Approximate Parametrization of Space Algebraic Curves*

Sonia L. Rueda
Dpto. de Matemática Aplicada
E.T.S. Arquitectura, Universidad Politécnica de Madrid
E-28040 Madrid, Spain
sonialuisa.rueda@upm.es

Juana Sendra
Dpto. de Matemática Aplicada a la I.T. de Telecomunicación
E.U.I.T.Telecomunicación, Universidad Politécnica de Madrid
E-28031 Madrid, Spain
jsendra@euitt.upm.es

J. Rafael Sendra
Dpto. de Matemáticas
Universidad de Alcalá
E-28871 Madrid, Spain
rafael.sendra@uah.es

Abstract

Given a non-rational real space curve and a tolerance $\epsilon > 0$, we present an algorithm to approximately parametrize the curve. The algorithm checks whether a planar projection of the space curve is ϵ-rational and, in the affirmative case, generates a planar parametrization that is lifted to an space parametrization. This output rational space curve is of the same degree as the input curve, both have the same structure at infinity, and the Hausdorff distance between them is always finite.

*Authors supported by the Spanish "Ministerio de Ciencia e Innovación" under the Project MTM2008-04699-C03-01.

Introduction

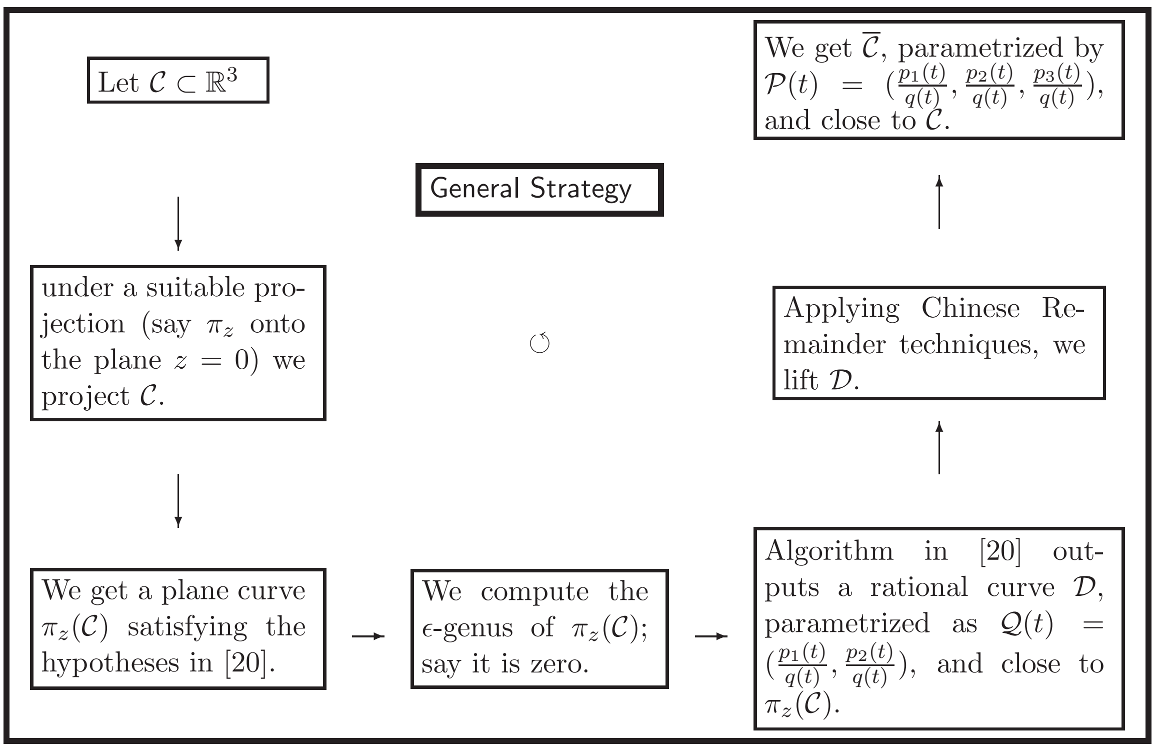
The development of approximate algorithms for algebraic and geometric problems is an active research area (see e.g. [21] and [23]) that focuses on different problems as, for instance, the computation of gcds (see [4], [10], [16]), the factorization of polynomials ([6], [12], [15]), the implicicitization of surfaces ([7], [9]), the parametrization of curves and surfaces ([2], [11], [14], [17], [18], [20]), etc. These approximate algorithms are applicable by themselves since they face symbolic computation to real world problems. Moreover, those of geometric nature are of special interest in the field of CAGD. For instance, providing parametric representations of algebraic geometric objects helps in some CAGD constructions as surface-surface intersection or performance of planar sections (see e.g. Example 5.3. in [20]).

In this context, when using the term "approximate", there is certain risk of ambiguity since it can have a double meaning (see e.g. [24]). Let us clarify what we mean in our case. Here, as in our previous papers [17], [18], [20], with the term "approximate" we do not mean "numerical" but something different (see introduction to [20] for further details): our input is the perturbation of an unknown input; once the perturbation is received we treat it exactly to provide an output that is close (in this sense it is "approximate"), under certain distance, to the theoretical output of the unperturbed unknown input.

More precisely, the problem in this paper is as follows. Let $\mathcal{C}^*$ be a rational real space curve defined as the complex-zero set of a finite set $\mathcal{M} \subset \mathbb{R}[x,y,z]$ of real polynomials; in practice card$(\mathcal{M}) = 2$. Nevertheless, instead of getting $\mathcal{M}$ as input of our problem, we get a new finite subset $\mathcal{F} \subset \mathbb{R}[x,y,z]$ (which is a perturbation of $\mathcal{M}$) of real polynomials that defines a new curve $\mathcal{C}$, obviously different to $\mathcal{C}^*$. Since the genus of a curve is unstable under perturbations, the input curve $\mathcal{C}$ will have positive genus and hence it will not be parametrizable by rational functions. Ideally, the problem would consists in finding the initial curve $\mathcal{C}^*$ or, even better, a rational parametrization of it. However, this goal is unrealistic. Instead, one might require to find a rational parametrization of the closest rational curve to $\mathcal{C}$ under certain distance; say, under the Hausdorff distance. Nevertheless, in this paper we deal with a weaker statement of the problem. Namely, finding a rational parametrization of one rational space curve being close (in comparison to a given tolerance $\epsilon > 0$) to $\mathcal{C}$ under the Hausdorff distance. Our statement, although may not yield to the best output rational curve, generates one good answer. This can be seen as a first step for the harder, more general, and theoretical problem of finding the best (in the sense of closest) rational curve being, our solution, meanwhile ready to be used in applications.

In [17], the authors show how to solve the problem for the particular case of ϵ-monomial plane curves (i.e. plane curves having an ϵ-singularity of maximum ϵ-multiplicity); see also [18] for the case of surfaces. Later, in [20], the problem was solved for the more general case of ϵ-rational plane curves. The current paper is, therefore, the natural continuation of this research since it deals with the next step, namely the case of space curves.

In the unperturbed case, the problem can be solved by birationally projecting the space curve on a plane, checking the genus of the projected curve and, in case of genus zero, parametrizing the plane curve to afterwards inverting the parametrization to a rational parametrization of the input curve (see e.g. [22] for further details). Now, the situation is more complicated. More precisely the strategy (see box below) is as follows.



We assume some conditions on the original space curve $\mathcal{C}$ (see Section 1) such that when it is projected onto a plane we get a curve satisfying the hypotheses required by the algorithm in [20]; let us denote by $\pi_z(\mathcal{C})$ the projected curve, so we are assuming w.l.o.g. in this explanation that projection has been performed on the plane $z = 0$. Then, the algorithm in [20] determines whether $\pi_z(\mathcal{C})$ is ϵ-rational, where ϵ is a fixed given tolerance. If $\pi_z(\mathcal{C})$ is not ϵ-rational one may try a different projection, but here we simply ask the algorithm to terminate since, although in some examples this seems to work, we do not have any theoretical argumentation to ensure when that projection exists. Otherwise, the algorithm in [20] goes ahead and computes a rational parametrization $\mathcal{Q}(t)$ of a plane rational curve $\mathcal{D}$. The last step consists in lifting $\mathcal{D}$ to a rational space curve $\overline{\mathcal{C}}$ being close to $\mathcal{C}$. For this purpose, we first realize that a sufficient condition for the finite Hausdorff distance requirement, between both curves, is given by the structure at infinity of the input curve $\mathcal{C}$. Taking into account this fact, and using a Chinese-remainder type interpolation, we get a rational parametrization of $\overline{\mathcal{C}}$. As a consequence of this process, we get a rational space curve $\overline{\mathcal{C}}$ of the same degree as $\mathcal{C}$, having the same structure at infinity as $\mathcal{C}$, and such that the Hausdorff distance between $\overline{\mathcal{C}}$ and $\mathcal{C}$ is finite.

The structure of the paper is as follows. In Section 1, we introduce the notation that will be used throughout the paper as well as the general assumptions. Moreover, we comment on the reasons for the inclusion of these assumptions, we discuss how to check them algorithmically, and we show that they (the assumptions) are general enough. Section 2 is devoted to the projected curve $\pi_z(\mathcal{C})$ and, more precisely, to prove that under the general assumptions imposed in 1 $\pi_z(\mathcal{C})$ satisfies all requirements in the algorithm in [20]. Section 3 focuses on how to lift the rational plane curve $\mathcal{D}$ (generated by applying the algorithm in [20] to $\pi_z(\mathcal{C})$) to the curve $\overline{\mathcal{C}}$ such that both curves, $\mathcal{C}$ and $\overline{\mathcal{C}}$, have the same structure at infinity; note that π_z is a birational map between $\mathcal{C}$ and $\pi_z(\mathcal{C})$, but we are lifting $\mathcal{D} \neq \pi_z(\mathcal{C})$. In Section 4 we summarize these ideas to derive an algorithm that is illustrated by two examples. In Section 5, we prove that the Hausdorff distance between the input and output curves, of our algorithm, is always finite. For this purpose, we briefly study the asymptotes of space curves. Finally, in Section 6, we approach the study of the Hausdorff distance empirically analyzing the examples in Section 4.

1 General Assumptions and Notation

We consider a computable subfield $\mathbb{K}$ of $\mathbb{R}$, as well as its algebraic closure $\mathbb{F}$; in practice, we may think that $\mathbb{K} = \mathbb{Q}$. We denote by $\mathbb{F}^2$ and $\mathbb{F}^3$ the affine plane an affine space over $\mathbb{F}$, respectively. Similarly, we denote by $\mathbb{P}^2(\mathbb{F})$ and $\mathbb{P}^3(\mathbb{F})$ the projective plane and projective space over $\mathbb{F}$, respectively. Furthermore, if $\mathcal{A} \subset \mathbb{F}^3$ (similarly if $\mathcal{A} \subset \mathbb{F}^2$) we denote by $\mathcal{A}^* \subset \mathbb{F}^3$ its Zariski closure, and by $\mathcal{A}^h \subset \mathbb{P}^3(\mathbb{F})$ the projective closure of $\mathcal{A}^*$. We will consider (x, y, z) as affine coordinates and $(x : y : z : w)$ as projective coordinates. Also, for $\mathcal{A}$ as above, we denote by $\mathcal{A}^\infty$ the intersection of $\mathcal{A}^h$ with the projective plane of equation $w = 0$. In addition, for every polynomial $H \in \mathbb{K}[x, y, z]$ we denote by $H^h(x, y, z, w)$ the homogenization of H.

Our method will be based on the projection of the space curve on a plane. Without loss of generality (see below) we will consider that $z = 0$ is the projection plane. So we introduce the map

$$\pi_z : \mathbb{F}^3 \to \mathbb{F}^2, (x, y, z) \mapsto (x, y),$$

as well as

$$\pi_z^h : \mathbb{P}^3(\mathbb{F}) \setminus \{(0 : 0 : 1 : 0)\} \to \mathbb{P}^2(\mathbb{F}), (x : y : z : w) \mapsto (x : y : w).$$

Our main object of study will be an irreducible (over $\mathbb{F}$) affine real (non-planar) space curve $\mathcal{C} \subset \mathbb{F}^3$. Although, in practice, in most cases, $\mathcal{C}$ will be given by two generators, we present the results for the general case where a finite set of generators is provided.

Therefore, we assume that $\mathcal{C}$ is given as the zero-set (over $\mathbb{F}$) of a finite set of real polynomials $\mathcal{F} = \{F_1, \ldots, F_s\} \subset \mathbb{K}[x, y, z]$, $s \geq 2$. ϵ will be the tolerance and we assume that $0 < \epsilon < 1$. In addition, we assume the following:

General Assumptions

1. The cardinality of $\mathcal{C}^\infty$ is $\deg(\mathcal{C})$.
2. $\pi_z : \mathcal{C} \to \pi_z(\mathcal{C})^*$ is birational and $\deg(\mathcal{C}) = \deg(\pi_z(\mathcal{C})^*)$.
3. $(1 : 0 : \lambda : 0), (0 : 1 : \mu : 0), (0 : 0 : 1 : 0) \notin \mathcal{C}^\infty$ for any $\lambda, \mu \in \mathbb{F}$.
4. If $(1 : \lambda : \mu : 0), (1 : \lambda : \mu^* : 0) \in \mathcal{C}^\infty$ then $\mu = \mu^*$.
5. The coefficient of F_1 in $z^{\mathrm{tdeg}(F_1)}$ is a non-zero constant; where tdeg denotes the total degree of F_1.

We briefly comment on the reasons for the inclusion of the above assumptions, and we describe how to check them algorithmically. The condition on irreducibility is natural since rational curves are irreducible varieties. In any case, one can always consider the irreducible decomposition of the input to apply the results to each of the irreducible components. The assumption on the reality of the curve is included because of the nature of the problem, but the theory can be similarly developed for the case of complex non-real curves. The exclusion of planar curves is to simplify the exposition. Note that this is not a loss of generality, since one can always apply the algorithm in [20].

Concerning the general assumptions, condition (1) will play a fundamental role in the error analysis, and it will be used to ensure that the Hausdorff distance between output and input is always finite. The birational requirement in condition (2) is introduced to reduce the problem to a plane curve after projection, and the degree fact will be used, in combination with (3) and (4), to ensure that $\pi_z(\mathcal{C})^*$ has as many different points at infinity as its degree; condition that is required by the algorithm in [20]. Conditions (3) and (4) are related to the projection π_z. On one hand, $(1 : 0 : \lambda : 0), (0 : 1 : \mu : 0) \notin \mathcal{C}^\infty$, for any $\lambda, \mu \in \mathbb{F}$, ensures that $(1 : 0 : 0), (0 : 1 : 0) \notin \pi_z(\mathcal{C})^\infty$ which is a requirement for the algorithm in [20] to be applied to $\pi_z(\mathcal{C})^*$. On the other, $(0 : 0 : 1 : 0) \notin \mathcal{C}^\infty$ guarantees that π_z^h is well defined on $\mathcal{C}^h$. In addition, conditions (3)-(4) ensure that π_z^h is injective on $\mathcal{C}^\infty$. Condition (5) is also introduced to guarantee that $\pi_z(\mathcal{C})^*$ satisfies the hypotheses in [20] (see Theorem 2.4). Note that this property can always be achieved by means of a suitable orthogonal affine change of coordinates, and hence preserving distances.

Taking into account that, in practice, $\mathcal{C}$ is expected to come from the perturbation of a rational space real curve, in general, all above conditions will hold. Nevertheless, let us discuss how to decide algorithmically whether a given input satisfies them. Checking the irreducibility of $\mathcal{C}$ can be approached by checking whether the corresponding ideal is prime (see, for instance, Section 4.5 in [8] or [5]). In order to check the reality, one can apply cylindrical algebraic decomposition techniques to decide the existence of real regular points (see e.g. [3]). The non-planarity of $\mathcal{C}$ can be deduced from a Gröbner basis of $\mathcal{F}$. Let us now deal with the general assumptions. One can compute $\mathcal{C}^h$ by homogenizing a Gröbner basis of $\mathcal{F}$, w.r.t. a graded order (see e.g. page 382 in [8]). The degree of $\mathcal{C}$ can de determined by counting the number of intersections of $\mathcal{C}$ with a generic plane; in fact a randomly chosen plane might be enough. So, (1) is also checkable. Also, (3) and (4) are checkable. Condition (2) can be analyzed by direct application of elimination theory techniques. Condition (5) is trivially checkable.

In the previous description, we have considered that $z = 0$ is the projection plane. Indeed, conditions (3)-(5) depend on this fact. So, if any of these conditions fails we might either consider a suitable orthogonal affine change of coordinates or choose another projection plane. Also, if (2) fails we need to find a different projection plane. We recall that, for almost every plane, the corresponding projection is birational over $\mathcal{C}$ and that for almost every plane the number of intersection points of the plane with $\mathcal{C}$ is $\deg(\mathcal{C})$. Therefore, the combination of these two facts with Lemma 1.1 ensures that condition (2) must be achieved by taking the projection plane randomly.

Lemma 1.1. *Let $\Pi \subset \mathbb{F}^3$ be a plane such that $\mathrm{card}(\mathcal{C} \cap \Pi) = \deg(\mathcal{C})$, let u be a (non-zero) parallel vector to Π and non-parallel to the vectors in $\{P - Q \mid P, Q \in \mathcal{C} \cap \Pi,\ P \neq Q\}$, and let Π^u be any plane orthogonal to u. Then, $\deg(\pi_{\Pi^u}(\mathcal{C})^*) = \deg(\mathcal{C})$, where π_{Π^u} is the projection map from $\mathbb{F}^3$ onto Π^u.*

Proof. Let $d = \deg(\mathcal{C})$ and $\mathcal{C} \cap \Pi = \{P_1, \ldots, P_d\}$, and let L be the line $\Pi \cap \Pi^u$. By construction, $\{\pi_{\Pi^u}(P_i)\}_{i=1,\ldots,d} \subset \pi_{\Pi^u}(\mathcal{C})^* \cap L$. Since u is not parallel to $P_i - P_j$, with $i \neq j$, then $\mathrm{card}(\{\pi_{\Pi^u}(P_i)\}_{i=1,\ldots,d}) = d$. Therefore, $\deg(\mathcal{C}) \leq \deg(\pi_{\Pi^u}(\mathcal{C})^*)$. Now, let L' be a line in Π^u such that $L' \cap (\pi_{\Pi^u}(\mathcal{C})^* \setminus \pi_{\Pi^u}(\mathcal{C})) = \emptyset$ and such that $\mathrm{card}(L' \cap \pi_{\Pi^u}(\mathcal{C})^*) = \deg(\pi_{\Pi^u}(\mathcal{C})^*)$; note that almost all lines in Π^u satisfy this property. Let $L' \cap \pi_{\Pi^u}(\mathcal{C})^* = \{Q_1, \ldots, Q_{d'}\}$ and let Π' be the plane containing L' and being parallel to u; note that u is normal to Π^u, and hence L' is not parallel to u. Because of the construction $\pi_{\Pi^u}^{-1}(Q_i) \cap \mathcal{C} \neq \emptyset$ and it is contained in Π'. Therefore, $\cup_{i=1}^{d'} \pi_{\Pi^u}^{-1}(Q_i) \cap \mathcal{C} \cap \Pi'$ has cardinality at least d', and hence $\deg(\pi_{\Pi^u}(\mathcal{C})^*) = d' \leq \deg(\mathcal{C})$. □

2 The Projected Curve

In this section, we analyze the basic properties of the projected curve $\pi_z(\mathcal{C})^*$. In particular, we show that it satisfies the hypotheses in [20]. We recall that, since π_z is birational and $\mathcal{C}$ is irreducible, $\pi_z(\mathcal{C})^*$ is irreducible. We start with a technical lemma on Gröbner bases

Lemma 2.1. *Let $\mathbb{L} \subset \mathbb{F}$ be a field and $G_1, \ldots, G_m \in \mathbb{L}[x_1, \ldots, x_n]$ be such that $\deg_{x_n}(G_1) = \mathrm{tdeg}(G_1) > 0$; where tdeg denotes the total degree. Let $\{H_1, \ldots, H_r\}$ be a Gröbner basis of $(G_1, \ldots, G_m)$ w.r.t. the graded lex order with $x_1 < \cdots < x_n$.*

Then, there exists $i \in \{1, \ldots, r\}$ such that $\deg_{x_n}(H_i) = \operatorname{tdeg}(H_i)$*. Moreover, if the variety defined by* $\{G_1, \ldots, G_m\}$ *over* $\mathbb{F}$ *is not empty then* $\deg_{x_n}(H_i) = \operatorname{tdeg}(H_i) > 0$*.*

Proof. Let $\ell = \deg_{x_n}(G_1)$. Since $\ell = \operatorname{tdeg}(G_1)$, because of the ordering, the leading term of G_1 is x_n^ℓ. Now, by Exercise 5, page 78, [8], there exists $i \in \{1, \ldots, r\}$ such that the leading term of F_i divides x_n^ℓ. Finally, because of the ordering, $\operatorname{tdeg}(H_i) = \deg_{x_n}(H_i)$. Now, if the variety of $\{G_1, \ldots, G_m)\}$ is empty, we assume that the Gröbner basis is normal (this does not affect to the previous reasoning). By Theorem 8.4.3 in [25], H_i is not constant. So $\operatorname{tdeg}(H_i) > 0$. □

The next lemma shows how generalized resultants can be used to compute the projection.

Lemma 2.2. *Let*

$$F_\Delta(x, y, \Delta) = \begin{cases} F_2 + \Delta F_3 + \cdots + \Delta^{s-2} F_s & \text{if } s > 2 \\ F_2 & \text{if } s = 2 \end{cases},$$

where Δ is a new variable, and let F_Δ^h be the homogenization of $F_\Delta(x, y, w, \Delta)$ as a polynomial in $\mathbb{K}[\Delta][x, y, z]$. Let

$$R = \operatorname{Res}_z(F_1, F_\Delta) = \sum_{j=0}^{m} \alpha_j(x, y)\Delta^j, \;\; S = \operatorname{Res}_z(F_1^h, F_\Delta^h) = \sum_{i=0}^{m'} \beta_i(x, y, w)\Delta^i.$$

It holds that

1. *$\pi_z(\mathcal{C})^*$ is the affine plane curve defined by $\gcd(\alpha_0, \ldots, \alpha_m)$, and $m = m'$.*
2. *If $\mathcal{F}$ is a Gröbner basis, w.r.t. the graded lex order with $x < y < z$, then $\pi_z(\mathcal{C})^h$ is the projective plane curve defined by $\gcd(\beta_0, \ldots, \beta_m)$.*

Proof. (1) We first prove that $\pi_z(\mathcal{C})^*$ is the variety defined by $\{\alpha_0, \ldots, \alpha_m\}$. Indeed, let $(a, b) \in \pi_z(\mathcal{C})$. Then, there exists $c \in \mathbb{F}$ such that $P = (a, b, c) \in \mathcal{C}$. So, $F_1(P) = 0, F_\Delta(P, \Delta) = 0$. Thus, $R(a, b, \Delta) = 0$, and hence $\alpha_0(a, b) = \cdots = \alpha_m(a, b) = 0$. Conversely, let $\alpha_0, \ldots, \alpha_m$ vanish at (a, b). Then $R(a, b, \Delta) = 0$. Now, since $\deg_z(F_1) = \operatorname{tdeg}(F_1)$, there exists c in the algebraic closure of $\mathbb{F}(\Delta)$ such that $F_1(a, b, c) = 0, F_\Delta(a, b, c, \Delta) = 0$. Since c is a root of $F_1(a, b, z) \in \mathbb{F}[z]$ then $c \in \mathbb{F}$. Therefore, from $F_\Delta(a, b, c, \Delta) = 0$, we get that $F_2(a, b, c) = \cdots = F_s(a, b, c) = 0$. So, $(a, b, c) \in \mathcal{C}$ and $(a, b) \in \pi_z(\mathcal{C})$.

Let $\alpha = \gcd(\alpha_0, \ldots, \alpha_m)$ and $\overline{\alpha}_i$ be such that $\alpha_i = \overline{\alpha}_i \alpha$. Let $\mathcal{V}$ and $\mathcal{W}$ be the varieties defined by α and $\{\overline{\alpha}_0, \ldots, \overline{\alpha}_m\}$, respectively. Then, $\pi_z(\mathcal{C})^* = \mathcal{V} \cup \mathcal{W}$. Since $\mathcal{C}$ is irreducible and π_z birational, we have that $\pi_z(\mathcal{C})$ is an irreducible curve. So, $\mathcal{V}$ is 1-dimensional and $\mathcal{W}$ is either empty or 0-dimensional. In any case, because of the irreducibility, $\mathcal{W} \subset \mathcal{V}$. So $\pi_z(\mathcal{C})^* = \mathcal{V}$.

Finally, let us see that $m = m'$. We assume w.l.o.g. that all β_i are non-zero. Since $\deg_z(F_1) = \deg_z(F_1^h)$, by Lemma 4.3.1. in [25], we get that $R(x, y, \Delta) = S(x, y, 1, \Delta)$, up to multiplication by a non-zero constant. Moreover, S is homogeneous as a polynomial in $\mathbb{F}[\Delta][x,y,w]$. Thus, β_i are homogeneous (of th e same degree). Therefore, $\beta_i(x,y,1)$ does not vanish. Thus, $m=\deg_\Delta(R)=\deg_\Delta(S(x,y,1,\Delta))=\deg_\Delta(S)=m'$.

(2) We first prove that w does not divide S. Let $S=wM(x,y,w,\Delta)$. Then, for all $(a,b)\in\mathbb{F}^2$, since $\deg(F_1^h)=\deg_z(F_1^h)$, there exists $c\in\mathbb{F}$ (in principle, c is in the algebraic closure of $\mathbb{F}(\Delta)$ but, reasoning as above, we get that $c\in\mathbb{F}$) such that $F_1^h(a,b,c,0)=F_\Delta^h(a,b,c,0,\Delta)=0$. Therefore, since $c\in\mathbb{F}$, $F_i^h(a,b,c,0)=0, i=1,\ldots,s$; let us call $\rho(a,b)$ the corresponding c associated to (a,b). Then, the infinitely many points $\{(1:n:\rho(1,n):0)\}_{n\in\mathbb{N}}$ are included in the intersection of $\mathcal{C}^h$ with the plane $w=0$, which is a contradiction; note that since $\mathcal{F}$ is a Gröbner basis w.r.t. a graded order then $\{F_i^h\mid i=1,\ldots,s\}$ generates $\mathcal{C}^h$.

From $R(x,y,\Delta)=S(x,y,1,\Delta)$ we get that $\alpha_j(x,y)=\beta_j(x,y,1)$. Therefore, since β_j is homogeneous, $\alpha_j^h w^{n_j}=\beta_j$, for some $n_j\in\mathbb{N}$. Moreover, since w does not divide S, there exists $i_0\in\{0,\ldots,m\}$ such that $\alpha_{i_0}^h=\beta_{i_0}$ and $\gcd(\alpha_{i_0}^h,w)=1$.

Let $\alpha=\gcd(\alpha_0,\ldots,\alpha_m)$ and $\gamma=\gcd(\alpha_0^h,\ldots,\alpha_m^h)$. We see that $\alpha^h=\gamma$. Let $\alpha_i=\alpha\overline{\alpha}_i$. Then, $\alpha_i^h=\alpha^h\overline{\alpha}_i^h$. So, α^h divides γ. Conversely, let $\alpha_i^h=\gamma\tilde{\alpha}_i$. Then, $\gamma(x,y,1)$ divides $\alpha_i^h(x,y,1)=\alpha_i$. Therefore, $\gamma(x,y,1)$ divides α. In addition, since α^h divides γ, α divides $\gamma(x,y,1)$. Hence, up to multiplication by non-zero constants, $\alpha=\gamma(x,y,1)$. Therefore, since by construction w does not divide γ, we get that $\alpha^h=\gamma$.

Finally, it remains to prove that $\gamma=\gcd(\beta_0,\ldots,\beta_m)$. We know that $\gcd(\beta_0,\ldots,\beta_m)=\gcd(\alpha_0^h w^{n_0},\ldots,\alpha_m^h w^{n_m})$. Let $a=\gcd(\alpha_0^h w^{n_0},\ldots,\alpha_m^h w^{n_m})$. Clearly γ divides a. Conversely, a divides $\alpha_{i_0}^h$ (see above). Since $\gcd(\alpha_{i_0}^h,w)=1$, then $\gcd(a,w)=1$. Therefore, a must divide all α_j^h. Hence, a divides γ.

Summarizing $\gcd(\alpha_0,\ldots,\alpha_m)^h=\gcd(\alpha_0^h,\ldots,\alpha_m^h)=\gcd(\alpha_0^h w^{n_0},\ldots,\alpha_m^h w^{n_m})=\gcd(\beta_0,\ldots,\beta_m)$. □

Remark 2.3. We observe that in the proof of Lemma 2.2, from all the hypotheses imposed in Section 1, we have only used the following: general assumption (5) is used in both (1) and (2). The fact that $\mathcal{C}$ has dimension 1 and that is irreducible is used in (1), jointly with the fact that π_z is finite. Finally, in (2), we use that $\mathcal{C}^h$ intersects the plane $w=0$ in finitely many points.

We finish the section by stating the main properties of the projected curve.

Theorem 2.4. *It holds that*

1. $\pi_z^h(\mathcal{C}^\infty)=\pi_z(\mathcal{C})^\infty$.
2. $\mathrm{card}(\pi_z(\mathcal{C})^\infty)=\deg(\pi_z(\mathcal{C})^*)$.
3. $(1:0:0),(0:1:0)\notin\pi_z(\mathcal{C})^\infty$.

Proof. (1) Because of Lemma 2.1, we can assume w.l.o.g. that $\{F_1, \ldots, F_s\}$ is a Gröbner basis w.r.t the graded lex order with $x < y < z$, and that $\deg_z(F_1) = \mathrm{tdeg}(F_1)$. Also, let $F_\Delta, F_\Delta^h, S, R, \alpha_i, \beta_i$ be as in Lemma 2.2, and $\alpha = \gcd(\alpha_0, \ldots, \alpha_m)$.

Note that $\mathcal{C}^\infty$ is the zero set in $\mathbb{P}^3(\mathbb{F})$ of $\{F_1^h(x, y, z, 0), \ldots, F_s^h(x, y, z, 0)\}$. So, since $\mathcal{C}^\infty$ is zero-dimensional, then $\gcd(F_1^h(x, y, z, 0), \ldots, F_s^h(x, y, z, 0)) = 1$. In addition, by Lemma 2.2, $\pi_z(\mathcal{C})^\infty$ is the zero set in $\mathbb{P}^2(\mathbb{F})$ of $\alpha^h(x, y, 0)$.

Now, let $(a : b : c : 0) \in \mathcal{C}^\infty$. Then, $F_1^h(a, b, c, 0) = F_\Delta^h(a, b, c, 0) = 0$. Therefore, $S(a, b, 0, \Delta) = 0$. Thus, $\beta_i(a, b, 0) = 0$. By Lemma 2.2, we know that $\alpha^h(x, y, w) = \gcd(\beta_0, \ldots, \beta_m)$. So, $\beta_i = \alpha^h \overline{\beta}_i$. Let us assume that $\alpha^h(a, b, 0) \neq 0$ (i.e. that $(a : b : 0) \notin \pi_z(\mathcal{C})^\infty$). By general assumption (3), a, b cannot be both zero. We assume w.l.o.g. that $a = 1$. Then, $\overline{\beta}_i(1, b, 0) = 0$ for all i. We now consider the polynomials $H_i(y, z, w) = F_i^h(1, y, z, w)$ as well as the affine variety $\mathcal{D}$ defined by them. Note that, since $(1 : b : c : 0) \in \mathcal{C}^h$, $(b, c, 0) \in \mathcal{D} \neq \emptyset$. Moreover, since $\mathcal{C}$ is irreducible, $\mathcal{D}$ is an irreducible curve. Furthermore, $\mathrm{tdeg}(H_1) = \deg_z(H_1) = \deg_z(F_1) > 0$. Furthermore, since $\mathcal{C}$ is not planar, $\mathcal{D}$ is not a line perpendicular to the plane $z = 0$, so π_z is finite over $\mathcal{D}$. Also, since $\mathcal{C}$ is not planar, $\mathcal{D}^h$ intersection $x = 0$ has only finitely many points. Furthermore, because of Lemma 2.1, we can assume w.l.o.g. that $\{H_1, \ldots, H_s\}$ is a Gröbner basis w.r.t the graded lex order with $w < y < z$, and that $\deg_z(H_1) = \mathrm{tdeg}(H_1)$. Thus, $\mathcal{D}$ satisfies the hypotheses of Lemma 2.2 (see Remark 2.3). Let H_Δ as in Lemma 2.2, let $T(y, w, \Delta) = \mathrm{Res}_z(H_1, H_\Delta)$, and let $S, \alpha_i, \alpha^h, \beta_i$ be as in the proof of Lemma 2.2. Reasoning as in the proof Lemma 2.2, we get that $\deg_\Delta(T) = \deg_\Delta(S)$ and that, if $T = \sum_{i=0}^m \rho_i \Delta^i$ then $\rho_i(y, w) = \beta_i(1, y, w)$. Moreover, by Lemma 2.2, we get that $\pi_z(\mathcal{D})^*$ is defined by $\rho = \gcd(\rho_0, \ldots, \rho_m)$; note that $\pi_z(\mathcal{D})^*$ is irreducible, and hence ρ is an irreducible polynomial.

From $\rho_i(y, w) = \beta_i(1, y, w) = \alpha^h(1, y, w)\overline{\beta_i}(1, y, w)$ we get that $\alpha^h(1, y, w)$ divides $\rho(y, w)$. Also, since $\mathcal{C}$ is not planar, $\pi_z(\mathcal{C})^*$ is not a line, and hence $\alpha^h(1, y, w)$ is not constant. Thus, since ρ is irreducible, we get that, up to multiplication by non-zero constants, $\rho(y, w) = \alpha^h(1, y, w)$. Finally, from $(b, c, 0) \in \mathcal{D}$, we get that $\rho(b, 0) = \alpha^h(1, b, 0) = 0$, which is a contradiction. This proves that $\pi_z^h(\mathcal{C}^\infty) \subset \pi_z(\mathcal{C})^\infty$.

On the other hand, because of general assumptions (3) and (4) one has that π_z^h is injective over $\mathcal{C}^\infty$, and hence we get that $\mathrm{card}(\pi_z^h(\mathcal{C}^\infty)) = \mathrm{card}(\mathcal{C}^\infty)$. Then, from general assumptions (1) and (2), we get that $\pi_z^h(\mathcal{C}^\infty) = \pi_z(\mathcal{C})^\infty$.

(2) Because of general assumptions (3) and (4), $\mathrm{card}(\mathcal{C}^\infty) = \mathrm{card}(\pi_z^h(\mathcal{C}^\infty))$ and, by general assumptions (1) and (2), $\mathrm{card}(\mathcal{C}^\infty) = \deg(\mathcal{C}) = \deg(\pi_z(\mathcal{C})^*)$. Now the proof ends by applying statement (1) in this theorem.

(3) It follows from general assumption (3) and statement (1) in this theorem. □

3 The Lifted Curve

In Theorem 2.4 we have seen that, under the assumptions introduced in Section 1, $\pi_z(\mathcal{C})^*$ satisfies the hypotheses required by the parametrization algorithm in [20]. In this situation, we apply algorithm in [20] to $\pi_z(\mathcal{C})^*$. If $\pi_z(\mathcal{C})^*$ is not ϵ-rational, then we can not use $\pi_z(\mathcal{C})^*$ to parametrize $\mathcal{C}$ approximately by this method. However, it might be that there exists another projection such that the projected curve is ϵ-rational and hence the method applicable to this other projection. Nevertheless, we have not researched in this direction leaving this as a future research line. So, let us suppose that $\pi_z(\mathcal{C})^*$ is ϵ-rational, and let

$$\mathcal{Q}(t) = \left(\frac{p_1(t)}{q(t)}, \frac{p_2(t)}{q(t)}\right)$$

be the parametrization output by the algorithm in [20]. Let $\mathcal{D}$ be the rational plane curve parametrized by $\mathcal{Q}(t)$. We want to lift $\mathcal{D}$ from $\mathbb{F}^2$ to a rational curve $\overline{\mathcal{C}}$ in $\mathbb{F}^3$. For this purpose, in order to guarantee that the Hausdorff distance between $\mathcal{C}$ and $\overline{\mathcal{C}}$ is finite (see Corollary 5.5), we will associate to $\mathcal{D}$ a rational curve $\overline{\mathcal{C}}$ in $\mathbb{F}^3$ such that $\pi_z(\overline{\mathcal{C}}) = \mathcal{D}$, $\deg(\overline{\mathcal{C}}) = \deg(\mathcal{C})$ and $\mathcal{C}^\infty = \overline{\mathcal{C}}^\infty$.

We know that $\pi_z(\mathcal{C})^*$ and $\mathcal{D}$ have the same degree and the same structure at infinity (see Theorem 4.5. in [20]). Thus, by Theorem 2.4, $\mathcal{D}^\infty = \pi_z^h(\mathcal{C}^\infty)$. In addition, it also holds that $\deg(p_i) \leq \deg(q) = \deg(\mathcal{D})$ (see proof of Lemma 4.2 in [20]). Moreover, by construction, $\gcd(p_i, q) = 1$ (see Step 10 in the algorithm in [20]). Furthermore, $(p_1(t) : p_2(t) : q(t))$ reaches all points in $\mathcal{D}^\infty$ (see proof of Theorem 4.5. in [20]). Therefore, since $\mathrm{card}(\mathcal{D}^\infty) = \deg(\mathcal{D})$ (see Theorem 2.4 and note that $\mathcal{D}^\infty = \pi_z^h(\mathcal{C}^\infty)$), $q(t)$ is square-free. Thus, if $\{\xi_1, \ldots, \xi_d\}$ are the roots of $q(t)$,

$$\mathcal{D}^\infty = \left\{\left(1 : \frac{p_2(\xi_i)}{p_1(\xi_i)} : 0\right)\right\}_{i=1,\ldots,d},$$

because of general assumption (4), for every i there exists a unique $\chi_i \in \mathbb{F}$ such that

$$\mathcal{C}^\infty = \left\{\left(1 : \frac{p_2(\xi_i)}{p_1(\xi_i)} : \chi_i : 0\right)\right\}_{i=1,\ldots,d}.$$

Note that, if $\{G_1, \ldots, G_m\}$ is a Gröbner basis of $\{F_1, \ldots, F_s\}$ w.r.t. the graded lex order with $x < y < z$, then χ_i is the root of

$$\gcd\left(G_1^h\left(1, \frac{p_2(\xi_i)}{p_1(\xi_i)}, z, 0\right), \ldots, G_m^h\left(1, \frac{p_2(\xi_i)}{p_1(\xi_i)}, z, 0\right)\right).$$

Let $p_3(t)$ be the interpolating polynomial such that $p_3(\xi_i) = p_1(\xi_i)\chi_i$, for $i = 1, \ldots, d$; recall that $q(t)$ is square-free. We then define $\overline{\mathcal{C}}$ as the rational curve

$$\mathcal{P}(t) = \left(\frac{p_1(t)}{q(t)}, \frac{p_2(t)}{q(t)}, \frac{p_3(t)}{q(t)}\right).$$

Note that $\gcd(p_1, p_2, p_3, q) = 1$, q is square-free, $\deg(p_1), \deg(p_2) \leq \deg(q)$ and $\deg(p_3) < \deg(q)$.

Taking into account the previous reasonings, we have the following theorem.

Theorem 3.1. *The lifted curve $\overline{\mathcal{C}}$, defined as above, satisfies that*

1. $\overline{\mathcal{C}}$ *is rational.*
2. $\mathcal{C}^\infty = \overline{\mathcal{C}}^\infty$.
3. $\deg(\mathcal{C}) = \deg(\overline{\mathcal{C}})$.
4. $\pi_z(\overline{\mathcal{C}})^* = \mathcal{D}$.

We finish this section explaining how to compute $\overline{\mathcal{C}}$ (i.e. the polynomial $p_3(t)$) without having to explicitly compute the roots of $q(t)$. The idea is to adapt the Chinese Remainder interpolation techniques. Let $\{G_1, \ldots, G_m\}$ be as above, and let $q(t) = \prod_{j=1}^{\ell} q_j(t)$ be an irreducible factorization of $q(t)$ over $\mathbb{K}$. Now, for each q_j we consider the field $\mathbb{L} = \mathbb{K}(\mu)$, where μ is the algebraic element over $\mathbb{K}$ defined by $q_j(t)$, as well as the polynomial ring $\mathbb{L}[z]$. Let

$$D_j(z) = \gcd_{\mathbb{L}[z]}\left(G_1^h\left(1, \frac{p_2(\mu)}{p_1(\mu)}, z, 0\right), \ldots, G_m^h\left(1, \frac{p_2(\mu)}{p_1(\mu)}, z, 0\right)\right),$$

where the gcd is taken in the Euclidean domain $\mathbb{L}[z]$. Because of the previous reasoning, we know that $D_j(z)$ can be expressed as

$$D_j(z) = (a_j(\mu)z - b_j(\mu))^u \in \mathbb{L}[z],$$

where $u \in \mathbb{N}$. Let $c_j(\mu)$ be the polynomial expression of $b_j(\mu)a_j(\mu)^{-1}p_1(\mu)$ as an element in $\mathbb{L}$. On the other hand, for $i \neq j$, $\gcd(q_i, q_j) = 1$. So, there exist $u_{i,j}, u_{j,i} \in \mathbb{K}[t]$ such that $u_{i,j}q_i + u_{j,i}q_j = 1$. We introduce the following polynomial

$$A(t) = \begin{cases} c_1(t)\prod_{i=2}^{\ell} u_{i,1}(t)q_i(t) + \cdots + c_\ell(t)\prod_{i=1}^{\ell-1} u_{i,\ell}(t)q_i(t) & \text{if } \ell > 1 \\ c_1(t) & \text{if } \ell = 1. \end{cases}$$

Then, we have the following result.

Lemma 3.2. *$p_3(t)$ is the remainder of the division of $A(t)$ by $q(t)$.*

Proof. If $\ell = 1$ the result is trivial. Let $\ell > 1$ and let $R(t), Q(t)$ be the remainder and quotient of the division of $A(t)$ by $q(t)$, respectively. Clearly $\deg(R) < \deg(q)$. Now, let ξ_i be a root of $q(t)$; say w.l.o.g. that ξ_i is a root of $q_1(t)$. Then, by construction, $c_1(\xi_i) = \chi_i p_1(\xi_i)$. Therefore,

$$R(\xi_i) = A(\xi_i) - q(\xi_i)Q(\xi_i) = A(\xi_i) = c_1(\xi_i)u_{2,1}(\xi_i)q_2(\xi_i)\cdots u_{\ell,1}(\xi_i)q_\ell(\xi_i).$$

However, for $k \neq 1$, $u_{k,1}(\xi_i)q_k(\xi_i) = 1 - u_{1,k}(\xi_i)q_1(\xi_i) = 1$. So, $R(\xi_i) = c_1(\xi_i) = \chi_i p_1(\xi_i) = p_3(\xi_i)$. □

4 Algorithm and Examples

In this section we collect all the ideas developed in the previous sections to derive the approximate parametrization algorithm, and we illustrate it by a couple of examples. For this purpose, we assume that we are given a tolerance $0 < \epsilon < 1$ as well as an space curve $\mathcal{C}$ satisfying all the hypotheses imposed in Section 1. Then the algorithm is as follows

Algorithm

1. Compute the defining polynomial of $\pi_z(\mathcal{C})^*$ (apply e.g. Lemma 2.2).
2. Apply to $\pi_z(\mathcal{C})^*$ the parametrization algorithm in [20]. If the plane curve is not ϵ-rational exit returning no parametrization else let $(\frac{p_1(t)}{q(t)}, \frac{p_2(t)}{q(t)})$ be the output parametrization.
3. Apply Lemma 3.2 to determine $p_3(t)$.
4. Return $(\frac{p_1(t)}{q(t)}, \frac{p_2(t)}{q(t)}, \frac{p_3(t)}{q(t)})$.

Remark 4.1. Note that, because of Theorem 3.1, it holds that the rational curve output by the algorithm has the same degree and structure at infinity as the input curve. Also, as already mentioned in Section 3, if in step 2 we do not get ϵ-rationality, it does not imply that under another projection one could not get an ϵ-rational curve. However we can not guarantee theoretically when such a projection exists.

In the following examples, the polynomial f defining $\pi_z(\mathcal{C})^*$ and the parametrizations $\mathcal{Q}(t)$ of $\mathcal{D}$, and $\mathcal{P}(t)$ of $\overline{\mathcal{C}}$, are expressed with 10-digits floating point coefficients, but the executions have been performed with exact arithmetic; the precise data can be found in http://www2.uah.es/rsendra/datos.html.

Example 4.2. Let $\mathcal{C}$ be the space curve defined by the polynomials

$$\begin{aligned} F_1 = & -\frac{718945312497}{100}\,x + \frac{698623125001}{100}\,y - 671015625\,z + 13865578693\,z\,y \\ & - 12118499950\,z\,x + 24392628607\,x\,y - 18401807886\,y^2 - 1311877532\,z^2 \\ F_2 = & -\frac{431020499999}{25}\,x + \frac{1675347948801}{100}\,y - 1609143200\,z + 4365980240\,z\,y \\ & - 401217042\,z\,x - 24936051360\,y^2 - 683547137\,z^2 + 24392628607\,x^2 \end{aligned}$$

and let $\epsilon = \frac{1}{100}$. One can check that $\mathcal{C}$ satisfies all the hypotheses imposed in Section 1. Moreover, $\deg(\mathcal{C}) = 4$. The projected curve $\pi_z(\mathcal{C})^*$ is defined by the polynomial (see Fig. 4.2)

$f(x,y) = 5.192147942 \cdot 10^{29}\, xy - 2.214420657 \cdot 10^{28}\, y - 5.059350678 \cdot 10^{28}\, x - 2.636990684 \cdot 10^{29}\, x^2 - 3.506554787 \cdot 10^{42}\, x^2y + 2.001041491 \cdot 10^{42}\, y^4 - 1.375243688 \cdot 10^{42}\, y^3 + 1.181135404 \cdot 10^{42}\, x^3 + 3.822854018 \cdot 10^{42}\, xy^2 - 2.315025392 \cdot 10^{40}\, y^2 - 2.990857566 \cdot 10^{42}\, xy^3 - 1.221346211 \cdot 10^{42}\, x^2y^2 + 3.915698981 \cdot 10^{42}\, x^3y - 1.812915331 \cdot 10^{42}\, x^4.$

Note that $\deg(\pi_z(\mathcal{C})^*) = 4$. Applying the approximate parametrization algorithm for plane curves in [20] we get that $\pi_z(\mathcal{C})^*$ is ϵ-rational. Furthermore the algorithm outputs the parametrization $\mathcal{Q}(t) = (\frac{p_1(t)}{q(t)}, \frac{p_2(t)}{q(t)})$

$$\left(\frac{-0.4173571408 + 1.171283433\, t - 0.8477221239\, t^2 - 0.1445883061\, t^3 + 0.2133409452\, t^4}{-0.9059858774 + 1.956830479\, t - 0.6103552658\, t^2 - 1.494650450\, t^3 + t^4},\right.$$

$$\left.\frac{0.1828752070\, t + 0.6268800173\, t^2 - 1.028340444\, t^3 + 0.3822448988\, t^4 - 0.1884116000}{-0.9059858774 + 1.956830479\, t - 0.6103552658\, t^2 - 1.494650450\, t^3 + t^4}\right)$$

It only remains to compute the numerator of the third component of the rational parametrization of the lifted curve; namely $p_3(t)$. Applying Lemma 3.2 we get the approximate parametrization (see Fig. 4.2 $\mathcal{P}(t) = (\frac{p_1(t)}{q(t)}, \frac{p_2(t)}{q(t)}, \frac{p_3(t)}{q(t)})$ of the space curve $\mathcal{C}$ (i.e. the parametrization of $\overline{\mathcal{C}}$), where

$$\frac{p_3(t)}{q(t)} = \frac{-1.067157288\, t^3 - 0.2783759249 - 0.7182447737\, t + 1.955832944\, t^2}{-0.9059858774 + 1.956830479\, t - 0.6103552658\, t^2 - 1.494650450\, t^3 + t^4}.$$

Example 4.3. Let $\mathcal{C}$ be the space curve defined by the polynomials

$$\begin{aligned} F_1 =& 20052827033xy + 2850904342zy - 7155364672zx - \frac{215763180597}{100}x \\ &- 7869010116z + \frac{1743412651801}{100}y - 43102722226y^2 + 1610946062z^2 \\ F_2 =& -18330943984zy + 33857630124zx - \frac{390188402999}{25}x - 56921602320z + \\ &\frac{12611223036001}{100}y - 166608514760y^2 + 57179742076z^2 + 20052827033x^2 \end{aligned}$$

and let $\epsilon = \frac{1}{600}$. One can check that $\mathcal{C}$ satisfies all the hypotheses imposed in Section 1. Moreover, $\deg(\mathcal{C}) = 4$. The projected curve $\pi_z(\mathcal{C})^*$ is not ϵ-rational, but $\pi_y(\mathcal{C})$ is. So we work with the projection on the plane $y = 0$. The defining polynomial of $\pi_y(\mathcal{C})^*$ is

$f(x,z) = 6.959832072 \cdot 10^{47}\, zx - 4.075715387 \cdot 10^{36}\, x - 6.207866771 \cdot 10^{35}\, z + 1.769623619 \cdot 10^{47}\, x^3 + 9.541705261 \cdot 10^{46}\, x^2 + 1.269145848 \cdot 10^{48}\, z^2 + 8.077561390 \cdot 10^{47}\, x^3z - 1.355904241 \cdot 10^{48}\, x^2z - 2.573514563 \cdot 10^{48}\, z^3 + 2.289865008 \cdot 10^{48}\, z^4 - 3.292700550 \cdot 10^{48}\, z^2x + 4.798217962 \cdot 10^{48}\, xz^3 + 3.090311649 \cdot 10^{48}\, x^2z^2 - 2.981944666 \cdot 10^{47}\, x^4.$

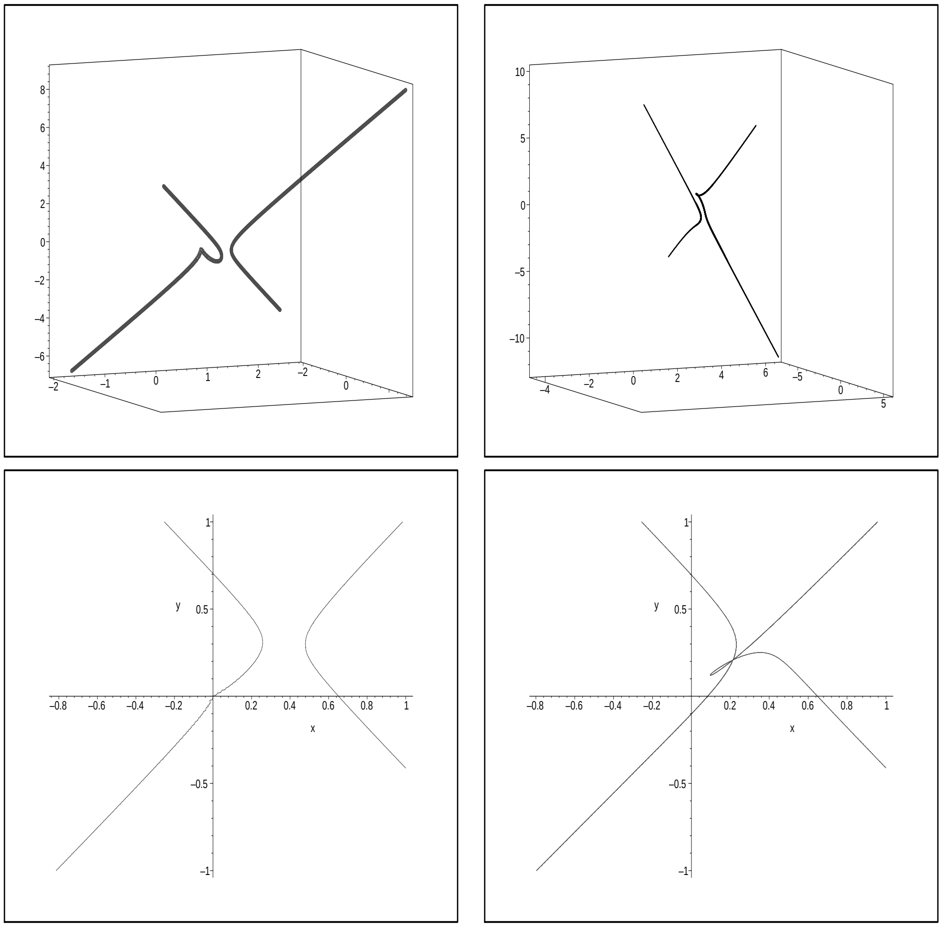


Figure 1: Up left: plot of $\mathcal{C}$; Up right: plot of $\overline{\mathcal{C}}$; Down left: plot of $\pi_z(\mathcal{C})$; Down right: plot $\mathcal{D}$.

Note that $\deg(\pi_y(\mathcal{C})^*) = 4$. Applying the approximate parametrization algorithm for plane curves in [20] we get that $\pi_y(\mathcal{C})^*$ is ϵ-rational. Furthermore the algorithm outputs $\mathcal{Q}(t) = (\frac{p_1(t)}{q(t)}, \frac{p_3(t)}{q(t)})$

$$\begin{aligned} p_1(t) =& -1.304559082 \cdot 10^{415}\, t - 2.995071314 \cdot 10^{415}\, t^2 - 2.096039950 \cdot 10^{414} - \\ & 1.114733279 \cdot 10^{415}\, t^4 - 3.005548232 \cdot 10^{415}\, t^3, \\ p_3(t) =& 6.238758852 \cdot 10^{418}\, t - 5.937809784 \cdot 10^{419}\, t^3 + 3.175932541 \cdot 10^{418} \\ & - 3.618736499 \cdot 10^{419}\, t^4 - 2.083861701 \cdot 10^{419}\, t^2, \\ q(t) =& 3.555348439\, t^3 + t^4 + 4.622830832\, t^2 + 2.625458073\, t + 0.5529230644. \end{aligned}$$

It only remains to compute the numerator of the second component of the rational parametrization of the lifted curve; namely $p_2(t)$. Applying Lemma 3.2 we get the approximate parametrization $\mathcal{P}(t) = (\frac{p_1(t)}{q(t)}, \frac{p_2(t)}{q(t)}, \frac{p_3(t)}{q(t)})$ of the space curve $\mathcal{C}$ (i.e. the

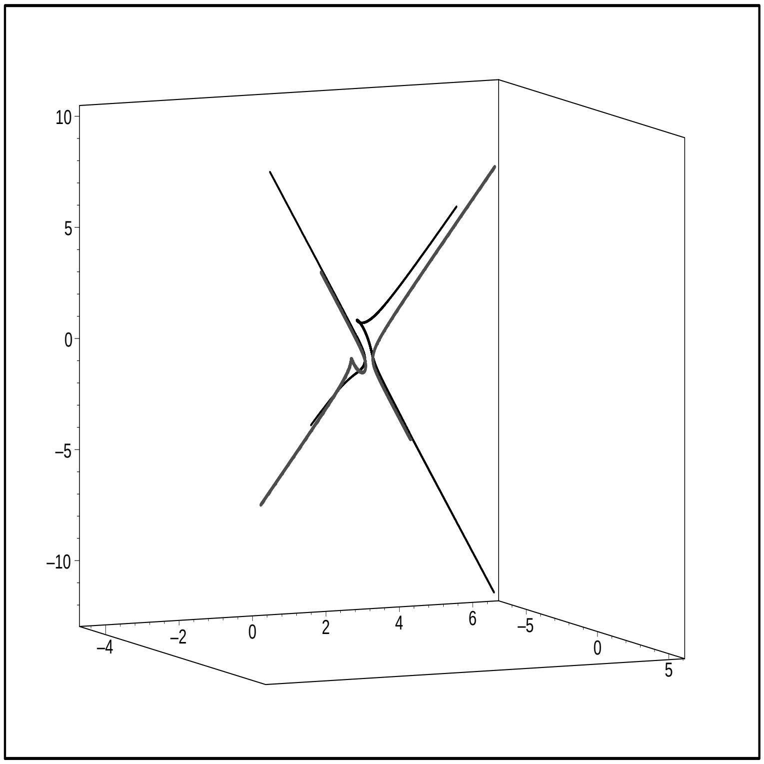


Figure 2: Joint plot of $\mathcal{C}$ and $\overline{\mathcal{C}}$

parametrization of $\overline{\mathcal{C}}$) where

$$p_2(t) == 8.923772403 \cdot 10^{705}\, t + 1.249180934 \cdot 10^{706}\, t^2 + 2.137471224 \cdot 10^{705} + 5.846606727 \cdot 10^{705}\, t^3.$$

5 Error Analysis

In this section, we prove that the Hausdorff distance between the input and output curves, of our algorithm, is always finite. For this purpose, we first need to develop some results on asymptotes of space curves. Afterwards we will analyze the distance. To start, we briefly recall the notion of Hausdorff distance; for further details we refer to [1]. In a metric space (X, d), for $\emptyset \neq B \subset X$ and $a \in X$ we define

$$\mathrm{d}(a, B) = \inf_{b \in B}\{\mathrm{d}(a, b)\}.$$

Moreover, for $A, B \subset X \setminus \emptyset$ we define

$$\mathrm{H_d}(A, B) = \max\{\sup_{a \in A}\{\mathrm{d}(a, B)\}, \sup_{b \in B}\{\mathrm{d}(b, A)\}\}.$$

By convention $\mathrm{H_d}(\emptyset, \emptyset) = 0$ and, for $\emptyset \neq A \subset X$, $\mathrm{H_d}(A, \emptyset) = \infty$. The function $\mathrm{H_d}$ is called the Hausdorff distance induced by d. In our case, since we will be working in

$(\mathbb{C}^3, \mathrm{d})$ or $(\mathbb{R}^3, \mathrm{d})$, being d the usual unitary or Euclidean distance, we simplify the notation writing $\mathrm{H}(A, B)$.

Let $\mathcal{E}$ be an space curve in $\mathbb{C}^3$; similarly if we consider the curve in $\mathbb{C}^n$. The intuitive idea of asymptote is clear, but here we formalize it and state some results. Although these results might be part of the background on the theory of asymptotes, we have not been able to find a reference in the literature suitable for our needs.

We say that a line $\mathcal{L}$ in $\mathbb{C}^3$ is an asymptote of $\mathcal{E}$ if there exists a sequence $\{P_n\}_{n\in N}$ of points in $\mathcal{E}$ such that $\lim_n \|P_n\| = \infty$ and $\lim_n \mathrm{d}(P_n, \mathcal{L}) = 0$; where d denotes the usual unitary distance in $\mathbb{C}^3$ and $\| \, \|$ the associated norm. In the following, we show how the tangents at the simple points at infinity of $\mathcal{E}$ are related with the asymptotes. More precisely, we have the following lemma. In the sequel, if $\mathcal{V}$ is a projective variety in $\mathbb{P}^3(\mathbb{F})$, we denote by $\mathcal{V}_a$ the open set $\mathcal{V} \cap \{w \neq 0\}$. In addition, for $\lambda \in \mathbb{C}$, $\overline{\lambda}$ denotes its conjugate.

Lemma 5.1. *Let $P = (a : b : c : 0) \in \mathcal{E}^\infty$ be simple and let $\mathbb{T}(P, \mathcal{E}^h)$ be the tangent line to $\mathcal{E}^h$ at P. If $\mathbb{T}(P, \mathcal{E}^h)$ is not included in the plane $w = 0$, then $\mathbb{T}(P, \mathcal{E}^h)_a$ is an asymptote of $\mathcal{E}$. Moreover, $(\overline{a}, \overline{b}, \overline{c})$ is a direction vector of the asymptote.*

Proof. Let $\{H_1, \ldots, H_m\} \subset \mathbb{F}[x, y, z, w]$ be homogeneous polynomials defining the ideal of $\mathcal{E}^h$. Let

$$\pi_i(x, y, z, w) = \frac{\partial H_i}{\partial x}(P)x + \frac{\partial H_i}{\partial y}(P)y + \frac{\partial H_i}{\partial z}(P)z + \frac{\partial H_i}{\partial w}(P)w.$$

Then, $\mathbb{T}(P, \mathcal{E}^h)$ is the projective variety defined by $\{\pi_1(x, y, z, w), \ldots, \pi_m(x, y, z, w)\}$ (see e.g. pp. 181 in [13]). Note that, since $\mathbb{T}(P, \mathcal{E}^h)$ is not included in the plane $w = 0$, $\mathbb{T}(P, \mathcal{E}^h)_a$ is an affine line. Now, we consider a local parametrization $\mathcal{P}(t) = (\tilde{x}(t) : \tilde{y}(t) : \tilde{z}(t) : w(t))$ of $\mathcal{E}^h$ centered at P. Since P is simple, and its tangent is not included in $w = 0$, the multiplicity of intersection of $\mathcal{E}^h$ and the plane $w = 0$ at P is 1. Thus, $w(t)$ can be expressed as $w(t) = tu(t)$, where $u(t)$ has order 0. Therefore, $u(t)^{-1}$ is a power series and $\mathcal{P}(t)$ can be expressed as

$$\mathcal{P}(t) = (x(t) : y(t) : z(t) : t)$$

where $x(t) = \tilde{x}(t)u^{-1}(t)$, $y(t) = \tilde{y}(t)u^{-1}(t)$, $z(t) = \tilde{z}(t)u^{-1}(t)$ are power series. Moreover, since $\mathbb{T}(P, \mathcal{E}^h)$ is the tangent, the order of $\pi_i(\mathcal{P}(t))$ has to be, at least, 2. Therefore, $\pi_i(\mathcal{P}(t))$ can be expressed as $\pi_i(\mathcal{P}(t)) = t^{\ell_i}v(t)$, where $\ell_i > 1$ and $v(t)$ has order 0.

Now, let $\{t_n\}$ be a sequence of complex numbers converging to 0, and such that $t_n \neq 0$. Then, for all n, $P_n = (\frac{x(t_n)}{t_n}, \frac{y(t_n)}{t_n}, \frac{z(t_n)}{t_n}) \in \mathcal{E}$. Moreover, $\lim_n \|P_n\| = \infty$. Let Π_i be the affine plane defined by $\pi_i(x, y, z, 1)$. We prove that, for all i, $\lim_n \mathrm{d}(P_n, \Pi_i) = 0$. From where, one deduces that $\lim_n \mathrm{d}(P_n, \mathbb{T}(P, \mathcal{E}^h)_a) = 0$, and hence that $\mathbb{T}(P, \mathcal{E}^h)_a$ is an asymptote.

Indeed,

$$\mathrm{d}(P_n, \Pi_i) = \frac{|\pi_i(P_n, 1)|}{\left\| \left(\frac{\partial H_i}{\partial x}(P), \frac{\partial H_i}{\partial y}(P), \frac{\partial H_i}{\partial z}(P) \right) \right\|} = \frac{\left| t_n^{\ell_i - 1} v(t_n) \right|}{\left\| \left(\frac{\partial H_i}{\partial x}(P), \frac{\partial H_i}{\partial y}(P), \frac{\partial H_i}{\partial z}(P) \right) \right\|}.$$

Since the denominator is not zero, because $\mathbb{T}(P, \mathcal{E}^h)$ is not included in $w = 0$, and since $\ell_i - 1 > 0$ and order of v is 0, we get that $\lim_n \mathrm{d}(P_n, \Pi_i) = 0$.

Finally, we see that $u = (\overline{a}, \overline{b}, \overline{c})$ is a direction vector of the asymptote. First we observe that u is not zero, since $P \in P^3(\mathbb{F})$. Now, by Euler equality we have that

$$\frac{\partial H_i}{\partial x} x + \frac{\partial H_i}{\partial y} y + \frac{\partial H_i}{\partial z} z + \frac{\partial H_i}{\partial w} w = \deg(H_i) H_i.$$

Substituting by P, we get

$$\frac{\partial H_i}{\partial x}(P) a + \frac{\partial H_i}{\partial y}(P) b + \frac{\partial H_i}{\partial z}(P) c + \frac{\partial H_i}{\partial w}(P) 0 = \deg(H_i) H_i(P) = 0.$$

Hence,

$$\left(\frac{\partial H_i}{\partial x}(P), \frac{\partial H_i}{\partial y}(P), \frac{\partial H_i}{\partial z}(P) \right) \cdot u = \frac{\partial H_i}{\partial x}(P) a + \frac{\partial H_i}{\partial y}(P) b + \frac{\partial H_i}{\partial z}(P) c = 0.$$

Thus u is orthogonal to all the planes Π_i. □

Remark 5.2. Note that the previous lemma is also true for P singular and for each simple tangent not included at the plane at infinity.

Applying the previous lemmas we get the next theorem.

Theorem 5.3. *Let $\mathcal{E}_1, \mathcal{E}_2 \subset \mathbb{C}^3$ be such that*

1. $\mathcal{E}_1^\infty = \mathcal{E}_2^\infty$
2. $\mathrm{card}(\mathcal{E}_1^\infty) = \mathrm{card}(\mathcal{E}_2^\infty) = \deg(\mathcal{E}_1) = \deg(\mathcal{E}_2)$.

Then, $\mathrm{H}(\mathcal{E}_1, \mathcal{E}_2) < \infty$.

Proof. By (2), all points at infinity of both curves are simple and none tangent line is included at the plane infinity. Therefore, by Lemma 5.1, all branches of the curves go to infinity following asymptotes. Since the direction vectors of the asymptotes depend only on the points at infinity (see Lemma 5.1), by (1) the asymptotes of $\mathcal{E}_1$ and $\mathcal{E}_2$ are parallel. Now, the result follows reasoning as in the proof of Lemma 6.1. in [20]. □

Remark 5.4. Note that, under the assumptions of Theorem 5.3, it also holds that $\mathrm{H}(\mathcal{E}_1 \cap \mathbb{R}^3, \mathcal{E}_2 \cap \mathbb{R}^3) < \infty$. We also observe that the previous theorem can be used under weaker assumptions for bounding $\mathrm{H}(\mathcal{E}_1 \cap \mathbb{R}^3, \mathcal{E}_2 \cap \mathbb{R}^3)$, since the result would follow analyzing the real asymptotes.

Corollary 5.5. *Let $\mathcal{C}, \overline{\mathcal{C}}$ be the input and output curves of our algorithm. Then* $\mathrm{H}(\mathcal{C}, \overline{\mathcal{C}}) < \infty$ *and* $\mathrm{H}(\mathcal{C} \cap \mathbb{R}^3, \overline{\mathcal{C}} \cap \mathbb{R}^3) < \infty$.

Proof. It follows from the general assumptions, and from Theorems 3.1 and 5.3. □

6 Empirical Analysis of the Error

We proved in the previous section that the Hausdorff distance $\mathrm{H}(\mathcal{C},\overline{\mathcal{C}})$ is finite. In this section, because of the computational difficulties, instead of computing or bounding theoretically $\mathrm{H}(\mathcal{C},\overline{\mathcal{C}})$ we approach the study of the Hausdorff distance empirically and apply it to the examples in Section 4. Recall that

$$\mathrm{H}(\mathcal{C},\overline{\mathcal{C}}) := \max\{\sup_{P\in\mathcal{C}}\{\mathrm{d}(P,\overline{\mathcal{C}})\}, \sup_{Q\in\overline{\mathcal{C}}}\{\mathrm{d}(Q,\mathcal{C})\}\},$$

where $\mathcal{C},\overline{\mathcal{C}}$ are the input and output curves of our algorithm.

We explain next how to estimate $\sup_{P\in\mathcal{C}}\{\mathrm{d}(P,\overline{\mathcal{C}})\}$ and $\sup_{Q\in\overline{\mathcal{C}}}\{\mathrm{d}(Q,\mathcal{C})\}$ independently. Let $\overline{\mathcal{P}}(t) = (\overline{p_1}(t), \overline{p_2}(t), \overline{p_3}(t)) \in \mathbb{R}(t)^3$ be the parametrization of $\overline{\mathcal{C}}$ output by our algorithm.

Estimation of $\sup_{Q\in\overline{\mathcal{C}}}\{\mathrm{d}(Q,\mathcal{C})\}$

For every $t_0 \in \mathbb{Q}$, such that $\overline{\mathcal{P}}(t_0)$ is well defined, and $\overline{p_1}'(t_0)\overline{p_2}'(t_0)\overline{p_3}'(t_0) \neq 0$, we consider the normal plane to $\overline{\mathcal{C}}$ at the point $\overline{\mathcal{P}}(t_0)$ given by the parametrization:

$$\mathcal{L}_1(t_0,k_1,k_2) = \overline{\mathcal{P}}(t_0) + k_1 v_1(t_0) + k_2 v_2(t_0),$$

where $v_1(t_0)$ and $v_2(t_0)$ are unitary vectors in the direction of $(-\overline{p_3}'(t_0), 0, \overline{p_1}'(t_0))$ and $(0, -\overline{p_3}'(t_0), \overline{p_2}'(t_0))$ respectively. Moreover, we introduce the polynomials

$$\mathcal{D}_i(t_0,k_1,k_2) = F_i(\mathcal{L}_1(t_0,k_1,k_2)) \in \mathbb{Q}[k_1,k_2],\ i = 1,\ldots,s;$$

we recall that $\{F_1,\ldots,F_s\}$ are the polynomials generating $\mathcal{C}$. In this situation, it holds that

$$\mathrm{d}(\overline{\mathcal{P}}(t_0),\mathcal{C}) \le \min\{||k_1 v_1(t_0) + k_2 v_2(t_0)|| \mid \mathcal{D}_i(t_0,k_1,k_2) = 0,\ k_1,k_2 \in \mathbb{C},\ i = 1,\ldots,s\}.$$

Let $\rho_1(t_0)$ denote the r.h.s. of the previous inequality.

We explain next how to choose an appropriate finite set $\mathcal{T} \subset \mathbb{Q}$ to give $\max_{t_0\in\mathcal{T}}\{\rho_1(t_0)\}$ as an estimation of $\sup_{Q\in\overline{\mathcal{C}}}\{\mathrm{d}(Q,\mathcal{C})\}$. First, we obtain a finite set $\mathcal{T}_0 \subset \mathbb{Q}$ as follows. For each real pole of the parametrization $\overline{\mathcal{P}}(t)$ we consider a finite sequence of isolating intervals $\{J_i\}_{i=1,\ldots,e_0}$ of length $1/10^{(i+5)}$, and we take the middle point. Then $\mathcal{T}_0$ is the set containing all the middle points. Secondly we consider the set $\mathcal{T}_1 = \{(-2)^i \mid i = 1,\ldots,10^{e_1}\}$ for some $e_1 \in \mathbb{N}$ and finally we take $\mathcal{T} = \mathcal{T}_0 \cup \mathcal{T}_1$.

Estimation of $\sup_{P\in\mathcal{C}}\{\mathrm{d}(P,\overline{\mathcal{C}})\}$

For every non singular point $P_0 = (a,b,c) \in \mathcal{C}$, we consider the normal plane to $\mathcal{C}$ at P_0:

$$\mathcal{L}_2(P_0,x,y,z) = N_1(P_0)(x-a) + N_2(P_0)(y-b) + N_3(P_0)(z-c)$$

where $(N_1(P_0), N_2(P_0), N_3(P_0))$ is a unitary normal vector to $\mathcal{C}$ at P_0. Moreover let $\mathcal{G}(P_0, t)$ be the numerator of $\mathcal{L}_2(P_0, \overline{p_1}(t), \overline{p_2}(t), \overline{p_3}(t))$. Then it holds that

$$\mathrm{d}(P_0, \overline{\mathcal{C}}) \leq \min\{||P_0 - \overline{\mathcal{P}}(t)|| \,/\, \mathcal{G}(P_0, t) = 0 \text{ and } t \in \mathbb{C}\}.$$

Let $\rho_2(P_0)$ denote the r.h.s. of the previous inequality.

We explain next how to choose an appropriate finite set $\mathcal{E} \subset \mathcal{C}$ to give $\max_{P_0 \in \mathcal{E}}\{\rho_2(P_0)\}$ as an estimation of $\sup_{P \in \mathcal{C}}\{\mathrm{d}(P, \overline{\mathcal{C}})\}$. For each $i = 1, \ldots, e_2$, where $e_2 \in \mathbb{N}$, we compute the sets ω_i^x, ω_i^y and ω_i^z of intersection points of $\mathcal{C}$ with the planes $x = (-2)^i$, $y = (-2)^i$ and $z = (-2)^i$, respectively. Then $\mathcal{E} = \cup_{i=1}^{e_2}(\omega_i^x \cup \omega_i^y \cup \omega_i^z)$. It should be noticed that, in practice, the points in $\mathcal{E}$ cannot be taken as exact points on the curve but as ϵ-points (see [19]), thus contributing to an increment of the magnitude of the estimation. Observe that this is avoided when taking $\mathcal{T}$.

Distance Estimation for Examples in Section 4

Example 4.2. The parametrization $\mathcal{P}(t)$ of $\overline{\mathcal{C}}$ has 2 real poles. For $e_0 = 20$ we get $\max_{t_0 \in \mathcal{T}_0}\{\rho_1(t_0)\} = 0.2203928911$ and for $\mathcal{T}_1 = \{(-2)^i \mid i = 1, \ldots, 10^3\}$ we obtain $\max_{t_0 \in \mathcal{T}_1}\{\rho_1(t_0)\} = 0.1036637452$. Then our estimation of $\sup_{Q \in \overline{\mathcal{C}}}\{\mathrm{d}(Q, \mathcal{C})\}$ is equal to 0.2203928911.

For $\mathcal{E} = \cup_{i=1}^{30}(\omega_i^x \cup \omega_i^y \cup \omega_i^z)$ we obtain an estimation of $\sup_{P \in \mathcal{C}}\{\mathrm{d}(P, \overline{\mathcal{C}})\}$ equal to $\max_{P_0 \in \mathcal{E}}\{\rho_2(P_0)\} = 0.4705723389$. Thus our estimation of $\mathrm{H}(\mathcal{C}, \overline{\mathcal{C}})$ is 0.4705723389.

Example 4.3. The parametrization $\mathcal{P}(t)$ of $\overline{\mathcal{C}}$ has 2 real poles. For $e_0 = 20$ we get $\max_{t_0 \in \mathcal{T}_0}\{\rho_1(t_0)\} = 0.1558549452$ and for $\mathcal{T}_1 = \{(-2)^i \mid i = 1, \ldots, 10^3\}$ we obtain $\max_{t_0 \in \mathcal{T}_1}\{\rho_1(t_0)\} = 0.1603882181$. Then our estimation of $\sup_{Q \in \overline{\mathcal{C}}}\{\mathrm{d}(Q, \mathcal{C})\}$ is equal to 0.1603882181.

For $\mathcal{E} = \cup_{i=1}^{30}(\omega_i^x \cup \omega_i^y \cup \omega_i^z)$ we obtain an estimation of $\sup_{P \in \mathcal{C}}\{\mathrm{d}(P, \overline{\mathcal{C}})\}$ equal to $\max_{P_0 \in \mathcal{E}}\{\rho_2(P_0)\} = 0.1562381230$. Thus our estimation of $\mathrm{H}(\mathcal{C}, \overline{\mathcal{C}})$ is 0.1603882181.

References

[1] Aliprantis C.D., Border K.C. (2006). *Infinite Dimensional Analysis.* Springer Verlag (2006).

[2] Bajaj C., Royappa A., (2000). *Parameterization In Finite Precision.* Algorithmica, Vol. 27, No. 1. pp. 100-114.

[3] Caviness B.F, Johnson J.R. (1998). *Quantifier Elimination and Cylindrical Algebraic Decomposition.* Text and Monographs in Symbolic Computation. Springer Verlag, pp 269289.

[4] Corless R.M., Gianni P.M., Trager B.M., Watt S.M. (1995). *The Singular Value Decomposition for Polynomial Systems.* Proc. ISSAC 1995, pp. 195-207, ACM Press.

[5] Gianni P., Trager B., and Zacharias G. (1988). *Grobner bases and primary decompositions of polynomial ideals.* Journal of Symbolic Computation, Vol. 6, pp. 149-167.

[6] Corless R.M., Giesbrecht M.W., Kotsireas I.S., van Hoeij M., Watt S.M. (2001). *Towards Factoring Bivariate Approximate Polynomials*. Proc. ISSAC 2001, London, Bernard Mourrain, ed. pp 85–92.

[7] Corless R.M., Giesbrecht M.W., Kotsireas I.S., Watt S.M. (2000). *Numerical Implicitization of Parametric Hypersurfaces with Linear Algebra*. Proc. Artificial Intelligence with Symbolic Computation (AISC 2000), pp 174-183, Springer Verlag LNAI 1930.

[8] Cox D., Little J., O'Shea D. (1997). *Ideals, Varieties, and Algorithms (2nd ed.)*. Springer-Verlag, New York.

[9] Dokken T., (2001). *Approximate Implicitization*. Mathematical Methods in CAGD;Oslo 2000, Tom Lyche anf Larry L. Schumakes (eds). Vanderbilt University Press.

[10] Emiris I.Z., Galligo A., Lombardi H., (1997). *Certified Approximate Univariate GCDs* J. Pure and Applied Algebra, Vol.117 and 118. pp. 229–251.

[11] Gahleitner J., Jüttler B., Schicho J. (2002). *Approximate Parameterization of Planar Cubic Curve Segments*. Proc. Fifth International Conference on Curves and Surfaces. Saint-Malo 2002. pp. 1-13, Nashboro Press, Nashville, TN.

[12] Galligo A., Rupprech D. (2002). *Irreducible Decomposition of Curves*. J. Symbolic Computation, Vol. 33. pp. 661 - 677.

[13] Harris J. (1992). *Algebraic Geometry, a First Course*. Springer-Verlag.

[14] Hartmann E., (2000). *Numerical Parameterization of Curves and Surfaces*. Computer Aided Geometry Design, Vol. 17. pp. 251-266.

[15] Kaltofen E., May J.P., Yang Z., Zhi L., (2008). *Approximate Factorization of Multivariate Polynomials Using Singular Value Decomposition*. Journal of Symbolic Computation. Vol.43/5. pp.359-376.

[16] Pan V.Y., (1996). *Numerical Computation of a Polynomial GCD and Extensions*. Tech.report, N. 2969. Sophia-Antipolis, France.

[17] Pérez–Díaz S., Sendra J., Sendra J.R., (2004). *Parametrization of Approximate Algebraic Curves by Lines*. Theoretical Computer Science. Vol.315/2-3. pp.627-650.

[18] Pérez–Díaz S., Sendra J., Sendra J.R., (2005). *Parametrization of Approximate Algebraic Surfaces by Lines*. Computer Aided Geometric Design. Vol 22/2. pp. 147-181.

[19] Pérez–Díaz S., Sendra J., Sendra J.R., (2006). *Distance Bounds of ϵ-Points on Hypersurfaces*. Theoretical Computer Science. Vol. 359, pp. 344-368.

[20] Pérez–Díaz S., Rueda S.L., Sendra J., Sendra J.R., (2010). *Approximate Parametrization of Plane Algebraic Curves by Linear Systems of Curves*. Computer Aided Geometric Design vol 27, 212231.

[21] Robbiano L, J. Abbott J. (ed) (2010). *ApCoA = Embedding Commutative Algebra into Analysis.* In Approximate Commutative Algebra Texts and Monographs in Symbolic Computation. Springer-Velag.

[22] Sendra J.R., Winkler J.R., Pérez-Díaz S. (2007). *Rational Algebraic Curves: A Computer Algebra Approach*. Springer-Verlag Heidelberg, in series Algorithms and Computation in Mathematics. Volume 22.

[23] Stetter H.J. (2004). *Numerical Polynomial Algebra*. SIAM.

[24] Stetter H.J. (2010). *ApCoA = Embedding Commutative Algebra into Analysis.* In [21] pp. 205-217

[25] Winkler F., (1996). *Polynomial Algorithms in Computer Algebra.* Springer-Verlag, Wien New York.