Computing the topology of a planar or space hyperelliptic curve

Juan Gerardo Alcázar, Jorge Caravantes, Gema M Diaz-Toca, Elias Tsigaridas

Computing the topology of a planar or space hyperelliptic curve.

Juan Gerardo Alcázar[a,1,2], Jorge Caravantes[a,1], Gema M. Diaz-Toca[b,1,3], Elias Tsigaridas[c,4]

[a] *Departamento de Física y Matemáticas, Universidad de Alcalá, E-28871 Madrid, Spain*
[b] *Departamento de Ingeniería y Tecnología de Computadores, Universidad de Murcia, E-30100 Murcia, Spain*
[c] *Inria Paris-Rocquencourt, Paris, France*

Abstract

We present algorithms to compute the topology of 2D and 3D hyperelliptic curves. The algorithms are based on the fact that 2D and 3D hyperelliptic curves can be seen as the image of a planar curve (the Weierstrass form of the curve), whose topology is easy to compute, under a birational mapping of the plane or the space. We report on a `Maple` implementation of these algorithms, and present several examples. Complexity and certification issues are also discussed.

1. Introduction

Rational curves are widely used in Computer Aided Geometric Design. *Hyperelliptic curves* are not rational, but they are birationally equivalent to planar algebraic curves (the corresponding *Weierstrass forms*), quadratic in one variable, and as a consequence they are parametrizable by square-roots.

Email addresses: `juange.alcazar@uah.es` (Juan Gerardo Alcázar), `jcaravan@mat.ucm.es` (Jorge Caravantes), `gemadiaz@um.es` (Gema M. Diaz-Toca), `elias.tsigaridas@inria.fr` (Elias Tsigaridas)

[1]Supported by the Spanish Ministerio de Ciencia, Innovación y Universidades and by the European Regional Development Fund (ERDF), under the project MTM2017-88796-P.

[2]Member of the Research Group ASYNACS (Ref. CCEE2011/R34)

[3]Supported by the Research Group E078-04 of the University of Murcia

[4]Partially supported by a Giner de los Ríos Grant of the Universidad de Alcalá, ANR JCJC GALOP (ANR-17-CE40-0009) and the PGMO grant ALMA.

Thus, hyperelliptic curves are one of the simplest examples of non-rational families of curves. Furthermore, this type of curves appears frequently in Computer Aided Geometric Design. A good account of the occurrence of hyperelliptic curves in this field is given in [7], where the problem of approximating hyperelliptic curves by means of rational parametrizations is addressed. As a brief summary of [7], non-rational offsets of rational planar curves and some bisector curves (line/rational curve, or circle/rational curve) are planar hyperelliptic curves. Contour curves of canal surfaces, intersections of two quadrics or intersections of a quadric and a ruled surface are examples of hyperelliptic curves in 3-space. With more generality, every planar or space algebraic curve $\mathcal{C}$ admitting a square-root parametrization (see also [23]) is hyperelliptic.

In this paper we address the problem of computing the topology of a hyperelliptic curve $\mathcal{C}$. In order to determine the topology of $\mathcal{C}$, one might compute an implicit representation of $\mathcal{C}$ using elimination methods. This yields one implicit equation in the case $n = 2$, and at least two implicit equations in the case $n = 3$. In both cases, after computing the implicit equation(s) one might use existing algorithms to find the topology of the curve: see for instance [6, 12, 16, 20], among many others, for the planar case, or [4, 11, 13, 17] for the space case. However, such an implicit representation typically has a high degree and big coefficients, which makes it difficult to use. Moreover, many algorithms have additional assumptions, for example generic position, complete intersection, that are computationally expensive to fulfill. As a consequence, it is useful to have an alternative method for computing the topology of $\mathcal{C}$ that avoids using an implicit representation.

In our method we see $\mathcal{C}$ as the image of a planar algebraic curve, the Weierstrass form of the curve, under a planar, in the case of 2D curves, or space, in the case of 3D curves, birational mapping. Since the topology of the Weierstrass form of the curve is easy to capture, the topology of $\mathcal{C}$ is determined by studying how the birational mapping modifies the topology of the Weierstrass form. In a way, we might say that the Weierstrass form guides us to build the topology of $\mathcal{C}$. Additionally, for the 3D case we need to compute first the topology of a birational projection of $\mathcal{C}$ onto a plane, so we need to use the ideas of the 2D case to solve the 3D case.

It is worth comparing our paper with some other related papers. In [3] the topology of 2D and 3D rational curves is addressed. In [3] the curve is seen as the image of the real line under a planar or space birational mapping, so one might say that the germ of the idea in this paper is somehow in [3]. In [10], a

method to compute the topology of a (non-necessarily rational) offset curve of a rational planar curve is provided. The method exploits similar ideas to [3], but focuses on offset curves, which have certain special properties. Finally, in [7] the problem of approximating a hyperelliptic curve by means of rational curves is considered. The Weierstrass form is also used in [7], but the goal is different, and in particular the computation of the topology of the hyperelliptic curve is not addressed.

Our method has been implemented in the computer algebra system `Maple` 2017, and the implementation can be freely downloaded from [24]. In order to certify the topology we need to certify self-intersections, i.e., we need to certify whether or not the image of two points under the birational mapping giving rise to our curve, is the same. This requires to work with algebraic numbers, and it is computationally difficult. We address this problem, and we provide a complexity analysis of the algorithm with, and without the certification step. While the complexity bound that we get is not better than the known complexity for the implicit planar case [21], it is, however, definitely better compared to the implicit space case [14, 11].

The structure of this paper is the following. We motivate and present the problem in Section 2, where some preliminary notions and ideas are given. The planar case is addressed in Section 3, and the space case is studied in Section 4. In Section 5 we report on the results of our experimentation, carried out in the computer algebra system `Maple 2017`; we refer the interested reader to the ArXiv version of the paper [2] for the parametrizations used in the experimentation section. In Section 6, we address the complexity of the algorithm, we consider certification issues, and we compare the complexity of our algorithm with the known complexities of algorithms using an implicit representation of the curve. Section 7 contains our conclusions. The proofs of some results in Section 3 are postponed to Appendix I, so as not to stop the flow of the paper.

2. Motivation and presentation of the problem.

Consider a *biquadratic* patch S, commonly used in Computer Aided Geometric Design, parametrized by

$$\mathbf{x}(t,s) = (x(t,s), y(t,s), z(t,s)) = \sum_{i=0}^{2}\sum_{j=0}^{2} \mathbf{c}_{ij} B_i(t) B_j(s), \tag{1}$$

where $B_k(u) = \binom{2}{k} u^k (1-u)^{2-k}$ for $k = 0, 1, 2$, and $\mathbf{c}_{ij} \in \mathbb{R}^3$ for $i, j = 0, 1, 2$. Assume that we want to describe the topology of the intersection curve $\mathcal{C}$ of S with a general plane Π of equation $Ax + By + Cz + D = 0$, i.e. the topology of $S \cap \Pi$. In order to do this, substituting the components of $\mathbf{x}(t, s)$ into the equation of Π we get an algebraic condition $g(t, s) = 0$; since the components of $\mathbf{x}(t, s)$ have bidegree $(2, 2)$, one can see that

$$g(t, s) = A(t)s^2 + B(t)s + C(t) = 0, \tag{2}$$

where A, B, C are polynomials in the variable t. Then the curve $\mathcal{C} = S \cap \Pi$ can be described as the closure of the image of the planar curve $\mathcal{G}$, defined by $g(t, s) = 0$ in the (t, s)-plane, under the (rational) mapping $\mathbf{x}$, i.e. $\mathcal{C} = \overline{\mathbf{x}(\mathcal{G})}$. Notice that $\mathcal{C} - \mathbf{x}(\mathcal{G})$ reduces to finitely many points corresponding to either the image of points of $\mathcal{G}$ at infinity, or limit points in $\mathcal{C}$ corresponding to base points of $\mathbf{x}$, lying in $\mathcal{G}$.

The situation presented above is an example of the general problem treated in this paper. Given a planar curve $\mathcal{G}$, implicitly defined in the plane (t, s) by a polynomial equation like Eq. (2), of degree 2 in the variable s, our goal is to compute the topology of the curve $\mathcal{C} = \overline{\mathbf{x}(\mathcal{G})}$, where $\mathbf{x} : \mathbb{R}^2 \to \mathbb{R}^n$, with $n = 2$ or $n = 3$, is *birational* when restricted to $\mathcal{G}$; in particular, in that case the inverse mapping $\mathbf{x}^{-1} : \mathcal{C} \to \mathcal{G}$ exists and is rational. If $\mathcal{C}$ is a rational curve, then the problem can be solved using already existing methods [3]. Thus, we will assume that $\mathcal{C}$ is not rational, in which case $\mathcal{C}$ is said to be a *hyperelliptic curve*. With some generality (see for instance [7]), we say that a curve $\mathcal{C}$ is *hyperelliptic* if there exists a generically two-to-one map $\mathcal{C} \to \mathbb{R}$. Furthermore, such a curve is birationally equivalent to a planar curve

$$s^2 - p(t) = 0, \tag{3}$$

where $p(t)$ is a square-free polynomial of degree $2g + 1$ or $2g + 2$, with g the *genus* of $\mathcal{C}$; Eq. (3) is called the *Weierstrass form* of $\mathcal{C}$. Notice (see p. 59 of [7]) that we can always transform Eq. (2) into Eq. (3) by considering a change of parameters

$$t := t, \;\; s := \frac{-B(t) + s}{2A(t)}.$$

In this paper we will assume that such a change of parameters has already been performed, so that the curve $\mathcal{G}$ is described by means of Eq. (3). Additionally, we will assume that the curve $\mathcal{G}$ is real, i.e. that it contains infinitely

many real points; if $\mathcal{G}$ is not real, then because of the birationality of $\mathbf{x}|_{\mathcal{G}}$, $\mathcal{C}$ cannot be real either. Observe also that since $s^2 - p(t)$ is an irreducible polynomial in t, s, so is the curve $\mathcal{G}$; since irreducibility is a birational invariant, we deduce that $\mathcal{C}$ is irreducible as well.

In order to describe the topology of the curve $\mathcal{C}$, we will compute, as it is common, a graph $G_{\mathcal{C}}$ isotopic to $\mathcal{C}$; we will refer to $G_{\mathcal{C}}$ as the graph *associated with* $\mathcal{C}$. However, in our case we will not compute $G_{\mathcal{C}}$ directly: instead, we will compute a graph $G_{\mathcal{G}}$ associated with $\mathcal{G}$, and we will derive $G_{\mathcal{C}}$ from $G_{\mathcal{G}}$ by studying how the topology of $\mathcal{G}$ changes when $\mathbf{x}$ is applied. Let us briefly recall how graphs associated with planar and space curves are computed.

Graph associated with a planar curve.

Let $f(x, y) = 0$ define a planar algebraic curve $\mathcal{F}$ without vertical asymptotes. We say that $P \in \mathcal{F}$ is *regular* if either $f_x(P) \neq 0$ or $f_y(P) \neq 0$; otherwise, we say that P is *singular*. We say that $P \in \mathcal{F}$ is *critical* if P satisfies that $f(P) = f_y(P) = 0$. A critical point which is not singular is called a *ramification* point. The graph G_f associated with $\mathcal{F}$ can be described as follows (see Fig. 1, left):

- The **vertices** of the graph G_f are: (1) the critical points of $\mathcal{F}$; (2) the points of $\mathcal{F}$ lying on the vertical lines through the critical points of $\mathcal{F}$ (we call these vertical lines, *critical lines*); (3) the points of $\mathcal{F}$ lying on vertical lines placed: (3.1) between two consecutive critical lines, (3.2) at the left of the left-most critical point, and (3.3) at the right of the right-most critical point.

- Two vertices of G_f are connected by an **edge** of G_f iff there is a real branch of $\mathcal{F}$ connecting the corresponding points on $\mathcal{F}$.

Although it is customary, in many papers dealing with the problem of computing the graph G_f, to start with the assumption that $\mathcal{F}$ does not have vertical asymptotes or vertical components, one can adapt the strategy without assuming these properties; see for instance [5].

Graph associated with a space curve.

Let $\{f_1(x, y, z) = 0, \ldots, f_m(x, y, z) = 0\}$ define a space algebraic curve $\mathcal{F}$: (i) without asymptotes parallel to the z-axis; (ii) without components parallel to the z-axis; (iii) such that the projection $\pi_{xy}(\mathcal{F})$ of $\mathcal{F}$ onto the xy-plane

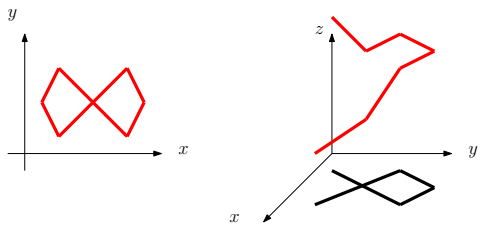

Figure 1: Graphs associated with planar and space curves

is birational. Hypothesis (iii) ensures that there are not two different real branches of $\mathcal{F}$ projecting onto a same branch of $\pi_{xy}(\mathcal{F})$. Taking advantage of Hypothesis (iii), the usual strategy to compute a graph G_f isotopic to $\mathcal{F}$ is to birationally project $\mathcal{F}$ onto some plane, say, the xy-plane, then compute a graph isotopic to the projection $\pi_{xy}(\mathcal{F})$, which is a planar algebraic curve, and later "lift" the graph associated with $\pi_{xy}(\mathcal{C})$ to a space graph. Since the projection π_{xy} is birational, one can be sure that every edge of the graph associated with $\pi_{xy}(\mathcal{F})$ lifts to one, and just one, edge of the graph associated with $\mathcal{F}$. More precisely, the graph G_f associated with $\mathcal{F}$ can be described as follows (see Fig. 1, right):

- The **vertices** of the graph G_f are the points of $\mathcal{F}$ projecting as vertices of the graph associated with $\pi_{xy}(\mathcal{F})$.
- Two vertices of G_f are connected by an **edge** of G_f iff the corresponding points of $\mathcal{C}$ are connected by a real branch of $\mathcal{C}$. Furthermore, if the vertices are not singularities of $\pi_{xy}(\mathcal{C})$, we connect them iff their projections are connected in the graph associated with $\pi_{xy}(\mathcal{F})$. For vertices corresponding to singularities of $\pi_{xy}(\mathcal{C})$ the process is more complicated, since we can have two non-overlapping branches of $\mathcal{C}$ whose projections onto the xy-plane overlap (see Fig. 1, left); for references on how to deal with this problem, one can check [13, 17].

Again, as it also happens in the planar case, the strategy can be adapted to the case when $\mathcal{F}$ has vertical components or vertical asymptotes.

In our case.

In our case, we need to compute the graph associated with $\mathcal{G}$ plus some extra vertices, namely the points $Q_i = (t_i, s_i) \in \mathcal{G}$ giving rise to certain

notable points $P_i \in \mathcal{C}$, as we will see in the next sections. Whenever $\mathbf{x}$ is well-defined, in which case $\mathbf{x}$ is continuous, the image of any connected subset of $\mathcal{G}$ is also connected, so every edge of $G_{\mathcal{G}}$ gives rise to an edge of $G_{\mathcal{C}}$. The fact that $\mathbf{x}$ is birational over $\mathcal{G}$ guarantees that all the edges of $G_{\mathcal{C}}$ are obtained this way, since there cannot be any real branch of $\mathcal{C}$ coming from a complex branch of $\mathcal{G}$: indeed, if $\mathcal{B} \subset \mathcal{G}$ is a complex branch such that $\mathbf{x}(\mathcal{B})$ is real, then $\mathbf{x}(\mathcal{B}) = \overline{\mathbf{x}(\mathcal{B})}$, where $\overline{\mathbf{x}(\mathcal{B})}$ denotes the conjugate of $\mathbf{x}(\mathcal{B})$. But then there are infinitely many points of $\mathcal{C}$ with at least two pre-images, which cannot happen because $\mathbf{x}|_{\mathcal{G}}$ is birational.

Therefore, in order to build $G_{\mathcal{C}}$ we compute the $Q_i = (t_i, s_i)$, the graph $G_{\mathcal{C}}$, and the images $P_i = \mathbf{x}(Q_i)$. Then, whenever $\mathbf{x}(Q_i)$ is defined, we connect the P_i according to how their preimages $Q_i = \mathbf{x}^{-1}(P_i)$ are connected in $\mathcal{G}$. If $\mathbf{x}(Q_i)$ is not defined, then in $\mathcal{C}$ w can have an affine point, or a branch of $\mathcal{C}$ going to infinity. Fig. 2 represents this idea, for the case $n = 2$: each edge, marked with a different color, of the graph $G_{\mathcal{G}}$ (left), gives rise to an edge, marked with the same color, of the graph $G_{\mathcal{C}}$ (right).

Observe that since $\mathcal{G}$ is implicitly defined by Eq. (3), the leading coefficient in the variable s is constant, so $\mathcal{G}$ has no asymptotes parallel to the s-axis, i.e. no vertical asymptotes. Additionally, since the Weierstrass form implies that $p(t)$ is square-free, one can see that $\mathcal{G}$ is regular, and that the only critical points are the points $\{s = 0, p(t) = 0\}$, all of which are ramification points. Because of this, $\mathcal{G}$ consists of open branches and/or closed components, without self-intersections.

Certainly, there can also be some points of $\mathcal{C}$ which do not belong to $\mathbf{x}(\mathcal{G})$. The points in $\mathcal{C} - \mathbf{x}(\mathcal{G})$ correspond to the images of the point at infinity of $\mathcal{G}$, which is the projective point in the direction of the s-axis, and the limit points coming from the base points of $\mathbf{x}$ lying in $\mathcal{G}$, i.e. points of $\mathcal{G}$ where all the numerators and denominators of the components of $\mathbf{x}$ vanish simultaneously. We also need to include these points as vertices of $G_{\mathcal{C}}$.

3. The planar case.

Let $\mathbf{x} : \mathbb{R}^2 \to \mathbb{R}^2$, where

$$\mathbf{x}(t, s) = (x(t, s), y(t, s)) = \left(\frac{A_1(t, s)}{B_1(t, s)}, \frac{A_2(t, s)}{B_2(t, s)} \right),$$

and let $\mathcal{C} = \mathbf{x}(\mathcal{G})$, where $\mathcal{G}$ is implicitly defined by an equation $g(t, s) = s^2 - p(t) = 0$ like Eq. (3). We require $\mathbf{x}$ to be a rational mapping satisfying

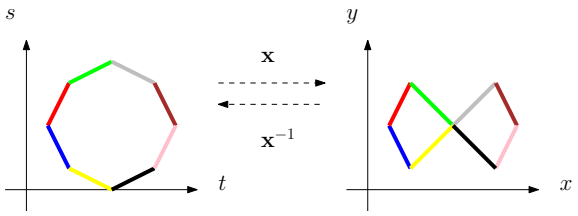

Figure 2: $G_{\mathcal{G}}$ and $G_{\mathcal{C}}$

that the restriction $\mathbf{x}|_{\mathcal{G}}$ is birational, so that $\mathbf{x}^{-1} : \mathcal{C} \to \mathcal{G}$ is well-defined, and therefore rational. We can always check this assumption with a probabilistic algorithm; we take a random point $(t_0, s_0) \in \mathcal{G}$, compute the point $P = \mathbf{x}(t_0, s_0)$, and finally determine the preimages of $\mathbf{x}(t_0, s_0)$: if we get only one preimage, then with probability one the required hypothesis holds. Additionally, using repeatedly the fact that $s^2 = p(t)$, we can write $\mathbf{x}(t, s)$ in the following form:

$$\mathbf{x}(t,s) = \left(\frac{A_1(t,s)}{B_1(t,s)}, \frac{A_2(t,s)}{B_2(t,s)}\right) = \left(\frac{a_{11}(t) + sa_{12}(t)}{b_{11}(t) + sb_{12}(t)}, \frac{a_{21}(t) + sa_{22}(t)}{b_{21}(t) + sb_{22}(t)}\right), \quad (4)$$

where we can assume that A_i, B_i are relatively prime for $i = 1, 2$. Observe that this implies $\gcd(a_{11}, a_{12}, b_{11}, b_{12}) = 1$ and $\gcd(a_{21}, a_{22}, b_{21}, b_{22}) = 1$.

As observed in Section 2, we first need to describe the topology of $\mathcal{G}$ by means of a graph $G_{\mathcal{G}}$ isotopic to it, with some additional vertices. We need to include the following points as vertices of $G_{\mathcal{G}}$:

(i) *Critical points of* $g(t, s) = 0$, i.e. points of $\mathcal{G}$ where $g_s = 0$.

(ii) *Points of* $\mathcal{G}$ *giving rise to critical points of* $\mathcal{C}$.

(iii) *Points of* $\mathcal{G}$ *where some component of* $\mathbf{x}$ *is not defined.*

(iv) *Starting and ending points for open branches of* $\mathcal{G}$.

The points in (i) are the solutions of $g = g_s = 0$, i.e. the points $\{s = 0, p(t) = 0\}$. The points in (iv) can be easily computed by taking a t-value at the left (resp. right) of the left-most (resp. the right-most) solution of $g = g_s$. The points in (iii) are the points $(t, s) \in \mathcal{G}$ such that $B_1(t, s) \cdot B_2(t, s) = 0$.

In particular, some of the points in (iii) may generate asymptotes of $\mathcal{C}$; also, *base points* of $\mathbf{x}$ in $\mathcal{G}$, i.e. the points of $\mathcal{G}$ where

$$A_1(t,s) = B_1(t,s) = A_2(t,s) = B_2(t,s) = g(t,s) = 0,$$

are included in (iii).

3.1. Computing the points of $\mathcal{G}$ giving rise to critical points of $\mathcal{C}$

If $\mathbf{x}$ has base points on $\mathcal{G}$, some of these points may generate critical points of $\mathcal{C}$. We will analyze base points in the next subsection, so in this subsection we will assume that $\mathbf{x}$ has no base points on $\mathcal{G}$. Some observations on how to use the results in this subsection in the presence of base points will be done at the end of the subsection.

Now in Section 2 we recalled that the critical points of $\mathcal{C}$ are either singularities, or ramification points. It is useful to distinguish two types of singularities : *local singularities*, which correspond to singular points $P \in \mathcal{C}$ with just one branch of $\mathcal{C}$ through P, and *self-intersections* of $\mathcal{C}$, which correspond to points $P \in \mathcal{C}$ with at leat two different branches of $\mathcal{C}$ through P.

In order to compute the points of $\mathcal{G}$ giving rise to local singularities and ramification points of $\mathcal{C}$, we analize $\mathbf{x}(\mathcal{G})$, where $\mathcal{G}$ is implicitly defined by $g(t,s) = 0$. The differential of $\mathbf{x}$ defines a mapping between the tangent space to $\mathcal{G}$ and the tangent space to $\mathcal{C}$, at corresponding points. Denoting a generic element of the tangent space to $\mathcal{C}$ by $\boldsymbol{v} = (v_1, v_2)$, we have the following relationship; here, x_t represents the partial derivative of $x(t,s)$ with respect to the variable t, and similarly for y_t, x_s, y_s, g_t, g_s:

$$\begin{bmatrix} x_t & x_s \\ y_t & y_s \end{bmatrix} \cdot \begin{bmatrix} g_s \\ -g_t \end{bmatrix} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \tag{5}$$

Lemma 1. *Suppose that $\mathbf{x}$ has no base points lying on $\mathcal{G}$. Then the local singularities of $\mathcal{C}$ and the ramification points of $\mathcal{C}$ are generated by points of $\mathcal{G}$ such that*

$$g = x_t g_s - x_s g_t = 0. \tag{6}$$

Remark 1. *Notice that the local singularities of $\mathbf{x}$ satisfy*

$$g = x_t g_s - x_s g_t = y_t g_s - y_s g_t = 0. \tag{7}$$

However, Lemma 1 does not necessarily provide the self-intersections of $\mathcal{C}$. In order to find these last singularities, we imitate the strategy in [1]. First we define

$$\begin{array}{rcl} \xi_1(x,t) & = & \text{square-free part of } \mathrm{Res}_s(\mathrm{num}(x-x(t,s)), g(t,s)), \\ \xi_2(x,y,t) & = & \text{square-free part of } \mathrm{Res}_s(\mathrm{num}(x-x(t,s)), \mathrm{num}(y-y(t,s))). \end{array} \tag{8}$$

Notice that in general, eliminating t in $\xi_1(x,t)=0,\ \xi_2(x,y,t)=0$ by means of the resultant $\mathrm{Res}_t(\xi_1(x,t),\xi_2(x,y,t))$, we obtain a polynomial in x,y containing, as a factor, the implicit equation of $\mathcal{C}$. Using the definition of the resultant, one can easily check that $\xi_1(x,t)$ is a quadratic polynomial in x, and $\xi_2(x,y,t)$ is quadratic as a polynomial in x,y, and linear in x and in y.

Now the key idea to find the self-intersections of $\mathcal{C}$ is that these points are among the points $(x,y)\in\mathcal{C}$ where $t=\mathbf{x}^{-1}(x,y)$ is not defined. For a generic point $(x_0,y_0)\in\mathcal{C}$, we can find $t_0=\mathbf{x}^{-1}(x_0,y_0)$ as the *only* root of $\gcd(\xi_1(x_0,t),\xi_2(x_0,y_0,t))$. In order to find the *function* $t=t(x,y)=\mathbf{x}^{-1}(x,y)$, we can compute the gcd of $\xi_1(x,t)$ and $\xi_2(x,y,t)$ as polynomials in the variable t whose coefficients are real polynomials in x,y, with the additional condition $f(x,y)=0$, where f is the implicit equation of $\mathcal{C}$. More formally, one sees $\xi_1(x,t)$ and $\xi_2(x,y,t)$ as elements of $\mathbb{R}(\mathcal{C})[t]$, where $\mathbb{R}(\mathcal{C})$ is the field of real rational functions of $\mathcal{C}$. Since $\mathcal{C}$ is irreducible $\mathbb{R}(\mathcal{C})$ is a Euclidean domain. Therefore

$$D(x,y,t)=\gcd_{\mathbb{R}(\mathcal{C})[t]}(\xi_1,\xi_2)$$

is well-defined and can be computed, for instance, by means of the Euclidean algorithm. Since $\mathbf{x}$ is proper, $D(x,y,t)$ is linear in t and solving $D(x,y,t)=0$ for t, one gets $t=\mathbf{x}^{-1}(x,y)$.

Following the ideas of [1], one can compute $\mathbf{x}^{-1}(x,y)$ more eficiently as follows (see [1] for further detail). By the fundamental property of subresultants, $D(x,y,t)$ is the first subresultant different from zero (modulo $f(x,y)$) in the subresultant chain of ξ_1,ξ_2, seen as elements of the domain $\mathbb{R}[x,y][t]$. If the degrees of ξ_1,ξ_2 as elements of $\mathbb{R}[x,y][t]$ are n_1,n_2, the elements of the subresultant chain are represented as

$$\{\mathbf{Subres}_i(\xi_1,n_1,\xi_2,n_2)_{i\geq 0}\},$$

with $0\leq i\leq \inf(n_1,n_2)-1$, and can be defined as determinants of order n_1+n_2-i of Sylvester-like matrices whose entries are related to the coefficients of ξ_1,ξ_2 (see Section 2.2 of [1]). Since $\deg(\mathbf{Subres}_i(\xi_1,n_1,\xi_2,n_2))\leq i$,

and by the birationality of $\mathbf{x}$ we have $\deg(G(x_0, y_0, t)) = 1$ for almost all $(x_0, y_0) \in \mathcal{C}$, we deduce that $D(x, y, t)$ is equal to $\mathbf{Subres}_1(\xi_1, n_1, \xi_2, n_2)$; notice that $\mathbf{Subres}_1(\xi_1, n_1, \xi_2, n_2)$ can be computed without actually knowing the implicit equation of $\mathcal{C}$. Writing

$$\mathbf{Subres}_1(\xi_1, n_1, \xi_2, n_2)(t) = \mathbf{sres}_1(x, y)\, t + \mathrm{sr}_1(x, y),$$

we have that

$$t = \mathbf{x}^{-1}(x, y) = -\frac{\mathrm{sr}_1(x, y)}{\mathbf{sres}_1(x, y)}. \tag{9}$$

The polynomial $\mathbf{sres}_1(x, y)$ is called the first principal subresultant of ξ_1, n_1 and ξ_2, n_2. Finally we get the following result.

Theorem 2. *Suppose that* $\mathbf{x}$ *has no base points lying on* $\mathcal{G}$*. Then the self-intersections of* $\mathcal{C}$ *are among the solutions of the bivariate polynomial system*

$$\mathbf{sres}_1(x(t, s), y(t, s)) = 0,\ \ g(t, s) = 0. \tag{10}$$

The next result shows that, in fact, *all* the singularities of $\mathcal{C}$, i.e. the local singularities and the self-intersections, are solutions of Eq. (10). The proof of this result in given in Appendix I, so as not to stop the flow of the paper.

Proposition 3. *Let* $(t_0, s_0) \in \mathcal{G}$ *be a point such that*

$$(x_0, y_0) = (x(t_0, s_0), y(t_0, s_0)) \in \mathcal{C}$$

is not a self-intersection, with

$$x_t(t_0, s_0)g_s(t_0, s_0) - x_s(t_0, s_0)g_t(t_0, s_0) = y_t(t_0, s_0)g_s(t_0, s_0) - y_s(t_0, s_0)g_t(t_0, s_0) = 0. \tag{11}$$

Then $\mathbf{sres}_1(x_0, y_0) = 0$.

Proposition 3 provides the following result.

Theorem 4. *Suppose that* $\mathbf{x}$ *has no base points lying on* $\mathcal{G}$*. Then every singularity of* $\mathcal{C}$ *of the type* $P = \mathbf{x}(t_0, s_0)$ *is a solution of Eq.* (10)*.*

There is one point missing in the discussion before. In order for the subresultant chain of ξ_1, ξ_2 not to vanish completely, we must require that ξ_1, ξ_2 do not share any factor depending on t. We identify the cases when this happens in the following two results. The proofs of these results are postponed to Appendix I.

Lemma 5. *The polynomials $\xi_1(x,t)$ and $\xi_2(x,y,t)$ have a common factor $t-t_0$ iff t_0 corresponds to a base point of $\mathbf{x}$, lying on $\mathcal{G}$.*

Lemma 6. *The polynomials $\xi_1(x,t)$ and $\xi_2(x,y,t)$ have a common factor $\eta(x,t)$ depending on both x,t iff $x(t,s)$ depends only on t.*

In the case of Lemma 5, if $\mathbf{x}$ has some base point lying on $\mathcal{G}$, we remove the common factor depending on t, and perform the procedure presented before. In the case of Lemma 6, we replace $\xi_2(x,y,t)$ by

$$\tilde{\xi}_2(y,t) = \text{square-free part of } \mathrm{Res}_s(\mathrm{num}(y-y(t,s)), g(t,s)),$$

and proceed as before.

3.2. Behavior of $\mathcal{C}$ around the base points of $\mathbf{x}$.

Let $Q=(t_0,s_0)\in\mathcal{G}$ be a base point of $\mathbf{x}$. Notice that by Lemma 5, $t=t_0$ must be a root of the content of ξ_1,ξ_2 with respect to t, and therefore has been previously determined. In this case, $\mathbf{x}(t_0,s_0)$ is not defined. In order to determine the behavior of $\mathbf{x}$ when the point (t_0,s_0) is approached, we distinguish two situations:

(i) *The point (t_0,s_0) is not a critical point of $\mathcal{G}$:* in this case, by the Implicit Function Theorem $s^2-p(t)=0$ implicitly defines $s=s(t)$ at $t=t_0$. In fact, we can easily find the Taylor expansion of the function $s(t)$ at $t=t_0$, and then study the limits

$$\lim_{t\to t_0} x(t,s(t)),\ \lim_{t\to t_0} y(t,s(t)).$$

If both limits are finite, then (t_0,s_0) generates an affine point of $\mathcal{C}$. Otherwise we have a branch going to infinity, which is an asymptote of $\mathcal{C}$ whenever one of the above limits is finite.

(ii) *The point (t_0,s_0) is a critical point of $\mathcal{G}$:* in this case t_0 is a root of $p(t)$, so $s_0=0$. Now we consider $s=\pm\sqrt{p(t)}$ and we study each branch $s=\sqrt{p(t)}$ and $s=-\sqrt{p(t)}$ separately. We address in more detail the case $s=\sqrt{p(t)}$; for $s=-\sqrt{p(t)}$ the analysis is similar. Now if $s=\sqrt{p(t)}$, for the component $x(t,s)$ we have

$$x\left(t,\sqrt{p(t)}\right)=\frac{a_{11}(t)+\sqrt{p(t)}a_{12}(t)}{b_{11}(t)+\sqrt{p(t)}b_{12}(t)}.$$

We are interested in analyzing the behavior of this function when $t \to t_0$. Since $(t_0, 0)$ is a base point of $x(t,s)$, $a_{11}(t_0) = b_{11}(t_0) = 0$. Additionally, since $a_{11}(t)$, $a_{12}(t)$, $b_{11}(t)$, $b_{12}(t)$ are relatively prime, it cannot be $a_{12}(t_0) = 0$ and $b_{12}(t_0) = 0$ simultaneously. Furthermore, $t = t_0$ is a root of $p(t)$, and since $p(t)$ does not have multiple roots, the multiplicity of t_0 is 1. Hence we can factor out $(t - t_0)^{1/2}$ in the numerator and denominator of $x(t, \sqrt{p(t)})$, and we get

$$x\left(t, \sqrt{p(t)}\right) = \frac{\tilde{a}_{11}(t) + \sqrt{\tilde{p}(t)}a_{12}(t)}{\tilde{b}_{11}(t) + \sqrt{\tilde{p}(t)}b_{12}(t)},$$

where $\tilde{a}_{11}(t) = \dfrac{a_{11}(t)}{(t-t_0)^{1/2}}$, $\tilde{b}_{11}(t) = \dfrac{b_{11}(t)}{(t-t_0)^{1/2}}$, and $\tilde{p}(t) = \dfrac{p(t)}{t-t_0}$.

Observe that since $a_{11}(t_0) = b_{11}(t_0) = 0$ and $a_{11}(t), b_{11}(t)$ are polynomials, $\tilde{a}_{11}(t_0) = \tilde{b}_{11}(t_0) = 0$. Therefore, when $t \to t_0$ the limit of the function $x(t, \sqrt{p(t)})$ is equal to the limit of $a_{12}(t)/b_{12}(t)$ when $t \to t_0$. Since not both $a_{12}(t_0), b_{12}(t_0)$ are zero, the limit is defined whenever $b_{12}(t_0) \neq 0$, and is infinite (in which case we have a branch at infinity) whenever $b_{12}(t_0) = 0$. Similarly for the component $y(t,s)$, and for $s = -\sqrt{p(t)}$.

Notice that these ideas can be also used at points (t_0, s_0) where only one component of $\mathbf{x}(t,s)$ is undefined.

3.3. Construction of $G_{\mathcal{C}}$.

Let $Q_1 = (t_1, s_1), \ldots, Q_r = (t_r, s_r)$ be the points of $\mathcal{G}$ computed in (i)-(iv). Since the Q_i belong to $\mathcal{G}$ and the graph associated with $\mathcal{G}$ is easy to compute, we know how to connect the Q_i to each other. Furthermore, from the preceding sections the behavior of $\mathbf{x}$ around the Q_i is clear. Now the vertices of $G_{\mathcal{C}}$ are the images $P_i = \mathbf{x}(Q_i)$, whenever $\mathbf{x}(Q_i)$ (or the limit of $\mathbf{x}(t,s)$ as $(t,s) \to Q_i$, in the case of base points) is defined, and we connect two of these vertices iff their preimages Q_i are connected to each other in $G_{\mathcal{G}}$. Furthermore, we also include as vertices of $G_{\mathcal{C}}$ the points $P_{\pm\infty} \in \mathcal{C}$ coming from the point at infinity of $\mathcal{G}$, in case they are affine.

The following proposition, which follows from the fact that $\mathbf{x}|_{\mathcal{G}}$ is birational, guarantees that all the branches of $\mathcal{C}$ can be obtained this way.

Proposition 7. *Let $G_{\mathcal{G}}$ and $G_{\mathcal{C}}$ be the graphs associated with $\mathcal{G}$ and $\mathcal{C}$ according to the description in the preceding subsections. Then there is a $1:1$ correspondence between the edges of $G_{\mathcal{G}}$ and $G_{\mathcal{C}}$.*

Example 1. *Let*

$$g(t,s) = s^2 + t^4 - t^3 - 27t^2 + 25t + 50 = 0,$$

and let

$$\mathbf{x}(t,s) = (x(t,s), y(t,s)) = \left(\frac{t^4 - t^3 + t^2 + 5\,s - t}{t^6 + 1}, \frac{t^4 + t^3 - t^2 - 5\,s + t}{t^6 + 1} \right).$$

The curve $\mathcal{C} = \mathbf{x}(\mathcal{G})$ is a hyperelliptic curve of genus one.

First we compute the real points $(t,s) \in \mathcal{G}$ generating the vertices of $G_{\mathcal{C}}$:

(i) Critical points of $g(t,s) = 0$, i.e. points $(t,0)$ with $p(t) = 0$:

$$Q_1 = (-5,0), Q_2 = (-1,0), Q_3 = (2,0) \text{ and } Q_4 = (5,0).$$

(ii) Points of $\mathcal{G}$ giving rise to critical points of $\mathcal{C}$. Local singularities and ramification points are generated by the points (t,s) solutions of the system

$$g(t,s) = 0, \quad x_t g_s - x_s g_t = 0.$$

The real solutions (written only with two digits) are:

$$Q_5 = (-4.98, -2.05), Q_6 = (-3.21, -13.00), Q_7 = (-1.16, -3.47),$$

$$Q_8 = (-1.12, 3.08), Q_9 = (2.15, 3.11), Q_{10} = (2.24, -3.97),$$

$$Q_{11} = (3.76, -9.54), Q_{12} = (4.96, -2.52).$$

Now we compute the points of $\mathcal{G}$ giving rise to self-intersections of $\mathcal{C}$. We have:

$$\xi_1(x,t) \;=\; \left(t^{12} + 2\,t^6 + 1\right) x^2 + \left(-2\,t^{10} + 2\,t^9 + \cdots\right) x + t^8 + \cdots + 1250,$$

and

$$\xi_2(x,y,t) = (t^6 + 1)(x + y) - 2t^4.$$

The self-intersections of $\mathcal{C}$ are generated by the real solutions of the system $\{\mathbf{sres}_1(x(t,s), y(t,s)) = 0, \quad g(t,s) = 0\}$, which are $Q_{13} = (-3.75, -13.14)$, $Q_{14} = (-2.32, -10.61)$, $Q_{15} = (2.32, -4.62)$ and $Q_{16} = (3.75, 9.53)$.

The points Q_{13} and Q_{16} both generate the same point, P_{13}, and the points Q_{14} and Q_{15} both generate the point P_{14} (see Figure 4).

(iii) *Points of $\mathcal{G}$ where some component of $\mathbf{x}$ is not defined: there are neither base points nor vertical asymptotes.*

(iv) *Starting and ending points for open branches of G: There are not open branches.*

Finally, we compute the images $P_i = \mathbf{x}(Q_i)$, and we connect them according to how the Q_i are connected in $\mathcal{G}$. The graph associated with $\mathcal{G}$ is shown in Fig. 3 (left). The graph associated with $\mathcal{C}$ is also shown in Fig. 3 (right). Additionally, in the graph associated there are several points very close to each other: some details on the topology of $\mathcal{C}$ are given in Fig. 4.

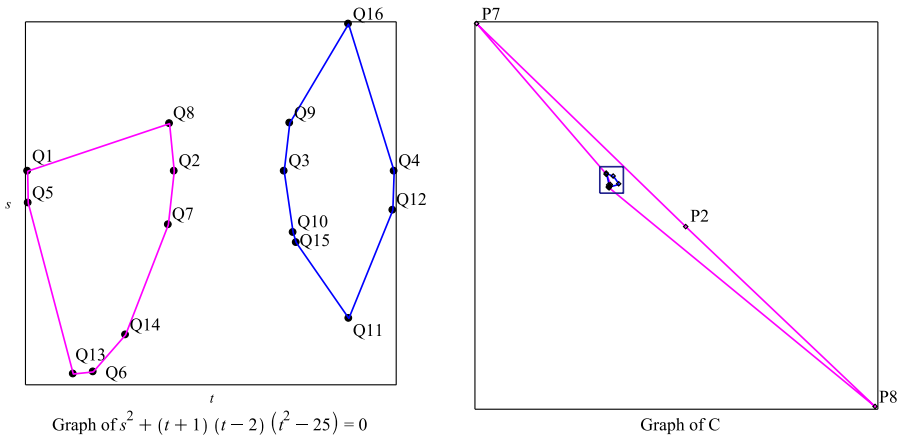

Figure 3: Correspondence between the edges of $G_{\mathcal{G}}$ and $G_{\mathcal{C}}$.

4. The space case.

Here we consider $\mathbf{x} : \mathbb{R}^2 \to \mathbb{R}^3$, where

$$\mathbf{x}(t,s) = (x(t,s), y(t,s), z(t,s)) = \left(\frac{A_1(t,s)}{B_1(t,s)}, \frac{A_2(t,s)}{B_2(t,s)}, \frac{A_3(t,s)}{B_3(t,s)} \right).$$

We let $\mathcal{C} = \mathbf{x}(\mathcal{G})$, where $\mathcal{G}$ is defined by Eq. (2), we let $\mathcal{C}^\star = \pi_{xy}(\mathcal{C})$, where π_{xy} denotes the projection onto the xy-plane, and we also define $\tilde{\mathbf{x}} = \pi_{xy} \circ \mathbf{x}$. Fig. 5 illustrates the relationship between $\mathcal{G}$, $\mathcal{C}$ and $\mathcal{C}^\star$. We need two hypotheses this time:

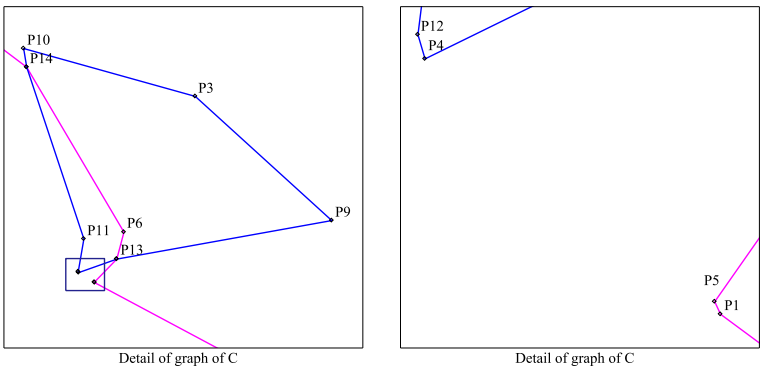

Figure 4: Details

(H1) The restriction $\tilde{\mathbf{x}}|_{\mathcal{G}}$ is birational.

(H2) The curve $\mathcal{C}^\star$ does not have any asymptotes parallel to the either the y-axis, or the z-axis.

It is also customary, when computing the topology of a space curve $\mathcal{C}$, to require that $\mathcal{C}$ has no component parallel to the z-axis. However, in our case $\mathcal{C}$ is irreducible, i.e. $\mathcal{C}$ consists of only one component. If $\mathcal{C}$ reduces to a line parallel to the z-axis, then the only possibility is that both $x(t,s), y(t,s)$ are constant, which is a trivial case.

Hypothesis (H1) implies that $\mathbf{x}$ itself is birational when restricted to $\mathcal{G}$, and that π_{xy} is also birational when restricted to $\mathcal{C}$; in turn, this means that there are not two different branches of $\mathcal{C}$ projecting as a same branch of $\mathcal{C}^\star$, and therefore that the branches of $\mathcal{C}$ are the result of lifting to space the branches of the projection $\mathcal{C}^\star = \pi_{xy}(\mathcal{C})$. Hypothesis (H1) can be checked, as observed in Section 3, by taking a random point $(t_0, s_0) \in \mathcal{G}$ and determining the preimages of $\tilde{\mathbf{x}}(t_0, s_0)$. Hypothesis (H2) can be checked by testing whether or not $B_2(t,s) = g(t,s) = 0$ has some solution where $A_2(t,s) \cdot B_1(t,s) \neq 0$. Both hypotheses, (H1) and (H2), guarantee that: (i) the topology of $\mathcal{C}^\star$ could be computed by applying the ideas in Section 3; (ii) the topology of $\mathcal{C}$ could be computed from the topology of $\mathcal{C}^\star$, by lifting a (planar) graph isotopic to $\mathcal{C}^\star$. In our case, however, we do not need to compute first the topology of $\mathcal{C}^\star$; instead, as in Section 3, we determine all the points $(t,s) \in \mathcal{G}$ giving rise to "notable" points of $\mathcal{C}$, and incorporate those points as vertices of $G_{\mathcal{G}}$. Then the edges of $G_{\mathcal{G}}$ are mapped onto edges of $G_{\mathcal{C}}$ as we did in Section 3.

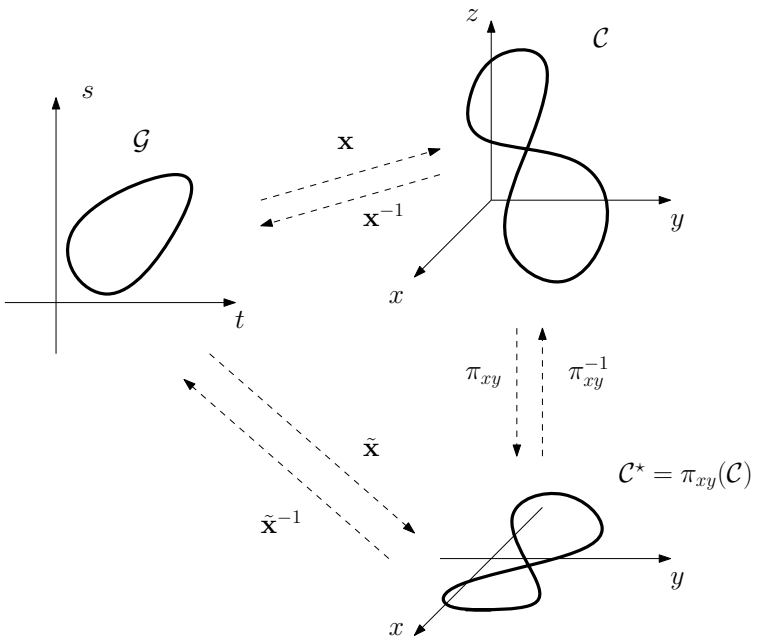

Figure 5: Relationship between the curves $\mathcal{G}$, $\mathcal{C}$, and $\mathcal{C}^\star$.

Hypotheses (H1) and (H2) can always be achieved when $\mathbf{x}|_{\mathcal{G}}$ is birational. Indeed, under this assumption, for almost all random orthogonal changes of coordinates ϕ and renaming $\mathbf{x} := \mathbf{x} \circ \phi$, $\pi_{xy}|_{\mathcal{C}}$ is birational, i.e. two different branches of $\mathcal{C}$ do not project as a same branch of $\mathcal{C}^\star$. As a consequence $\tilde{\mathbf{x}}|_{\mathcal{G}}$ must be birational.

In this case, we need to include the following points as vertices of $G_{\mathcal{G}}$:

(i) *Critical points of* $g(t,s) = 0$, i.e. points of $\mathcal{G}$ where $g_s = 0$.

(ii) *Points of* $\mathcal{G}$ *giving rise to critical points of* $\mathcal{C}^\star$.

(iii) *Points of* $\mathcal{G}$ *where some component of* $\mathbf{x}$ *is not defined.*

(iv) *Starting and ending points for open branches of* $\mathcal{G}$.

The points in (i), (ii), (iii) are computed as in Section 3; observe that the pairs (t,s) generating singularities and points of $\mathcal{C}$ with tangent parallel to the z-axis are among the critical points of $\mathcal{C}^\star$ (see [4, 3]). Once the points $Q_i = (t_i, s_i)$, $i = 1, \ldots, r$ in (i)-(iv) are computed, we can find, whenever

they are defined, the images $P_i = \mathbf{x}(Q_i)$ or the limit points and proceed as in Section 3 in order to connect the Q_i.

5. Experimentation.

In this section we report on the experimentation carried out in the case of both 2D and 3D curves. The algorithms have been implemented in `Maple 2017`, and the examples run on an Intel Core i3 processor with speeds revving up to 3.06 GHz.

Next, we first present examples of the 2D algorithm. In Table 1, we include for each curve, the genus, the total degree (d_i) and the number of terms of the implicit equation (n.terms), the timings in seconds (t_0) taken by our algorithm, and the timings in seconds (t_1) corresponding to the algorithm in [20], also implemented in `Maple`, which uses the implicit equation of the curve. The parametrizations corresponding to these examples are given in Appendix II of [2], the ArXiv version of this paper. The graphs corresponding to the examples in Table 1 are shown in Figure (6); from left to right, we have Examples 1, 2, 3 in the first row, 4, 5, 6 in the second row and 7, 8, 9 in the third row.

Example	genus	d_i	n.terms	t_0	t_1
1	0	10	57	0.310	0.270
2	1	14	81	0.625	*
3	2	6	26	0.398	0.110
4	1	12	81	0.529	*
5	2	12	75	0.543	*
6	2	11	75	0.777	*
7	2	12	75	0.443	*
8	1	6	23	0.484	0.108
9	2	9	55	1.069	0.308

Table 1: 2D Examples.

*: Computation was cancelled after fifteen minutes.

Finally, we present examples of the 3D algorithm. In Table 2, for each curve we include the genus, the total degree (d_i) and the number of terms of the implicit equation of the projection onto the xy-plane (d_i), and the timing in seconds taken by our algorithm (t_0); the parametrizations corresponding

to each curve are given in Appendix III of [2], the ArXiv version of this paper. Additionally, we add some observations on the nature of the curve in the last column; for instance, the first three curves were generated by intersecting a quadric with a ruled surface. The parametrizations corresponding to these examples are given in Appendix III.

Example	genus	d_i	n.terms	t_0
1	4	10	66	1.543
2	2	6	16	0.344
3	7	16	153	78.252
4	3	8	42	0.537
5	2	5	6	0.095
6	1	4	9	0.201
7	1	10	34	0.352
8	3	8	45	0.457
9	4	10	66	0.281

Table 2: 3D Examples.

The pictures corresponding to these curves are shown in Figure 7.

6. Complexity and certification issues.

In this section we present the complexity of the algorithms presented in the previous sections, and we elaborate on how to certificate the topology of the curves. To certify the topology we must be sure whether two different points $(t_i, s_i) \neq (t_j, s_j)$, both belonging to $\mathcal{G}$, satisfy $\mathbf{x}(t_i, s_i) = \mathbf{x}(t_j, s_j)$, that is whether they give rise to the same point $P \in \mathcal{C}$. We first analyze the complexity of the algorithm without the certification step: in particular, the timings corresponding to Section 5 do not include this certification. Then, we address certification issues and provide the complexity of the algorithm including the certification step. We analyze the algorithm for 3D curves: the complexity bound is the same for 2D and 3D curves.

6.1. Complexity (I)

In this section we present the bit complexity analysis of the algorithm without the certification step. This is the algorithm we report on in Section 5. We denote the maximum bitsize by $\mathcal{L}(f)$ of the coefficients of a polynomial f. Additionally, we denote by $\mathcal{O}, \widetilde{\mathcal{O}}, \widetilde{\mathcal{O}}_B$ the arithmetic complexity, the

arithmetic complexity neglecting logarithmic factors, and the bit complexity (also neglecting logarithmic factors), respectively.

Let

$$\mathbf{x}(t,s) = \left(\frac{a_{11}(t)+sa_{12}(t)}{b_{11}(t)+sb_{12}(t)}, \frac{a_{21}(t)+sa_{22}(t)}{b_{21}(t)+sb_{22}(t)}, \frac{a_{31}(t)+sa_{32}(t)}{b_{31}(t)+sb_{32}(t)} \right).$$

We consider the following 3 polynomials:

$$\begin{aligned} X(t,s) &= (b_{11}(t)+sb_{12}(t))x - (a_{11}(t)+sa_{12}(t)), \\ Y(t,s) &= (b_{21}(t)+sb_{22}(t))x - (a_{21}(t)+sa_{22}(t)), \\ Z(t,s) &= (b_{31}(t)+sb_{32}(t))x - (a_{31}(t)+sa_{32}(t))). \end{aligned}$$

We also recall that $g(t,s) = s^2 - p(t)$. We assume that all the univariate polynomials in t, that is the $a_{ij}(t), b_{ij}(t)$, and $p(t)$, have degree at most d, and that their coefficients are integers of maximum bitsize at most τ.

In the process of the algorithm we first compute the resultants

$$E_0 = \mathrm{res}_s(X,Y),\ E_1 = \mathrm{res}_s(X,g).$$

The polynomial E_0 satisfies that $E_0 \in \mathbb{Z}[x,y,t]$. The degree of E_0 with respect to x and y is 1 and with respect to t is $\leq 2d = \mathcal{O}(d)$; moreover $\mathcal{L}(E_0) = \widetilde{\mathcal{O}}(\tau)$. The polynomial E_1 satisfies that $E_1 \in \mathbb{Z}[x,t]$. The degree of E_1 with respect to x is 2 and with respect to t is $\leq 3d = \mathcal{O}(d)$; also $\mathcal{L}(E_1) = \widetilde{\mathcal{O}}(\tau)$.

Since the degree of X, Y, Z and g with respect to x, y, s is at most 2, we can compute the resultants E_0 and E_1 by performing a constant number of multiplications of univariate polynomials in t. By recalling that the maximum degree with respect to t is $\widetilde{\mathcal{O}}(d)$, we deduce that the cost of computing E_0 and E_1 is $\widetilde{\mathcal{O}}_B(d\tau)$ [25].

Next, we consider the subresultant sequence of E_0 and E_1 with respect to t. From this sequence we are interested in the polynomial of degree 1 with respect to t. This is the first subresultant polynomial; we can compute it in $\widetilde{\mathcal{O}}_B(d^4\tau)$ [15, Lemma 8]. Let the coefficient of degree 1 of this polynomial be $\mathbf{sres}_1 \in \mathbb{Z}[x,y]$ (i.e. the first principal subresultant). It has degree $\widetilde{\mathcal{O}}(d)$ and bitsize $\widetilde{\mathcal{O}}(d\tau)$ [15, Lemma 8].

Then we substitute the parametrization $\mathbf{x}(t,s)$ in $\mathbf{sres}_1$. After clearing denominators we obtain a polynomial $M(t,s) \in \mathbb{Z}[t,s]$. The degree of $M(t,s)$ with respect to t and s is $\widetilde{\mathcal{O}}(d)$ and its bitsize is $\widetilde{\mathcal{O}}(d^2\tau)$. This calculation

of $M(t,s)$ involves $\mathcal{O}(d)$ multiplications of bivariate polynomials in s and t. This cost is $\widetilde{\mathcal{O}}_B(d^5\tau)$ [22, 25].

Finally, we solve the polynomial system $M(t,s) = g(t,s) = 0$. We can solve the system in $\widetilde{\mathcal{O}}_B(d^7\tau)$ (or $\widetilde{\mathcal{O}}_B(d^8\tau)$) [18, 9]. After solving the system, we compute the images under the birational mapping $\mathbf{x}(t,s)$ of all the points (t,s) computed along the way, and connect them properly. The whole complexity is dominated by the complexity of solving the polynomial system $M(t,s) = g(t,s) = 0$, so we get a final bound of $\widetilde{\mathcal{O}}_B(d^7\tau)$ (or $\widetilde{\mathcal{O}}_B(d^8\tau)$), without including certification.

6.2. Certification and complexity (II)

In this subsection we consider certification strategies, and we present the complexity of the algorithm including this certification.

Within the complexity bound given in the previous subsection for solving the bivariate system $M(t,s) = g(t,s) = 0$, we can compute both an isolating interval representation of the real roots, as a well a (sparse) rational univariate representation (SRUR) [9], see also [22]. The latter represents the tuples (t,s) of the solutions as $\left(\frac{F_1(\theta)}{F_0(\theta)}, \frac{F_2(\theta)}{F_0(\theta)}\right)$, where θ runs over all the (real) roots of a (univariate) polynomial $F(\theta)$. This representation involves univariate polynomials of degree $\widetilde{\mathcal{O}}(d^2)$ and bitsize $\widetilde{\mathcal{O}}(d^3\tau)$.

Now we want to identify which tuples of solutions of the polynomial system $M(t,s) = g(t,s) = 0$ give rise to the same point on space curve. Say that (α_1, β_1) and (α_2, β_2) are two different solutions of the system. Assume further that they correspond to the roots θ_1 and θ_2 of the polynomial $F(\theta)$. Thus their rational univariate representation is $\left(\frac{F_1(\theta_1)}{F_0(\theta_1)}, \frac{F_2(\theta_1)}{F_0(\theta_1)}\right)$ and $\left(\frac{F_1(\theta_2)}{F_0(\theta_2)}, \frac{F_2(\theta_2)}{F_0(\theta_2)}\right)$, respectively, with $F(\theta_1) = 0$, $F(\theta_2) = 0$.

We check if they correspond to the same point by exploiting the parametrization $\mathbf{x}$. For example, to test if they result in the same x-coordinate, we should test whether or not

$$\frac{a_{11}(\alpha_1) + \beta_1 a_{12}(\alpha_1)}{b_{11}(\alpha_1) + \beta_1 b_{12}(\alpha_1)} = \frac{a_{11}(\alpha_2) + \beta_2 a_{12}(\alpha_2)}{b_{11}(\alpha_2) + \beta_2 b_{12}(\alpha_2)}.$$

Clearing denominators, we get $\widehat{G}(\alpha_1, \alpha_2) = 0$. Now if we substitute the rational univariate representation of the roots and clear denominators, then we get a new bivariate polynomial G, and we need to test whether or not $G(\theta_1, \theta_2) = 0$.

The degree of G is $\widetilde{\mathcal{O}}(d^3)$, in θ_1 and θ_2 and its bitsize is $\widetilde{\mathcal{O}}(d^4\tau)$. The complexity of computing G involves the multiplication of $\widetilde{\mathcal{O}}(d)$ univariate polynomials and is $\widetilde{\mathcal{O}}_B(d^8\tau)$. The cost of this bivariate sign evaluation is $\widetilde{\mathcal{O}}_B(d^{15}\tau)$.

We must perform this bivariate sign evaluation for every pair (θ_i, θ_j) of roots of F, and test for all coordinates (x, y, z). There are $\widetilde{\mathcal{O}}(d^4)$ pairs of solutions to test and the total cost is $\widetilde{\mathcal{O}}_B(d^{19}\tau)$. This complexity bound of certification dominates the overall complexity of the algorithm.

We have implemented the certification part, and the timings we get are in agreement with this complexity: although there can be examples where the computing time is reasonable, in general the timings are very high, and further research needs to be done. It seems plausible to improve the complexity of certification by exploiting more carefully aggregate separation bounds for the real roots of polynomial systems [19]. For example, we can apply this aggregation when we perform the time consuming sign evaluation of G over all the roots of the polynomial F. There should be a gain of a factor d^2 with this approach.

However, the most promising direction is to use more advanced (probabilistic) tests for checking equality of real algebraic numbers [8]. The reader might notice that we do not really need the actual sign evaluation of G. What we really need is to test is whether or not the evaluation of G at (θ_1, θ_2) is zero.

6.3. Comparison of complexities with implicit algorithms.

A possibility to compute the topology of $\mathcal{C}$ is to compute first an implicit representation of the curve, and then to apply an algorithm to complete the topology of an implicit curve. In the planar case, the implicit representation requires just one bivariate polynomial $f(x, y)$, that can be computed using Gröbner bases. Denoting the degree of $f(x, y)$ by n, and denoting by τ_f the bitsize of the coefficients of f, the complexity of computing the topology of $f(x, y) = 0$ is $\widetilde{\mathcal{O}}_B(n^6 + n^5\tau_f)$. In our case $n = \widetilde{\mathcal{O}}(d)$ and $\tau_f = \widetilde{\mathcal{O}}(d\tau)$, so we reach a complexity of $\widetilde{\mathcal{O}}_B(d^6\tau)$, certainly better than the bound we give in Subsection 6.2.

In the space case, however, the situation is much more difficult. An implicit representation of $\mathcal{C}$ requires to compute a basis for the ideal of the curve, which might have more than two polynomials. Even if $\mathcal{C}$ is implicitly defined by only two polynomials $f_i(x, y, z)$, with $i = 1, 2$, the known com-

plexities for implicit algorithms are worse than ours. In [14], one has the bound $\widetilde{\mathcal{O}}(n^{21}\tau_f)$, where n, τ_f are bounds for the degrees and bitsizes of the f_i, respectively. For the same case, in [11] one has the bound $\widetilde{\mathcal{O}}(n^{37}\tau_f)$.

7. Conclusion.

We have presented algorithms to compute the topology of 2D and 3D hyperelliptic curves that do not require to compute or make use of the implicit representation of the curve. The main idea is to see the hyperelliptic curve as the image of a planar curve, the Weierstrass form of the curve, under a birational mapping of the plane or the space. Seeing the curve this way, the algorithms determines how the topology of the Weierstrass form changes when the birational mapping is applied. While a not completely certified algorithm produces good and fast results, a completely certified algorithm is much slower, although it is competitive in the space case, in terms of complexity, with algorithms using an implicit representation of the curve. Some lines of improvement to speed up the certification are suggested in the paper. We plan to exploit these ideas in the future to get a faster, certified, algorithm.

References

[1] Juan Gerardo Alcázar, Jorge Caravantes, and Gema M Díaz-Toca. A new method to compute the singularities of offsets to rational plane curves. *Journal of Computational and Applied Mathematics*, 290:385–402, 2015.

[2] Juan Gerardo Alcázar, Jorge Carvantes, Gema María Díaz Toca, and Elias Tsigaridas. ArXiv 1812.11498, 2018.

[3] Juan Gerardo Alcázar and Gema María Díaz-Toca. Topology of 2d and 3d rational curves. *Computer Aided Geometric Design*, 27(7):483–502, 2010.

[4] Juan Gerardo Alcázar and J Rafael Sendra. Computation of the topology of real algebraic space curves. *Journal of Symbolic Computation*, 39(6):719–744, 2005.

[5] Eric Berberich, Pavel Emeliyanenko, Alexander Kobel, and Michael Sagraloff. Arrangement computation for planar algebraic curves. In *Proceedings of the 2011 International Workshop on Symbolic-Numeric Computation*, pages 88–98. ACM, 2012.

[6] Eric Berberich, Pavel Emeliyanenko, Alexander Kobel, and Michael Sagraloff. Exact symbolic–numeric computation of planar algebraic curves. *Theoretical Computer Science*, 491:1–32, 2013.

[7] Michal Bizzarri, Miroslav Lávička, and Jan Vršek. Piecewise rational approximation of square-root parameterizable curves using the weierstrass form. *Computer Aided Geometric Design*, 56:52–66, 2017.

[8] Johannes Blomer. Computing sums of radicals in polynomial time. In *Foundations of Computer Science, 1991. Proceedings., 32nd Annual Symposium on*, pages 670–677. IEEE, 1991.

[9] Yacine Bouzidi, Sylvain Lazard, Guillaume Moroz, Marc Pouget, Fabrice Rouillier, and Michael Sagraloff. Solving bivariate systems using rational univariate representations. *J. Complex.*, 37(C):34–75, December 2016.

[10] Jorge Caravantes, Gema M Díaz-Toca, Laureano González-Vega, and Ioana Necula. An algebraic framework for computing the topology of offsets to rational curves. *Computer Aided Geometric Design*, 52:28–47, 2017.

[11] Jin-San Cheng, Kai Jina, and Daniel Lazard. Certified rational parametric approximation of real algebraic space curves with local generic position method. *Journal of Symbolic Computation*, 58:18–40, 2013.

[12] Jinsan Cheng, Sylvain Lazard, Luis Peñaranda, Marc Pouget, Fabrice Rouillier, and Elias Tsigaridas. On the topology of planar algebraic curves. In *Proceedings of the twenty-fifth annual symposium on Computational geometry*, pages 361–370. ACM, 2009.

[13] Diatta Niang Daouda, Bernard Mourrain, and Olivier Ruatta. On the computation of the topology of a non-reduced implicit space curve. In *Proceedings of the twenty-first international symposium on Symbolic and algebraic computation*, pages 47–54. ACM, 2008.

[14] Daouda Diatta. *Calcul effectif de la topologie de courbes et surfaces algebriques reelles*. Ph. D. Thesis, Universite de Limoges, 2009.

[15] Dimitrios I Diochnos, Ioannis Z Emiris, and Elias P Tsigaridas. On the asymptotic and practical complexity of solving bivariate systems over the reals. *Journal of Symbolic Computation*, 44(7):818–835, 2009.

[16] Arno Eigenwillig, Michael Kerber, and Nicola Wolpert. Fast and exact geometric analysis of real algebraic plane curves. In *Proceedings of the 2007 international symposium on Symbolic and algebraic computation*, pages 151–158. ACM, 2007.

[17] Mohammed El Kahoui. Topology of real algebraic space curves. *Journal of Symbolic Computation*, 43(4):235–258, 2008.

[18] Pavel Emeliyanenko and Michael Sagraloff. On the complexity of solving a bivariate polynomial system. In *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*, pages 154–161. ACM, 2012.

[19] Ioannis Z Emiris, Bernard Mourrain, and Elias P Tsigaridas. The dmm bound: Multivariate (aggregate) separation bounds. In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, pages 243–250. ACM, 2010.

[20] Laureano González-Vega and Ioana Necula. Efficient topology determination of implicitly defined algebraic plane curves. *Computer aided geometric design*, 19(9):719–743, 2002.

[21] Alexander Kobel and Michael Sagraloff. On the complexity of computing with planar algebraic curves. *Journal of Complexity*, 31(2):206–236, 2015.

[22] Angelos Mantzaflaris, Éric Schost, and Elias Tsigaridas. Sparse rational univariate representation. In *ISSAC 2017-International Symposium on Symbolic and Algebraic Computation*, page 8, 2017.

[23] J Rafael Sendra, David Sevilla, and Carlos Villarino. Algebraic and algorithmic aspects of radical parametrizations. *Computer Aided Geometric Design*, 55:1–14, 2017.

[24] G.M. Díaz Toca. `http://webs.um.es/gemadiaz/miwiki/doku.php?id=papers`, 2018.

[25] Joachim Von Zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge university press, 2013.

8. Appendix I: proofs.

In this section we provide the proofs of some results in Section 3. We start with Proposition 3.

Proof. (of Proposition 3) Let $\mathcal{V}$ be the variety (the curve) in $\mathbb{R}^4(t,s,x,y)$ defined as

$$\mathcal{V} = V(\mathrm{num}(x - x(t,s)), \mathrm{num}(y - y(t,s)), g(t,s)),$$

and let $\widehat{\mathcal{V}} = \Pi_{txy}(\mathcal{V})$ be the projection of $\mathcal{V}$ onto $\mathbb{R}^3(t,x,y)$; notice that $\widehat{\mathcal{V}} \subset V(\xi_1, \xi_2)$. Suppose that (t_0, s_0, x_0, y_0) is smooth in $\mathcal{V}$. Using the Jacobian matrix of $F_1(t,s,x) = \mathrm{num}(x - x(t,s))$, $F_2(t,s,y) = \mathrm{num}(y - y(t,s))$, $g(t,s)$ and condition (11), we observe that the tangent line to $\mathcal{V}$ at (s_0, t_0, x_0, y_0) is parallel to $(-g_s(t_0,s_0), g_t(t_0,s_0), 0, 0)$. If $g_s(t_0,s_0) \neq 0$ (i.e. if $s_0 \neq 0$) then the point (t_0, x_0, y_0) is regular in $\widehat{\mathcal{V}}$ and the tangent line to $\widehat{\mathcal{V}}$ at (t_0, x_0, y_0) is $\{x = x_0, y = y_0\}$, which is parallel to the t-axis. Therefore, $\xi_1(t, x_0) = 0$ and $\xi_2(t, x_0, y_0) = 0$ share the root t_0 with multiplicity higher than 1, and $\mathbf{sres}_1(x_0, y_0) = 0$. If $g_s(t_0,s_0) = 0$ (i.e. if $s_0 = 0$) then (t_0, x_0, y_0) is singular in $\widehat{\mathcal{V}}$ and we can derive the same conclusion.

If, however, (s_0, t_0, x_0, y_0) is a singular point of $\widehat{\mathcal{V}}$, then the tangent space to $\mathcal{V}$ at (s_0, t_0, x_0, y_0), i.e. the kernel of the Jacobian matrix, consists of the vectors $(\alpha, \beta, 0, 0)$ with $\alpha, \beta \in \mathbb{C}$. Therefore, the line $\{x = x_0, y = y_0\}$ is tangent to $\widehat{\mathcal{V}}$ at (t_0, x_0, y_0) and, therefore, all $\xi_i(t, x_0, y_0)$, $i = 1, 2$ have a multiple root at $t = t_0$. This implies that $\mathbf{sres}_1(x_0, y_0) = 0$. □

Now we prove Lemma 5. From definitions of ξ_1, ξ_2 in Eq. (8) and taking into account that $\mathbf{x}$ can be written as in Eq. (4), the polynomial $\xi_1(t,x)$ is the square-free part of the resultant with respect to s of $g(t,s) = s^2 - p(t)$ and

$$\begin{aligned} h(t,s,x) &:= \mathrm{num}(x - x(t,s)) = \\ &= x(b_{11}(t) + s b_{12}(t)) - (a_{11}(t) + s a_{12}(t)) = \\ &= s(x b_{12}(t) - a_{12}(t)) + x b_{11}(t) - a_{11}(t). \end{aligned}$$

Since $\mathrm{degree}_s(g) = 2$ and $\mathrm{degree}_s(h) \leq 1$, it is easy to compute such a resultant; if $\mathrm{degree}_s(h) = 1$, i.e. if $x(t,s)$ explicitly depends on s, then

$$\mathrm{Res}_s(h,g) = \left(b_{11}^2 - p\, b_{12}^2\right) x^2 - 2\left(a_{11}\, b_{11} - p\, a_{12}\, b_{12}\right) x + a_{11}^2 - p\, a_{12}^2, \quad (12)$$

where $b_{ij} = b_{ij}(t)$, $a_{ij} = a_{ij}(t)$ for $i = 1, 2$, $j = 1, 2$. If $\text{degree}_s(h) = 0$, i.e. if $x(t, s)$ does not depend on s, then

$$\text{Res}_s(h, g) = h = x(b_{11}(t) + sb_{12}(t)) - (a_{11}(t) + sa_{12}(t)). \tag{13}$$

As for $\xi_2(t, x, y)$, that is is the square-free part of the resultant with respect to s of $h(t, s, x)$ and

$$\begin{aligned} j(t, s, y) &:= \text{num}(y - y(t, s)) = \\ &= y(b_{21}(t) + sb_{22}(t)) - (a_{21}(t) + sa_{22}(t)) = \\ &= s(yb_{22}(t) - a_{22}(t)) + yb_{21}(t) - a_{21}(t). \end{aligned}$$

If $\text{degree}_s(h) = \text{degree}_s(j) = 1$, i.e. if both $x(t, s)$ and $y(t, s)$ explicitly depend on s, then

$$\text{Res}_s(h, j) = (a_{22}b_{11} - a_{21}b_{12})x + (a_{11}b_{22} - a_{12}b_{21})y + (b_{12}b_{21} - b_{11}b_{22})xy - a_{11}a_{22} + a_{12}a_{21}, \tag{14}$$

where $b_{ij} = b_{ij}(t)$, $a_{ij} = a_{ij}(t)$ for $i = 1, 2$, $j = 1, 2$. If $\text{degree}_s(h) = 0$, i.e. if $x(t, s)$ does not depend on s, then

$$\text{Res}_s(h, j) = h = x(b_{11}(t) + sb_{12}(t)) - (a_{11}(t) + sa_{12}(t)), \tag{15}$$

and if $\text{degree}_s(j) = 0$, i.e. if $y(t, s)$ does not depend on s, then

$$\text{Res}_s(h, j) = j = yb_{21}(t) - a_{21}(t). \tag{16}$$

Proof. (of Lemma 5) "$\Leftarrow$" Suppose that t_0 corresponds to a base point. The resultant of $h(t, s, x)$ and $g(t, s)$ is equal to Equation (12), and considered as a polynomial in x, it is easy to see that all its coefficients vanish at $t = t_0$. Thus, $t - t_0$ divides $\xi_1(x, t)$. Likewise, the resultant of $h(t, s, x)$ and $j(t, s, y)$ is equal to Equation (14), and we can check that all its coefficients vanish in $t = t_0$. Thus, $t - t_0$ divides also $\xi_2(x, t)$.

"$\Rightarrow$" If $t - t_0$ divides ξ_1, then, by properties of resultants, since the leading coefficient of $g(t, s)$ with respect to s is 1, there is s_0 with $g(t_0, s_0) = 0$ and

$$h(t_0, s_0, x) = x(b_{11}(t_0) + s_0b_{12}(t_0)) - (a_{11}(t_0) + s_0a_{12}(t_0)) = 0;$$

thus, $b_{11}(t_0) + s_0b_{12}(t_0) = a_{11}(t_0) + s_0a_{12}(t_0) = 0$.

Next, if $t - t_0$ divides ξ_2, then either the leading coefficients of both $h(t, s, x)$ and $j(t, s, y)$ with respect to s vanish at $t = t_0$, or there exists s_1 such that $h(t_0, s_1, x) = j(t_0, s_1, y) = 0$ for all x, y. In the first case, we would have

$$b_{12}(t_0) = a_{12}(t_0) = b_{22}(t_0) = a_{22}(t_0) = 0.$$

However, since also $b_{11}(t_0) + s_0 b_{12}(t_0) = a_{11}(t_0) + s_0 a_{12}(t_0) = 0$, we should have

$$a_{11}(t_0) = a_{12}(t_0) = b_{12}(t_0) = b_{11}(t_0) = 0,$$

but this cannot happen because $\gcd(a_{11}, a_{12}, b_{11}, b_{12}) = 1$. Therefore, there exists s_1 such that for all x, y

$$h(t_0, s_1, x) = x(b_{11}(t_0) + s_1 b_{12}(t_0)) - (a_{11}(t_0) + s_1 a_{12}(t_0)) = 0;$$

$$j(t_0, s_1, y) = y(b_{21}(t_0) + s_1 b_{22}(t_0)) - (a_{21}(t_0) + s_1 a_{22}(t_0)) = 0.$$

Then,

$$\begin{aligned} b_{11}(t_0) + s_1 b_{12}(t_0) = a_{11}(t_0) + s_1 a_{12}(t_0) = 0, \\ b_{21}(t_0) + s_1 b_{22}(t_0) = a_{21}(t_0) + s_1 a_{22}(t_0) = 0. \end{aligned}$$

Since we also know that $b_{11}(t_0) + s_0 b_{12}(t_0) = a_{11}(t_0) + s_0 a_{12}(t_0) = 0$, with $(t_0, s_0) \in \mathcal{G}$, we deduce that either $s_1 = s_0$, or $b_{12}(t_0) = a_{12}(t_0) = 0$. However, $b_{12}(t_0) = a_{12}(t_0) = 0$ implies that $b_{11}(t_0) = a_{11}(t_0) = 0$, which cannot happen because $\gcd(a_{11}, a_{12}, b_{11}, b_{12}) = 1$. $s_0 = s_1$ with $g(t_0, s_0) = 0$. So, we can conclude that t_0 corresponds to a base point of $\mathbf{x}$. □

Finally, we prove Lemma 6.

Proof. (of Lemma 6) "⇐" If $x(t, s) = x(t)$, then $\xi_1(t, x) = \xi_2(t, x, y) = b_{11}(t)x - a_{11}(t)$, and the result follows.

"⇒" By way of contradiction, suppose that $\xi_1(t, x)$ and $\xi_2(t, x, y)$ have a factor $\eta(t, x)$ depending on both x, t and that both $x(t, s)$ and $y(t, s)$ depend on s. From Eq. (16), $y(t, s)$ explicitly depends on s. So suppose that $x(t, s)$ also depends on s. Then $\xi_2(t, x, y)$ is the square-free part of Eq. (14), so $\eta(t, x)$ must be linear in x. Therefore either $\xi_2(t, x, y)$ coincides with $\eta(t, x)$, or $\xi_2(t, x, y)$ has another factor $\gamma(t, y)$ whose degree in y is at most 1. Now we distinguish two cases:

(i) If $\text{degree}_y(\gamma) = 1$, then for all (t_0, y_0) such that $\gamma(t_0, y_0) = 0$, either the leading coefficients of h, j with respect to s vanish at (t_0, y_0) for all x, or there exists s_0 such that h, j integrally vanish at (t_0, s_0, y_0) for all

x. The first possibility implies that both leading coefficients are zero modulo $\gamma(t, y)$, and this cannot happen because the leading coefficient of h with respect to s depends on x. But the second possibility cannot happen either, because that would imply that $x(t, s)$ has infinitely many base points.

(ii) If $\text{degree}_y(\gamma) = 0$, then for all (t_0, x_0) such that $\eta(t_0, x_0) = 0$, either the leading coefficients of h, j with respect to s vanish at (t_0, x_0) for all y, or there exists s_0 such that h, j integrally vanish at (t_0, s_0, y_0) for all y. Then we argue as before, this time with j and $y(t, s)$.

Thus we conclude that $x(t, s)$ cannot depend explicitly on s, and the result follows. □

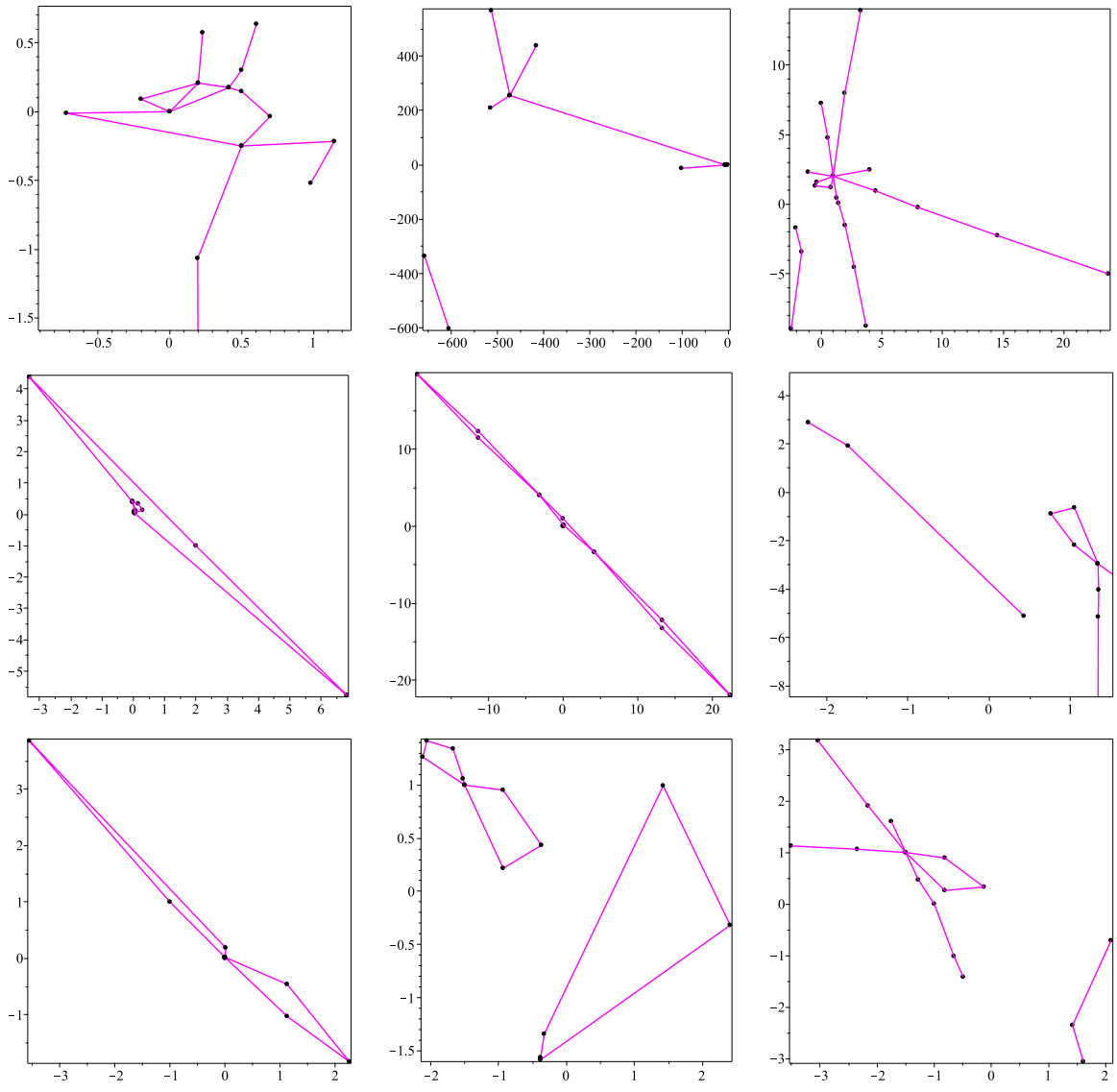

Figure 6: Examples of the 2D algorithm.

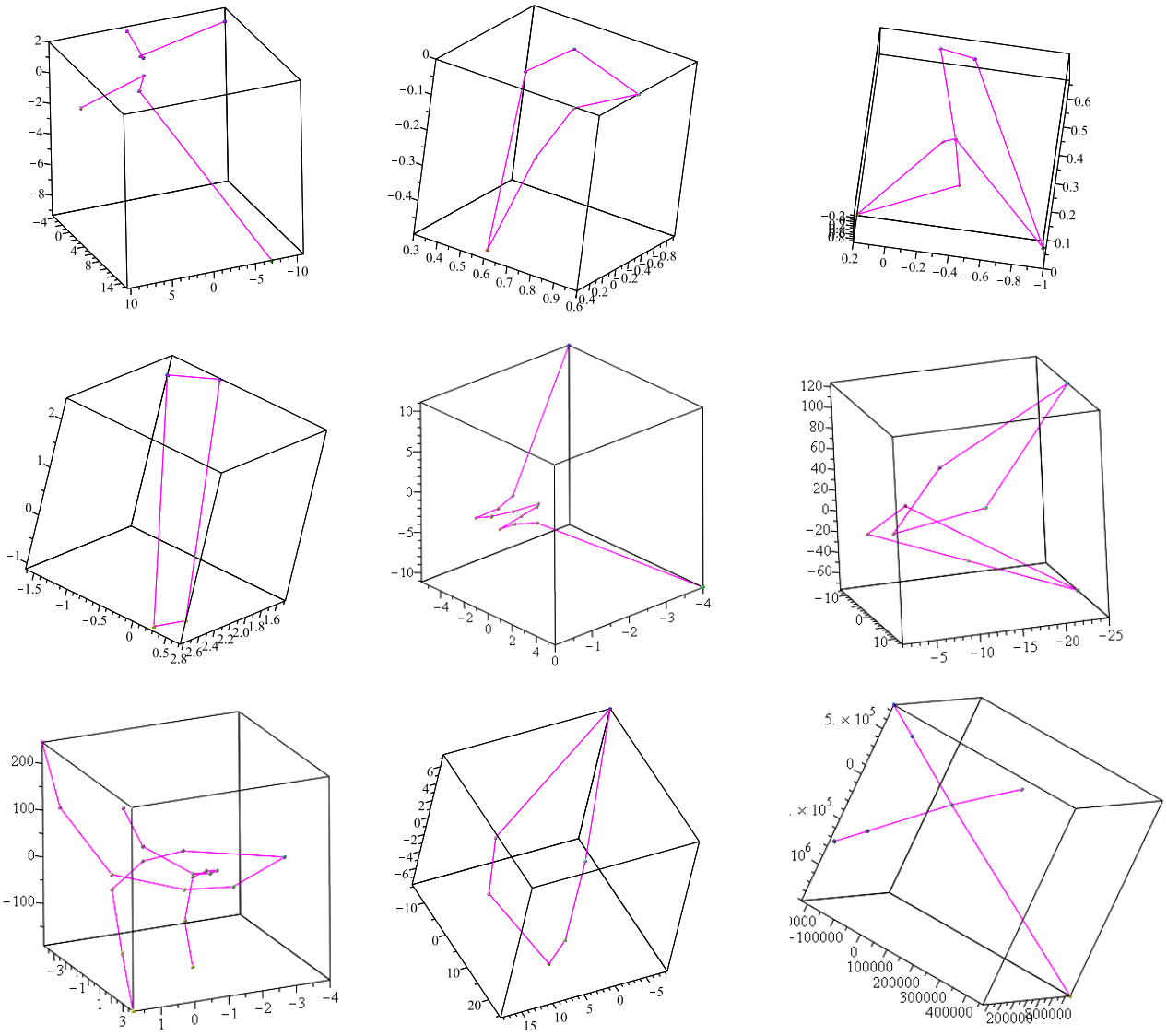

Figure 7: Examples of the 3D algorithm.