PTOPO: Computing the Geometry and the Topology of Parametric Curves
Christina Katsamaki, Fabrice Rouillier, Elias Tsiganidas, Zafeirakis Zafeirakopoulos

To cite this version:

HAL Id: hal-03090184
https://hal.science/hal-03090184v3
Submitted on 17 Feb 2022

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

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
PTOP0: Computing the Geometry and the Topology of Parametric Curves

Christina Katsamaki, Fabrice Rouillier, Elias Tsigaridas

Inria Paris, IMJ-PRG, Sorbonne Université and Paris Université

Zafeirakis Zafeirakopoulos

Institute of Information Technologies, Gebze Technical University, Turkey

Abstract

We consider the problem of computing the topology and describing the geometry of a parametric curve in \( \mathbb{R}^n \). We present an algorithm, PTOP0, that constructs an abstract graph that is isotopic to the curve in the embedding space. Our method exploits the benefits of the parametric representation and does not resort to implicitization.

Most importantly, we perform all computations in the parameter space and not in the implicit space. When the parametrization involves polynomials of degree at most \( d \) and maximum bitsize of coefficients \( \tau \), then the worst case bit complexity of PTOP0 is \( \tilde{O}_B(d^6 + nd^5 \tau + d^4(n^2 + n \tau) + d^3(n^2 \tau + n^3) + n^3 d^2 \tau) \). This bound matches the current record bound \( \tilde{O}_B(d^6 + d^5 \tau) \) for the problem of computing the topology of a plane algebraic curve given in implicit form. For plane and space curves, if \( N = \max\{d, \tau\} \), the complexity of PTOP0 becomes \( \tilde{O}_B(N^6) \), which improves the state-of-the-art result, due to Alcázar and Díaz-Toca [CAGD’10], by a factor of \( N^{10} \). In the same time complexity, we obtain a graph whose straight-line embedding is isotopic to the curve. However, visualizing the curve on top of the abstract graph construction, increases the bound to \( \tilde{O}_B(N^7) \).

For curves of general dimension, we can also distinguish between ordinary and non-ordinary real singularities and determine their multiplicities in the same expected complexity of PTOP0 by employing the algorithm of Blasco and Pérez-Díaz [CAGD’19]. We have implemented PTOP0 in MAPLE for the case of plane and space curves. Our experiments illustrate its practical nature.

Keywords: Parametric curve, topology, bit complexity, polynomial systems

1. Introduction

Parametric curves constitute a classical and important topic in computational algebra and geometry (Sendra and Winkler [1999]) that constantly receives attention, e.g., (Sederberg [1986], Cox et al. [2011], Buse et al. [2019], Sendra et al. [2008]). The motivation behind the continuous
interest in efficient algorithms for computing with parametric curves emanates, among others reasons, by the frequent presence of parametric representations in computer modeling and computer aided geometric design, e.g., (Farouki et al., 2010).

We focus on computing the topology of a real parametric curve, that is, the computation of an abstract graph that is isotopic (Boissonnat and Teillaud, 2006, p. 184) to the curve in the embedding space. We design an algorithm, PTOPO, that applies directly to rational parametric curves of any dimension and is complete, in the sense that there are no assumptions on the input. We consider different characteristics of the parametrization, like properness and normality, before computing the singularities and other interesting points on the curve. These points are necessary for representing the geometry of the curve, as well as for producing a certified visualization of plane and space curves.

**Previous work.** A common strategy when dealing with parametric curves is implicitization. There has been a lot of research effort, e.g., Sederberg and Chen (1995); Busé et al. (2019) and the references therein, in designing algorithms to compute the implicit equations describing the curve. However, it is also important to manipulate parametric curves directly, without converting them to implicit form. For example, in the parametric form it is easier to visualize the curve and to find points on it. The advantages of the latter become more significant for curves of high dimension.

The study of the topology of a real parametric curve is a topic that has not received much attention in the literature, in contrast to its implicit counterpart (Diatta et al., 2018; Kobel and Sagraloff, 2014). The computation of the topology requires special treatment, since for instance it is not always easy to choose a parameter interval such that when we plot the curve over it, we include all the important topological features (like singular and extreme points) (Alcázar and Díaz-Toca, 2010). Moreover, while visualizing the curve using symbolic computational tools, the problem of missing points and branches may arise (Recio, 2007; Sendra, 2002). Alcázar and Díaz-Toca (2010) study the topology of real parametric curves without implicitizing. They work directly with the parametrization and address both plane and space real rational curves. Our algorithm to compute the topology is to be juxtaposed to their work. We also refer to Caravantes et al. (2014) and Alberti et al. (2008) for other approaches based on computations by values and subdivision, respectively.

To compute the topology of a curve it is essential to detect its singularities. This is an important and well studied problem (Alcázar and Díaz-Toca, 2010; Rubio et al., 2009; Kobel and Sagraloff, 2014) of independent interest. To identify the singularities, we can first compute the implicit representation and then apply classical approaches (Walker, 1978; Fulton, 1969). Alternatively, we can compute the singularities using directly the parametrization. For instance, there are necessary and sufficient conditions to identify cusps and inflection points using determinants, e.g., (Li and Cripps, 1997; Manocha and Canny, 1992).

On computing the singularities of a parametric curve, a line of work related to our approach, does so by means of a univariate resultant (Abhyankar and Bajaj, 1989; van den Essen and YU, 1997; Park, 2002; Pérez-Díaz, 2007; Gutierrez et al., 2002a). We can use the Taylor resultant (Abhyankar and Bajaj, 1989) and the $D$-resultant (van den Essen and YU, 1997) of two polynomials in $K[t]$, to find singularities of plane curves parametrized by polynomials, where $K$ is a field of characteristic zero in the first case and of arbitrary characteristic in the latter, without resorting to the implicit form. Park (2002) extends previous results to curves parametrized by polynomials in affine $n$-space. The generalization of the $D$-resultant for a pair of rational functions and its application to the study of rational plane curves, is due to Gutierrez et al. (2002a).
In (Pérez-Díaz, 2007; Blasco and Pérez-Díaz, 2019) they present a method for computing the singularities of plane curves using a univariate resultant and characterizing the singularities using its factorization. Notably (Rubio et al., 2009) work on rational parametric curves in affine $n$-space; they use generalized resultants to find the parameters of the singular points. Moreover, they characterize the singularities and compute their multiplicities.

Cox et al. (2011) use the syzygies of the ideal generated by the polynomials that give the parametrization to compute the singularities and their structure. There are state-of-the-art approaches that exploit this idea and relate the problem of computing the singularities with the notion of the $\mu$-basis of the parametrization, e.g., (Jia et al., 2018) and references therein. Chionh and Sederberg (2001) reveal the connection between the implicitization Bézout matrix and the singularities of a parametric curve. Buse and D’Andrea (2012) present a complete factorization of the invariant factors of resultant matrices built from birational parametrizations of rational plane curves in terms of the singular points of the curve and their multiplicity graph. Let us also mention the important work on matrix methods (Buse, 2014; Buse and Luu Ba, 2010) for representing the implicit form of parametric curves, that is suitable for numerical computations. Bernardi et al. (2016) use the projection from the rational normal curve to the curve and exploit secant varieties.

Overview of our approach and our contributions. We introduce $\text{PTOP}$, a complete, exact, and efficient algorithm (Alg. [3]) for computing the geometric properties and the topology of rational parametric curves in $\mathbb{R}^n$. Unlike other algorithms, e.g. (Alcázar and Díaz-Toca, 2010), it makes no assumptions on the input curves, such as the absence of axis-parallel asymptotes, and is applicable to any dimension. Nevertheless, it does not identify knots for space curves nor it can be used for determining the equivalence of two knots.

If the (proper) parametrization of the curve consists of polynomials of degree $d$ and bitsize $\tau$, then $\text{PTOP}$ outputs a graph isotopic (Boissonnat and Teillaud, 2006, p.184), Alcázar et al. (2020) to the curve in the embedding space, by performing

$$\tilde{O}_b(n^d \tau + n^d \tau + d^4(n^2 + n\tau) + d^3(n^2 \tau + n^3) + n^3 d^2 \tau)$$

bit operations in the worst case (Thm. [24]), assuming no singularities at infinity. We also provide a Las Vegas variant with expected complexity

$$\tilde{O}_b(d^6 + d^5(n + \tau) + d^4(n^2 + n\tau) + d^3(n^2 \tau + n^3) + n^3 d^2 \tau).$$

If $n = O(1)$, the bounds become $\tilde{O}_b(N^6)$, where $N = \max\{d, \tau\}$. The vertices of the output graph correspond to special points on the curve, in whose neighborhood the topology is not trivial, given by their parameter values. Each edge of the graph is associated with two parameter values and corresponds to a unique smooth parametric arc. For an embedding isotopic to the curve, we map every edge of the abstract graph to the corresponding parametric arc.

For plane and space curves, our bound improves the previously known bound due to Alcázar and Díaz-Toca (2010) by a factor of $\tilde{O}_b(N^{10})$. The latter algorithm (Alcázar and Díaz-Toca, 2010) performs some computations in the implicit space. On the contrary, $\text{PTOP}$ is a fundamentally different approach since we work exclusively in the parameter space and we do not use a sweep-line algorithm to construct the isotopic graph. We handle only the parameters that give important points on the curve, and thus, we avoid performing operations such as univariate root isolation in an extension field or evaluation of a polynomial at an algebraic number.
Computing singular points is an essential part of PTOPO (Lem. 18). We chose not to exploit recent methods, e.g., (Blasco and Pérez-Díaz 2019), for this task because this would require introducing new variables (to employ the T-resultant). We employ older techniques, e.g., (Rubio et al., 2009; Pérez-Díaz, 2007; Alcázar and Díaz-Toca, 2010), that rely on a bivariate polynomial system, Eq. (2). We take advantage of this system’s symmetry and of nearly optimal algorithms for bivariate system solving and for computations with real algebraic numbers (Diatta et al., 2018; Bouzidi et al., 2016; Diochnos et al., 2009; Pan and Tsigaridas, 2017). In particular, we introduce an algorithm for isolating the roots of over-determined bivariate polynomial systems by exploiting the Rational Univariate Representation (RUR) (Bouzidi et al., 2015b, 2016, 2013) that has worst case and expected bit complexity that matches the bounds for square systems (Thm. 16). These are key steps for obtaining the complexity bounds of Thm. 23 and Thm. 24.

Moreover, our bound matches the current state-of-the-art complexity bound, $\tilde{O}(d^6 + d^5\tau)$ or $\tilde{O}(N^6)$, for computing the topology of implicit plane curves (Diatta et al., 2018; Kobel and Sagraloff, 2014). However, if we want to visualize the graph in 2D or 3D, then we have to compute a characteristic box (Lem. 20) that contains all the topological features of the curve and the intersections of the curve with its boundary. In this case, the complexity of PTOPO becomes $\tilde{O}(N^7)$ (Thm. 23).

A preprocessing step of PTOPO consists of finding a proper reparametrization of the curve (if it is not proper). We present explicit bit complexity bounds (Lem. 6) for the algorithm of Pérez-Díaz (2006) to compute a proper parametrization. Another preprocessing step is to ensure that there are no singularities at infinity. Lem. 7 handles this task and provides explicit complexity estimates.

Additionally, we consider the case where the embedding of the abstract graph has straight line edges and not parametric arcs; in particular for plane curves, we show that the straight line embedding of the abstract graph in $\mathbb{R}^2$ is already isotopic to the curve (Cor. 26). For space curves, the procedure supported by Thm. 28 adds a few extra vertices to the abstract graph, so that the straight line embedding in $\mathbb{R}^3$ is isotopic to the curve. The extra number of vertices serves in resolving situations where self-crossings occur when continuously deforming the graph to the curve. In Thm. 30 we also prove that for curves of any dimension, we can compute the multiplicities and the characterization of singular points in the same bit-complexity as computing the points (in a Las Vegas setting). For that, we use the method by Blasco and Pérez-Díaz (2019), which does not require any further computations apart from solving the system that gives the parameters of the singular points (cf. Alcázar and Díaz-Toca, 2010).

Last but not least, we provide a certified implementation of PTOPO in Maple. The implementation computes the topology of plane and space curves and visualizes them. If the input consists of rational polynomials, our algorithm and the implementation is certified, since, first of all, the algorithm always outputs the correct geometric and topological result. This is because we perform exact computations with real algebraic numbers based on arithmetic over the rationals. Moreover, no assumption that cannot be verified (for example by another algorithm) is made on the input.

A preliminary version of our work appeared in Katsamaki et al. (2020a). Compared with this version, we add all the missing proofs for the algebraic tools that we use in our algorithm, we present the isotopic embedding for plane and space curves (Sec. 6), and analyze the complexity.
of the algorithm of [Blasco and Pérez-Díaz (2019)] to determine the multiplicities and the character of real singular points (Sec. [7]).

Organization of the paper. The next section presents our notation and some useful results needed for our proofs. In Sec. [3] we give the basic background on rational curves in affine $n$-space. We characterize the parametrization by means of injectivity and surjectivity and describe a reparametrization algorithm. In Sec. [4] we present the algorithm to compute the singular, extreme points (in the coordinate directions), and isolated points on the curve. In Sec. [5] we describe our main algorithm, PTOPO, that constructs a graph isotopic to the curve in the embedding space and its complexity. In Sec. [6] we expatiate on the isotopic embedding for plane and space curves. In Sec. [7] we study the multiplicities and the character of real singular points for curves of arbitrary dimension. Finally, in Sec. [8] we give examples and experimental results.

2. Notation and Algebraic Tools

For a polynomial $f \in \mathbb{Z}[X]$, its infinity norm is equal to the maximum absolute value of its coefficients. We denote by $\mathcal{L}(f)$ the logarithm of its infinity norm. We also call the latter the size of the polynomial. A univariate polynomial is of size $(d, \tau)$ when its degree is at most $d$ and has bitsize $\tau$. The bitsize of a rational function is the maximum of the bitsizes of the numerator and the denominator. We represent an algebraic number $\alpha \in \mathbb{C}$ by the isolating interval representation. When $\alpha \in \mathbb{R}$ (resp. $\mathbb{C}$), it includes a square-free polynomial which vanishes at $\alpha$ and a rational interval (resp. Cartesian products of rational intervals) containing $\alpha$ and no other root of this polynomial (see for example [Yap 1999]). We denote by $\tilde{O}$ (resp. $O$) the arithmetic (resp. bit) complexity and we use $\hat{O}$ (resp. $\hat{O}$) to ignore (poly-)logarithmic factors. We denote the resultant of the polynomials $f, g$ with respect to $x$ by $\text{res}_x(f, g)$. For $t \in \mathbb{C}$, we denote by $t^\ast$ its complex conjugate. We use $[n]$ to signify the set $\{1, \ldots, n\}$.

We now present some useful results, needed for our analysis.

**Lemma 1.** Let $A = \sum_{i=0}^m a_i X^i$, $B = \sum_{j=0}^n b_j X^j \in \mathbb{Z}[X]$ of degrees $m$ and $n$ and of bitsizes $\tau$ and $\sigma$ respectively. Let $\alpha_1, \ldots, \alpha_m$ be the complex roots of $A$, counting multiplicities. Then, for any $\kappa = 1, \ldots, m$ it holds that

$$2^{-m\sigma - n\tau - (m+n)\log(m+n)} < |B(\alpha_\kappa)| < 2^{m\sigma + n\tau + (m+n)\log(m+n)}.$$

**Proof.** Following [Strzebonski and Tsigaridas (2019)], let $R = \text{res}_X(A(X), Y - B(X)) \in \mathbb{Z}[Y]$. Using the Poisson’s formula for the resultant we can write $R(Y) = a_n \prod_{i=0}^m (Y - B(\alpha_i))$. The maximum bitsize of the coefficients of $R(Y)$ is at most $m\sigma + n\tau + (m+n)\log(m+n)$. We observe that the roots of $R(Y)$ are $B(\alpha_\kappa)$ for $\kappa = 1, \ldots, m$. Therefore, using Cauchy’s bound we deduce that

$$2^{-m\sigma - n\tau - (m+n)\log(m+n)} < |B(\alpha_\kappa)| < 2^{m\sigma + n\tau + (m+n)\log(m+n)}.$$

**Lemma 2.** Let $f_1(X), \ldots, f_n(X) \in \mathbb{Z}[X]$ of sizes $(d, \tau)$. We can compute their gcd, which is of size $(d, \tilde{O}(d + \tau))$, in worst case complexity $\tilde{O}(n (d^2 + d^\tau))$, with a Monte Carlo algorithm in $\tilde{O}(d^2 + d\tau)$, or with a Las Vegas algorithm in $\tilde{O}(n (d^2 + d\tau))$. 


Proof. These are known results (von zur Gathen and Gerhard [2013]). We repeat the arguments adapted to our notation.

Worst case: We compute \( g \) by performing \( n \) consecutive gcd computations, that is

\[
gcd(f_1, \gcd(f_2, \gcd(\cdots, \gcd(f_{n-1}, f_n)))
\]

Since each gcd computation costs \( \tilde{O}_B(d^3 + d^2 \tau) \) (Bouzidi et al. [2015b] Lem.4), the result for this case follows.

Monte Carlo: We perform one gcd computation by allowing randomization. If we choose integers \( a_1, \ldots, a_n \) independently at random from the set \( \{1, \ldots, Kd\} \), where \( K = \mathcal{O}(1) \), we get that \( \gcd(f_1, \ldots, f_n) = \gcd(f_1, f_2 + a_1 f_3 + \cdots + a_n f_n) \) in \( \mathbb{Z}[x] \), with probability \( \geq 1/2 \) (von zur Gathen and Gerhard [2013] Thm. 6.46). This actually computes the monic gcd in \( \mathbb{Q} \). To compute the gcd in \( \mathbb{Z} \) we need to multiply with the gcd of the leading coefficients of \( f_1, f_2 + a_1 f_3 + \cdots + a_n f_n \) and then take the primitive part of the resulting polynomial. This is sufficient since the leading coefficient of the gcd in \( \mathbb{Z}[x] \) divides the leading coefficients of the two polynomials. Also, by (von zur Gathen and Gerhard [2013] Cor. 6.10) the monic gcd of two polynomials in \( \mathbb{Q}[x] \) is equal to their gcd in \( \mathbb{Z}[x] \) divided by their leading coefficient. The gcd of the two leading coefficients of \( f_1, f_2 + a_1 f_3 + \cdots + a_n f_n \) is an integer of bitsize \( \tilde{O}(\tau) \), therefore this does not pollute the total complexity.

We compute \( g^* = \gcd(f_1, f_2 + a_1 f_3 + \cdots + a_n f_n) \). Notice that the polynomial \( f_2 + a_1 f_3 + \cdots + a_n f_n \) is asymptotically of size \( (d, \tau) \). So, it takes \( \tilde{O}_B(d^2 + d \tau) \) to find \( g^* \), using the probabilistic algorithm in [Schönhage 1988].

Las Vegas: We can reduce the probability of failure in the Monte Carlo variant of the gcd computation to zero, by performing \( n \) exact divisions. In particular, we check if \( g^* \) divides \( f_3, \ldots, f_n \). Using (von zur Gathen and Gerhard [2013] Ex.10.21), the bit complexity of these operations is in total \( \tilde{O}_B(n(d^2 + d \tau)) \).

**Lemma 3.** Let \( f_1(X, Y), \ldots, f_n(X, Y) \in \mathbb{Z}[X, Y] \) of bidegrees \( (d, d) \) and \( L(f_i) = \tau \). We can compute their gcd, which is of bitsize \( \tilde{O}(d + \tau) \), in worst case complexity \( \tilde{O}_B(n(d^3 + d^2 \tau)) \), with a Monte Carlo algorithm in \( \tilde{O}_B(d^3 + d^2 \tau) \), or with a Las Vegas algorithm in \( \tilde{O}_B(n(d^3 + d^2 \tau)) \).

**Proof.** The straightforward approach is to perform \( n \) consecutive gcd computations, that is

\[
gcd(f_1, gcd(f_2, \gcd(\cdots, gcd(f_{n-1}, f_n)))).
\]

To accelerate the practical complexity we sort \( f_i \) in increasing order with respect to their degree. Each gcd computation costs \( \tilde{O}_B(d^3 + d^2 \tau) \) (Bouzidi et al. [2016] Lem. 5), so the total worst case cost is \( \tilde{O}_B(n d^3 + n d^2 \tau) \).

Alternatively, we consider the operation \( \gcd(f_1, \sum_{k=2}^n a_k f_k) \), where \( a_k \) are random integers, following (von zur Gathen and Gerhard [2013] Thm. 6.46). The expected cost of this gcd is \( \tilde{O}_B(d^3 + d^2 \tau) \). To see this, notice that we can perform a bivariate gcd in expected time \( \tilde{O}(d^2) \) (von zur Gathen and Gerhard [2013] Cor. 11.12), over a finite field with enough elements, and the bitsize of the result is \( \tilde{O}(d + \tau) \) [Mahler 1962].

Then, for a Las Vegas algorithm, using exact division, we test if the resulting polynomial divides all \( f_i \), for \( 2 \leq i \leq n \). This costs \( \tilde{O}_B(n d^3 + d^2 \tau) \), by adapting (von zur Gathen and Gerhard [2013] Ex.10.21) to the bivariate case. 

6
3. Rational curves

Following [Alcázar and Díaz-Toca (2010)] closely, we introduce basic notions for rational curves. Let \( \mathcal{C} \) be an algebraic curve over \( \mathbb{C}^n \), parametrized by the map

\[
\phi : \mathbb{C} \rightarrow \mathcal{C} \\
\phi(t) = (p_1(t)/q_1(t), \ldots, p_n(t)/q_n(t))
\]

(1)

where \( p_i, q_i \in \mathbb{Z}[t] \) are of size \((d, r)\) for \( i \in [n] \), and \( \mathcal{C} \) is the Zariski closure of Im(\( \phi \)). We call \( \phi(t) \) a parametrization of \( \mathcal{C} \).

We study the real trace of \( \mathcal{C} \), that is \( \mathcal{C} := \mathcal{C} \cap \mathbb{R}^n \). A parametrization \( \phi \) is characterized by means of properness (Sec. 3.1) and normality (Sec. 3.2). To ensure these properties, one can reparametrize the curve, i.e., apply a rational change of parameter to the given parametrization. We refer to (Sendra et al., 2008, Ch. 6) for more details on reparametrization.

Without loss of generality, we assume that no coordinate of the parametrization \( \phi \) is constant; otherwise we could embed \( \mathcal{C} \) in a lower dimensional space. We consider that \( \phi \) is in reduced form, i.e., \( \gcd(p_i(t), q_i(t)) = 1 \), for all \( i \in [n] \). The point at infinity, \( p_\infty \), is the point on \( \mathcal{C} \) we obtain for \( t \rightarrow \pm \infty \) (if it exists). For a parametrization \( \phi \), we consider the following system of bivariate polynomials:

\[
h_i(s, t) = \frac{p_i(s)q_i(t) - q_i(s)p_i(t)}{s - t}, \quad \text{for } i \in [n].
\]

(2)

**Remark 4.** For every \( i \in [n] \) \( h_i(s, t) \) is a polynomial since \((s, s)\) is a root of the numerator for every \( s \). Also, \( h_i(t, t) = \phi_i'(t)q_i^2(t) \) (Gutierrez et al., 2002h, Lem. 1.7).

3.1. Proper parametrization

A parametrization is proper if \( \phi(t) \) is injective for almost all points on \( \mathcal{C} \). In other words, almost every point on \( \mathcal{C} \) is the image of exactly one parameter value (real or complex). For other equivalent definitions of properness, we refer the reader to (Sendra et al., 2008, Ch. 4), (Rubio et al., 2009). As stated in (Alcázar and Díaz-Toca, 2010, Thm. 1), a parametrization is proper if and only if \( \deg(\gcd(h_1(s, t), \ldots, h_n(s, t))) = 0 \). This leads to an algorithm for checking properness. By applying Lem. 3 we get the following:

**Lemma 5.** There is an algorithm that checks if a parametrization \( \phi \) is proper in worst-case bit complexity \( \tilde{O}_B(n(d^3 + d^2r)) \) and in expected bit complexity \( \tilde{O}_B(n(d^3 + d^2r)) \).

**Proof.** We construct the polynomials \( h_i(s, t) \) for all \( i \in [n] \) in \( O_B(nd^2r) \). Then, we need to check if \( \deg(\gcd(h_1(s, t), \ldots, h_n(s, t))) = 0 \) (Alcázar and Díaz-Toca, 2010, Thm. 1). For the gcd computation, we employ Lem. 3 and the result follows.

If \( \phi \) is a not a proper parametrization, then there always exists a parametrization \( \psi \in \mathbb{Z}(t)^n \) and \( R(t) \in \mathbb{Z}(t) \) such that \( \psi(R(t)) = \phi(t) \) and \( \psi \) is proper (Sendra et al., 2008, Thm. 7.6). There are various algorithms for obtaining a proper parametrization, e.g., (Sederberg, 1986, Gutierrez et al., 2002a, Sendra et al., 2008, Pérez-Díaz, 2006, Gao and Chou, 1992). We consider the algorithm in (Pérez-Díaz, 2006) for its simplicity; its pseudo-code is in Alg. 1.
Lemma 6. Consider a non-proper parametrization of a curve \( C \), consisting of univariate polynomials of size \( (d, \tau) \). Alg. 1 computes a proper parametrization of \( C \), involving polynomials of degree at most \( d \) and bitsize \( O(\tau(d^2 + d^3 \tau)) \), in \( O(g(n(d^3 + d^4 \tau))) \), in the worst case.

Proof. The correctness of the algorithm is proved in [Perez-Diaz 2006]. We analyze its complexity. The algorithm first computes the bivariate polynomials \( H_i(s, t) = p_i(s)q_i(t) - p_i(t)q_i(s) \) for \( i = 1, \ldots, n \). They have bi-degree at most \( (d, d) \) and bitsize at most \( 2 \tau + 1 \). Then, we compute their gcd, which we denote by \( H \), in \( O(g(n(d^3 + d^4 \tau))) \) (Lem. 3). By [Mahler 1962] and [Basu et al. 2003] Prop. 10.12 we have that \( L(H) = O(d + \tau) \). If we write \( H = C_m(t)s^m + \cdots + C_0(t) \), it also holds that \( L(C_j) = O(d + \tau) \), \( j = 1, \ldots, m \).

If the degree of \( H \) is one, then the parametrization is already proper and we have nothing to do. Otherwise, we consider \( H \) as a univariate polynomial in \( s \) and we find two of its coefficients that are relatively prime, using exact division. The complexity of this operation is \( m^2 \times O(g(d^2 + d^3 \tau)) = O(g(n(d^2 + d^4 \tau))) \) (von zur Gathen and Gerhard 2013 Ex. 10.21).

Subsequently, we perform \( n \) resultant computations to get \( L_1, \ldots, L_n \), as defined in Alg. 1. From these we obtain the rational functions of the new parametrization. We focus on the computation of \( L_1 \). The same arguments hold for all \( L_n \). The bi-degree of \( L_1(s, x) = (d, d) \) [Basu et al. 2003 Prop. 8.49] and \( L(L_1) = O(d^2 + d^3 \tau) \) [Basu et al. 2003 Prop. 8.50]; the latter dictates the bitsize of the new parametrization.

To compute \( L_1 \), we consider \( F_1 \) and \( G \) as univariate polynomials in \( t \) and we apply a fast algorithm for computing the univariate resultant based on subresultants [Lickteig and Roy 2001]; it performs \( O(d) \) operations. Each operation consists of multiplying bivariate polynomials of bi-degree \( (d, d) \) and bitsize \( O(d^2 + d^3 \tau) \) so it costs \( O(g(d^3 + d^4 \tau)) \). We compute the resultant in \( O(g(d^5 + d^6 \tau)) \). We multiply the latter bound by \( n \) to conclude the proof. \[\square\]

\begin{algorithm}
\caption{MakeProper(\( \phi \))}
\begin{algorithmic}[1]
\Require A parametrization \( \phi \in \mathbb{Z}(t)^n \) as in Eq. (1)
\Ensure A proper parametrization \( \psi = (\psi_1, \ldots, \psi_n) \in \mathbb{Z}(t)^n \)
\For {\( i \in [n] \)} \( H_i(s, t) \leftarrow p_i(s)q_i(t) - p_i(t)q_i(s) \in \mathbb{Z}[s, t] \)
\EndFor \( H \leftarrow \gcd(H_1, \ldots, H_n) = C_m(t)s^m + \cdots + C_0(t) \in (\mathbb{Z}[t])[s] \)
\If {\( m = 1 \)} \Return \( \psi(t) \)
\EndIf \( R(t) \leftarrow \frac{C_m(t)}{C_0(t)} \)
\EndFor \( r \leftarrow \deg(R) = \max\{\deg(C_k), \deg(C_l)\} \)
\EndFor \( G \leftarrow sC_k(t) - C_l(t) \)
\Return \( \psi(t) = (\frac{\hat{p}_1(t)}{\hat{q}_1(t)} \cdots \frac{\hat{p}_n(t)}{\hat{q}_n(t)}) \)
\end{algorithmic}
\end{algorithm}
3.2. Normal parametrization

Normality of the parametrization concerns the surjectivity of the map $\phi$. The parametrization $\phi(t)$ is $\mathbb{R}$-normal if for all points $p$ on $C$ there exists $t_0 \in \mathbb{R}$ such that $\phi(t_0) = p$. When the parametrization is not $\mathbb{R}$-normal, the points that are not in the image of $\phi$ for $t \in \mathbb{R}$ are $p_\infty$ (if it exists) and the isolated points that we obtain for complex values of $t$ (Recio, 2007, Prop. 4.2). An $\mathbb{R}$-normal reparametrization does not always exist. We refer to (Sendra et al., 2008, Sec. 7.3) for further details. However, if $p_\infty$ exists, then we reparametrize the curve to avoid possible singularities at infinity. The point $p_\infty$ exists if $\deg(p_i) \leq \deg(q_i)$, for all $i \in [n]$.

**Lemma 7.** If $p_\infty$ exists, then we can reparametrize the curve using a linear rational function to ensure that $p_\infty$ is not a singular point, using a Las Vegas algorithm in expected time $O_B(n(d^2 + d\tau))$. The new parametrization involves polynomials of size $(d, \tilde{O}(d + \tau))$.

**Proof.** The point at infinity depends on the parametrization. So, for this proof, let us denote the point at infinity of $\phi$ by $p_\infty^\phi$. This point is obtained for $t \to \infty$.

The reparametrization consists of choosing $t_0 \in \mathbb{R}$ and applying the map $r : t \mapsto \frac{t + t_0}{1 - t_0}$ to $\phi$. The point at infinity of the new parametrization is $p_\infty^\psi = \phi(t_0)$. We need to ensure that $p_\infty^\phi = \phi(t_0)$ is not singular. There are $\leq d^2$ singular points, so we choose $t_0$ uniformly at random from the set $\{1, \ldots, Kd^2\}$ where $K \geq 2$. Then, with probability $\geq 1/2$, $\phi(t_0)$ is not singular and $p_\infty^\phi$ is also not singular. The bound on the possible values of $t_0$ implies that the bitsize of $t_0$ is $O(\log(d))$.

We compute the new parametrization, $\psi$, in $O_B(n(d^2 + d\tau))$ using multipoint evaluation and interpolation, by exploiting the fact that the polynomials in $\psi$ have degrees at most $d$ and bitsize $\tilde{O}(d + \tau)$.

For a Las Vegas algorithm we need to check if $\phi(t_0)$ is a cusp or a multiple point. For the former, we evaluate $\phi'$ at $t_0$ (see Rem. 4). This costs $O_B(nd\tau)$ (Bouzidi et al., 2013, Lem. 3). For the latter, we check if $\deg(\gcd(\phi_1(t_0)q_1(t) - p_1(t), \ldots, \phi_d(t_0)q_d(t) - p_d(t))) = 0$ in $O_B(n(d^2 + d\tau))$ (Lem. 2). If $\phi'(t_0)$ is not the zero vector and the degree of the gcd is zero, then $\phi(t_0)$ is not singular. 

**Remark 8.** Since the reparametrizing function in the previous lemma is linear, it does not affect properness (Sendra et al., 2008, Thm. 6.3).

4. Special points on the curve

We consider a parametrization $\phi$ of $C$ as in Eq. (1), such that $\phi$ is proper and there are no singularities at infinity. We highlight the necessity of these assumptions when needed. We detect the parameters that generate the special points of $C$, namely the singular, the isolated, and the extreme points (in the coordinate directions). We identify the values of the parameter for which $\phi$ is not defined, namely the poles (see Def. 9). In presence of poles, $C$ consists of multiple components.

**Definition 9.** The parameters for which $\phi(t)$ is not defined are the poles of $\phi$. The sets of poles over the complex and the reals are:

$$T_p^C = \{t \in \mathbb{C} : \prod_{i \in [n]} q_i(t) = 0\} \quad \text{and} \quad T_p^R = T_p^C \cap \mathbb{R}, \text{ respectively.}$$
We consider the solution set $S$ of the system of Eq. (2) over $\mathbb{C}^2$: 

$$S = \{(t, s) \in \mathbb{C}^2 : h_i(t, s) = 0 \text{ for all } i \in [n]\}.$$ 

**Remark 10.** Notice that when $\phi$ is in reduced form, if $(s, t) \in S$ and $(s, t) \in (\mathbb{C} \setminus T_p^S) \times \mathbb{C}$, then also $t \notin T_p^S$ [Rubio et al. 2009] (in the proof of) Lem. 9.

Next, we present some well-known results [Rubio et al., 2009; Sendra et al., 2008] that we adapt to our notation.

**Singular points.** Quoting Manocha and Canny (1992), “Algebraically, singular points are points on the curve, in whose neighborhood the curve cannot be represented as an one-to-one and $C^\infty$ bijective map with an open interval on the real line”. Geometrically, singularities correspond to shape features that are known as cusps and self-intersections of smooth branches. Cusps are points on the curve where the tangent vector is the zero vector. This is a necessary and sufficient condition when the parametrization is proper [Manocha and Canny (1992)]. Self-intersections are multiple points, i.e., points on $C$ with more than one preimages.

**Lemma 11.** The set of parameters corresponding to real cusps is

$$T_C = \left\{ t \in \mathbb{R} \setminus T_p^S : (t, t) \in S \right\}.$$

The set of parameters corresponding to real multiple points is

$$T_M = \{ t \in \mathbb{R} \setminus T_p^S : \exists s \neq t, s \in \mathbb{R} \text{ such that } (t, s) \in S \}.$$

**Proof.** The description of $T_C$ is an immediate consequence of Rem. 4. It states that $h_i(t, t) = \phi_i'(t)q_i^2(t)$, for $i \in [n]$.

Now let $p = \phi(t)$ be a multiple point on $C$. Then, there is $s \in \mathbb{R} \setminus T_p^S$ with $\phi(t) = \phi(s) \Rightarrow h_i(t, s) = 0$ for all $i \in [n]$ and so $t \in T_M$. Conversely, let $t \in T_M$ and $s \neq t, s \in \mathbb{R}$ such that $h_i(t, s) = 0$ for all $i \in [n]$. From [Rubio et al. 2009] (in the proof of) Lem. 9, when $\phi$ is in reduced form, if $(t, s) \in S$ and $(t, s) \in (\mathbb{R} \setminus T_p^S) \times \mathbb{R}$, then also $s \notin T_p^S$. So, $h_i(t, s) = 0 \Rightarrow \frac{\dot{\phi}(s)}{\phi(t)} = \frac{\dot{\phi}(t)}{\phi(s)}$ for all $i \in [n]$, and thus $p = \phi(t) = \phi(s)$ is a real multiple point.

Notice that $T_C$ and $T_M$ are not necessarily disjoint, for we may have both cusps and smooth branches that intersect at the same point.

**Isolated points.** An isolated point on a real curve can only occur for complex values of the parameter. The point at infinity is not isolated because it is the limit of a sequence of real points. So, additional care is needed in order to avoid cases where the point at infinity is obtained also for complex values of the parameter.

**Lemma 12.** The set of parameters generating isolated points of $C$ is

$$T_I = \{ t \in \mathbb{C} \setminus (\mathbb{R} \cup T_p^S) : (t, t) \in S \text{ and } \exists s \in \mathbb{R} \text{ s.t. } (t, s) \in S \text{ and } \phi(t) \neq \lim_{s \to \infty} \phi(s) \}.$$

**Proof.** Let $p = \phi(t) \in \mathbb{R}^n$ be an isolated point, where $t \in \mathbb{C} \setminus (\mathbb{R} \cup T_p^S)$. Notice that $p$ is also a multiple point, since it holds that $\phi(t) = \phi_i(t) = \phi_i(t)$ for $i \in [n]$. Thus, $h_i(t, t) = 0$ for all $i \in [n]$ and $(t, t) \in S$. Moreover, since $p$ is isolated, there are no real branches through $p$ and there does not exist $s \in \mathbb{R}$ such that $\phi(t) = \phi(s) \Rightarrow h_i(t, s) = 0$, for all $i \in [n]$. So, $t \in T_I$. 

10
Conversely, let \((t, \tilde{t}) \in S\) with \(t \in C \setminus \mathbb{R} \cup T_p^C\). Since \(\phi\) is in reduced form, we have that \(\tilde{t} \notin P^C\) (Rubio et al. 2009) (in the proof of Lem. 9), therefore \(h_i(t, \tilde{t}) = 0\), for all \(i \in [n]\), implies that \(\phi(t) = \phi(\tilde{t}) = \phi(t) \in \mathbb{R}^n\). Since there does not exist \(s \in \mathbb{R}\) with \(\phi(t) = \phi(s)\), \(p\) is an isolated point on \(C\).

**Extreme points.** Consider a vector \(\delta\) and a point on \(C\) whose normal vector is parallel to \(\delta\). If the point is not singular, then it is an extreme point of \(C\) with respect to \(\delta\). We compute the extreme points with respect to the direction of each coordinate axis. Rem. 4 leads to the following lemma:

**Lemma 13.** The set of parameters generating extreme points in the coordinate directions is

\[
T_E = \{t \in \mathbb{R} \setminus T_p^R : \prod_{i \in [n]} h_i(t, t) = 0 \text{ and } t \notin T_C \cup T_M\}.
\]

**4.1. Computation and Complexity**

From Lemmata 11, 12, and 13, it follows that given a proper parametrization \(\phi\) without singular points at infinity, we can easily find the poles and the set of parameters generating cusps, multiple, extreme, and isolated points. We do so by solving an over-determined bivariate polynomial system and univariate polynomial equations. Then, we classify the parameters that appear in the solutions, by exploiting the fact the system is symmetric. For sake of completeness, we describe the procedure in Alg. 2.

To compute the Rational Univariate Representation (RUR) (Rouillier 1999) of an overdetermined bivariate system (Thm. 16), we employ Lem. 14 and Prop. 15, which adapt the techniques used in Bouzidi et al. (2016) to our setting.

**Lemma 14.** Let \(f, g, h_1, \ldots, h_n \in \mathbb{Z}[X, Y]\) with degrees bounded by \(\delta\) and bitsize of coefficients bounded by \(L\). Computing a common separating element in the form \(X + \alpha Y, \alpha \in \mathbb{Z}\) for the \(n+1\) systems of bivariate polynomial equations \(\{f = g = 0\}, \{f = h_i = 0\}, i = 1 \ldots n\) needs \(\tilde{O}_B(n(\delta^5 + \delta^5 L))\) bit operations in the worst case, and \(\tilde{O}_B(n(\delta^5 + \delta^5 L))\) in the expected case with a Las Vegas Algorithm. Moreover, the bitsize of \(\alpha\) does not exceed \(\log(2n\delta^4)\).

**Proof.** A straightforward strategy consists of simultaneously running Algorithm 5 (worst case) or Algorithm 5’ (Las Vegas) from Bouzidi et al. (2016) on all the systems. The only modifications needed are that the values of \(\alpha\) to be considered are less than \(2n\delta^4\) (twice a bound on the total number of solutions of all the systems) and that the exit test is valid if and only if it is valid for all the systems.

**Proposition 15.** Let \(f, g \in \mathbb{Z}[X, Y]\) with degrees bounded by \(\delta\) and coefficients’ bitsizes bounded by \(L\). We can compute a rational parametrization \(\{h(T), X = \frac{h_x(T)}{h_T}, Y = \frac{h_y(T)}{h_T}\}\) of \(f, g\) with \(h, h_1, h_2, h_Y \in \mathbb{Z}[T]\) with degrees less than \(\delta^5\) and coefficients’ bitsizes in \(\tilde{O}_B(\delta^5 (L + \delta))\) bit operations in the worst case and \(\tilde{O}_B(\delta^5 (L + \delta))\) expected bit operations with a Las Vegas Algorithm.

**Proof.** Algorithms 6 and 6’ from Bouzidi et al. (2016) compute an RUR decomposition of \(f = g = 0\) in \(\tilde{O}_B(\delta^5 (L + \delta))\) bit operations in the worst case and \(\tilde{O}_B(\delta^5 (L + \delta))\) expected bit operations with a Las Vegas Algorithm respectively. They provide \(s \leq \delta\) parametrizations in the form \(\{h_i(T), \frac{h_{x_i}(T)}{h_i(T)}, \frac{h_{y_i}(T)}{h_i(T)}\}\), where \(i = 1, \ldots, s\), with the following properties:
Algorithm 2: Special_Points(φ)

**Input:** Proper parametrization φ ∈ ℤ(t)^n without singularity at infinity, as in Eq. (1)

**Output:** Real poles and parameters that give real cusps, multiple, isolated and extreme points with respect to the direction the coordinate axes.

/* The subroutines SOLVE_R and SOLVE_C return the solution set of a univariate polynomial or a system of polynomials over the real and complex numbers resp. */

1. Compute polynomials h_1(s, t), . . . , h_n(s, t)
2. T_p^R ← \bigcup_{i=1}^n SOLVE_R(q_i(t) = 0)
3. T_p^C ← \bigcup_{i=1}^n SOLVE_C(q_i(t) = 0)
4. S ← SOLVE_C(h_1(s, t) = 0, . . . , h_n(s, t) = 0)
5. T_C, T_M, T_f, W ← ∅
6. for (s, t) ∈ S do
   7.   if s = t and s ∈ ℝ \ T_p^R then
      8.     T_C ← T_C ∪ {t}
   9.   else if s ≠ t then
      10.  if t ∈ ℝ \ T_p^R then
           11.     if t ∈ ℝ then
                   12.       T_M ← T_M ∪ {t}
           13.     else
                   14.       W ← W ∪ {t}
      15.  else if s = t and s ∈ T_p^C then
           16.     T_f ← T_f ∪ {t}
    17.  T_f ← T_f \ W
/* Extreme points */
18.  T_E ← \bigcup_{i=1}^n SOLVE_R(h_i(t, t) = 0)
19.  T_E ← T_E \ (T_E \cap (T_C \cup T_M))

- \(\prod_{i=1}^n h_i\) is a polynomial of degree at most \(δ^2\) with coefficients of bitsize \(\tilde{O}(δL + δ^2)\).
- The degrees of \(h_{1,1}(T), h_{X,1}(T)\) and \(h_{Y,1}(T)\) are less than the degree of \(h_i\).
- The coefficients’ bitsizes of \(h_{1,1}(T), h_{X,1}(T)\) and \(h_{Y,1}(T)\) are in \(O(δL + δ^2)\).

Also,

\[\prod_{i=1}^t h_i, \sum_{i=1}^n h_{j,i} X \prod_{i̸=j} h_i, \sum_{i=1}^n h_{j,Y} Y \prod_{i̸=j} h_i, \sum_{i=1}^n h_{j,1} \prod_{i̸=j} h_i\]

is a rational parametrization of the system \(f = g = 0\), defined by polynomials of degree less than \(δ^2\) with coefficients of bitsize \(\tilde{O}(δ(L + δ))\) and can be computed from the RUR decomposition performing \(O(s)\) multiplications of polynomials of degree at most \(δ^2\) with coefficients of bitsize \(\tilde{O}(δ(L + δ))\), which requires \(\tilde{O}(δ^2(L + δ))\) bit operations. \(\square\)

12
Theorem 16. There exists an algorithm that computes the RUR and the isolating boxes of the roots of the system \(|h_1(s, t) = \cdots = h_n(s, t) = 0\) with worst-case bit complexity \(\tilde{O}_B(n(d^6 + d^2\tau)).\) There is also a Las Vegas variant with expected complexity \(\tilde{O}_B(d^6 + nd^3 + nd^2\tau).\)

Proof. Assume that we know a common separating linear element \(\ell(s, t) = \ell_0 + \ell_1 s + \ell_2 t\) that separates the roots of the \(n-1\) systems of bivariate polynomial equations \(|h_1 = h_2 = 0\), \(|h_1 = h_i = 0\), for \(3 \leq i \leq n\). We can compute \(\ell\) with \(\tilde{O}_B(n(d^6 + d^2\tau))\) bit operations in the worst case and with \(\tilde{O}_B(n(d^6 + d^2\tau))\) expected bit operations with a Las Vegas algorithm (Lem. [14]).

We denote an RUR for \(|h_1 = h_2 = 0\) with respect to \(\ell\) by \(\{\tau(T), \frac{r_1(T)}{r_3(T)}, \frac{r_2(T)}{r_3(T)}\}\). In addition, for \(i = 3 \ldots n\), let \(\{r_i(T), \frac{r_{i-2}(T)}{r_j(T)}, \frac{r_{i-1}(T)}{r_j(T)}\}\) be the RUR of \(|h_1 = h_i = 0\), also with respect to \(\ell\). We compute these representations for all \(i = 3 \ldots n\) with \(\tilde{O}_B(n(d^6 + d^2\tau))\) bit operations in the worst case, and with \(\tilde{O}_B(n(d^6 + d^2\tau))\) in expected case with a Las Vegas algorithm (Lem. [15]).

Then, for the system \(|h_1 = h_2 = \ldots = h_n = 0\) we can define a rational parametrization \(\chi(T) = \gcd(r(T), r_3(T), \ldots, r_n(T), r_3(T) r_3(T) - r_3(T) r_1(T), r_3(T) r_3(T) - r_3(T) r_1(T), \ldots, r_n(T) r_n(T) - r_n(T) r_1(T))\), where

\[
\chi(T) = \gcd(r(T), r_3(T), \ldots, r_n(T), r_3(T) r_3(T) - r_3(T) r_1(T), r_3(T) r_3(T) - r_3(T) r_1(T), \ldots, r_n(T) r_n(T) - r_n(T) r_1(T)).
\]

So to compute such a parametrization, we still need to compute the \(\gcd\) of \(3n-5\) univariate polynomials of degrees at most \(d^2\) and coefficients of bitsizes in \(\tilde{O}(d\tau)\) which needs \(\tilde{O}_B(n(d^6 + d^2\tau))\) bit operations in the worst case. Isolating the roots of such a parametrization requires \(\tilde{O}_B(d^6 + d^2\tau)\) according to Alg. 7 from Bouzidi et al. [2016].

Remark 17 (RUR and isolating interval representation). If we use Thm [10] to solve the over-determined bivariate system of the \(h_i\) polynomials of Eq. (2), then we obtain in the output an RUR for the roots, which is as follows: There is a polynomial \(\chi(T) \in \mathbb{Z}[T]\) of size \(\tilde{O}(d^2), \tilde{O}(d^2 + d\tau))\) and a mapping:

\[
V(\chi) \to V(h_1, \ldots, h_n), \quad T \mapsto \left(\frac{r_3(T)}{r_1(T)}, \frac{r_3(T)}{r_1(T)}\right),
\]

that defines an one-to-one correspondence between the roots of \(\chi\) and those of the system. The polynomials \(r_n, r_n,\) and \(r_1\) are in \(\mathbb{Z}[T]\) and have also size \(\tilde{O}(d^2), \tilde{O}(d^2 + d\tau))\).

Taking into account the cost to compute this parametrization of the solutions (Thm [10]), we can also compute the resultant of \(|h_1, h_2|\) with respect to \(s\) or \(t\) at no extra cost. Notice that both resultants are the same polynomial, since the system is symmetric. Let \(R_s(t) = \res_s(h_1, h_2).\) It is of size \(\tilde{O}(d^2), \tilde{O}(d^2 + d\tau)\) (Basu et al. [2002], Prop. 8.46).

Under the same bit complexity, we can sufficiently refine the isolating boxes of the solutions of the bivariate system (computed in Thm [10]), so that every root \((\frac{r_3(T)}{r_1(T)}, \frac{r_3(T)}{r_1(T)})\), where \(\chi(\xi) = 0\), has a representation as a pair of algebraic numbers in isolating interval representation:

\[
((R_s, I_{1,2} \times I_{2,2}), (R_s, J_{1,2} \times J_{2,2})).
\]
Both coordinates in the latter representation, are algebraic numbers which are roots of the same polynomial. Moreover, \(I_{2 \xi}, J_{2 \xi}\) are empty sets when the corresponding algebraic number is real. Therefore, we can immediately distinguish between real and complex parameters. At the same time, we associate to each isolating box of a root of \(R\), the algebraic numbers \(\rho = (\chi, I_\rho, J_\rho)\) for which it holds that \(\frac{\varphi(t)}{\tau^d}\) projects inside this isolating box. We can interchange between the two representations in constant time and this will simplify our computations in the sequel.

**Lemma 18.** Let \(C\) be a curve with a proper parametrization \(\phi(t)\) as in Eq. 4, that has no singularities at infinity. We compute the real poles of \(\phi\) and the parameters corresponding to singular, extreme (in the coordinate directions), and isolated points of \(C\) in worst-case bit complexity

\[
\widetilde{O}_B(n^d + n d^3 \tau + d^4 (n^2 + n \tau) + d^3 (n^2 \tau + n^3) + n^3 d^2 \tau),
\]

and using a Las Vegas algorithm in expected bit complexity

\[
\widetilde{O}_B(d^6 + d^4 (n + \tau) + d^4 (n^2 + n \tau) + d^3 (n^2 \tau + n^3) + n^3 d^2 \tau).
\]

**Proof.** The proof is an immediate consequence of the following:

- We compute all \(h_i \in \mathbb{Z}[s, t]\) in \(\tilde{O}_B(n d \tau)\): To construct each \(h_i\) we perform \(d^2\) multiplications of numbers of bitsize \(\tau\); the cost for this is \(\widetilde{O}_B(d^2 \tau)\). The bi-degree of each is at most \((d, d)\) and \(L(h_i) \leq 2 \tau + 1 = O(\tau)\).

- The real poles of \(\phi\) are computed in \(\widetilde{O}_B(n^2 (d^4 + d^2 \tau))\): To find the poles of \(\phi\), we isolate the real roots of each polynomial \(q_i(t)\), for \(i \in [n]\). This costs \(\widetilde{O}_B(n (d^3 + d^2 \tau))\) (Pan and Tsigaridas, 2017). Then we sort the roots in \(\widetilde{O}_B(n d (n^3 + d^2 \tau)) = \widetilde{O}_B(n^2 (d^4 + d^2 \tau))\).

- The parameters corresponding to cusps, multiple and isolated points of \(C\) are computed in \(\widetilde{O}_B(n (d^6 + d^4 \tau))\):

We solve the bivariate system of Eq. 6 in \(\widetilde{O}_B(n (d^6 + d^4 \tau))\) or in expected time \(\widetilde{O}_B(n^d + n d^3 + d^5 \tau + n d^4 \tau)\) (Thm. 16). Then we have a parametrization of the solutions of the bivariate system of Eq. 6 of the form of Eq. 7 and in the same time of the form of Eq. 8 (see Rem. 17). Some solutions \((s, t) \in S\) may not correspond to points on the curve, since \(s, t\) can be poles of \(\phi\).

Notice that from Rem. 10, \(s\) and \(t\) are either both poles or neither of them is a pole. We compute \(g_i = \gcd(R_s, Q)\), where \(Q(t) = \prod_{i \in [n]} q_i(t)\), and the gcd-free part of \(R_s\) with respect to \(Q\). This is done in \(\widetilde{O}_B(n^2 (d^2 \tau + n d^2 \tau))\) (Bouzidi et al., 2015b, Lem. 5).

Every root of \(R_s\) is an algebraic number of the form \((R_s, I_{1 \xi} \times I_{2 \xi})\), for some \(\xi\) that is root of \(\chi\).

We can easily determine if it corresponds to a cusp, a multiple or an isolated point; when real (i.e., \(I_{2 \xi} = \emptyset\)) it corresponds to a cusp of \(C\) if and only if \((\{R_s, I_{1 \xi}\}, (R_s, I_{2 \xi}))\) is in \(S\). Otherwise, it corresponds to a multiple point. When it is complex (i.e., \(I_{2 \xi} \neq \emptyset\)), it corresponds to an isolated point of \(C\) if and only if \((\{R_s, I_{1 \xi} \times I_{2 \xi}\}, \{R_s, I_{1 \xi} \times (-I_{2 \xi})\}) \in S\) and there is no root in \(S\) of the form \((\{R_s, I_{1 \xi} \times I_{2 \xi}\}, \{R_s, I_{1 \xi}\})\).

- The parameters corresponding to extreme points of \(C\) with respect to the direction of each coordinate axis are computed in \(\widetilde{O}_B(d^3 n \tau + d^3 (n^2 + n) + d^2 n^2 \tau)\):

For all \(i \in [n]\), \(h_i(t, t)\) is a univariate polynomial of size \(\widetilde{O}(d)\). Then, \(H(t) = \prod_{i \in [n]} h_i(t, t)\) is of size \(\widetilde{O}(n d \tau, \widetilde{O}(n \tau))\). The parameters that correspond to the extreme points are among the roots of \(H(t)\). To make sure that poles and parameters that give singular points are excluded, we compute good\(H, Q \cdot R_s\), where \(Q(t) = \prod_{i \in [n]} q_i(t)\), and the gcd-free part of \(H \) with respect to \(Q \cdot R_s\), say \(H\). Since \(Q \cdot R_s\) is a polynomial of size \((d^2 + nd) (d + n) \tau)\), the computation of the gcd and the gcd-free part costs \(\widetilde{O}(n (d^4 + n d^3 \tau + n^2 d^2 \tau))\) (Bouzidi et al., 2015b, Lem. 5).
Then, \( H = \gcd(H, Q \cdot R, H)H' \), and the real roots of \( H' \) give the parameters that correspond to the extreme points. We isolate the real roots of \( H' \) in \( \tilde{O}(n^3(d^3 + d^2\tau)) \), since it is a polynomial of size \( (\tilde{O}(nd), \tilde{O}(nd + \tau)) \).

5. **PTOP0: Topology and Complexity**

We present PTOP0, an algorithm to construct an abstract graph \( G \) that is isotopic (Boissonnat and Teillaud, 2006, p.184) to \( C \) when we embed it in \( \mathbb{R}^n \). We emphasize that, currently, we do not identify knots in the case of space curves. The embedding consists of a graph whose vertices are points on the curve given by their parameter values. The edges are smooth parametric arcs that we can continuously deform to branches of \( C \) without any topological changes. We need to specify a bounding box in \( \mathbb{R}^n \) inside which the constructed graph results in an isotopic embedding to \( C \). We comment at the end of the section on the case where an arbitrary box is provided at the input. We determine a bounding box in \( \mathbb{R}^n \), which we call characteristic, that captures all the topological information of \( C \).

**Definition 19.** A characteristic box of \( C \) is a box enclosing a subset of \( \mathbb{R}^n \) that intersects all components of \( C \) and contains all its singular, extreme (in the coordinate directions), and isolated points.

Let \( \mathcal{B}_C \) be a characteristic box of \( C \). If \( C \) is bounded, then \( C \subset \mathcal{B}_C \). If \( C \) is unbounded, then the branches of \( C \) that extend to infinity intersect the boundary of \( \mathcal{B}_C \). A branch of the curve extends to infinity if for \( t \to t_0 \), it holds \( ||\phi(t)|| > M \), for any \( M > 0 \), where \( t_0 \in \mathbb{R} \cup \{\infty\} \). 

Let \( \mathcal{B}_C \) be a characteristic box of \( C \). If \( C \) is bounded, then \( C \subset \mathcal{B}_C \). If \( C \) is unbounded, then the branches of \( C \) that extend to infinity intersect the boundary of \( \mathcal{B}_C \). A branch of the curve extends to infinity if for \( t \to t_0 \), it holds \( ||\phi(t)|| > M \), for any \( M > 0 \), where \( t_0 \in \mathbb{R} \cup \{\infty\} \). 

**Lemma 20.** Let \( C \) be a curve with a parametrization as in Eq. (7). For \( b = 15d^2(\tau + \log d) = \tilde{O}(d^2\tau) \), \( \mathcal{B}_C = [-2^b; 2^b]^n \) is a characteristic box of \( C \).

**Proof.** We estimate the maximum and minimum values of \( \phi_i \), \( i \in [n] \), when we evaluate it at the parameter values that correspond to special points and also at each pole that is not a root of \( q_i \).

Let \( t_0 \) be a parameter that corresponds to a cusp or an extreme point with respect to the \( i \)-th direction. Then, it is a root of \( \phi_i'(t_0) = 0 \). The degree of \( \phi_i(t) \) is \( \leq 2d - 1 \) and \( \mathcal{L}(\mathcal{N}) \leq 2^{d^2 + \log d^2 - 1} \). From Lem. 1 we conclude that \( |\phi_i(t_0)| \leq 2^{d^2 + \log d^2} \). Analogously, it holds that \( |q_i(t_0)| \geq 2^{d^2 + \log d^2 - 1} \).

Therefore,

\[ |\phi_i(t_0)| \leq 2^{d^2 + \log d^2} \]

Now, let \( (t_1, t_2) \) be two parameters corresponding to a multiple point of \( C \), i.e., \( (t_1, t_2) \) is a root of the bivariate system in Eq. (7). Take any \( j, k \in [n] \) with \( j \neq k \) and let \( R(t) = \text{res}_s(h_j, h_k) \). It holds that \( R(t_1) = 0 \). The degree of \( R \) is \( \leq 2d^2 \) and \( \mathcal{L}(\mathcal{R}) \leq 2d(\tau + \log d + \log(d + 1) + 1) \) (Basu et al., 2003, Prop. 8.29). By applying Lem. 1 we deduce that

\[ |\phi_i(t_1)| \leq 2^{d^2(\tau + \log d + \log(d + 1) + 1) + 4d^2 \tau(2d^2 + d) \log(2d^2 + d)} \]

Let \( t_1 \) be a pole of \( \phi \) with \( q_j(t_1) = 0 \), for some \( j \neq i \). If \( \phi_i(t_1) \) is defined, applying Lem. 1 gives

\[ |\phi_i(t_1)| \leq 2^{4d^2 + 4d \log 2d} \]

To conclude, we take the maximum of the three bounds. However, to simplify notation, we slightly overestimate the latter bound. \( \square \)
The vertices of the embedded graph must include the singular and the isolated points of C. Additionally, to rigorously visualize the geometry of C, we consider as vertices the extreme points of C, with respect to all coordinate directions, as well as the intersections of C with the boundary of the bounding box. We label the vertices of G using the corresponding parameter values generating these points, and we connect them accordingly. Alg. [3] presents the pseudo-code of PTOPO and here we give some more details on the various steps.

We construct G as follows: First, we compute the poles and the sets \( T_C, T_M, T_E, \) and \( T_I \) of parameters corresponding to “special points”. Then, we compute the characteristic box of \( \Gamma \) values generating these points, and we connect them accordingly.

**Lemma 21.** Let \( \mathcal{B} = [l_1, r_1] \times \cdots \times [l_n, r_n] \) in \( \mathbb{R}^n \) and \( \mathcal{L}(l_i) = \mathcal{L}(r_i) = \sigma_i \) for \( i \in [n] \). We can find the parameters that give the intersection points of \( \phi \) with the boundary of \( \mathcal{B} \) in \( \tilde{O}(n^d \sigma_i^2 + n^2 d^2 (\tau + \sigma_i)) \).

**Proof.** For each \( i \in [n] \) the polynomials \( q_i(t), p_i(t) = 0 \) and \( q_i(t) r_i - p_i(t) = 0 \) are of size \( (O(d), O(\tau + \sigma)) \). So, we compute isolating intervals for all their real solutions in \( \tilde{O}(d^2(\tau + \sigma)) \) [Pan, 2002]. For any root \( l_0 \) of each of these polynomials, since \( \phi \) is in reduced form (by assumption), we have \( l_0 \notin \mathcal{T}_P \). We check if \( l_0(e) \in [l_i, r_i], j \in [n] \setminus i \). This requires 3 sign evaluations of univariate polynomials of size \( (d, \tau + \sigma) \) at all roots of a polynomial of size \( (d, \tau + \sigma) \). The bit complexity of performing these operations for all the roots is \( \tilde{O}(d^3 + d^2(\tau + \sigma)) \) [Strzebonski and Tsagridas, 2019, Prop. 6]. Since we repeat this procedure \( n-1 \) times for every \( i \in [n] \), the total cost is \( \tilde{O}(n^d \sigma_i^2 + n^2 d^2 (\tau + \sigma)) \).

We partition \( T_C \cup T_M \cup T_E \cup T_I \cup T_B \) into groups of parameters that correspond to the same point on C. For each group, we add a vertex to G if and only if the corresponding point is strictly inside the bounding box \( B \); for the characteristic box it is strictly inside by construction.

**Lemma 22.** The graph G has \( \kappa = O(d^2 + nd) \) vertices, which can be computed using \( O(d^2 + nd) \) arithmetic operations.

**Proof.** Since \( T_B \cap T_M = \emptyset \) and \( T_E \cap T_M = \emptyset \), to each parameter in \( T_B \) and \( T_E \) corresponds a unique point on C. So for every \( t \in T_B \cup T_E \) we add a vertex to G, labeled by the respective parameter. Next, we group the parameters in \( T_C \cup T_M \cup T_I \) that give the same point on C and we add for each group a vertex at \( G \) labeled by the corresponding parameter values.

Grouping the parameters is done as follows: For every \( t \in T_C \cup T_M \) we add a vertex to G labeled by the set \( \{ s \in \mathbb{R} : (s, t) \in S \} \cup \{ t \} \) and for every \( t \in T_I \) we add a vertex to G labeled by the set \( \{ s \in C : (s, t) \in S \} \cup \{ t \} \). We compute these sets simply by reading the elements of \( S \).

It holds that \( T_B = O(nd) \), \( T_E = O(nd) \) and \( |S| = O(d^2) \). Since for each vertex, we can find the parameters that give the same point in constant time, the result follows.

We denote by \( v_1, \ldots, v_k \) the vertices (with distinct labels) of G and by \( \lambda(v_1), \ldots, \lambda(v_k) \) their label sets (i.e., the parameters that correspond to each vertex). Let T be the sorted list of parameters in \( T_C \cup T_M \cup T_E \cup T_B \) (notice that we exclude the parameters of the isolated points). If for two consecutive elements \( t_1 < t_2 \) in T, there exists a pole \( s \in \mathcal{T}_P^2 \) such that \( t_1 < s < t_2 \), then we split T into two lists: \( T_1 \) containing the elements \( \leq t_1 \) and \( T_2 \) containing the elements \( \geq t_2 \). We continue recursively for \( T_1 \) and \( T_2 \), until there are no poles between any two elements of the resulting list. This procedure partitions T into \( T_{v_1}, \ldots, T_{v_k} \).

To add edges to G, we consider each \( T_i \) with more than one element, where \( i \in [\ell] \), independently. For any consecutive elements \( t_1 < t_2 \) in \( T_i \), with \( t_1 \in \lambda(v_{i,1}) \) and \( t_2 \in \lambda(v_{i,2}) \), we add the
edge \([v_{i_1}, v_{i_2}]\). To avoid multiple edges, we make the convention that we add an edge between 
v_{i,j}, j = 1, 2, and an (artificial) intermediate point corresponding to a parameter in \((t_1, t_2)\). If \(p_\infty\) exists, we add an edge to the graph connecting the vertices corresponding to the last element of \(T_t\) and the first element of the \(T_1\).

**Algorithm 3: PTOPO(\(\phi\))** (Inside the characteristic box)

**Input:** A proper parametrization \(\phi \in \mathbb{Z}(t)^n\) without singular points at infinity.

**Output:** Abstract graph \(G\)

```plaintext
1 Compute real poles \(T_p^R\).
2 Compute parameters of ‘special points’ \(T_C, T_M, T_E, T_I\).
3 /* Characteristic box */
4 \(b ← 15d^2(\tau + \log d), \quad B_C ← [-2^b, 2^b]^n\)
5 \(T_B ← \) parameters that give to intersections of \(C\) with \(B_C\)
6 Construct the set of vertices of \(G\) using Lem 22
7 Sort the list of all the parameters \(T = [T_C, T_M, T_E, T_B]\).
8 Let \(T_1, \ldots, T_l\) the sublists of \(T\) when split at parameters in \(T_p^R\)
9 for every list \(T_t = [t_1, \ldots, t_{k_t}]\) do
10     for \(j = 1, \ldots, k_t - 1\) do
11         Add the edge \([t_{i,j}, t_{i,j+1}]\) to the graph
12         Add the edge \([t_{1,1}, t_{k_t}]\) to the graph
```

**Theorem 23 (PTOP0 inside the characteristic box).** Consider a proper parametrization \(\phi\) of curve \(C\) involving polynomials of degree \(d\) and bitsize \(\tau\), as in Eq. (1), that has no singularities at infinity. Alg. 3 outputs a graph \(G\) that, if embedded in \(\mathbb{R}^n\), is isotopic to \(C\), within the characteristic box \(B_C\). It has worst case complexity

\[
\tilde{O}_B(d^6(n + \tau) + nd^6\tau + n^2 d^4\tau + d^3(n^2\tau + n^3) + n^3 d^2\tau),
\]

while its expected complexity is

\[
\tilde{O}_B(d^6\tau + nd^6\tau + n^2 d^4\tau + d^3(n^2\tau + n^3) + n^3 d^2\tau).
\]

If \(n = O(1)\), then bounds become \(\tilde{O}_B(N^n)\), where \(N = \max[d, \tau]\).

**Proof.** We count on the fact that \(\phi\) is continuous in \(\mathbb{R} \setminus T_p^R\). Thus, for each real interval \([s, t]\) with \([s, t] \cap T_p^R = \emptyset\), there is a parametric arc connecting the points \(\phi(s)\) and \(\phi(t)\). Since for any (sorted) list \(T_t\), for \(i \in [t]\), the interval defined by the minimum and maximum value of its elements has empty intersection with \(T_p^R\), then for any \(s, t \in T_t\), there exists a parametric arc connecting \(\phi(s)\) and \(\phi(t)\) and it is entirely contained in \(B_C\). If \(p_\infty\) exists, then \(p_\infty\) is inside \(B_C\). Let \([t_{1,1}, t_{k_t}]\) be the first element of the first list and the last element of the last list. There is a parametric arc connecting \(\phi(t_{1,1})\) with \(p_\infty\) and \(p_\infty\) with \(\phi(t_{k_t})\). So we add the edge \([t_{1,1}, t_{k_t}]\) to \(G\). Then, every edge of \(G\) is embedded to a unique smooth parametric arc and the embedding of \(G\) can be trivially continuously deformed to \(C\).
For the complexity analysis, we know from Lem.18 that steps 1-2 can be performed in worst-case bit complexity
\[ \tilde{O}_b(nd^6 + nd^5 \tau + d^4(n^2 + n \tau) + d^3(n^2 \tau + n^3) + n^3 d^2 \tau), \]
and in expected bit complexity
\[ \tilde{O}_b(d^6 + d^5(n + \tau) + d^4(n^2 + n \tau) + d^3(n^2 \tau + n^3) + n^3 d^2 \tau), \]
using a Las Vegas algorithm. From Lemmata 20, 21, and 22 steps 4-5 cost \( \tilde{O}_b(n^2(d^3 \tau)) \).

To perform steps 6-7 we must sort all the parameters in \( T \cup T_P^R \), i.e., we sort \( O(d^2 + nd) \) algebraic numbers. The parameters that correspond to cusps and extreme points with respect to the \( i \)-th coordinate direction can be expressed as roots of \( \prod_{t \in [0, \tau]} h_i(t, \tau) \), which is of size \( (nd, n \tau) \). The poles are roots of \( \prod_{t \in [0, \tau]} q(t) \), which has size \( (nd, n \tau) \). The parameters that correspond to multiple points are roots of \( R \), which has size \( (d^3, d \tau) \). At last, parameters in \( T_B \) are roots of a polynomial of size \( (d, d^2 \tau) \).

We can consider all these algebraic numbers together as roots of a single univariate polynomial (the product of all the corresponding polynomials). It has degree \( O(d^2 + nd) \) and bitsize \( \tilde{O}(d^5 \tau + nd \tau) \). Hence, its separation bound is \( \tilde{O}(d^5 \tau + nd^2 \tau + nd^3 \tau + n^3 d \tau) \). To sort the list of all the algebraic numbers, we have to perform \( O(d^2 + nd) \) comparisons and each costs \( \tilde{O}(d^5 \tau + nd^2 \tau + nd^3 \tau + n^3 d \tau) \). Thus, the overall cost for sorting is \( \tilde{O}_b(d^6 \tau + nd^5 \tau + nd^3 \tau + n^3 d^3 \tau + n^3 d^2 \tau) \). The overall bit complexities in the worst and expected case follow by summing the previous bounds.

Following the proof of Thm. 23 we notice that the term \( d^5 \tau \) in the worst case bound is due to the introduction of the intersection points of \( C \) with \( B_C \). For visualizing the curve within \( B_C \), these points are essential and we cannot avoid them. However, if we are interested only in the topology of \( C \), i.e., the abstract graph \( G \), these points are not important any more. We sketch a procedure to avoid them and gain a factor of \( d \) in the complexity bound:

Assume that we have not computed the points on \( C \cap B_C \). We split again the sorted list \( T = [T_C, T_M, T_B] \) at the real poles, and we add an artificial parameter at the beginning and at the end of each sublist. The rest of the procedure remains unaltered.

To verify the correctness of this approach, it suffices to prove that the graph that we obtain by this procedure, is isomorphic to the graph \( G \). It is immediate to see that the latter holds, possibly up to the dissolution of the vertices corresponding to the first and last artificial vertices. Adding these artificial parameters does not affect the overall complexity, since we do not perform any algebraic operations. Therefore, the bit complexity of the algorithm is determined by the complexity of computing the parameters of the special points (Lem. 18), and so we have the following theorem:

**Theorem 24 (PTOP0 and an abstract graph).** Consider a proper parametrization \( \phi \) of curve \( C \) involving polynomials of degree \( d \) and bitsize \( \tau \), as in Eq. (1), that has no singularities at infinity. Alg. 2 outputs a graph \( G \) that, if we embed it in \( \mathbb{R}^n \), then it is isotopic to \( C \). It has worst case complexity
\[ \tilde{O}_b(nd^6 + nd^5 \tau + d^4(n^2 + n \tau) + d^3(n^2 \tau + n^3) + n^3 d^2 \tau), \]
while its expected complexity is
\[ \tilde{O}_b(d^6 + d^5(n + \tau) + d^4(n^2 + n \tau) + d^3(n^2 \tau + n^3) + n^3 d^2 \tau), \]
If \( n = O(1) \), then bounds become \( \tilde{O}_b(N^6) \), where \( N = \max\{d, \tau\} \).
Remark 25. If we are given a box \( B \subset \mathbb{R}^n \) at the input, we slightly modify \( \text{PTOP} \), as follows: We discard the parameter values in \( T_C \cup T_M \cup T_E \cup T_I \) that correspond to points not contained in \( B \). The set of \( G \)'s vertices is constructed similarly. To connect the vertices, we follow the same method with a minor modification: For any consecutive elements \( t_1 < t_2 \) in a list \( T_i \) with more than two elements, such that \( t_1 \in \lambda(v_{i,1}) \) and \( t_2 \in \lambda(v_{i,2}) \), we add the edge \( \{v_{i,1}, v_{i,2}\} \) if and only if \( \phi(t_1), \phi(t_2) \) are not both on the boundary of \( B \); or in other words \( t_1 \) and \( t_2 \) are not both in \( T_B \).

6. Isotopic embedding for the special cases of plane and space curves

In this section we elaborate on the isotopic embedding of the output graph \( G \) of Thm. 24 for the case of plane and space parametric curves \( C \). We embed every edge of the abstract graph \( G \) in the corresponding parametric arc by sampling many parameter values in the associated parametric interval and then connecting the corresponding points accordingly, in \( \mathbb{R}^2 \) or \( \mathbb{R}^3 \). The larger the number of sampled parameters, the more likely it is for the embedding to be isotopic to \( C \). However, we might need a prohibitive large number of points to sample; their number is related to the distance between two branches of the curve. We show that by introducing a few additional points, we can replace the parametric arcs of the embedded graph with straight line segments and count on it being isotopic to \( C \). Following Alcázar et al. (2020) closely, if
For plane curves, there is no need to take intermediate points on each parametric arc. We consider the embedding of the abstract graph \( G \) in \( \mathbb{R}^2 \) as a straight-line graph \( \tilde{G} \), i.e., with straight lines for edges, whose vertices are mapped to the corresponding points of the curve. The vertices of \( \tilde{G} \) are all the singular and extreme points with respect to the \( x \)- and \( y \)-directions. Therefore, the edges of \( \tilde{G} \) correspond to smooth and monotonous parametric arcs and so they cannot intersect but at their endpoints. The embedding \( \tilde{G} \) is then trivially continuously deformed to \( C \). The above discussion summarizes as follows:

**Corollary 26** (PT0P0 and isotopic embedding for plane curves). Consider a proper parametrization \( \phi \) of a curve \( C \) in \( \mathbb{R}^2 \) involving polynomials of degree \( d \) and bitsize \( \tau \), as in Eq. (1), that has no singularities at infinity. Alg 3 computes an abstract graph whose straight-line embedding in \( \mathbb{R}^2 \) is isotopic to \( C \) in worst case complexity \( \tilde{O}_B(d^6 + d^5 \tau) \).

For space curves, a straight-line embedding of \( G \) is not guaranteed to be isotopic to \( C \) for knots may be present. To overcome this issue, we need to segment some edges of \( G \) into two or more edges. To find the extra vertices that we need to add to the graph, we follow a common approach (Alc´azar and D´ıaz-Toca, 2010; Alc´azar et al., 2020; Kahoui, 2008; Diatta et al., 2008; Cheng et al., 2013) that projects the space curve to a plane one. For a projection defined by the map \( \pi : C \to \mathbb{R}^2 \), we write \( \tilde{C} = \pi(C) \). We will ensure in the sequel that the following two conditions are satisfied:

1. (C1) \( C \) has no asymptotes parallel to the direction of the projection.
2. (C2) The map \( \pi \) is birational (Sendra et al., 2008 Def. 2.37).

The first condition is to ensure that the point at infinity \( p_\infty \) of \( C \) exists if and only if the point at infinity of \( \tilde{C} \) exists and is equal to \( \pi(p_\infty) \) (Alc´azar and D´ıaz-Toca, 2010 Lem. 10); see Fig 3b for an instance where this condition is violated. The second condition ensures that only a finite number of points on \( \tilde{C} \) have more than one point as a preimage. We call these points apparent singularities (Diatta et al., 2008); see Fig 3a. Thus, with this condition we avoid the "bad" cases where two branches of \( C \) project to the same branch of \( \tilde{C} \).

**Lemma 27.** Consider a proper parametrization \( \phi \) of curve \( C \) in \( \mathbb{R}^3 \) involving polynomials of degree \( d \) and bitsize \( \tau \), as in Eq. (1), that has no singularities at infinity. We compute a map \( \pi : C \to \mathbb{R}^2 \) satisfying conditions (C1), (C2) in worst case complexity \( \tilde{O}_B(d^5 + d^4 \tau) \) and using a Las Vegas algorithm in expected complexity \( \tilde{O}_B(d^3 + d^2 \tau) \).

**Proof.** By (Walker, 1978 Thm. 6.5, pg. 146), any space curve can be birationally projected to a plane curve. We choose an integer \( a \) uniformly at random from the set \( \{1, \ldots, Kd^2\} \), where \( K = O(1) \); we explain later in the proof about the size of this set. We define the mapping:

\[
\pi : \mathbb{C}^3 \to \mathbb{C}^2 \\
(x, y, z) \mapsto (x, y + az)
\]

It will be useful in the sequel to regard the application of \( \pi(\cdot) \) to \( \phi(t) \) as being performed in two steps:
Graph of the curve parametrized by \( \phi \) with two points in its preimage, i.e., apparent singularities (purple). (b) Graph of the curve parametrized by (green) and its orthogonal projection on the xy-plane (blue). In red, a double point in the projected curve (Díaz-Toca, 2010, Lem. 9); this is no more costly than solving a univariate polynomial of size \((O(\log n), \log^2 n))\). The asymptotes of \( C \) to infinity.

To infinity.

To infinity.

To infinity.

To infinity.

To infinity.

To infinity.

To infinity.

To infinity.

To infinity.

To infinity.

To infinity.

To infinity.

To infinity.

To infinity.

To infinity.

To infinity.

To infinity.

To infinity.

To infinity.

To infinity.

To infinity.
To find the values of $a$ that result in a ‘bad’ map: Let $h_1(s,t), h_2(s,t)$ be the polynomials of Eq. (1) associated to $\pi(\phi(t))$. The parametrization $\pi(\phi(t))$ is proper if and only if $\gcd(h_1(s,t), h_2(s,t)) = 1$. If $\gcd(h_1(s,t), h_2(s,t)) \neq 1$ then, by letting $R(s) = \text{res}_t(h_1(s,t), h_2(s,t))$, we have that $R(s) = 0$. Notice that $R(s)$ is not always identically zero (e.g., for $h_1(s,t) = t + s$, $h_2(s,t) = t + s - 1$ we get $R(s) = 1$). We consider $R(s)$ as a polynomial in $\mathbb{Z}[a][s]$: 

$$R(s) = c_d(a)s^d + \cdots + c_1(a)s + c_0(a),$$

where $c_i \in \mathbb{Z}[a]$ is of size $(d, \tilde{O}(d^2))$ for $0 \leq i \leq d$. The bad values of $a \in \mathbb{R}$ satisfy then the equation:

$$c_d(a) + \cdots + c_1(a) + c_0(a) = 0.$$

The polynomial has degree $O(d^2)$ and so there are $O(d^2)$ bad values to avoid. This points to the worst case complexity $\tilde{O}_B(d^5 + d^4 \tau)$. \hfill $\square$

Given a map $\pi$ computed through Lem. 27 we find the parameters that give the real multiple points of $\tilde{C}$ and its extreme points with respect to the two coordinate axes. We add the corresponding vertices to $G$ and we obtain an augmented graph, say $G'$. The straight-line embedding of $G'$ in $\mathbb{R}^2$ is isotopic to $\tilde{C}$ by Cor. 26, possibly up to the isolated points [Alcázar and Díaz-Toca, 2010] Thm. 13 and Lem. 15. Then, by lifting this embedding to the corresponding straight-line graph in $\mathbb{R}^3$, we obtain a graph isotopic to $C$ [Alcázar and Díaz-Toca, 2010] Thm. 13 and Thm. 14). The following theorem summarizes the previous discussion and states its complexity:

**Theorem 28 (PTOP0 and isotopic embedding for 3D space curves).** Consider a proper parametrization $\phi$ of curve $C$ in $\mathbb{R}^3$ involving polynomials of degree $d$ and bitsize $\tau$, as in Eq. (1), that has no singularities at infinity. There is an algorithm that computes an abstract graph whose straight-line embedding in $\mathbb{R}^3$ is isotopic to $C$ in worst case complexity $\tilde{O}_B(d^5 + d^4 \tau)$.

**Proof.** Given a projection map $\pi(\cdot)$ such that (C1) and (C2) hold, correctness follows from the previous discussion. From Lem. 27 we find such a map in expected complexity $\tilde{O}_B(d^3 + d^2 \tau)$ and $\tilde{O}_B(d^2 + d^2 \tau)$. Using Alg. 2 for $\pi(\phi(t))$ we find the parameters of the extreme (in the coordinate directions) and real multiple points of $\tilde{C}$, say $\tilde{T}$, in $\tilde{O}_B(d^6 + d^5 \tau)$ (Lem. 18). Then, we employ Alg. $8$ for $\phi(t)$, by augmenting the list of parameters that are treated with $\tilde{T}$. The last step dominates the complexity and is not affected by the addition of extra parameters to the list since $|\tilde{T}| = O(d^2)$. The complexity result in Thm. 24 allows us to conclude. \hfill $\square$

**Remark 29.** The complexity in Thm. 28 is no higher than the complexity in Thm. 24 i.e., no costlier than the computation of the topology itself.

7. Multiplicities and characterization of singular points

We say that a singularity is ordinary if it is at the intersection of smooth branches only and the tangents to all branches are distinct [Walker, 1978 p.54]. In all the other cases, we call it a non-ordinary singularity. The character of a singular point is either ordinary or non-ordinary. To determine the multiplicity and the character of each real singular point in $\tilde{C}$ we follow the method presented in the series of papers Pérez-Díaz (2007), Blasco and Pérez-Díaz (2017), Blasco and Pérez-Díaz (2019). They provide a complete characterization using resultant computations that
Also, when the parameters in the black squares.

The multiple points are indicated by the red squares. (b) a space curve parametrized by $(\frac{\phi_1}{\phi_2}, \frac{\phi_2}{\phi_3}, \frac{\phi_3}{\phi_4})$.

The apparent singularities are indicated by the black squares.

Figure 4: Output of $PTOP$ for (a) a Lissajous curve parametrized by $(\frac{-t^2-1}{t^2+1}, \frac{-8t^2-19t^4-6t^4+1}{t^2-1}, \frac{-16t^2+6t^4+1}{t^2+1} \cdot \frac{1}{5} \cdot \frac{6t^4+28t^2+25t}{5t^3} \cdot \frac{6t^4+28t^2+25t}{5t^3+11t+6} \cdot \frac{3t^4+3t^3}{3t^4+3t^3+11} )$.

The multiple points are indicated by the red squares. (b) a space curve parametrized by $(\frac{-2t^2}{t^2+1}, \frac{-2t^2-19t^4+6t^4-16}{t^2+1} \cdot \frac{3t^4+3t^3}{3t^4+3t^3+11}, t)$. The apparent singularities are indicated by the black squares.

applies to curves of any dimension. In the sequel, we present the basic ingredients of their approach and we estimate the bit complexity of the algorithm.

Let $n = 2$ and $H_i(s, t) = p_i(s)q_i(t) - p_i(t)q_i(s)$, for $i \in [2]$. Consider a point $p \in C$ given by the parameter values $\{s_1, \ldots, s_k\}$, $k \geq 1$; that is $p = \phi(s_i)$, for all $i \in [k]$. The fiber function at $p$ (Blasco and Perez-Diaz, 2019) Def. 2) is

$$F_p(t) = \gcd(H_1(s_j, t), H_2(s_j, t)), $$

for any $j \in [k]$. It is a univariate polynomial, the real roots of which are the parameter values that correspond to the point $p$. When the parametrization of the curve is proper, for any point $p$ on $C$ other than $p$, it holds that $\deg(F_p(t)) = \text{mult}_p(C)$ (Blasco and Perez-Diaz, 2019) Cor. 1).

Also, when the parameters in $\{s_1, \ldots, s_k\}$ are all real, $k$ equals the number of real branches that go through $p$.

To classify ordinary and non-ordinary singularities we proceed as follows: For a point $p \in C$ the delta invariant $\delta_p$ is a nonnegative integer that measures the number of double points concentrated around $p$. We can compute it by taking into account the multiplicities of $p$ and its neighboring singularities. Blasco and Perez-Diaz (2019) consider three different types of non-ordinary singularities and use the delta invariant to distinguish them. In particular:

1. If $k = \text{mult}_p(C)$ and $2\delta_p = \text{mult}_p(C)(\text{mult}_p(C) - 1)$, then $p$ is an ordinary singularity.
2. If $k < \text{mult}_p(C)$ and $2\delta_p = \text{mult}_p(C)(\text{mult}_p(C) - 1)$, then $p$ is a type I non-ordinary singularity.
3. If $k = \text{mult}_p(C)$ and $2\delta_p > \text{mult}_p(C)(\text{mult}_p(C) - 1)$, then $p$ is a type II non-ordinary singularity.
4. If $k < \text{mult}_p(C)$ and $2\delta_p > \text{mult}_p(C)(\text{mult}_p(C) - 1)$, then $p$ is a type III non-ordinary singularity.
Theorem 30. Let $C$ be a curve with a proper parametrization $\phi(t)$ as in Eq. (7), that has no singularities at infinity. Alg. 4 computes the singular points of $C$, their multiplicity and character (ordinary/non-ordinary) in

$$\mathcal{O}_B(d^6 + d^5\tau)$$

worst-case complexity when $n = 2$ and for $n > 2$ in expected complexity

$$\mathcal{O}_B(d^6 + d^5(n + \tau) + d^4(n^2 + n\tau) + d^3(n^2\tau + n^3) + n^3d^2\tau).$$

Proof. We compute the parameters that give the singular points of $C$ using Alg. 2 in $\mathcal{O}_B(d^6 + d^5(n + \tau) + d^4(n^2 + n\tau) + d^3(n^2\tau + n^3) + n^3d^2\tau)$ when $n > 2$, which becomes worst-case when $n = 2$ (Lem. 13).

When $n > 2$, lines 5-8 compute a birational projection of $C$ to a plane curve parametrized by $\tilde{\phi}(t)$ (note that the projection is birational if and only if $\phi(t)$ is proper since $\phi(t)$ is proper). The expected complexity of this is $\tilde{\mathcal{O}}_B(d^3 + nd^2\tau)$ by slightly adapting the proof of Lem. 27.

We can group the parameter values that give singular points using Lem. 22 in $O(d^2 + nd)$ arithmetic operations. We have that $\gcd(H_1(s,t), H_2(s,t)) = s - t$. For $h_1(s,t) = H_1(s,t)/(s-t)$, $h_2(s,t) = H_2(s,t)/(s-t)$, we compute a triangular decomposition of the system $[h_1(s,t) = h_2(s,t) = 0]$ which consists of the systems $[A_i(s,t), B_i(s,t)]_{i\in I}$. For any root $\alpha$ of $A_i, B_i(\alpha,t)$ is of degree $i$ and equals $\gcd(h_1(\alpha,t), h_2(\alpha,t))$ (up to a constant factor). By (Bouzidi et al., 2015a, Prop. 16), the triangular decomposition is computed in $\tilde{\mathcal{O}}_B(d^6 + d^5\tau)$ worst case \footnote{In a Las Vegas setting this computation could be reduced to $\tilde{\mathcal{O}}_B(d^4 + d^3\tau)$, but since it does not affect the total complexity we chose not to expand onto this.}.

Blasco and Pérez-Díaz (2019) compute the delta invariant, $\delta_p$, using the formula

$$\delta_p = \frac{1}{2} \sum_{j=1}^{k} \sum_{t \text{ s.t. } h_j(s,t)=h_j(t,t)=0} \text{Int}_{h_1,h_2}(s_j,t),$$

(6)

where $\text{Int}_{h_1,h_2}(\alpha,\beta)$ is the intersection multiplicity of the coprime polynomials $h_1(s,t)$ and $h_2(s,t)$ at a point $(\alpha,\beta)$. Using a well known result, e.g., (Fulton 1984, 1.6) as stated in (Busé et al., 2005, Prop. 5), we can compute the intersection multiplicities using resultant computations. Let $R(s) = \text{res}_t(h_1(s,t), h_2(s,t))$. For a root $\alpha$ of $R(s)$, its multiplicity $\mu(\alpha)$ is equal to the sum of the intersection multiplicities of solutions of the system of $[h_1,h_2]$ in the form $(\alpha,t)$, and so

$$\mu(\alpha) = \sum_{t \text{ s.t. } h_1(\alpha,t)=h_2(\alpha,t)=0} \text{Int}_{h_1,h_2}(\alpha,t).$$

(7)

Therefore, from Eq. (6) and Eq. (7), we conclude that:

$$\delta_p = \frac{1}{2} \sum_{j=1}^{k} \mu(s_j).$$

(8)

For space curves, we birationally project $C$ to a plane curve (Walker 1978, Thm. 6.5, pg. 146). The multiplicities of the singular points of $C$ and their delta invariant are preserved under the birational map realizing the projection (Blasco and Pérez-Díaz, 2019, Prop. 1 and Cor. 4). The pseudo code of the algorithm appears in Alg. 4.
For a singular point \( p \) and \( s_0 \in M_p \): To compute the degree of \( \gcd(H_1(s_0), H_2(s_0)) \), since \( s_0 \) is a root of \( \res_s(h_1(s,t), h_2(s,t)) \), it suffices to find for which \( i \in I A_i(s_0) = 0 \). The latter is not immediate when \( s_0 \) is given in isolated interval representation as a root of \( \res_s(h_1(s,t), h_2(s,t)) \). However, we can isolate the roots of all \( A_i \) by taking care that the isolating intervals are small enough so that the isolating interval of \( s_0 \) intersects only one of them. Because they are roots of the same polynomial this cannot exceed the complexity of isolating the roots of \( \res_s(h_1(s,t), h_2(s,t)) \). This is can be done in \( \tilde{O}(d^n + d^2 \tau) \). In the same bit complexity, we have the multiplicity \( \mu(s_j) \) of \( s_j \) as a root of \( \res_s(h_1, h_2) \). \( \square \)
Figure 5: Output of PTOPO for a curve parametrized by (a) 
\[(−7t^4+22t^3−55t^2−94t+87, −50t^3+22t^2+37t−71, −56t^4+62t^3+97t−73)\]
(b) 
\[(−3t^2+1) \left(\frac{−3t^2+1}{t^2+1}\right), \left(−3t^2+1\right) \left(\frac{−3t^2+1}{t^2+1}\right), \left(−3t^2+1\right) \left(\frac{−3t^2+1}{t^2+1}\right)\]
The red star in (a) corresponds to an isolated point, whereas the red square in (b) corresponds to a multiple point. Examples are taken from Alcázar and Díaz-Toca (2010).

8. Implementation and examples

PTOP0 is implemented in Maple for plane and 3D curves. A typical output appears in Figures 1, 2, 5a, and 5b. Besides the visualization the software computes all the points of interest of curve (singular, extreme, etc) in isolating interval representation as well as in suitable floating point approximations.

We build upon the real root isolation routines of Maple’s RootFinding library and the slv package (Diochnos et al., 2009), to use a certified implementation of general purpose exact computations with one and two real algebraic numbers, like comparison and sign evaluations, as well as exact (bivariate) polynomial solving.

PTOP0 computes the topology and visualizes parametric curves in two (and in the near future in three) dimensions. For a given parametric representation of a curve, PTOP0 computes the special points on the curve, the characteristic box, the corresponding graph, and then it visualizes the curve (inside the box). The computation, in all examples from literature we tested, takes less than a second in a MacBook laptop, running Maple 2020. We refer the reader to the website of the software and to (Katsamaki et al., 2020b) for further details.

Acknowledgments. We acknowledge partial support by the Fondation Mathématique Jacques Hadamard through the PGMO grand ALMA, by ANR JCJC GALOP (ANR-17-CE40-0009), by the PHC GRAPE, by the projects 118F321 under the program 2509, 118C240 under the program 2232, and 117F100 under the program 3501 of the Scientific and Technological Research Council of Turkey.

https://gitlab.inria.fr/ckatsama/ptopo

This project has received funding from the European Union’s Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement No 754362.
References

URL https://doi.org/10.1145/77269.77273


URL https://hal.inria.fr/hal-01342211

URL http://doi.acm.org/10.1145/2465506.2465519

URL https://hal.inria.fr/hal-00977671

URL https://hal.inria.fr/hal-00847802


URL https://hal.inria.fr/hal-00077671


Diatta, D. N., Mourrain, B., Ruatta, O., 2008. On the computation of the topology of a non-reduced implicit space curve.
URL https://doi.org/10.1145/1390768.1390778


Li, Y.-M., Cripps, R. J., 1997. Identification of inflection points and cusps on rational curves. CAGD 14 (5), 491 – 497.

URL https://doi.org/10.1006/jsco.2000.0427


28


