a critical point of \( \mathcal{C} \) then this point is the only one intersection of \( \mathcal{C} \) with the line \( x = \alpha, \ y = \beta \),

(iv) if \((\alpha, \beta, \gamma)\) is a critical nonsingular point of \( \mathcal{C} \) then the line \( x = \alpha, \ y = \beta \) is not tangent to \( \mathcal{C} \) at this point,

(v) if \((\alpha, \beta, \gamma)\) is a plane singular point of \( \mathcal{C} \) then its tangent plane does not contain the line \( x = \alpha, \ y = \beta \),

(vi) if \((\alpha, \beta, \gamma)\) is nonsingular in \( \mathcal{C} \) but \((\alpha, \beta)\) is singular in \( \mathcal{C}_f \) then \((\alpha, \beta)\) is a node.

In what follows, we call such curves in generic position without reference to the plane of projection. Let us now give some precise details concerning the conditions of generic position.

Condition (ii) means that the ideal \( \mathcal{I}(\mathcal{C}) \) of the curve contains a monic polynomial with respect to \( z \). As a consequence of this, any point of \( \mathcal{C}_f \) is the projection of at least one point of \( \mathcal{C} \).

Conditions (i) and (ii) imply the existence of a *monoid* in \( \mathcal{I}(\mathcal{C}) \), i.e., a polynomial of the form \( a(x)z - b(x, y) \). Indeed, since \( \pi_z \) is birational there exists a subvariety \( \mathcal{V} \) of \( \mathcal{C}_f \) of codimension at least 1 such that \( \pi_z : \mathcal{C} \setminus \mathcal{V}_1 \rightarrow \mathcal{C}_f \setminus \mathcal{V} \), where \( \mathcal{V}_1 = \pi_z^{-1}(\mathcal{V}) \) is of codimension at most 1 in \( \mathcal{C} \), is an isomorphism. The fact that \( \mathcal{C}_f \) is of dimension 1 implies that \( \mathcal{V} \) is finite and so there exists a polynomial \( c(x) \) such that \( c = 0 \) on \( \mathcal{V} \). Now if we let \( \mathcal{W} \) be the set of points \((\alpha, \beta)\) in \( \mathcal{C}_f \) such that \( c(\alpha) = 0 \) then clearly \( \mathcal{V} \subseteq \mathcal{W} \) and so \( \pi_z : \mathcal{C} \setminus \mathcal{W}_1 \rightarrow \mathcal{C}_f \setminus \mathcal{W} \), where \( \mathcal{W}_1 = \pi_z^{-1}(\mathcal{W}) \), is an isomorphism. Moreover, the fact that \( f \) is assumed to be monic with respect to \( y \) implies that \( \mathcal{W} \) is a finite set and so is \( \mathcal{W}_1 \) according to the fact that \( \mathcal{I}(\mathcal{C}) \) contains a monic polynomial with respect to \( z \). In algebraic terms, this means that the morphism \( \pi_z^* : c^{-n} p(x, y) \in K[\mathcal{C}_f]_c \mapsto c^{-n} p(x, y) \in K[\mathcal{C}]_c \) is in fact an isomorphism. Thus, there exists \( n \geq 0 \) and \( p(x, y) \) such that \( z = c^{-n} p(x, y) \) in the localization ring \( K[\mathcal{C}]_c \). Since \( \mathcal{W}_1 \) is finite the polynomial \( c(x) \) does not vanish on the open Zariski subset \( \mathcal{C} \setminus \mathcal{W}_1 \) of \( \mathcal{C} \), and so is not a zero divisor in \( K[\mathcal{C}]_c \). Thus, \( c(x)z - p(x, y) = 0 \) in \( K[\mathcal{C}]_c \).

Conditions (iii), (iv) and (v) prevent from making the critical points more complicated after projection. Let \( p \in \mathcal{C} \) be a critical point which is at most a plane singularity and let \( q = \pi_z(p) \). If \( \mathcal{O}_{\mathcal{C}, p} \) (resp. \( \mathcal{O}_{\mathcal{C}_f, q} \)) is the local ring of \( \mathcal{C} \) (resp. \( \mathcal{C}_f \)) at \( p \) (resp. \( q \)) then conditions (iii), (iv) and
(v) mean that the natural morphism from $O_{\mathscr{C},d}$ into $O_{\mathscr{C},p}$ induced by $\pi_z$ is an isomorphism. It is in general impossible to project a curve into a plane without introducing new singularities. So, condition (vi) simply means that we manage to make the new singularities as simple as possible. The simplest situation is to introduce only nodes as new singularities.

Assume that $\mathscr{C}$ is in generic position, and let $a(x)z - b(x, y) \in I(\mathscr{C})$ be a monoid. Even if it means reducing by $f$, we may assume that $\deg_y(b) < \deg_y(f)$. On the other hand, let $c(x)$ be the gcd of $a(x)$ and the coefficients with respect to $y$ of $b(x, y)$, and write $az - b = c(x)(a_1z - b_1)$. Since $I(\mathscr{C})$ contains monic polynomials with respect to $y$ and $z$ the set of points in $\mathscr{C}$ where $c(x)$ vanishes is finite, and so $c(x)$ is not a zero divisor in $K[\mathscr{C}]$. Since moreover $c(x)(a_1z - b_1) = 0$ in $K[\mathscr{C}]$ we have $a_1z - b_1 = 0$ in $K[\mathscr{C}]$, which means that $a_1z - b_1 \in I(\mathscr{C})$. Thus, starting from a monoid we easily construct a monoid $a(x)z - b(x, y) \in I(\mathscr{C})$ which is primitive as polynomial in $K[x][y, z]$, and $\deg_y(b) < \deg_y(f)$. We will call such a polynomial a reduced monoid. In fact, a reduced monoid is unique up to a multiplicative constant in $K^\ast$. Notice that if $a(x)z - b(x, y)$ is a reduced monoid of $I(\mathscr{C})$ then for any root $\alpha$ of $a(x)$ the polynomial $b(\alpha, y)$ is nonzero.

**Lemma 4.1.** Let $\mathscr{C}$ be a space algebraic curve and $I(\mathscr{C})$ be its ideal. Assume that $I(\mathscr{C}) \cap K[x, y] = I(f)$, $\mathscr{C}_f$ is in generic position, $K[\mathscr{C}]$ is integral over $K[\mathscr{C}_f]$ and the projection $\pi_z$ is birational. Let $a(x)z - b(x, y)$ be a reduced monoid in $I(\mathscr{C})$, $(\alpha, \beta)$ be a point in $\mathscr{C}_f$ and $y(x) \in \overline{K}[x - \alpha]^\ast$ be a Newton–Puiseux expansion of $\mathscr{C}_f$ at $(\alpha, \beta)$ and set $z(x) = \frac{b(x, y)}{a(x)}$. Then

(i) $z(x) \in \overline{K}[x - \alpha]^\ast$ and $h(x, y(x), z(x)) = 0$ for any $h \in I(\mathscr{C})$,

(ii) if moreover $y(x) \in \overline{K}[x - \alpha]$ then $z(x) \in \overline{K}[x - \alpha]$.

**Proof.** (i) Given any $h \in I(\mathscr{C})$ we may write by Euclidean division, with respect to $z$, $a^m h = u.(az - b) + r(x, y)$ for a suitable positive integer $m$. Since $I(\mathscr{C}) \cap K[x, y] = I(f)$ we have $r = v f$, and so $a^m h(x, y(x), z(x)) = 0$. Therefore, $h(x, y(x), z(x)) = 0$ for any $h \in I(\mathscr{C})$.

The fact that $K[\mathscr{C}]$ is integral over $K[\mathscr{C}_f]$ implies the existence of $h_0 \in I(\mathscr{C})$ which is monic with respect to $z$. From $h_0(x, y(x), z(x)) = 0$ we deduce that $z(x)$ is integral over $\overline{K}[x - \alpha]^\ast$, and since $\overline{K}[x - \alpha]^\ast$ is integrally closed we have $z(x) \in \overline{K}[x - \alpha]^\ast$.

(ii) Assume that $y(x) \in \overline{K}[x - \alpha]$, and write $b(x, y(x)) = (x - \alpha)^{m_1} b_1(x)$ and $a(x) = (x - \alpha)^{m_2} a_1(x)$, where $a_1$ and $b_1$ are units of $\overline{K}[x - \alpha]$. Since $z(x) \in \overline{K}[x - \alpha]^\ast$ we have $m_1 \geq m_2$, and this gives the claimed result. □

**Lemma 4.2.** Let $\mathscr{C}$ be a space algebraic curve and $I(\mathscr{C})$ be its ideal. Assume that $I(\mathscr{C}) \cap K[x, y] = I(f)$, $\mathscr{C}_f$ is in generic position, $K[\mathscr{C}]$ is integral over $K[\mathscr{C}_f]$ and the projection $\pi_z$ is birational. Let $a(x)z - b(x, y) \in I(\mathscr{C})$ be a reduced monoid, $(\alpha, \beta)$ be a critical point of $\mathscr{C}_f$ and assume that $(\alpha, \beta)$ is either nonsingular or a node and that $a(\alpha) = 0$. Then $b(\alpha, y)$ is square-free of degree $d - 1$, where $d = \deg(f)$, and has the same roots as $f(\alpha, y)$.

**Proof.** The fact that $a(x)z - b(x, y)$ is primitive as polynomial of $K[x][y, z]$ implies that $b(\alpha, y) \neq 0$. Let $\beta'$ be a root of $f(\alpha, y)$. Since $K[\mathscr{C}]$ is integral over $K[\mathscr{C}_f]$ there exists a point $(\alpha, \beta', \gamma) \in \mathscr{C}$. Since moreover $a(x)z - b(x, y) \in I(\mathscr{C})$ and $a(\alpha) = 0$ we have $b(\alpha, \beta') = 0$, and so any root of $f(\alpha, y)$ is a root of $b(\alpha, y)$. On the other hand, since $\mathscr{C}_f$ is in generic position $\beta$ is the only one multiple root of $f(\alpha, y)$, and the fact that $(\alpha, \beta)$ is either a node or a critical nonsingular point which implies that $\beta$ is a double root of $f(\alpha, y)$ according to Proposition 3.2. This means in particular that $f(\alpha, y)$ has $d - 1$ roots properly counted. Since these roots are also
roots of $b(\alpha, y) \neq 0$ and $\deg(b(\alpha, y)) \leq d - 1$ these are the only roots of $b(\alpha, y)$ and they are all simple.

**Lemma 4.3.** Let $\mathcal{C}$ be a space algebraic curve and $\mathcal{I}(\mathcal{C})$ be its ideal. Assume that $\mathcal{I}(\mathcal{C}) \cap K[x, y] = \mathcal{I}(f)$, $\mathcal{C}_f$ is in generic position, $K[\mathcal{C}]$ is integral over $K[\mathcal{C}_f]$ and the projection $\pi_z$ is birational. Let $a(x)z - b(x, y)$ be a reduced monoid in $\mathcal{I}(\mathcal{C})$, $(\alpha, \beta)$ be a node of $\mathcal{C}_f$ and assume that $\alpha$ is a root of $a(x)$. Then $\alpha$ is a simple root of $a(x)$ and the line $x = \alpha$, $y = \beta$ intersects the curve $\mathcal{C}$ at exactly 2 points which are both noncritical.

**Proof.** Since $(\alpha, \beta)$ is of multiplicity 2 in $\mathcal{C}_f$ and $\mathcal{C}_f$ is in generic position, $\beta$ is a double root of $f(\alpha, y)$ according to Proposition 3.2. This shows that $\mathcal{C}_f$ has exactly two Newton–Puiseux expansions $y_1(x), y_2(x)$ at $(\alpha, \beta)$. Moreover, the fact that $(\alpha, \beta)$ is a node which implies that $y_1, y_2 \in K[[x - \alpha]]$ and $y_1'(\alpha) \neq y_2'(\alpha)$. Let $z_i(x) = \frac{b(x, y_i(x))}{a(x)}$ and notice that $z_i(x) \in K[[x - \alpha]]$ by Lemma 4.1.

By applying the operator $\partial_x$ to the identity $a(x)z_i(x) - b(x, y_i(x)) = 0$ and then evaluating at $(\alpha, \beta)$ we obtain the relation

$$a'(\alpha)z_i(\alpha) = \partial_x b(\alpha, \beta) + y_i'(\alpha)\partial_y b(\alpha, \beta).$$

By Lemma 4.2 the polynomial $b(\alpha, y)$ has exactly $d - 1$ roots which are all simple. Since $\partial_x b(\alpha, \beta) \neq 0$ and $y_i'(\alpha) \neq y_j'(\alpha)$ we have $a'(\alpha)(z_1(\alpha) - z_2(\alpha)) \neq 0$. Therefore, $\alpha$ is a simple root of $a(x)$ and the line $x = \alpha$, $y = \beta$ contains at least the two points $(\alpha, \beta, z_1(\alpha))$. Let us now prove that this line contains exactly two points, which are not critical. For this we construct a polynomial $c(x)z^2 - d(x)z - e(x, y) \in \mathcal{I}(\mathcal{C})$ such that $c(\alpha) \neq 0$. By Euclidean division we may write

$$b(x, y) = q(x, y)f(x, y) + r(x, y),$$

where $\deg_y(r) \leq d - 1$. Notice on the other hand that $\beta$ is a double root of $f(\alpha, y)$ and also of $b(\alpha, y)^2$. Since moreover all the other roots of $f(\alpha, y)$ are simple and are roots of $b(\alpha, y)$ the polynomial $f(\alpha, y)$ divides $b(\alpha, y)^2$, and so $r(\alpha, y) = 0$. This means that $x - \alpha$ divides all the coefficients with respect to $y$ of $r(x, y)$, and since $\alpha$ is a simple root of $a(x)$ we may write $r(x, y) = a(x)r_1(x, y)$, where $r_1(x, y) \in K[x]_\alpha$ and $K[x]_\alpha$ is the localization ring of $K[x]$ at the maximal ideal $\mathcal{I}(x - \alpha)$.

Applying $\partial_x$ to both sides of the relation (3) and then substituting $\alpha$ to $x$ we get the identity

$$2\partial_x b(\alpha, y)b(\alpha, y) = \partial_x q(x, y)f(\alpha, y) + q(\alpha, y)\partial_y f(\alpha, y) + a'(\alpha)r_1(\alpha, y).$$

For any simple root $\beta'$ of $f(\alpha, y)$ we have $b(\alpha, \beta') = q(\alpha, \beta') = 0$, and since $a'(\alpha) \neq 0$ we have $r_1(\alpha, \beta') = 0$. On the other hand, since $(\alpha, \beta)$ is a singular point of $\mathcal{C}_f$ we have $\partial_x f(\alpha, \beta) = 0$ and so $r_1(\alpha, \beta) = 0$. From this we deduce that $b(\alpha, y)$ divides $r_1(\alpha, y)$, and so the Euclidean division of $r_1(x, y)$ by $b(x, y)$ writes as

$$r_1(x, y) = d_1(x)b(x, y) + a(x)e_1(x, y),$$

where $d_1(x) \in K[x]_\alpha$ and $e_1(x, y) \in K[x]_\alpha[y]$. The fact that $d_1(x)$ does not depend on $y$ follows from the bound $\deg_y(r_1(x, y)) \leq d - 1$. Combining (3) and (4) and getting rid of denominators we get

$$c(x)b(x, y)^2 - d(x)b(x, y) - a(x)^2e(x, y) = c(x)q(x, y)f(x, y),$$

where $c(x), d(x) \in K[x], e(x, y) \in K[x, y]$ and $c(\alpha) \neq 0$. 

244  

Now let us consider the polynomial \( g(x, y, z) = c(x)z^2 - d(x)z - e(x, y) \). By using Euclidean division and the identity (5) we get

\[
\frac{a(x)}{\partial_y}g(x, y, z) = k_1(x, y)(a(x)z - b(x, y)) + k_2(x, y)f(x, y),
\]

and so \( g \in \mathcal{I}(f, a(x)z - b(x, y)) : a(x)\infty = \mathcal{I}(\mathcal{C}). \)

We have \( g(\alpha, \beta, z_1(\alpha)) = 0 \) for \( i = 1, 2, \) and since on the other hand \( \deg_y(g) = 2 \) we have \( \partial_yg(\alpha, \beta, z_1(\alpha)) \neq 0 \), and the points \((\alpha, \beta, z_i(\alpha))\) are the only points of \( \mathcal{C} \) in the line \( x = \alpha \), \( y = \beta \). The Jacobian matrix of \((a(x)z - b(x, y), g)\) with respect to \((y, z)\) is

\[
\begin{pmatrix}
-\partial_y b & a(x) \\
\partial_y g & \partial_z g
\end{pmatrix}.
\]

Its determinant, evaluated at \((\alpha, \beta, z_i(\alpha))\), is \(-\partial_y b(\alpha, \beta)\partial_z g(\alpha, \beta, z_i(\alpha)) \neq 0\). This shows that \((\alpha, \beta, z_i(\alpha))\) is not a critical point of \( \mathcal{C} \). ■

### 4.2. The main result

The following theorem gathers what we gain, from the purely algebraic point of view, in considering space curves in generic position. Semi-algebraic properties of such curves will be studied in Section 6.

**Theorem 4.1.** Let \( \mathcal{C} \) be a space algebraic curve in generic position, \( \mathcal{I}(\mathcal{C}) \) be its ideal and \( \mathcal{C}_f \) be its projection into the \((x, y)\)-plane. Let \( a(x)z - b(x, y) \in \mathcal{I}(\mathcal{C}) \) be a reduced monoid. Then, for any point \((\alpha, \beta, \gamma)\) of \( \mathcal{C} \) the following statements hold.

(i) \((\alpha, \beta, \gamma)\) is a nonsingular critical point of \( \mathcal{C} \) if and only if \((\alpha, \beta)\) is critical and nonsingular in \( \mathcal{C}_f \). In this case, we have \( a(\alpha) \neq 0 \) and \( \gamma = \frac{b(\alpha, \beta)}{a(\alpha)} \).

(ii) \((\alpha, \beta, \gamma)\) is nonsingular and \((\alpha, \beta)\) is singular in \( \mathcal{C}_f \) if and only if \((\alpha, \beta)\) is a node of \( \mathcal{C}_f \) and \( \alpha \) is a root of \( a(x) \). In this case, \( \alpha \) is a simple root of \( a(x) \) and we have

\[
\gamma = \frac{(\partial_x b_s + s\partial_y b)(\alpha, \beta)}{a'(\alpha)}, \tag{6}
\]

where \( s \) is such that the line \( y = \beta + s(x - \alpha) \) is tangent to \( \mathcal{C}_f \) at \((\alpha, \beta)\),

(iii) \((\alpha, \beta, \gamma)\) is a plane singularity of \( \mathcal{C} \) if and only if \((\alpha, \beta)\) is singular in \( \mathcal{C}_f \) and \( a(\alpha) \neq 0 \).

In this case, we have \( \gamma = \frac{b(\alpha, \beta)}{a(\alpha)} \).

(iv) \((\alpha, \beta, \gamma)\) is not a plane singular point of \( \mathcal{C} \) if and only if \( \alpha \) is a multiple root of \( a(x) \) or \((\alpha, \beta)\) is singular but not a node in \( \mathcal{C}_f \) and \( \alpha \) is a simple root of \( a(x) \). In this case, there exists a polynomial \( \sigma_2(x) \) such that \( \gamma = \sigma_2(\alpha) \).

**Proof.** (i) Let us write \( \mathcal{I}(\mathcal{C}) = \mathcal{I}(g_1, \ldots, g_s) \) and \( f = u_1g_1 + \cdots + u_sg_s \). Applying the operators \( \partial_z, \partial_y, \partial_x \) and evaluating at \((\alpha, \beta, \gamma)\) we get

\[
(u_1\partial_x g_1 + \cdots + u_s\partial_x g_s)_{(\alpha, \beta, \gamma)} = 0, \tag{7}
\]

\[
(u_1\partial_y g_1 + \cdots + u_s\partial_y g_s)_{(\alpha, \beta, \gamma)} = \partial_y f(\alpha, \beta). \tag{8}
\]

\[
(u_1\partial_x g_1 + \cdots + u_s\partial_x g_s)_{(\alpha, \beta, \gamma)} = \partial_x f(\alpha, \beta, \gamma). \tag{9}
\]

Since \((\alpha, \beta, \gamma)\) is a critical point of the curve \( \mathcal{C} \) the rows \((\partial_y g_1, \ldots, \partial_y g_s)_{(\alpha, \beta, \gamma)}\) and \((\partial_z g_1, \ldots, \partial_z g_s)_{(\alpha, \beta, \gamma)}\) are linearly dependent, and so \( \partial_y f(\alpha, \beta) = 0 \) according to (7) and (8). This shows that \((\alpha, \beta)\) is a critical point of \( \mathcal{C}_f \).
Assume that $a(\alpha) = 0$ and write $a(x)z - b(x, y) = v_1g_1 + \cdots + v_sg_s$. By applying $\partial_y$ and $\partial_z$ and evaluating at $(\alpha, \beta, \gamma)$ we get

$$
(v_1\partial_y g_1 + \cdots + v_s\partial_y g_s)|_{(\alpha, \beta, \gamma)} = -\partial_y b(\alpha, \beta).
$$

$$
(v_1\partial_z g_1 + \cdots + v_s\partial_z g_s)|_{(\alpha, \beta, \gamma)} = a(\alpha).
$$

(10)

(11)

Since the rows $(\partial_y g_1, \ldots, \partial_y g_s)|_{(\alpha, \beta, \gamma)}$ and $(\partial_z g_1, \ldots, \partial_z g_s)|_{(\alpha, \beta, \gamma)}$ are linearly dependent and $a(\alpha) = 0$ we should have $\partial_y b(\alpha, \beta) = 0$.

On the other hand, from the property (vi) of Definition 4.1 we deduce that $(\alpha, \beta)$ is either a critical nonsingular point or a node of $\mathcal{C}_f$. According to Lemma 4.2 the polynomial $b(\alpha, \gamma)$ is square-free and this contradicts the fact that $\partial_y b(\alpha, \beta) = 0$. Therefore, $a(\alpha) \neq 0$ and so $f(x, y), a(x)z - b(x, y)$ generate the ideal $\mathcal{I}(\mathcal{C})$ in the local ring $\overline{K}[x, y, z]_{(\alpha, \beta, \gamma)}$. Since $(\alpha, \gamma)$ is nonsingular the Jacobian matrix of $f, az - b$ at $(\alpha, \beta)$ is of rank two. This shows that $(\partial_y f, \partial_z f)|_{(\alpha, \beta)} \neq 0$ and so $(\alpha, \beta)$ is nonsingular in $\mathcal{C}_f$.

Assume now that $(\alpha, \beta)$ is a critical nonsingular point of the curve $\mathcal{C}_f$. We have then $\partial_y f(\alpha, \beta) \neq 0$ and according to the equations (8) and (9) we have the relations $(u_1\partial_y g_1 + \cdots + u_s\partial_y g_s)|_{(\alpha, \beta, \gamma)} = 0$ and $(u_1\partial_z g_1 + \cdots + u_s\partial_z g_s)|_{(\alpha, \beta, \gamma)} \neq 0$. This implies that the rows $(\partial_y g_1, \ldots, \partial_y g_s)|_{(\alpha, \beta, \gamma)}$ and $(\partial_z g_1, \ldots, \partial_z g_s)|_{(\alpha, \beta, \gamma)}$ are linearly independent and so $(\alpha, \beta, \gamma)$ is nonsingular. Since the matrix $\text{Jac}(G)$ is of rank two we may write

$$(\partial_z g_1, \ldots, \partial_z g_s)|_{(\alpha, \beta, \gamma)} = (\mu_1(\partial_y g_1, \ldots, \partial_y g_s) + \mu_2(\partial_z g_1, \ldots, \partial_z g_s))|_{(\alpha, \beta, \gamma)}.
$$

This gives

$$
\sum_i u_i\partial_z g_i|_{(\alpha, \beta, \gamma)} = \left(\mu_1 \sum_i u_i\partial_y g_i + \mu_2 \sum_i u_i\partial_z g_i\right)|_{(\alpha, \beta, \gamma)}
$$

From (7) and (9) we get the equality $\mu_2 = 0$, and so the rows $(\partial_y g_1, \ldots, \partial_y g_s)|_{(\alpha, \beta, \gamma)}$ and $(\partial_z g_1, \ldots, \partial_z g_s)|_{(\alpha, \beta, \gamma)}$ are linearly dependent. Therefore, $(\alpha, \beta, \gamma)$ is a critical point of $\mathcal{C}$.

(ii) Assume that $(\alpha, \beta, \gamma)$ is nonsingular in $\mathcal{C}$ and $(\alpha, \beta)$ is singular in $\mathcal{C}_f$. According to the property (vi) of Definition 4.1, $(\alpha, \beta)$ is a node of $\mathcal{C}_f$. If $a(\alpha) \neq 0$ then the system $f, az - b$ generates $\mathcal{I}(\mathcal{C})$ in the local ring $\overline{K}[x, y, z]_{(\alpha, \beta, \gamma)}$, and the computation of $\text{Jac}(f, az - b)$ immediately shows that $(\alpha, \beta, \gamma)$ should be a singular point of $\mathcal{C}$. Therefore, we have $a(\alpha) = 0$.

Conversely, assume that $(\alpha, \beta)$ is a node of $\mathcal{C}_f$ and $\alpha$ is a root of $a(x)$. As a direct consequence of Lemma 4.3, $\alpha$ is a simple root of $a(x)$ and $(\alpha, \beta, \gamma)$ is a nonsingular point of $\mathcal{C}$. The relation (6) is a direct consequence of the relation (2).

(iii) Assume that $(\alpha, \beta, \gamma)$ is a plane singularity of $\mathcal{C}$, and let $g \in \mathcal{I}(\mathcal{C})$ be such that the surface $\mathcal{S}$ defined by the equation $g = 0$ is nonsingular at $(\alpha, \beta, \gamma)$. By genericity conditions the tangent plane to $\mathcal{S}$ at $(\alpha, \beta, \gamma)$ does not contain the line $x = \alpha, y = \beta$, and hence $\partial_z g(\alpha, \beta, \gamma) \neq 0$. By the formal implicit function theorem there exists $s(x, y) \in \overline{K}[[x - \alpha, y - \beta]]$ such that $s(\alpha, \beta) = \gamma$ and $g(x, y, s(x, y)) = 0$. We may therefore write $g = (z - s(x, y))g_1(x, y, z)$, with $g_1 \in \overline{K}[[x - \alpha, y - \beta]][z]$ and $g_1(\alpha, \beta, \gamma) \neq 0$.

Let $\mathcal{J}$ be the ideal generated by $\mathcal{I}(\mathcal{C})$ in $\overline{K}[[x - \alpha, y - \beta, z - \gamma]]$. We have $g \in \mathcal{J}$, and the fact that $g_1(\alpha, \beta, \gamma) \neq 0$ implies that $g_1$ is a unit in the ring $\overline{K}[[x - \alpha, y - \beta, z - \gamma]]$. This shows that $z - s(x, y) \in \mathcal{J}$.

On the other hand, let $f_1(x, y) \in \mathcal{J}$ and let $y(x)$ be a Newton–Puiseux expansion of $\mathcal{C}_f$ at $(\alpha, \beta)$ and set $z(x) = \frac{b(x, y(x))}{a(x)}$. Then $z(x) \in \overline{K}[[x - \alpha]]$ by Lemma 4.1, $z(\alpha) = \gamma$ according to the fact that $(\alpha, \beta, \gamma)$ is the only one point in the intersection of $\mathcal{C}$ and the line $x = \alpha, y = \beta$.
and we have $h(x, y(x), z(x)) = 0$ for any $h \in \mathcal{J}$. In particular, $f_1(x, y(x)) = 0$ and so $f_1$ is a multiple of $f$ in $\overline{K}[[x - \alpha, y - \beta]]$ according to the fact that $f$ is square-free. Therefore, $\mathcal{J}$ is generated by $f$ and $z - s(x, y)$.

Assume towards contradiction that $a(\alpha) = 0$. Applying Euclidean division, with respect to $z$, of $a(x)z - b$ by $z - s(x, y)$ we get $a(x)s(x, y) - b(x, y) = kf(x, y)$, with $k \in \overline{K}[[x - \alpha, y - \beta]]$. After substituting $\alpha$ to $x$ in this relation we deduce that $b(\alpha, y) = -k(\alpha, y)f(\alpha, y)$ in $\overline{K}[[y - \beta]]$. In particular, if $p$ is the multiplicity of $\beta$ as root of $f(\alpha, y)$, then the multiplicity of $\beta$ as root of $b(\alpha, y)$ is at least $p$.

By genericity conditions on $\mathcal{C}_f$ the only one multiple root of $f(\alpha, y)$ is $\beta$, and so there are $d - p$ other simple roots of $f(\alpha, y)$. The assumption $a(\alpha) = 0$ implies that these roots are roots of $b(\alpha, y)$ as well, and this means that $b(\alpha, y)$ has at least $d$ roots, counted with multiplicity. This is impossible because $b(\alpha, y) \neq 0$ and $\deg_y(b) \leq d - 1$.

Assume that $(\alpha, \beta)$ is singular in $\mathcal{C}_f$ and $a(\alpha) \neq 0$. Then the surface defined by $a(x)z - b(x, y) = 0$ is nonsingular at the point $(\alpha, \beta, \gamma)$, and this is enough to show that $(\alpha, \beta, \gamma)$ is a plane singularity of $\mathcal{C}$.

(iv) This case follows directly from (ii) and (iii). The only thing left is to prove the existence of $\sigma_z(x)$. The ideal $\mathcal{I}(x - \alpha, y - \beta) + \mathcal{I}(\mathcal{C})$ has a reduced Gröbner basis, with respect to the lexicographic order $x < y < z$, of the form $x - \alpha, y - \beta, h(x, y, z)$, where $h$ is monic with respect to $z$. Since $(\alpha, \beta, \gamma)$ is the only one intersection of $\mathcal{C}$ with the line $x = \alpha$, $y = \beta$ the polynomial $h(\alpha, \beta, z)$ has only one root properly counting. This gives $\gamma = -\frac{a_r-1(\alpha, \beta)}{r}$, where $r = \deg_z(h)$ and $a_r-1$ is the coefficient of degree $r - 1$ with respect to $z$ of $h$. Since $\mathcal{C}_f$ is in generic position $\beta$ is a polynomial in terms of $\alpha$, and after substituting in $a_{r-1}(x, y)$ this polynomial to $y$ we get $\sigma_z$.

5. Generic position checking

In this section we give an algorithmic method to check the genericity conditions of Definition 4.1. The following theorem gives equivalent geometric conditions to the ones in Definition 4.1. These conditions have the advantage of being easy to translate into gcd computations of univariate polynomials.

**Theorem 5.1.** Let $\mathcal{C}$ be a space algebraic curve and $\mathcal{I}(\mathcal{C})$ be its ideal. Assume that $\mathcal{I}(\mathcal{C}) \cap \mathbb{K}[x, y] = \mathcal{I}(f)$, $\mathcal{C}_f$ is in generic position, $\mathbb{K}[\mathcal{C}]$ is integral over $\mathbb{K}[\mathcal{C}_f]$ and the projection $\pi_z$ is birational. Let $a(x)z - b(x, y)$ be a reduced monoid in $\mathcal{I}(\mathcal{C})$. Then $\mathcal{C}$ is in generic position if and only if the following conditions hold.

(i) to each root $\alpha$ of $a(x)$ corresponds a unique singular point $(\alpha, \beta)$ of $\mathcal{C}_f$,

(ii) if $\alpha$ is a multiple root of $a(x)$ or $\alpha$ is simple but $(\alpha, \beta)$ is not a node of $\mathcal{C}_f$ then there exists a unique point $(\alpha, \beta, \gamma)$ of $\mathcal{C}$ in the line $x = \alpha$, $y = \beta$. Moreover, this point is singular and not plane.

**Proof.** “$\Rightarrow$” Let $\alpha$ be a root of $a(x)$ and $\beta$ be a root of $f(\alpha, y)$. The fact that $\mathbb{K}[\mathcal{C}]$ is integral over $\mathbb{K}[\mathcal{C}_f]$ implies the existence of a point $(\alpha, \beta, \gamma)$ of $\mathcal{C}$. Since $a(\alpha) = 0$ and $a(x)z - b(x, y) \in \mathcal{I}(\mathcal{C})$ we have $b(\alpha, \beta) = 0$. This shows that all the roots of $f(\alpha, y)$ are roots of $b(\alpha, y)$, and since $\deg(b(\alpha, y)) < \deg(f(\alpha, y))$ one of the roots of $f(\alpha, y)$, say $\beta$, is multiple.
Theorem 4.1. Definition and the property $K$.

Let $5.1$ that the curve $C$ has only plane singularities, for example $C$ is contained in a nonsingular surface, we have the following simplification of Theorem 5.1.

Corollary 5.1. Let $C$ be a space algebraic curve which has only plane singularities. Assume that $I(C) \cap \mathbb{K}[x, y] = I(f)$. $C_f$ is in generic position, $\mathbb{K}[C]$ is integral over $\mathbb{K}[C_f]$ and the projection $\pi_z$ is birational. Let $a(x)z - b(x, y)$ be a reduced monoid in $I(C)$. Then $C$ is in generic position if and only if the polynomial $a(x)$ is square-free and its roots are $x$-coordinates of nodes of $C_f$.

Proof. “$\Rightarrow$” Let $a$ be a root of the polynomial $a(x)$. By property (i) of Theorem 5.1 the curve $C_f$ has a singular point with $a$ as $x$-coordinate, say $(\alpha, \beta)$. From the fact that $C$ has only plane singularities we deduce from property (ii) of Theorem 5.1 that $(\alpha, \beta)$ is a node of $C_f$ and $a$ is a simple root of $a(x)$.

“$\Leftarrow$” Let $a$ be a root of the polynomial $a(x)$. Then $a$ is simple and is the $x$-coordinate of a node $(\alpha, \beta)$ of $C_f$. This proves in particular property (i) of Theorem 5.1. Since $C$ has only plane singularities property (ii) of Theorem 5.1 obviously holds. From Theorem 5.1 the curve $C$ is in generic position.
Let us now explain how the conditions of Theorem 5.1 are translated into gcd computations. So, assume that $C_f$ is in generic position and let $sr_0(x)$ be the resultant of $f$ and $\partial_y f$ with respect to $y$. Let us write the maximal square-free factor of $sr_0(x)$ as $\delta_1 \delta_2 \delta_3$, where $\delta_1$ corresponds to simple roots of $sr_0(x)$, $\delta_2$ corresponds to its double roots while $\delta_3$ corresponds to its higher multiplicity roots. Let us also write the maximal square-free factor of $a(x)$ as $a_1 a_2$, where $a_1$ corresponds to simple roots of $a(x)$ while $a_2$ corresponds to its multiple roots. The condition (i) of Theorem 5.1 is then equivalent to the fact that $a_1 a_2$ divides $\delta_2 \delta_3$. In case $C$ has only plane singularities the condition of Corollary 5.1 holds if and only if $a(x)$ is square-free and divides the polynomial $\delta_2$.

To reduce property (ii) of Theorem 5.1 to gcd computations we need to work a little bit more. Notice that we also need to check whether the projection $\pi_x$ is birational, and if so to compute a reduced monoid of $I(C)$. We will give in what follows two solutions to these problems, depending on the used elimination tool. The first one is special for the important case of complete intersection curves and builds on subresultants theory, while the second one works in the general case but resorts to computationally intensive ideal-theoretic methods, namely the Gröbner bases.

5.1. The case of complete intersection

In this subsection we assume that the ideal $I(C)$ is generated by two polynomials $g_1, g_2$, and without loss of generality that both $g_1$ and $g_2$ are monic with respect to $z$. We also overload the notation of subresultants used in Section 3.5 and let $Sr_j(x, y, z) = sr_j(x, y)z^j + sr_j, j-1(x)z^{j-1} + \cdots + sr_{j,0}(x, y)$ be the $j$th subresultant of $g_1$ and $g_2$ with respect to $z$.

The following classical result solves the problem of checking whether the projection $\pi_z$ is birational, as well as finding a monoid in the ideal $I(C)$. A proof of it may for instance be found in Abhyankar and Bajaj (1989).

**Proposition 5.1.** Let $sr_0(x, y)$ and $Sr_1(x, y, z) = sr_1(x, y)z + sr_{1,0}(x, y)$ be the two first subresultants of $g_1$ and $g_2$ with respect to $z$. Then the projection $\pi_z$ is birational if and only if $sr_1 \neq 0$ and $\gcd(sr_0, sr_1) = 1$. In this case we have the following properties.

(i) $sr_0$ is the equation of the projection of $C$ into the $(x, y)$-plane,

(ii) if $a(x)$ is the resultant of $sr_0$ and $sr_1$ with respect to $y$ and $a = usr_0 + vsr_1$ then $a(x)z + vsr_{1,0}$ is a monoid in $I(C)$.

Let $\xi = \gcd(a_1, \delta_2)$ and write $a_1 = \xi \xi_1$ and $\vartheta = \xi_1 a_2$. To check the property (ii) of Theorem 5.1 we first apply Algorithm 1 to get a factorization $\vartheta = \vartheta_1 \cdots \vartheta_r$ and rational representations $[\vartheta_i, \sigma_i, y]$ of the singular points of $C_f$ whose $x$-coordinates are roots of $\vartheta$. Then after substituting, for any $i$, $\sigma_i, y$ to $y$ in the polynomials $Sr_j(x, y, z)$ we get, by Proposition 3.1, the subresultant sequence of $g_1(x, \sigma_i, y(x), z)$ and $g_2(x, \sigma_i, y(x), z)$.

Let us write $\vartheta_i = \vartheta_{i,1} \cdots \vartheta_{i,t_i}$, where for any root $\alpha$ of $\vartheta_{i,j}$ the gcd of the polynomials $g_1(\alpha, \sigma_i, y(\alpha), z)$ and $g_2(\alpha, \sigma_i, y(\alpha), z)$ is of degree $p_{i,j}$, and is $Sr_{p_{i,j}}(\alpha, \sigma_i, y(\alpha), z)$, and we have $p_{i,1} < p_{i,2} < \cdots < p_{i,t_i}$. The fact that the degree of $Sr_{p_{i,j}}(\alpha, \sigma_i, y(\alpha), z)$ is the same for any root $\alpha$ of $\vartheta_{i,j}$ implies that its leading coefficient is a unit modulo $\vartheta_{i,j}$. By inverting this coefficient modulo $\vartheta_{i,j}$ we get a polynomial $H_{i,j}(x, z)$ which is monic of degree $p_{i,j}$ with respect to $z$. If we let $h_{i,j}(x)$ be the coefficient of degree $p_{i,j} - 1$ with respect to $z$ of $H_{i,j}(x, z)$ then the first part of the condition (ii) of Theorem 5.1 means that $H_{i,j}(x, y) = (y + h_{i,j}(x))^{p_{i,j}}$ modulo $\vartheta_{i,j}$. The second part means that after substituting $\sigma_i, y(x)$ to $y$ and $-h_{i,j}(x)$ to $z$ in the partial derivatives of $g_1$ and $g_2$ we get multiples of $\vartheta_{i,j}$.
5.2. The general case

Let $F$ be a reduced Gröbner basis of $\mathcal{I}(\mathscr{C})$ with respect to the lexicographic order $x < y < z$. Since $F$ is reduced the ideal $\mathcal{I}(\mathscr{C}) \cap K[x, y]$ is generated by a single polynomial if and only if $F$ contains a unique polynomial $f \in K[x, y]$. In this case, $f$ is the square-free polynomial defining the projection of $\mathscr{C}$ into the $(x, y)$-plane. Notice also that $K[\mathscr{C}]$ is integral over $K[\mathscr{C}_f]$ if and only if $F$ contains a monic polynomial with respect to $z$.

Assume now that $\mathcal{I}(\mathscr{C}) \cap K[x, y] = \mathcal{I}(f)$, where $f$ is monic with respect to $y$, and that $K[\mathscr{C}]$ is integral over $K[\mathscr{C}_f]$. Then, $\pi_z$ is birational if and only if $F$ contains a reduced monoid $a(x)z - b(x, y)$. Indeed, assume that $F$ contains a reduced monoid $a(x)z - b(x, y)$ and let $\mathcal{V}$ be the subset of $\mathcal{C}_f$ defined by $a(x) = 0$, $f(x, y) = 0$. Since $f$ is monic with respect to $y$ the algebraic set $\mathcal{V}$ is finite. Since on the other hand $\mathcal{I}(\mathscr{C})$ contains a monic polynomial with respect to $z$ the algebraic set $\mathcal{V}_1 = \pi_z^{-1}(\mathcal{V})$ is finite as well. Clearly, $\pi_z : \mathcal{C} \setminus \mathcal{V}_1 \rightarrow \mathcal{C}_f \setminus \mathcal{V}$ is an isomorphism. Conversely, assume that $\pi_z$ is birational and let $a(x)z - b(x, y)$ be a reduced monoid in $\mathcal{I}(\mathscr{C})$. Since $F$ is a Gröbner basis of $\mathcal{I}(\mathscr{C})$ there exists $g \in F$ such that its leading monomial $x^{n_1}y^{n_2}z^{n_3}$ divides the leading monomial $x^p z$ of $a(x)z - b(x, y)$, where $p = \deg(a)$. This proves that the leading monomial of $g$ is of the form $x^{n_1}z^{n_3}$, where $n_1 \leq p$ and $n_3 = 1$. If $n_3 = 0$ then $g \in K[x, y]$, but this would mean that $f$ divides $g$ and so $g = f$ according to the fact that $\mathcal{I}(\mathscr{C}) \cap K[x, y] = \mathcal{I}(f)$ and $F$ is reduced. This is of course impossible since the leading monomial of $f$ is of the form $y^d$, with $d \geq 1$. Thus, $n_3 = 1$ and so $g = a_1(x)z - b_1(x, y)$. From the uniqueness property of the reduced monoid, and the fact that $\deg(a_1) = n_1 \leq \deg(a) = p$, we deduce that $g$ is, up to a nonzero multiplicative constant, equal to $a(x)z - b(x, y)$.

By applying Algorithm 1 to the curve $\mathcal{C}_f$ and the polynomial $\vartheta$, defined in the paragraph after Proposition 5.1, we get a factorization $\vartheta = \vartheta_1 \cdots \vartheta_r$ and rational representations $[\vartheta_i, \sigma_{i,y}]$ of the singular points of $\mathcal{C}_f$ whose $x$-coordinates are roots of $\vartheta$. Now for any $i = 1, \ldots, r$ we consider the system $G_i$ consisting of $\vartheta_i$ and the list of polynomials obtained by substituting $\sigma_{i,y}$ to $y$ in the elements of $F$. The system $G_i$ defines a zero-dimensional ideal of $K[x, z]$. To decompose this system we use the classical Lazard structure theorem (Lazard, 1985).

**Theorem 5.2.** Let $\mathcal{I}$ be an ideal of $K[x, z]$ and $F$ be a generating system of $\mathcal{I}$. Then $F$ is a Gröbner basis of $\mathcal{I}$ with respect to the lexicographic order $x < z$ if and only if

1. $F = \mu_1 \cdots \mu_t P$, $\mu_2 \cdots \mu_t H_1 P$, $\ldots$, $\mu_i H_{t-1} P$, $H_t P$, where:
   - $P \in K[x, z]$ is primitive with respect to $z$,
   - $\mu_1, \ldots, \mu_t$ are nonconstant polynomials in $K[x]$,
   - $H_1, \ldots, H_t$ are monic with respect to $z$ and $0 < \deg_z(H_i) < \deg_z(H_{i+1})$,
2. for any $i = 1, \ldots, t - 1$ we have $H_{i+1} \in \mathcal{I}(\mu_i, H_i)$.

In case $\mathcal{I}$ is zero-dimensional and $\mathcal{I} \cap K[x]$ is radical we have $\gcd(\mu_i, \mu_j) = 1$ for $i \neq j$, $P = 1$ and $\mathcal{I} = \bigcap \mathcal{I}(\mu_i, H_i)$.

Recall that the second condition of Theorem 5.1 means that each root of $\vartheta$ is the $x$-coordinate of a unique singular point of $\mathscr{C}$. Moreover, this singular point is not plane, i.e., all partial derivatives of the polynomials in a generating system of $\mathcal{I}(\mathscr{C})$ vanish at this point. To check this, let $F_i$ be a Gröbner basis of $\mathcal{I}(G_i)$ with respect to the lexicographic order $x < z$. Notice that in our case the ideal $\mathcal{I}(G_i)$ is zero-dimensional and its trace on $K[x]$ is radical since it contains the square-free polynomial $\vartheta_i$. By applying Theorem 5.2 we get a factorization $\vartheta_i = \vartheta_{i,1} \cdots \vartheta_{i,t_i}$ and monic polynomials, $H_{i,1}, \ldots, H_{i,t_i}$, with respect to $z$ such $\mathcal{I}(G_i) = \bigcap \mathcal{I}(\vartheta_{i,j}, H_{i,j})$. Notice also that this decomposition is minimal in so far as for any
Let \( j \neq k \) we have \( \mathcal{I}(\partial_{i,j}, H_{i,j}) + \mathcal{I}(\partial_{i,k}, H_{i,k}) = (1) \). For any root \( \alpha \) of \( \partial_{i,j} \) the polynomial \( H_{i,j}(\alpha, z) \) is the gcd of polynomials \( g_k(\alpha, \sigma_i,y(\alpha), z) \), where \( g_1, \ldots, g_s \) is a generating system of \( \mathcal{I}(\mathcal{C}) \).

Let \( p_{i,j} = \deg_z(H_{i,j}) \) and \( h_{i,j} \) be its coefficient of degree \( p_{i,j} - 1 \) with respect to \( z \). The first part of the condition (ii) in Theorem 5.1 is then equivalent to the fact that \( H_{i,j}(x, y) = (y + \frac{h_{i,j}(x)}{p_{i,j}})^{p_{i,j}} \mod \partial_{i,j} \). The second part means that after substituting \( \sigma_i,y(x) \) to \( y \) and \( -\frac{h_{i,j}(x)}{p_{i,j}} \) to \( z \) in the partial derivatives of \( g_1, \ldots, g_s \) we get multiples of \( \partial_{i,j} \).

5.3. An algorithm for checking generic position

In this subsection we give a pseudo-code description of our algorithm to check whether a given space algebraic curve is in generic position.

**Algorithm 2** Space generic position checking.

**Input:** A space algebraic curve \( \mathcal{C} \) and a generating system \( G = g_1, \ldots, g_s \) of \( \mathcal{I}(\mathcal{C}) \).

**Output:** Check whether \( \mathcal{C} \) is in generic position.

1: Check whether \( \mathcal{I}(\mathcal{C}) \) contains a monic polynomial with respect to \( z \).
2: Check whether the projection \( \pi_z \) is birational. If so, compute a reduced monoid \( a(x)z - b(x, y) \in \mathcal{I}(\mathcal{C}) \) and the defining equation \( f \) of \( \mathcal{C}_f = \pi_z(\mathcal{C}) \).
3: Check whether \( \mathcal{C}_f \) is in generic position. If so, write the square-free factor of \( \text{Disc}_y(f) \) as \( \delta_1\delta_2\delta_3 \), where \( \delta_1 \) corresponds to critical nonsingular points of \( \mathcal{C}_f \), \( \delta_2 \) to its nodes while \( \delta_3 \) corresponds to its other singularities.
4: Write the maximal square-free factor of \( a(x) \) as \( a_1a_2 \), where \( a_1 \) corresponds to simple roots of \( a(x) \) while \( a_2 \) corresponds to its multiple roots. Check whether \( a_1a_2 \) divides \( \delta_2\delta_3 \).
5: Let \( \xi = \gcd(a_1, \delta_2) \), \( a_1 = \xi\xi_1 \) and \( \bar{\theta} = \xi_1a_2 \). Apply Algorithm 1 to \( \mathcal{C}_f \) and \( \bar{\theta} \) to obtain a factorization \( \bar{\theta} = \bar{\theta}_1 \cdots \bar{\theta}_{r} \) and rational representations \( [\bar{\theta}_i, \sigma_i,y] \) of the singular points of \( \mathcal{C}_f \) whose \( x \)-coordinates are roots of \( \bar{\theta} \).
6: for \( i = 1 \) to \( r \) do
7: substitute \( \sigma_i,y(x) \) to \( y \) in the polynomials \( g_k(x, y, z) \). Let \( \bar{\theta}_i = \bar{\theta}_{i,1} \cdots \bar{\theta}_{i,t_i} \) be the factorization of \( \bar{\theta}_i \) with respect to gcd degree of the polynomials \( g_k(x, \sigma_i,y, z) \).
8: for \( j = 1 \) to \( t_i \) do
9: Let \( H_{i,j}(x, z) \) be a monic polynomial with respect to \( z \) such that for any root of \( \bar{\theta}_{i,j}(x) \) \( H_{i,j}(\alpha, z) \) is the gcd of the polynomials \( g_k(\alpha, \sigma_i,y(\alpha), z) \). Let \( p_{i,j} = \deg_z(H_{i,j}) \) and \( h_{i,j}(x) \) be its coefficient of degree \( p_{i,j} - 1 \) with respect to \( z \).
10: Check whether \( H_{i,j}(x, y) = (y + \frac{h_{i,j}(x)}{p_{i,j}})^{p_{i,j}} \mod \bar{\theta}_{i,j} \).
11: for \( k = 1 \) to \( s \) do
12: Check whether \( \partial_wg_k(x, \sigma_i,y, -\frac{h_{i,j}}{p_{i,j}}) \) is a multiple of \( \bar{\theta}_{i,j} \), where \( w \) ranges over the list \( x, y, z \) of variables.
13: end for
14: end for
15: end for

5.4. Putting space curves in generic position

Let \( \mathcal{C} \) be a space algebraic curve, let \( \pi_z \) : \((x, y, z) \in K^3 \longmapsto (x, y) \in K^2 \) and let \( \mathcal{C}_f \) be the projection under \( \pi_z \) of \( \mathcal{C} \). The conditions of Definition 4.1 are in fact equivalent to the
following ones.

(1) The projection \( \pi_x \) restricted to \( \mathcal{C} \) is a finite morphism,
(2) the curve \( \mathcal{C}_f \) is in generic position,
(3) for almost any point \( p \in \mathcal{C} \), with \( q = \pi_x(p) \), the natural morphism \( \pi_{x,q}^* : \mathcal{O}_{\mathcal{C}_f,q} \to \mathcal{O}_{\mathcal{C},p} \)
is an isomorphism. If \( \pi_{x,q}^* \) is not an isomorphism then either \( q \) is a node or \( \pi_x^{-1}(q) \) is a single point which is a nonplane singularity of \( \mathcal{C} \).

It is well known that conditions (1) and (3) may be obtained by applying to \( \mathcal{C} \) a general linear change of coordinates, see, e.g., Hartshorne (1977). On the other hand, once the conditions (1) and (3) are obtained we may apply a change of coordinates of the type \( x = x + au \), \( y = y \) without affecting them. As seen in Section 3.5, such a change of coordinates puts the curve \( \mathcal{C}_f \) in generic position. Thus a general linear change of coordinates puts the curve \( \mathcal{C} \) in generic position.

6. Topology of real algebraic space curves

In what follows, we assume that \( \mathcal{K} \) is an ordered field and we let \( \mathcal{R} \) be its real closure. We also let \( \mathcal{C} \) be a space curve in generic position defined over \( \mathcal{K} \) and \( \mathcal{C}_R \) be its real part. The real part of the projection \( \mathcal{C}_f \) of \( \mathcal{C} \) into the \((x, y)\)-plane is denoted by \( \mathcal{C}_{f,R} \). In this section we show how to explicitly read up the topological structure of the space curve \( \mathcal{C}_R \) from one of \( \mathcal{C}_{f,R} \) together with the information contained in a reduced monoid of \( \mathcal{I}(\mathcal{C}) \).

Let \( \alpha_1 < \alpha_2 < \cdots < \alpha_r \) be the ordered list consisting of the \( x \)-coordinates of the critical points of \( \mathcal{C}_{f,R} \), and set \( \alpha_0 = -\infty \) and \( \alpha_{r+1} = +\infty \). Then we have the following decomposition:

(1) For \( i = 0, \ldots, r \) there exist Nash functions \( (y_{i,j}, z_{i,j}) : [\alpha_i, \alpha_{i+1}[ \to \mathcal{R}^2, j = 1, \ldots, s_i, \) such that the intersection of the curve \( \mathcal{C}_R \) with the strip \( [\alpha_i, \alpha_{i+1}[ \times \mathcal{R} \) is the disjoint union of the graphs of the maps \( (y_{i,j}, z_{i,j}) \). The graphs of the maps \( (y_{i,j}, z_{i,j}) \) will be called the branches of the curve \( \mathcal{C}_R \) above \( [\alpha_i, \alpha_{i+1}[ \). We label the branches in such a way that \( y_{i,1} < \cdots < y_{i,s_i} \).

(2) For \( i = 1, \ldots, r \) the intersection of \( \mathcal{C}_R \) and the plane \( x = \alpha_i \) consists of finitely many noncritical points \( (\alpha_i, \beta_{i,j}, \gamma_{i,j}), j = 1, \ldots, t_i, \) and either one critical point \( (\alpha_i, \beta_i, \gamma_i) \) or two noncritical points \( (\alpha_i, \beta_i, \gamma), (\alpha_i, \beta_i, \tau) \) with \( \gamma < \tau \). Here again we label the points in such a way that \( \beta_{i,1} < \cdots < \beta_{i,t_i} \).

The curve \( \mathcal{C}_R \) is thus decomposed into several simple semi-algebraic sets, namely points and graphs of Nash functions. We will call this decomposition the decomposition of \( \mathcal{C} \) with respect to event points. Our main concern in what follows is to set up the rules which allow to glue together these semi-algebraic sets.

The fact that \( \mathcal{K}[\mathcal{C}] \) is integral over \( \mathcal{K}[x] \) implies the existence of a polynomial \( g(x, z) \) which is monic with respect to \( z \) and such that \( g(x, z_{i-1,k}(x)) = 0 \). We also have \( f(x, y_{i-1,k}(x)) = 0, \) and hence both \( y_{i-1,k} \) and \( z_{i-1,k} \) are bounded in \( [\alpha, \alpha_i[ \) for any \( \alpha > \alpha_{i-1}, \) provided that \( \alpha_i < +\infty \). Since they are also semi-algebraic, they can be continuously extended to \( [\alpha_{i-1}, \alpha_i[ \) (see e.g., Basu et al. (2003), Proposition 3.18). In the same way, the branches \( (y_{i,k}, z_{i,k}) \) can be continuously extended to \( [\alpha_i, \alpha_{i+1}[ \) in case \( -\infty < \alpha_i \). If we take into account the fact that any \( \alpha_i \) corresponds to at most one critical point of \( \mathcal{C}_R \) we get the following.

**Lemma 6.1.** With the notations as above, we have the following.

(1) for any noncritical point \( (\alpha_i, \beta_{i,j}, \gamma_{i,j}) \) of \( \mathcal{C}_R \) there exist unique \( (y_{i-1,k}, z_{i-1,k}) \) and \( (y_{i,k}, z_{i,k}) \) such that \( y_{i-1,k}(\alpha_i) = y_{i,k}(\alpha_i) = \beta_{i,j} \) and \( z_{i-1,k}(\alpha_i) = z_{i,k}(\alpha_i) = \gamma_{i,j} \). Moreover, by glueing \( (y_{i-1,k}, z_{i-1,k}) \) and \( (y_{i,k}, z_{i,k}) \) we get a Nash function on \( [\alpha_i, \alpha_{i+1}[ \).
(ii) For any critical point \((\alpha_i, \beta_i, \gamma_i)\), all branches \((y_{i-1,k}, z_{i-1,k})\) which do not end at a noncritical point satisfy \((y_{i-1,k}(\alpha_i), z_{i-1,k}(\alpha_i)) = (\beta_i, \gamma_i)\). In the same way, all branches \((y_{i,\ell}, z_{i,\ell})\) which do not start at a noncritical point satisfy \((y_{i,\ell}(\alpha_i), z_{i,\ell}(\alpha_i)) = (\beta_i, \gamma_i)\).

The branches of \(C_R\) above \([\alpha_{i-1}, \alpha_i]\) which end at a given point \((\alpha_i, \beta, \gamma)\) of the curve are called the incoming branches of this point. In the same way, the branches above \([\alpha_i, \alpha_{i+1}]\) which start at \((\alpha_i, \beta, \gamma)\) are called the outgoing branches of \((\alpha_i, \beta, \gamma)\). It may happen that the critical point \((\alpha_i, \beta_i, \gamma_i)\) has neither incoming nor outgoing branches. Such a point will be called an isolated point of the curve \(C_R\).

**Lemma 6.2.** Let \(C\) be a space algebraic curve in generic position, and \(a(x)z - b(x, y)\) be a reduced monoid in \(I(C)\). Then we have the following.

(i) if \(I \subseteq \mathbb{R}\) is an open interval which does not contain the \(x\)-coordinate of any event point of \(C_R\), then a Nash function \(y(x)\) is a branch of \(C_{f,R}\) above \(I\) if and only if \((y(x), \frac{b(x,y(x))}{a(x)})\) is a branch of \(C_R\) above \(I\).

(ii) a critical point \((\alpha, \beta, \gamma)\) of \(C\) is real if and only if \(\alpha\) is real. If so, it is isolated in \(C_R\) if and only if it is so for \((\alpha, \beta)\) in \(C_f, R\).

(iii) a noncritical point \((\alpha, \beta, \gamma)\) of \(C\) which projects onto a node of \(C_f\) is real if and only if \((\alpha, \beta, \gamma)\) is real and is not isolated in the curve \(C_{f,R}\).

**Proof.** (i) Let \(y(x)\) be a branch of \(C_{f,R}\) above \(I\). Since \(I\) does not contain the \(x\)-coordinates of the event points of \(C_R\) we have \(a(\alpha) \neq 0\) for any \(\alpha \in I\). So, \(z(x) = \frac{b(x,y(x))}{a(x)}\) is well defined on \(I\) and \(h(x, y(x), z(x)) = 0\) for any \(h \in I(C)\). This shows that \((y(x), \frac{b(x,y(x))}{a(x)})\) is a branch of \(C_R\) above \(I\).

Conversely, if \((y(x), z(x))\) is a branch of \(C_R\) above \(I\), then we have \(f(x, y(x)) = 0\) and so \(y(x)\) is a branch of \(C_{f,R}\) above \(I\). Moreover, the fact that \(a(x)\) does not vanish in \(I\) implies that \(z(x) = \frac{b(x,y(x))}{a(x)}\).

(ii) Let \((\alpha, \beta, \gamma)\) be a critical point of \(C\). Then there exist \(\sigma_y, \sigma_z \in \mathbb{K}[x]\) such that \(\beta = \sigma_y(\alpha)\) and \(\gamma = \sigma_z(\alpha)\). This shows that \((\alpha, \beta, \gamma) \in \mathbb{R}^3\) if and only if \(\alpha \in \mathbb{R}\). On the other hand, according to (i) the incoming and the outgoing branches of \((\alpha, \beta)\) are projections of the incoming and the outgoing branches of \((\alpha, \beta, \gamma)\). Thus \((\alpha, \beta, \gamma)\) is isolated in \(C_R\) if and only if \((\alpha, \beta)\) is isolated in \(C_{f,R}\).

(iii) Let \((\alpha, \beta, \gamma)\) be a noncritical point of \(C_R\) which projects onto a node of \(C_{f,R}\), and by Lemma 6.1(i) let \((y(x), z(x))\) be its unique incoming branch. Then according to (i) \(y(x)\) is an incoming branch of \((\alpha, \beta)\), and so \((\alpha, \beta)\) is not isolated in \(C_{f,R}\).

Conversely, let \(y(x)\) be an incoming branch of \((\alpha, \beta)\). Then by (i) \((y(x), z(x))\), where \(z(x) = \frac{b(x,y(x))}{a(x)}\), is a branch of \(C_R\). Since \(z(x)\) can be continuously extended to \(\alpha\), the point \((\alpha, \beta, z(\alpha))\) belongs to \(C_R\). On the other hand, there are exactly two points of \(C\) which project onto \((\alpha, \beta)\). The fact that one of them is real implies that both of them are real.

Lemma 6.2 shows that the branches of the curve \(C_{f,R}\) are projections of the branches of \(C_R\). It also shows that all the critical points of \(C_{f,R}\), but finitely many isolated points, are projections of event points of \(C_R\). The irrelevant isolated points are in fact easy to detect as we will see later.

**6.1. Extracting information from the plane projection**

Let \((\alpha_i, \beta_i)\) be a critical point of \(C_{f,R}\), \(\beta_{i,1} < \cdots < \beta_i\) be the real roots of \(f(\alpha_i, y)\) other than \(\beta_i\) and \(\beta_{i,1}, \ldots, \beta_{i,u_i}\) those roots in \([-\infty, \beta_{i}]\). Also, let \(y_{i-1,1}(x) < \cdots < y_{i-1,s_{i-1}}(x)\) be
the branches of $\mathcal{C}_{f, R}$ above $[\alpha_{i-1}, \alpha_i]$, and $y_{i-1}(x) < \cdots < y_{i+1}(x)$ those above $[\alpha_i, \alpha_{i+1}]$. The way the branches $y_{i-1,k}$ and $y_{i,t}$ are connected to $\beta_i$ and the $\beta_{i,j}$’s are completely determined by using the following two easy facts:

- Every point $\beta_{i,j}$ has a unique incoming branch and a unique outgoing branch,
- Every branch is connected to some point of the curve in the plane $x = \alpha_i$. Moreover, if $k < k'$ (resp. $\ell < \ell'$) then $y_{i-1,k}(\alpha_i) \leq y_{i-1,k'}(\alpha_i)$ (resp. $y_{i,\ell}(\alpha_i) \leq y_{i,\ell'}(\alpha_i)$), and equality holds if and only if the branches are connected to the critical point $(\alpha_i, \beta_i)$. In more technical terms this gives the following matching rules.

**Proposition 6.1.** With the notations as above, we have the following.

(i) Let $a_i = 0$. Then $\beta_{i,j}$ is connected to $\alpha_i$ if and only if $\beta_{i,j}$ is a node of $C$, and $a_i > 0$ if and only if $\beta_{i,j}$ is a critical point for $f_{\alpha_i}$. In more technical terms this gives the following matching rules.

(ii) Let $a_i = 0$. Then $\beta_{i,j}$ is connected to $\alpha_i$ if and only if $\beta_{i,j}$ is a node of $C$, and $a_i > 0$ if and only if $\beta_{i,j}$ is a critical point for $f_{\alpha_i}$. In more technical terms this gives the following matching rules.

(iii) Let $a_i = 0$. Then $\beta_{i,j}$ is connected to $\alpha_i$ if and only if $\beta_{i,j}$ is a node of $C$, and $a_i > 0$ if and only if $\beta_{i,j}$ is a critical point for $f_{\alpha_i}$. In more technical terms this gives the following matching rules.

(iv) Let $a_i = 0$. Then $\beta_{i,j}$ is connected to $\alpha_i$ if and only if $\beta_{i,j}$ is a node of $C$, and $a_i > 0$ if and only if $\beta_{i,j}$ is a critical point for $f_{\alpha_i}$. In more technical terms this gives the following matching rules.

(v) Let $a_i = 0$. Then $\beta_{i,j}$ is connected to $\alpha_i$ if and only if $\beta_{i,j}$ is a node of $C$, and $a_i > 0$ if and only if $\beta_{i,j}$ is a critical point for $f_{\alpha_i}$. In more technical terms this gives the following matching rules.

6.2. The lifting process

The aim of this subsection is to determine, for any $i = 1, \ldots, r$, how the branches $(y_{i-1,k}, z_{i-1,k})$ and $(y_{i,t}, z_{i,t})$ are connected to the points of $C$ in the real plane $x = \alpha_i$.

**Lemma 6.3.** Let $a(x)z - b(x, y)$ be a reduced monoid of $\mathcal{I}(\mathcal{C})$ and $(\alpha, \beta)$ be a critical point of $\mathcal{C}_{f, R}$. Then we have the following properties.

(i) Assume that $(\alpha, \beta)$ is the projection of a critical point $(\alpha, \beta, \gamma)$ of $C$. Then the incoming (resp. outgoing) branches of $(\alpha, \beta, \gamma)$ are in one-to-one correspondence with the incoming (resp. outgoing) branches of $(\alpha, \beta)$.

(ii) Assume that $(\alpha, \beta, \gamma)$ is the projection of two noncritical points $(\alpha, \beta, \gamma)$ and $(\alpha, \beta, \gamma)$ of $C$, with $\gamma < \tau$. Let $y_1(x), y_2(x)$ be the two branches of $C_{f, R}$ at $(\alpha, \beta)$, assume that $y_1(x) < y_2(x)$ for $x < \alpha$ and let $z_1(x) = \frac{b(x, y_1(x))}{a(x)}$. Then

\[
\begin{cases}
z_1(\alpha) = \tau, & z_2(\alpha) = \gamma \quad \text{iff} \quad a'(\gamma) \beta = b(\alpha, \beta) > 0, \\
z_1(\gamma) = z_2(\gamma) = \tau \quad \text{iff} \quad a'(\gamma) \beta = b(\alpha, \beta) < 0.
\end{cases}
\]

**Proof.**
(i) Let $(y(x), z(x))$ be an incoming branch of $(\alpha, \beta, \gamma)$. Then clearly, $y(x)$ is an incoming branch of $(\alpha, \beta)$ and we have $z(x) = \frac{b(x, y(x))}{a(x)}$ by Lemma 6.2. Conversely, let $y(x)$ be an incoming branch of $(\alpha, \beta)$ and let $z(x) = \frac{b(x, y(x))}{a(x)}$. By Lemma 6.2, $(y(x), z(x))$ is a branch of $C$ to the left of $\alpha$. If we let $y' = z(\alpha)$ then $(\alpha, \beta, y')$ is critical for $C_{f, R}$ since its projection is critical for $C_{f, R}$. By the uniqueness of $(\alpha, \beta, \gamma)$ we have $y' = \gamma'$, and so $(y(x), z(x))$ is an incoming branch of $(\alpha, \beta, \gamma)$.

(ii) Since $(\alpha, \beta)$ is a node of $C$, the slopes of the tangents to $C$ at this point are $y_1'(\alpha)$ and $y_2'(\alpha)$, and we have $y_1'(\alpha) \neq y_2'(\alpha)$. For $\epsilon > 0$ small enough we also have $y_1(x) - y_2(x) < 0$ for
\( \alpha - \epsilon < x < \alpha \) and \( y_1(x) - y_2(x) > 0 \) for \( \alpha < x < \alpha + \epsilon \). This shows that \( y'_1(\alpha) > y'_2(\alpha) \). According to the relation (6) we have

\[
\frac{z_1(\alpha) - z_2(\alpha)}{y'_1(\alpha) - y'_2(\alpha)} = \frac{(y'_1(\alpha) - y'_2(\alpha))\partial_y b(\alpha, \beta)}{a'(\alpha)}.
\]

Since \( y'_1(\alpha) - y'_2(\alpha) > 0 \) we have \( \text{sgn}(z_1(\alpha) - z_2(\alpha)) = \text{sgn}(a'(\alpha)\partial_y b(\alpha, \beta)) \). ■

In the following theorem we show that the data \([s_0, [s_i, t_i, u_i], i = 1, \ldots, r]\) contains enough information to reduce the sign conditions of Lemma 6.3(ii) to sign determination of univariate polynomials at the \( x \)-coordinates of the nodes of \( \mathcal{C}_{f, \mathcal{R}} \) coming from projection.

**Theorem 6.1.** Let \((\alpha, \beta)\) be a node of \( \mathcal{C}_{f, \mathcal{R}} \) which is the projection of two noncritical points of \( \mathcal{C}_{\mathcal{R}} \). Let \( a(x)z - b(x, y) \) be a reduced monoid of \( \mathcal{I}(\mathcal{C}) \), and assume that the leading coefficient of \( a(x) \) is positive. Then

\[
\text{sgn}(a'(\alpha)\partial_y b(\alpha, \beta)) = (-1)^u \text{sgn}(a'(\alpha)b_{d-1}(\alpha)),
\]

where \( b_{d-1} \) is the leading coefficient of \( b(x, y) \) with respect to \( y \), and \( u \) is the number of real roots of \( f(\alpha, y) \) in \( ]\beta, +\infty[ \). If moreover \( \mathcal{C} \) has only plane singularities then

\[
\text{sgn}(a'(\alpha)\partial_y b(\alpha, \beta)) = (-1)^{u+1} \text{sgn}(b_{d-1}(\alpha)),
\]

where \( v \) is the number of real roots of \( a(x) \) in \( ]\alpha, +\infty[ \).

**Proof.** By Lemma 4.2 the polynomial \( b(\alpha, y) \) is square-free of degree \( d - 1 \), where \( d = \deg(f) \), and has the same roots as \( f(\alpha, y) \). Let \( b_{d-1}(x) \) be the leading coefficient of \( b(x, y) \) with respect to \( y \), and write \( b(\alpha, y) = b_{d-1}(\alpha)(y - \beta)\prod_{i \leq d-2}(y - \beta_i) \), where the \( \beta_i \)'s are the roots of \( f(\alpha, y) \) other than \( \beta \). An easy computation shows that \( \partial_y b(\alpha, \beta) = b_{d-1}(\alpha)\prod(\beta - \beta_j) \), and clearly its sign is \((-1)^u \text{sgn}(b_{d-1}(\alpha)) \), where \( u \) is the number of \( \beta_j \)'s such that \( \beta < \beta_j \).

If \( \mathcal{C} \) has only plane singularities then by Corollary 5.1 all the roots of \( a(x) \) are simple. Since moreover its leading coefficient is positive the sign of \( a'(\alpha) \) is equal to \((-1)^v \) where \( v \) is the number of real roots of \( a(x) \) in \( ]\alpha, +\infty[ \). ■

Let \( \varepsilon_i = 0 \) if \((\alpha_i, \beta_i)\) is the projection of a critical point of \( \mathcal{C}_{\mathcal{R}} \). In case \((\alpha_i, \beta_i)\) is the projection of two noncritical points of \( \mathcal{C} \), we let \( \varepsilon_i = 2 \) if \((\alpha_i, \beta_i)\) is isolated, \( \varepsilon_i = 1 \) if \( a'(\alpha_i)\partial_y b(\alpha_i, \beta_i) > 0 \) and \( \varepsilon_i = -1 \) if \( a'(\alpha_i)\partial_y b(\alpha_i, \beta_i) < 0 \).

As for the case of knots, the data \([s_0, [s_i, t_i, u_i, \varepsilon_i], i = 1, \ldots, r]\) contains all the information we need to construct a space graph \( \mathcal{G}(\mathcal{C}_{\mathcal{R}}) \) such that \( \mathcal{C}_{\mathcal{R}} \) and \( \mathcal{G}(\mathcal{C}_{\mathcal{R}}) \) are semi-algebraically homeomorphic as embedded objects in \( \mathcal{R}^3 \).

### 6.3. Constructing the graph

To construct the graph \( \mathcal{G}(\mathcal{C}_{\mathcal{R}}) \) from the data \([s_0, [s_i, t_i, u_i, \varepsilon_i], i = 1, \ldots, r]\) we need Algorithm 3.

### 6.4. The algorithm

In this section we describe the different steps of our algorithm for computing the topology of real algebraic space curves.
Algorithm 3 The matching algorithm

Input: The data \([s_0, [s_i, t_i, u_i, \varepsilon_i], i = 1, \ldots, r]\).

Output: A graph \(G(\mathcal{C}_R)\) which is globally homeomorphic to \(\mathcal{C}_R\).

1: Remove the items in the data for which \(\varepsilon_i = 2\), and relabel.
2: for \(i = 1 \text{ to } r\) do
3:   Choose \(u_i\) points \(p_{i,1}, \ldots, p_{i,u_i}\) (resp. \(t_i - u_i\) points \(p_{i,u_i+1}, \ldots, p_{i,t_i}\)) lying in the half-plane \(\mathcal{H}_{\alpha_i}^\varepsilon\) (rep \(\mathcal{H}_{\alpha_i}^\varepsilon\)) with pairwise different \(y\)-coordinates. We assume that the chosen points are sorted increasingly with respect to their \(y\)-coordinates.
4:   Choose a point \(q_i\) in the line \(L_i\) if \(\varepsilon_i = 0\) and two points \(q_{i,1}, q_{i,2}\) with different \(z\)-coordinates if \(\varepsilon_i = \pm 1\). We assume that the points are sorted increasingly with respect to their \(z\)-coordinates.
5: end for
6: Connect each point \(p_{1,j}\) to a line. If \(\varepsilon_1 = \pm 1\) connect each \(q_{i,j}, j = 1, 2\), to a line. Otherwise, connect \(q_i\) to \(s_0 - t_0\) lines.
7: for \(i = 1 \text{ to } r - 1\) do
8:   \(v_i = \min(u_i, u_{i+1})\). Connect each point \(p_{i,j}, j = 1, \ldots, v_i\), to \(p_{i+1,j}\).
9:   \(w_i = \min(t_i - u_i, t_{i+1} - u_{i+1})\). Connect each point \(p_{i,j}, j = t_i, \ldots, t_i - w_i + 1\), to \(p_{i+1,j}\).
10: If \(\varepsilon_{i+1} = 0\) then connect the \(t_i - v_i - w_i\) remaining \(p_{i,j}'s\) to \(q_{i+1}\). If \(\varepsilon_i = \pm 1\) then connect \(q_{i,1}\) and \(q_{i,2}\) to \(q_{i+1}\), otherwise connect \(q_i\) to \(q_{i+1}\) by \(s_i - t_i\) edges.
11: If \(\varepsilon_{i+1} = \pm 1\) then there are exactly two points in the plane \(x = \alpha_i\) which still need to be connected. If \(\varepsilon_i = 1\) then connect the point with the smallest \(y\)-coordinate to \(q_{i,2}\) and the other to \(q_{i,1}\). Otherwise, connect the point with the smallest \(y\)-coordinate to \(q_{i,1}\) and the other point to \(q_{i,2}\).
12: end for
13: Connect each point \(p_{r,j}\) to a line. If \(\varepsilon_r = \pm 1\) connect each point \(q_{r,j}, j = 1, 2\), to a line. Otherwise, connect \(q_r\) to \(s_r - t_r\) lines.

Algorithm 4 Topology of space curves

Input: A space curve \(\mathcal{C}\) and \(I(\mathcal{C})\) its ideal in \(K[x, y, z]\).

Output: A graph \(G(\mathcal{C}_R)\) which is globally homeomorphic to \(\mathcal{C}_R\).

1: Check whether \(\mathcal{C}\) is in generic position.
   If not, put it in generic position, see Section 5.
2: Compute the equation \(f\) of the projection \(\mathcal{C}_f\) into the \((x, y)\)-plane.
   Compute a reduced monoid \(a(x)z - b(x, y)\) in \(I(\mathcal{C})\).
   Assume that the leading coefficient of \(a(x)\) is positive.
3: Compute the list \(L = [[\delta_i, \sigma_i, y], i = 1, \ldots, s]\) of rational representations of the critical points of \(\mathcal{C}_f\).
   Assume that \([\delta_2, \sigma_2, y]\) represents the nodes of \(\mathcal{C}_f\) which are projections of noncritical points.
4: Compute the real roots of the \(\delta_i's\) and order them increasingly to get \(\alpha_1 < \cdots < \alpha_r\). Let \(\alpha_0 = -\infty\) and \(\alpha_{r+1} = +\infty\).
5: Compute the data \([s_0, [s_i, t_i, u_i, \varepsilon_i], i = 1, \ldots, r]\).
6: Construct the graph \(G(\mathcal{C}_R)\) according to Algorithm 3.

Steps (1), (2) and (3) involve purely algebraic computations, basically subresultants and eventually Gröbner bases. Steps (4) and (5) make use of real algebraic computations which
ultimately reduce to real root counting of univariate polynomials. Here again, subresultants play a central role through Sturm–Habicht sequences, see e.g., Basu et al. (2003).

As pointed out in the introduction, the paper does not contain any details concerning implementation. We should also mention here that we did not give any bound on the number of linear coordinate changes to be potentially performed in order to meet generic position. In the case of a plane curve, if we restrict our selves to the subgroup of linear coordinate changes of the type $x + \mu y$, $y$ then the number of “bad” coordinate changes is finite and bounded by $d^4$, where $d$ is the degree of the curve. This makes in particular tractable the question of complexity bound. In the case of space curves it is still not clear, to us, what kind of subgroups to consider. It is not clear as well whether one can find a subgroup for which all but finitely many coordinate changes ascertain generic position. We do believe such questions are interesting for their own and deserve to be dealt with in a future work.

6.5. A rough comparison with the existing algorithms

The general approach used in Gatellier et al. (2005), Alcazar and Sendra (2005), Alcazar (2007), Cheng et al. (2005) consists of the following steps. One first projects the given curve $C$ into the $(x, y)$-plane. Here one should make sure that the branches do not overlap after projection and no branch projects into a single point, which basically means that the projection should be birational. One then computes a plane graph that encodes the topology of the projection, and tries to lift the obtained graph to get a space one isotopic to the curve. In general, it turns out to be that the lifting process is impossible without an additional information at the vertices of the plane graph. Such an information is then obtained by looking at another projection. Here again, one should make sure that the edges of the two obtained plane graphs are in one-to-one correspondence. This means that there is a birational correspondence between the two projections.

The algorithm we described in this paper shares the same approach as the existing ones, which consists in projecting under some genericity conditions and then lifting. But our lifting process is completely different. In fact, our genericity conditions allow us to extract more information, than the other methods do, from a plane projection. This renders the lifting process more transparent in so far as it exclusively concentrates on analyzing how the branches wind around each other. Moreover, such an information is completely captured in a single univariate sign determination.

All projection-based algorithms assume some genericity conditions to be fulfilled. This requires in general a quite heavy computation. It is thus important to have at disposal easy methods to check the required genericity conditions. In the important case of complete intersection curves with only plane singularities, and especially the curves contained in nonsingular surfaces, Corollary 5.1, give a particularly easy method to check our genericity conditions.

Acknowledgment

Major parts of this work done during a stay at the Max-Planck Institute of Computer Science, Saarbruecken, Germany.

References