



**HAL**  
open science

# Algorithm for connectivity queries on real algebraic curves

Nazrul Islam, Adrien Poteaux, Rémi Prébet

► **To cite this version:**

Nazrul Islam, Adrien Poteaux, Rémi Prébet. Algorithm for connectivity queries on real algebraic curves. ISSAC 2023 - 48th International Symposium on Symbolic and Algebraic Computation, Jul 2023, Tromsø, Norway. 10.1145/3597066.3597081 . hal-04000614v2

**HAL Id: hal-04000614**

**<https://hal.science/hal-04000614v2>**

Submitted on 16 Jun 2023

**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.



Distributed under a Creative Commons Attribution 4.0 International License

# Algorithm for Connectivity Queries on Real Algebraic Curves

Md Nazrul Islam  
Diebold Nixdorf  
London, Canada  
mdnazrul.islam@dieboldnixdorf.com

Adrien Poteaux  
Univ. Lille, CNRS, Centrale Lille, UMR  
9189 CRISTAL  
Lille, France  
adrien.poteaux@univ-lille.fr

Rémi Prébet  
Sorbonne Université, CNRS, LIP6  
F-75005 Paris, France  
remi.prebet@lip6.fr

## ABSTRACT

We consider the problem of answering connectivity queries on a real algebraic curve. The curve is given as the real trace of an algebraic curve, assumed to be in generic position, and being defined by some rational parametrizations. The query points are given by a zero-dimensional parametrization.

We design an algorithm which counts the number of connected components of the real curve under study, and decides which query point lie in which connected component, in time  $\log$ -linear in  $N^6$ , where  $N$  is the maximum of the degrees and coefficient bit-sizes of the polynomials given as input. This matches the currently best-known bound for computing the topology of real plane curves.

The main novelty of this algorithm is the avoidance of the computation of the complete topology of the curve.

## 1 INTRODUCTION

This work addresses the problem of designing an algorithm for answering connectivity queries on real algebraic curves in  $\mathbf{R}^n$ , defined as real traces of algebraic curves of  $\mathbf{C}^n$ .

*Motivation and problem statement.* Consider a real field  $\mathbf{Q}^1$ , its real closure  $\mathbf{R}$  and its algebraic closure  $\mathbf{C}$ . For  $n \geq 1$ , let  $X = (x_1, \dots, x_n)$  be a sequence of indeterminates, and denote  $\mathbf{Q}[X]$  and  $\mathbf{C}[X]$  the rings of multivariate polynomials in the  $x_i$ 's, with coefficients in resp.  $\mathbf{Q}$  and  $\mathbf{C}$ . We define an *algebraic set*  $\mathcal{C} \subset \mathbf{C}^n$  as the set of common zeros  $\mathbf{V}(f_1, \dots, f_p)$  of a sequence of polynomials  $(f_1, \dots, f_p) \subset \mathbf{C}[X]$ .  $\mathbf{I}(\mathcal{C}) \subset \mathbf{C}[X]$  is the radical of the ideal  $\langle f_1, \dots, f_p \rangle$  generated by the  $f_j$ 's, that is the *ideal of definition* of  $\mathcal{C}$ . The *function ring*  $\mathbf{C}[\mathcal{C}]$  of polynomial functions defined on  $\mathcal{C}$  is  $\mathbf{C}[X]/\mathbf{I}(\mathcal{C})$ . If  $\mathbf{I}(\mathcal{C}) \subset \mathbf{Q}[X]$ , we also denote  $\mathbf{Q}[\mathcal{C}]$  by  $\mathbf{Q}[X]/\mathbf{I}(\mathcal{C})$ . Finally,  $\mathcal{C}$  is an *algebraic curve* if  $\mathbf{I}(\mathcal{C})$  is equidimensional of dimension 1, and *plane* if contained in some plane of  $\mathbf{C}^n$ .

In this document,  $\mathcal{C}$  is an algebraic curve such that  $\mathbf{I}(\mathcal{C}) \subset \mathbf{Q}[X]$ . Given a generating system  $f$  of  $\mathbf{I}(\mathcal{C})$ ,  $\text{Jac}(f)$  is the Jacobian matrix of  $f$ ,  $\text{sing}(\mathcal{C})$  the set of singular points of  $\mathcal{C}$  (i.e. the points where  $\text{Jac}(f)$  has rank less than  $n - 2$ ; it is a finite subset of  $\mathcal{C}$ ) and  $\text{reg}(\mathcal{C}) = \mathcal{C} - \text{sing}(\mathcal{C})$ . For all  $\mathbf{x} \in \text{reg}(\mathcal{C})$ ,  $T_{\mathbf{x}}\mathcal{C}$  is the right-kernel of  $\text{Jac}(f)$ : it is the tangent line of  $\mathcal{C}$  at  $\mathbf{x}$ . For  $1 \leq i \leq n$  we let  $\pi_i : \mathbf{C}^n \rightarrow \mathbf{C}^i$  be the canonical projection on the first  $i$  variables. If  $\mathcal{C}_2 \subset \mathbf{C}^2$  is the Zariski closure of  $\pi_2(\mathcal{C})$ , the set of apparent singularities of  $\mathcal{C}_2$  is  $\text{app}(\mathcal{C}_2) = \text{sing}(\mathcal{C}_2) - \pi_2(\text{sing}(\mathcal{C}))$ . These are the singularities introduced by  $\pi_2$ . A singular point of  $\mathcal{C}_2$  is called

<sup>1</sup>Note that in Sections 2 and 3,  $\mathbf{Q}$  can be any arbitrary field of characteristic 0.

We thank I. Bannwarth, M. Safey El Din and É. Schost for sharing some preliminary private notes on this problem, which helped to understand the difficulties to lift. The last author is supported by the joint Agence nationale de la recherche (ANR) Austrian Science Fund FWF grant agreement ANR-FWF ANR-19-CE48-0015 ECARP project.

a node if it is an ordinary double point (see [31, §3.1]). We refer to [48] for definitions and propositions about algebraic sets.

For any  $\varphi \in \mathbf{C}[\mathcal{C}]$ , we denote by  $\mathcal{W}^\circ(\varphi, \mathcal{C})$  the set of *critical points of  $\varphi$  on  $\mathcal{C}$* , that is the set of points  $\mathbf{x} \in \text{reg}(\mathcal{C})$  such that  $d_{\mathbf{x}}\varphi : T_{\mathbf{x}}\mathcal{C} \rightarrow \mathbf{C}$  is not surjective. Then we note

$$\mathcal{K}(\varphi, \mathcal{C}) = \mathcal{W}^\circ(\varphi, \mathcal{C}) \cup \text{sing}(\mathcal{C})$$

the set of *singular points of  $\varphi$  on  $\mathcal{C}$* .

To satisfy some genericity assumptions, we will need to perform some linear changes of variables. Given  $A \in \text{GL}_n(\mathbf{C})$ , for  $f \in \mathbf{C}[X]$ ,  $f^A$  will denote the polynomial  $f(AX)$ . For  $V \subset \mathbf{C}^n$ , we denote by  $V^A$  the image of  $V$  by the map  $\Phi_A : \mathbf{x} \mapsto A^{-1}\mathbf{x}$ . Thus, for  $f = (f_1, \dots, f_p) \subset \mathbf{C}[X]$  we have  $\mathbf{V}(f^A) = \Phi_A(\mathbf{V}(f)) = \mathbf{V}(f)^A$ .

A *semi-algebraic (s.a.) set*  $S \subset \mathbf{R}^n$  is the set of solutions of a finite system of polynomial equations and inequalities with coefficients in  $\mathbf{R}$ . We say that  $S$  is *s.a. connected* if for any  $\mathbf{y}, \mathbf{y}' \in S$ ,  $\mathbf{y}$  and  $\mathbf{y}'$  can be connected by a *s.a. path* in  $S$ , that is an injective continuous s.a. function  $\gamma : [0, 1] \rightarrow S$  such that  $\gamma(0) = \mathbf{y}$  and  $\gamma(1) = \mathbf{y}'$ . A s.a. set  $S$  can be decomposed into finitely many *s.a. connected components* which are s.a. connected s.a. sets that are both closed and open in  $S$ . We refer to [4] and [8] for definitions and propositions about s.a. sets and functions. In this work, the s.a. sets in consideration will mainly be real traces of algebraic sets of  $\mathbf{C}^n$  (defined by polynomials with coefficients in  $\mathbf{R}$ ). In particular, we will note e.g.  $\mathcal{C}_{\mathbf{R}}$  and  $\mathcal{C}_{2,\mathbf{R}}$ , respectively the real traces of  $\mathcal{C}$ ,  $\mathcal{C}_2$ . Then, e.g.  $\mathcal{K}(\pi_1, \mathcal{C}) \cap \mathbf{R}^n$  and  $\mathcal{K}(\pi_1, \mathcal{C}_2) \cap \mathbf{R}^2$  will be denoted by  $\mathcal{K}(\pi_1, \mathcal{C}_{\mathbf{R}})$  and  $\mathcal{K}(\pi_1, \mathcal{C}_{2,\mathbf{R}})$ .

In this paper, we address the problem of designing an **algorithm for answering connectivity queries on real algebraic curves in  $\mathbf{R}^n$** , defined as real traces of algebraic curves of  $\mathbf{C}^n$ . More precisely, given representations of an algebraic curve  $\mathcal{C}$  and a finite set  $\mathcal{P}$  of points of  $\mathcal{C}$ , we want to compute a partition of  $\mathcal{P}$ , grouping the points lying in the same s.a. connected component of  $\mathcal{C}_{\mathbf{R}}$ .

It is a problem of importance in symbolic computation, and more specifically, in effective real algebraic geometry. Indeed, using the notion of roadmaps, introduced by Canny in [12, 13], one can reduce connectivity queries in real algebraic sets of arbitrary dimension to the such queries on real algebraic curves. Moreover, algorithms computing such roadmaps, on input a real algebraic set, has been continuously improved in a series of recent works [3, 5, 6, 46], making now tractable challenging problems in applications such as robotics [12, 14–16].

We say that  $f \in \mathbb{Z}[x_1, \dots, x_n]$  has magnitude  $(\delta, \tau)$ , if the total degree of  $f$  is bounded by  $\delta$  and all coefficients have absolute values at most  $2^\tau$ . This extends to a sequence of polynomials by bounding all entries in the same way. Complexity results are expressed with  $(\delta, \tau)$  bounding the magnitude of the polynomials defining  $\mathcal{C}$ . Moreover, we ignore logarithmic factors using the soft-Oh notation  $\tilde{O}(g)$  for denoting the class  $g \log(g)^{O(1)}$ .

*Prior works.* One can reduce our problem to a piecewise linear approximation sharing the same topology as the curve under study.

Computing the topology of plane algebraic curves in  $\mathbb{R}^2$  is extensively studied: by subdivision algorithm [11, 43], variants of Cylindrical Algebraic Decomposition methods [7, 17, 21, 22, 25–27, 29, 35, 41, 42, 44, 47], or also a hybrid approach such as [1]. In particular, [22, 42] obtain the best-known complexity bound in  $\tilde{O}(\delta^5(\delta + \tau))$ , by computing quantitative bounds on (bivariate) real root isolation of the considered polynomials.

The problem in  $\mathbb{R}^3$  has been less studied. This is done through various approaches such as computing the topology of the projection on various planes [2, 18, 33] or lifting the plane projection by algebraic considerations [23, 24, 31]. Yet, few of these papers give a complexity bound for the computation of such topology [18, 24], and [39] obtains the best-known complexity in  $\tilde{O}(\delta^{19}(\delta + \tau))$ .

*Main result.* Under genericity assumptions, we reduce the study of a curve  $\mathcal{C}$  in  $\mathbb{R}^n$  to the one of its image  $\mathcal{C}_{3,\mathbb{R}}$  by the projection  $\pi_3$ , as their real traces generically share the same connectivity properties. Moreover, by refining the approach developed in [38] (based on [31]), we show that *one does not need to compute the topology of  $\mathcal{C}_{3,\mathbb{R}}$  in order to answer connectivity queries*. More precisely, under genericity assumptions, that we made explicit below, we first compute the topology of  $\mathcal{C}_{2,\mathbb{R}}$  i.e. an isotopic graph. Next, the connectivity of  $\mathcal{C}_{3,\mathbb{R}}$  i.e. a homeomorphic graph, is deduced from the topology of  $\mathcal{C}_{2,\mathbb{R}}$ , adapting results from [31]. A geometric outcome is that the topological analysis needed to be done at some special points of  $\mathcal{C}_{2,\mathbb{R}}$ , which are called nodes, can be much simplified when one only needs to answer connectivity queries. This has a significant impact on the complexity.

Before providing our complexity result, let us introduce how our geometric objects are encoded. For a univariate function  $\varphi$ ,  $\varphi'$  is its derivative. For a bivariate function  $\psi$  in the variables  $x_1$  and  $x_2$ , we let  $\partial_{x_1}\psi$ ,  $\partial_{x_2}\psi$ ,  $\partial_{x_1}^2\psi$ ,  $\partial_{x_2}^2\psi$  and  $\partial_{x_1x_2}^2\psi$  be respectively the simple and double derivative with respect to the index variable(s).

To encode finite sets of points with algebraic coordinates over a field  $\mathcal{Q}$ , we use *zero-dimensional parametrizations*  $\mathcal{P} = (\Omega, \lambda)$  such that

- $\Omega = (\omega, \rho_1, \dots, \rho_n) \subset \mathcal{Q}[u]$  where  $u$  is a new variable,  $\omega$  is a monic square-free polynomial, and  $\deg(\rho_i) < \deg(\omega)$ ;
- $\lambda$  is a linear form  $\lambda_1x_1 + \dots + \lambda_nx_n$  in  $\mathcal{Q}[x_1, \dots, x_n]$  such that  $\lambda_1\rho_1 + \dots + \lambda_n\rho_n = u\partial_u\omega \pmod{\omega}$ .

We define the *degree* of such a parametrization  $\mathcal{P}$  as the degree of the polynomial  $\omega$ , and we say that it encodes the finite set:

$$Z(\mathcal{P}) = \{(\rho_1/\partial_u\omega, \dots, \rho_n/\partial_u\omega)(\vartheta) \in C^n \mid \omega(\vartheta) = 0\}.$$

Similarly, we encode algebraic curves with one-dimensional parametrizations over  $\mathcal{Q}$ , i.e.  $\mathcal{R} = (\Omega, (\lambda, \mu))$  with:

- $\Omega = (\omega, \rho_1, \dots, \rho_n) \subset \mathcal{Q}[u, v]$  with  $u$  and  $v$  new variables,  $\omega$  square-free and monic in  $u$  and  $v$ , and  $\deg(\rho_i) < \deg(\omega)$ ;
- $\lambda = \lambda_1x_1 + \dots + \lambda_nx_n$ ,  $\mu = \mu_1x_1 + \dots + \mu_nx_n$  are linear forms

$$\text{such that } \begin{cases} \lambda_1\rho_1 + \dots + \lambda_n\rho_n = u\partial_u\omega \pmod{\omega} \\ \mu_1\rho_1 + \dots + \mu_n\rho_n = v\partial_v\omega \pmod{\omega} \end{cases}$$

Such a data-structure encodes the algebraic curve  $Z(\mathcal{R})$ , defined as the Zariski closure of the following locally closed set of  $C^n$ :

$$\{(\rho_1/\partial_u\omega, \dots, \rho_n/\partial_u\omega)(\vartheta, \eta) \in C^n \mid \omega(\vartheta, \eta) = 0, \partial_u\omega(\vartheta, \eta) \neq 0\}.$$

We define the *degree* of such a parametrization  $\mathcal{R}$  as the degree of  $\omega$ , which coincides with the degree of  $Z(\mathcal{R})$ . Note that such a parametrization  $\mathcal{R}$  of degree  $\delta$  involves  $O(n\delta^2)$  coefficients.

We now give our aforementioned genericity properties, which can be seen as a generalization of the ones in [31]: let  $\mathcal{C} \subset C^n$  be an algebraic curve and  $\mathcal{P} \subset \text{reg}(\mathcal{C})$  finite.  $(\mathcal{C}, \mathcal{P})$  satisfies (H) if:

- (H<sub>1</sub>) for  $1 \leq i \leq n$ ,  $Q[\mathcal{C}]$  is integral over  $Q[\mathcal{C}_i]$ , where  $\mathcal{C}_i = \pi_i(\mathcal{C})$  is an algebraic curve;
- (H<sub>2</sub>) for all  $\mathbf{x} \in \text{reg}(\mathcal{C})$ ,  $\pi_2(T_{\mathbf{x}}\mathcal{C})$  is a tangent line to  $\mathcal{C}_2$  at  $\pi_2(\mathbf{x})$ ;
- (H<sub>3</sub>) the restriction of  $\pi_3$  to  $\mathcal{C}$  is injective;
- (H<sub>4</sub>) if  $\mathbf{y} \in \text{app}(\mathcal{C}_2)$  then
  - (H<sub>4'</sub>)  $\pi_2^{-1}(\mathbf{y}) \cap \mathcal{C}$  has cardinality 2;
  - (H<sub>4''</sub>)  $\mathbf{y}$  is a node of  $\mathcal{C}_2$ ;
- (H<sub>5</sub>)  $\mathcal{K}(\pi_1, \mathcal{C}_2) \cup \pi_2(\mathcal{P})$  is finite and  $\pi_1$  is injective on it;
- (H<sub>6</sub>)  $\pi_2^{-1}(\pi_2(\mathbf{x})) \cap \mathcal{C} = \{\mathbf{x}\}$ , for all  $\mathbf{x} \in \mathcal{K}(\pi_1, \mathcal{C}) \cup \mathcal{P}$ ;
- (H<sub>7</sub>) there is a one-dimensional parametrization  $\mathcal{R} = (\Omega, (x_1, x_2))$  encoding  $\mathcal{C}$ , with  $\Omega = (\omega, x_1, x_2, \rho_3, \dots, \rho_n) \subset \mathcal{Q}[x_1, x_2]$ .

We omit  $\mathcal{P}$  when the context is clear. Also, (H) is satisfied up to a generic linear change of coordinates over  $\mathcal{C}$  (see Section 2).

**Theorem 1.1.** *Let  $\mathcal{R} \subset \mathbb{Z}[x_1, x_2]$  be a one-dimensional parametrization encoding an algebraic curve  $\mathcal{C} \subset C^n$  satisfying (H) and  $\mathcal{P} \subset \mathbb{Z}[x_1]$  a zero-dimensional parametrization encoding a finite subset of  $\mathcal{C}$ . Let  $(\delta, \tau)$  and  $(\mu, \kappa)$  the magnitudes of  $\mathcal{R}$  and  $\mathcal{P}$ , respectively.*

*There exists an algorithm which, on input  $\mathcal{R}$  and  $\mathcal{P}$ , computes a partition of the points of  $Z(\mathcal{P}) \cap \mathbb{R}^n$  lying in the same s.a. connected component of  $\mathcal{C} \cap \mathbb{R}^n$ , using*

$$\tilde{O}(\delta^6 + \mu^6 + \delta^5\tau + \mu^5\kappa)$$

*bit operations.*

This is to be compared with the best complexity  $\tilde{O}(\delta^{19}(\delta + \tau))$  known to analyze the topology of space curve. Note that the dependency on  $n$  in the complexity bound is “hidden” within the potential degrees of the parametrizations and the corresponding algebraic sets. Indeed, according to Bézout’s bound, an algebraic set, defined by polynomials, of degree at most  $D$ , can have degree at most  $D^n$ .

*Structure of the paper.* After some preliminary results we prove that up to a generic change coordinate, assumption (H) holds. Then, under these assumptions, we describe two steps of our algorithm that is identifying the finitely many points of the curve where there is connectivity ambiguity and resolving these ambiguities. Finally, we describe the main algorithm together with complexity bounds.

## 2 CURVES IN GENERIC POSITION

We now prove that (H) holds for an algebraic curve in generic position  $\mathcal{C}$  that is, there is an open dense subset  $\mathfrak{A}$  of  $\text{GL}_n(C)$  such that for any  $A \in \mathfrak{A}$  the sheared curve  $\mathcal{C}^A$  satisfies (H).

### 2.1 Generic projections of affine curves

The results below are well known in the case of smooth projective curves (see e.g. [36, IV. Thm 3.10] or [45, §7B.] for  $C = \mathbb{C}$ ), and have been generalized subsequently in e.g. [37, 40]. A version for complex singular affine space curves is proved in [32, Prop 5.2] under regularity assumptions. We present here a generalization of [32, Prop 5.2] for any singular (affine) algebraic curve, following the proof and using more general objects and results from the literature.

Let  $n \geq 3$ ,  $\mathcal{C} \subset \mathbb{C}^n$  an affine algebraic curve and  $\mathcal{P} \subset \mathcal{C}$  a finite subset. Denote  $\mathbb{P}^n$  the projective space  $\mathbb{P}^n(\mathbb{C})$ , of dimension  $n$  over  $\mathbb{C}$ , and write  $[\mathbf{x}_0 : \dots : \mathbf{x}_n]$  its elements. Let  $\mathcal{H}^\infty = \{[\mathbf{x}_0 : \dots : \mathbf{x}_n] \in \mathbb{P}^n \mid \mathbf{x}_0 = 0\}$  be the hyperplane at infinity with respect to the affine open chart given by  $\mathbb{P}^n - \mathcal{H}^\infty$  (see e.g. [36, I.2]) We finally let  $\overline{\mathcal{C}}$  be the projective closure of  $\mathcal{C}$  in  $\mathbb{P}^n$ .

We denote by  $\mathbb{G}(1, n) = G(2, n + 1)$  the Grassmanian of lines in  $\mathbb{P}^n$ , and, for  $\mathbf{x} \neq \mathbf{y}$  in  $\mathbb{P}^n$ , by  $\mathcal{L}(\mathbf{x}, \mathbf{y}) \in \mathbb{G}(1, n)$  the line containing  $\mathbf{x}$  and  $\mathbf{y}$ . For distinct points  $\mathbf{x}, \mathbf{y}$  of  $\overline{\mathcal{C}}$ , the line  $s = \mathcal{L}(\mathbf{x}, \mathbf{y})$  will be called the *secant line of  $\overline{\mathcal{C}}$  determined by  $\mathbf{x}$  and  $\mathbf{y}$* . When  $s$  intersects  $\overline{\mathcal{C}}$  in a third point, distinct from  $\mathbf{x}$  and  $\mathbf{y}$ , we call it a *trisecant line of  $\overline{\mathcal{C}}$* . If there are distinct  $\mathbf{x}', \mathbf{y}' \in s \cap \text{reg}(\overline{\mathcal{C}})$  such that  $T_{\mathbf{x}'}\overline{\mathcal{C}}$  and  $T_{\mathbf{y}'}\overline{\mathcal{C}}$  are coplanar, then it will be called a *secant line with coplanar tangents of  $\overline{\mathcal{C}}$* . Then, we define  $\text{Sec}(\overline{\mathcal{C}})$ ,  $\text{Tri}(\overline{\mathcal{C}})$  and  $\text{CoTg}(\overline{\mathcal{C}})$  as the sets of points in  $\mathbb{P}^n$  that lie on respectively a secant, trisecant and secant with coplanar tangents of  $\overline{\mathcal{C}}$ . Finally, we denote by  $\text{Tg}(\overline{\mathcal{C}})$  the set of points in  $\mathbb{P}^n$  that lie on the tangent line  $T_{\mathbf{x}}\overline{\mathcal{C}}$  for some  $\mathbf{x} \in \text{reg}(\overline{\mathcal{C}})$ .

**Lemma 2.1.** *The sets  $\text{Sec}(\overline{\mathcal{C}})$  and  $\text{Tg}(\overline{\mathcal{C}})$  are algebraic sets of dimension  $\leq 3$  and  $\leq 2$ , respectively. If, in addition,  $\overline{\mathcal{C}}$  is not a plane curve, then  $\text{Tri}(\overline{\mathcal{C}})$  and  $\text{CoTg}(\overline{\mathcal{C}})$  are algebraic sets of dimension  $\leq 2$ . Finally, none of these sets contains  $\mathcal{H}^\infty$ .*

**PROOF.** Let  $\overline{\mathcal{C}}_1, \dots, \overline{\mathcal{C}}_m$  the irreducible components of  $\overline{\mathcal{C}}$ ,  $i, j \in \{1, \dots, m\}$ , possibly equal, and  $\Sigma_{i,j} \subset \mathbb{G}(1, n)$  the Zariski closure of the image of  $\overline{\mathcal{C}}_i \times \overline{\mathcal{C}}_j - \{(\mathbf{y}, \mathbf{y}) \mid \mathbf{y} \in \overline{\mathcal{C}}_i \cap \overline{\mathcal{C}}_j\}$  through the map  $(\mathbf{y}, \mathbf{z}) \mapsto \mathcal{L}(\mathbf{y}, \mathbf{z})$ . As the image of a Cartesian product of two irreducible curves,  $\Sigma_{i,j}$  is an irreducible algebraic set. Such a secant being uniquely determined by fixing two points in  $\overline{\mathcal{C}}_i$  and  $\overline{\mathcal{C}}_j$ ,  $\Sigma_{i,j}$  has dimension  $\leq 2$  by [48, Thm 1.25]. Then, if  $\Sigma = \bigcup_{i,j} \Sigma_{i,j}$  is the secant variety of  $\overline{\mathcal{C}}$ , it has dimension  $\leq 2$  and contains the secant lines in  $\mathbb{G}(1, n)$ . As elements of  $\mathbb{G}(1, n)$  are algebraic sets of dimension 1,  $\text{Sec}(\overline{\mathcal{C}})$  has Zariski closure of dimension  $\leq 3$ .

Consider now, the subset  $\Gamma_i \subset \mathbb{P}^n \times \overline{\mathcal{C}}_i$ , consisting of points  $(\mathbf{u}, \mathbf{y})$  such that  $\mathbf{y} \in \text{reg}(\overline{\mathcal{C}})$  and  $\mathbf{u} \in T_{\mathbf{y}}\overline{\mathcal{C}}$ , and consider the projections  $\varphi_i: \Gamma_i \rightarrow \mathbb{P}^n$  and  $\psi_i: \Gamma_i \rightarrow \overline{\mathcal{C}}_i$ . For all  $\mathbf{y}$  in the Zariski open subset  $\text{reg}(\overline{\mathcal{C}}) \cap \overline{\mathcal{C}}_i$  of  $\overline{\mathcal{C}}_i$ ,  $\psi_i^{-1}(\mathbf{y})$  is exactly  $T_{\mathbf{y}}\overline{\mathcal{C}}$ , which has dimension 1. Hence, by [48, Thm 1.25],  $\varphi_i(\Gamma_i)$  has Zariski closure of dimension  $\leq 2$ . Since  $\text{Tg}(\overline{\mathcal{C}}) = \bigcup_i \varphi_i(\Gamma_i)$ , we are done.

Assume now, that  $\overline{\mathcal{C}}$  is not a plane curve then, by [40, Thm 2], the set of trisecant lines of  $\overline{\mathcal{C}}$  is a subset of  $\mathbb{G}(1, n)$  whose Zariski closure has dimension  $\leq 1$ . Then, as seen above,  $\text{Tri}(\overline{\mathcal{C}})$  has Zariski closure of dimension  $\leq 2$ . Now, let  $M_{i,j}$  be the subset of  $\Sigma_{i,j}$  consisting of secant lines intersecting  $\overline{\mathcal{C}}$  at points whose tangents are all contained in the same plane. We are going to prove that the Zariski closure of  $M_{i,j}$  has dimension  $\leq 1$ . Together with the dimension bound on  $\text{Tri}(\overline{\mathcal{C}})$ , this will bound the dimension of  $\text{CoTg}(\overline{\mathcal{C}})$ . Suppose first that  $\overline{\mathcal{C}}_i$  and  $\overline{\mathcal{C}}_j$  are not coplanar components. Then, there is  $\mathbf{y} \in \overline{\mathcal{C}}_i - \text{sing}(\overline{\mathcal{C}})$  such that  $l = T_{\mathbf{y}}\overline{\mathcal{C}}$  and  $\overline{\mathcal{C}}_j$  are not coplanar. If  $\mathfrak{p}_l: \mathbb{P}^n \rightarrow \mathbb{P}^{n-2}$  denotes the projection of center  $l$ , then  $\mathfrak{p}_l(\overline{\mathcal{C}}_j)$  is not a point. As  $\overline{\mathcal{C}}_j$  is irreducible, and by [48, Thm 1.25], the Zariski closure  $\mathcal{R}$  of  $\mathfrak{p}_l(\overline{\mathcal{C}}_j)$  is an irreducible algebraic subset of  $\mathbb{P}^{n-2}$  of dimension 1. Hence, by [48, Thm 1.25] again, there is a finite set

$K_1 \subset \mathbb{P}^{n-2}$  such that for all  $\mathbf{w} \in \mathcal{R} \setminus K_1$ ,  $\mathfrak{p}_l^{-1}(\mathbf{w}) \cap \overline{\mathcal{C}}_j$  is finite. Besides, by Sard's Theorem [48, Thm 2.27], there exists a finite set  $K_2 \subset \mathbb{P}^{n-2}$  such that  $\mathcal{R} \setminus K_2$  does not contain any critical value of the restriction of  $\mathfrak{p}_l$  to  $\overline{\mathcal{C}}_j$ . Then, for  $\mathbf{w}$  in  $\mathcal{R} \setminus [K_1 \cup K_2 \cup \mathfrak{p}_l(\text{sing}(\overline{\mathcal{C}}))]$ ,

$$\mathfrak{p}_l^{-1}(\mathbf{w}) \cap \overline{\mathcal{C}}_j = \{z_1, \dots, z_k\}$$

with  $k \geq 1$ , and for all  $1 \leq i \leq k$ ,  $z_i \in \text{reg}(\overline{\mathcal{C}})$  and  $\mathfrak{p}_l(T_{z_i}\overline{\mathcal{C}})$  has dimension 1. Hence,  $\mathbf{y}$  and  $z_i$  have no coplanar tangents for all  $1 \leq i \leq k$ . In particular, the secant line  $\mathcal{L}(\mathbf{y}, z_1)$  contains two points having no coplanar tangents so that  $\mathcal{L}(\mathbf{y}, z_1) \in \Sigma_{i,j} - M_{i,j}$  and  $M_{i,j} \subsetneq \Sigma_{i,j}$ . In conclusion, the Zariski closure of  $M_{i,j}$  is a proper algebraic subset, and since  $\Sigma_{i,j}$  is irreducible, this closure has dimension  $\leq 1$ . If  $\overline{\mathcal{C}}_i$  and  $\overline{\mathcal{C}}_j$  are coplanar,  $\Sigma_{i,j}$  is the Zariski closure of  $M_{i,j}$  and one of the following holds. If  $i = j$  and  $\overline{\mathcal{C}}_i$  is a line, then  $\Sigma_{i,j}$  is reduced to the line associated to  $\overline{\mathcal{C}}_i$  and has dimension 0. Else, there exists a unique plane  $S_{i,j}$  containing  $\overline{\mathcal{C}}_i$  and  $\overline{\mathcal{C}}_j$ , so that any line of  $\Sigma_{i,j}$  must be contained in  $S_{i,j}$ . In both cases,  $\Sigma_{i,j}$ , thus the closure of  $M_{i,j}$ , have dimension  $\leq 1$ . Then, the Zariski closure of the union  $M$  of all  $M_{i,j}$  for  $i, j \in \{1, \dots, m\}$ , is an algebraic subset of  $\mathbb{G}(1, n)$  of dimension  $\leq 1$  as requested.

Remark now that a secant with coplanar tangents is either a trisecant, or a secant intersecting  $\overline{\mathcal{C}}$  in exactly two regular points with coplanar tangents. Hence, the set of secants with coplanar tangents of  $\overline{\mathcal{C}}$  is contained in the union of  $M$  and the set of trisecant lines of  $\overline{\mathcal{C}}$ . By the previous discussion, it has dimension  $\leq 1$ , so that the Zariski closure of  $\text{CoTg}(\overline{\mathcal{C}})$  has dimension  $\leq 2$ .

Since  $\overline{\mathcal{C}} - \mathcal{H}^\infty$  can be identified with  $\mathcal{C}$ , the former is a Zariski open subset of  $\overline{\mathcal{C}}$ , so that  $\overline{\mathcal{C}} \cap \mathcal{H}^\infty$  is finite. In particular,  $\mathcal{H}^\infty$  contains finitely many secant or tangent lines of  $\overline{\mathcal{C}}$  and then, cannot be contained in  $\text{Sec}(\overline{\mathcal{C}})$  or  $\text{Tg}(\overline{\mathcal{C}})$ . Since  $\text{Tri}(\overline{\mathcal{C}})$  and  $\text{CoTg}(\overline{\mathcal{C}})$  are contained in  $\text{Sec}(\overline{\mathcal{C}})$ , they cannot contain  $\mathcal{H}^\infty$  as well.  $\square$

In the following, for  $0 \leq r \leq n - 1$ , we denote by  $\mathbb{G}(r, n - 1) = G(r + 1, n)$  the set of  $r$ -dimensional projective linear subspaces of  $\mathcal{H}^\infty$ . Recall that using Plücker embedding (see e.g. [48, Example 1.24]),  $\mathbb{G}(r, n - 1)$  can be embedded in  $\mathbb{P}^{\binom{n}{r+1}-1}$  as an irreducible algebraic set of dimension  $(r + 1)(n - r)$ . The next lemma is then a direct consequence of [48, Thm 1.25].

**Lemma 2.2.** *Let  $X \subset \mathcal{H}^\infty$  be an algebraic set of dimension  $m \leq n - 1$ . Then, for any  $i \geq m$  there exists a non-empty Zariski open subset  $\mathfrak{E}_i$  of  $\mathbb{G}(n - 1 - i, n - 1)$  such that for every  $E \in \mathfrak{E}_i$ , the set  $E \cap X$  is finite and, if  $i > m$ , it is empty.*

Recall that  $\mathcal{P}$  is a finite set of control points in  $\overline{\mathcal{C}} - \text{sing}(\overline{\mathcal{C}})$ .

**Proposition 2.3.** *If  $\overline{\mathcal{C}}$  is not a plane curve, then for all  $1 \leq i \leq n - 1$ , there exists a non-empty Zariski open subset  $\mathfrak{E}_i$  of  $\mathbb{G}(n - 1 - i, n - 1)$  such that for all  $E \in \mathfrak{E}_i$ , the following holds. Let  $\mathfrak{p}_E: \overline{\mathcal{C}} \rightarrow \mathbb{P}^i$  be the projection with center  $E$ , then  $\mathfrak{p}_E$  is a finite regular map and*

(i) *for all  $\mathbf{x} \in \mathcal{P}$ ,  $\mathfrak{p}_E(T_{\mathbf{x}}\overline{\mathcal{C}})$  is a projective line of  $\mathbb{P}^i$ .*

*If, in addition,  $i \geq 2$  then,*

(ii) *item (i) holds for any  $\mathbf{x} \in \text{reg}(\overline{\mathcal{C}})$ ;*

(iii) *for any  $\mathbf{x} \in \overline{\mathcal{C}}$ , there exists at most one point  $\mathbf{x}' \in \overline{\mathcal{C}}$ , distinct from  $\mathbf{x}$ , such that  $\mathfrak{p}_E(\mathbf{x}) = \mathfrak{p}_E(\mathbf{x}')$ ;*

- (iv) there exists finitely many such couples  $(\mathbf{x}, \mathbf{x}')$ , all satisfying  $\mathbf{x}, \mathbf{x}' \in \text{reg}(\overline{\mathcal{C}}) - \mathcal{P}$  and  $\mathfrak{p}_E(T_{\mathbf{x}}\overline{\mathcal{C}}) \neq \mathfrak{p}_E(T_{\mathbf{x}'}\overline{\mathcal{C}})$ ;
- (v) if  $i \geq 3$ , there is no such couple.

PROOF. Fix  $1 \leq i \leq n - 1$  and suppose that  $\overline{\mathcal{C}}$  is not plane. As a proper Zariski closed set of  $\overline{\mathcal{C}}$ ,  $X_1 := \mathcal{H}^\infty \cap \overline{\mathcal{C}}$  is finite. By Lemma 2.2, as  $i > 0$ , there is a non-empty Zariski open subset  $\mathfrak{E}_1$  of  $\mathbb{G}(n - 1 - i, n - 1)$  such that for all  $E \in \mathfrak{E}_1$ ,  $E \cap X_1$  is empty. Moreover, any  $(n - i)$ -dimensional space containing  $E$  cannot contain an irreducible component of  $\overline{\mathcal{C}}$  (it would be a line, intersecting  $E$  at some point of  $E \cap \overline{\mathcal{C}} = E \cap X_1$ , which is empty). Thus, the projection with center  $E \in \mathfrak{E}_1$  induces a finite map on  $\overline{\mathcal{C}}$ , regular by definition.

According to Lemma 2.1, the set of points lying on a tangent or a trisecant line of  $\overline{\mathcal{C}}$  is an algebraic set of dimension  $\leq 2$ . Since  $\mathcal{H}^\infty$  contains finitely many such tangents or trisecants,

$$X_2 = (\text{Tg}(\overline{\mathcal{C}}) \cup \text{Tri}(\overline{\mathcal{C}})) \cap \mathcal{H}^\infty$$

has dimension at most 1. By Lemma 2.2, as  $i \geq 1$ , there exists a non-empty Zariski open subset  $\mathfrak{E}_2$  of  $\mathbb{G}(n - 1 - i, n - 1)$  such that any  $E \in \mathfrak{E}_2$  intersects finitely many points of  $\text{Tg}(\overline{\mathcal{C}}) \cup \text{Tri}(\overline{\mathcal{C}})$ . Besides, there are finitely many tangents intersecting the finite set  $\mathcal{P}$ , so that by Lemma 2.2, up to intersecting  $\mathfrak{E}_2$  with a non-empty Zariski open subset of  $\mathbb{G}(n - 1 - i, n - 1)$ , one can assume that none of these tangents intersect  $\mathcal{P}$ . This proves (i).

Assume now  $i \geq 2$ . By Lemma 2.2, no  $E \in \mathfrak{E}_2$  intersects points in  $\text{Tg}(\overline{\mathcal{C}}) \cup \text{Tri}(\overline{\mathcal{C}})$ . In particular, any  $(n - i)$ -dimensional space containing  $E$  cannot contain a tangent nor a trisecant, and, as seen above, this means that no tangent, or three distinct points, are mapped to one point. This proves respectively (ii) and (iii).

Then, by Lemma 2.1, the set  $X_3 = \text{Sec}(\overline{\mathcal{C}}) \cap \mathcal{H}^\infty$  of points in  $\mathcal{H}^\infty$ , lying on a secant line of  $\overline{\mathcal{C}}$ , is algebraic of dimension  $\leq 2$ . By Lemma 2.2 ( $i \geq 2$ ), there is a non-empty Zariski open subset  $\mathfrak{E}_3$  of  $\mathbb{G}(n - 1 - i, n - 1)$  such that any  $E \in \mathfrak{E}_3$  contains finitely many points lying on a secant line of  $\overline{\mathcal{C}}$  i.e., as before, there are finitely many couples of points which are mapped to the same point in  $\mathbb{P}^i$ . Besides, the set of secants intersecting  $\text{sing}(\overline{\mathcal{C}}) \cup \mathcal{P}$  is a proper algebraic subset of the secant variety of  $\overline{\mathcal{C}}$ . Hence, by Lemma 2.2, up to intersecting  $\mathfrak{E}_3$  with a non-empty Zariski open subset of  $\mathbb{G}(n - 1 - i, n - 1)$ , one can assume that none of these secants intersect  $\text{sing}(\overline{\mathcal{C}}) \cup \mathcal{P}$ . Finally, by Lemma 2.2, as  $\text{CoTg}(\overline{\mathcal{C}}) \cap \mathcal{H}^\infty$  has dimension  $\leq 1$ . As seen above, up to intersecting  $\mathfrak{E}_3$  with a non-empty Zariski open subset of  $\mathbb{G}(n - 1 - i, n - 1)$ , one can assume that these secants intersect  $\overline{\mathcal{C}}$  at points with no coplanar tangents, which cannot be mapped to the same line. All in all, for any  $E \in \mathfrak{E}_3$ , (iv) holds.

By Lemma 2.2, if moreover  $i \geq 3$ , no  $E \in \mathfrak{E}_3$  intersects points in  $\text{Sec}(\overline{\mathcal{C}})$  that is, no two distinct points are mapped to the same image. This proves (v). Taking  $\mathfrak{E}_i = \mathfrak{E}_1 \cap \mathfrak{E}_2 \cap \mathfrak{E}_3$  ends the proof.  $\square$

We can now state the affine counterpart of Proposition 2.3.

**Corollary 2.4.** *There exists a non-empty Zariski open set  $\mathfrak{A}$  of  $\text{GL}_n(\mathbb{C})$  such that for all  $A \in \mathfrak{A}$  and  $1 \leq i \leq n$ , the following holds: the restriction of  $\pi_i$  to  $\mathcal{C}^A$  is a finite morphism, and*

- (i) for all  $\mathbf{x} \in \mathcal{P}^A$ ,  $\pi_i(T_{\mathbf{x}}\mathcal{C}^A)$  is a line of  $\mathbb{C}^i$ .

If, in addition,  $i \geq 2$  then,

- (ii) item (i) holds for any  $\mathbf{x} \in \text{reg}(\mathcal{C}^A)$ ;
- (iii) the restriction of  $\pi_i$  to  $\mathcal{C}^A$  is not injective at  $\mathbf{x}$  if, and only if,  $i = 2$  and  $\pi_2(\mathbf{x}) \in \text{app}(\mathcal{C}_2^A)$ ;
- (iv)  $\text{app}(\mathcal{C}_2^A)$  contains only nodes, with exactly two preimages through  $\pi_2$ , none of them being in  $\mathcal{P}^A$ ;

PROOF. If  $\mathcal{C}$  is a plane curve, it is straightforward. Suppose from now on  $n \geq 3$  and  $\mathcal{C}$  not plane. If  $i = n$ , there is nothing to prove, so let  $1 \leq i \leq n - 1$ . Let  $\overline{\mathcal{C}}$  be the projective closure of  $\mathcal{C}$ , which is not a plane either. Let  $\mathfrak{E}_i$  be the non-empty Zariski open subset of  $\mathbb{G}(n - 1 - i, n - 1)$  given by Proposition 2.3. According to Plücker embedding, there exists a surjective regular map from the set of  $i$  linearly independent vectors  $\mathbf{a}_1, \dots, \mathbf{a}_i$  of  $\mathbb{C}^n$  to the set of  $(n - 1 - i)$ -dimensional (projective) linear subspaces of  $\mathcal{H}^\infty$ , defined by  $x_0 = 0$  and  $\mathbf{a}_{j,1}x_1 + \dots + \mathbf{a}_{j,n}x_n = 0$  for  $1 \leq j \leq i$ . Hence, there exists a non-empty Zariski open set  $\mathfrak{A}_i$  of  $\text{GL}_n(\mathbb{C})$  of matrices  $A$  such that the first  $i$  rows of  $A^{-1}$  are mapped to some  $E \in \mathfrak{E}_i$ , through the above map. Moreover, for any  $A \in \mathfrak{A}_i$  the following holds. Consider,

$$\tilde{A} = \begin{bmatrix} 1 & \mathbf{0} \\ \mathbf{0} & A \end{bmatrix},$$

and for  $1 \leq j \leq n$ , let  $\mathbf{a}_j = (\mathbf{a}_{j,1}, \dots, \mathbf{a}_{j,n})$  be the rows of  $A$ . If  $L_0 = x_0$  and for  $1 \leq j \leq i$ ,  $L_j = \mathbf{a}_{j,1}x_1 + \dots + \mathbf{a}_{j,n}x_n$ , then the equations  $L_0, \dots, L_i$  define a projective linear subspace  $E$  of  $\mathcal{H}^\infty$ , such that  $E \in \mathfrak{E}_i$  and, by definition (see e.g. [48, Example 1.27]),

$$\mathfrak{p}_E : \begin{array}{ccc} \overline{\mathcal{C}}^{\tilde{A}} & \rightarrow & \mathbb{P}^i \\ \mathbf{x} & \mapsto & [\mathbf{x}_0 : \dots : \mathbf{x}_i] \end{array}$$

Therefore, the restriction of  $\mathfrak{p}_E$  to the affine chart  $\mathbb{P}^n - \mathcal{H}^\infty$  can be identified with the restriction of  $\pi_i$  to  $\mathcal{C}^A$ . According to Proposition 2.3, the restriction of  $\pi_i$  to  $\mathcal{C}^A$  is a finite morphism satisfying item (i). Assume now that  $i \geq 2$  then, assertion (ii) is a direct consequence of item (ii) of Proposition 2.3.

Besides, let  $\mathbf{x} \in \mathcal{C}^A$  such that there is  $\mathbf{x}' \in \mathcal{C}^A$  satisfying  $\mathbf{x}' \neq \mathbf{x}$  and  $\pi_i(\mathbf{x}) = \pi_i(\mathbf{x}')$ . Then, by Proposition 2.3, (iii) to (v),  $\mathbf{x}'$  is unique, both  $\mathbf{x}, \mathbf{x}' \notin \text{sing}(\mathcal{C}^A) \cup \mathcal{P}^A$ , and necessarily  $i = 2$ . Moreover,  $T_{\mathbf{x}}\mathcal{C}^A$  and  $T_{\mathbf{x}'}\mathcal{C}^A$  map to distinct lines of  $\mathbb{C}^2$ , crossing at  $\pi_2(\mathbf{x})$ : it is a node. Hence,  $\mathbf{x} \in \text{app}(\mathcal{C}_2^A)$  and  $\pi_2(\mathbf{x})$  is a node, with exactly two preimages, none of them being in  $\mathcal{P}^A$ . Conversely from Proposition 2.3, (ii), all points of  $\text{app}(\mathcal{C}_2^A)$  have at least two preimages in  $\mathcal{C}^A$ . This proves (iii) and (iv). Taking  $\mathfrak{A} = \bigcap_{i=1}^{n-1} \mathfrak{A}_i$  concludes.  $\square$

## 2.2 Recovering (H)

**Proposition 2.5.** *Let  $\mathcal{C} \subset \mathbb{C}^n$  be an algebraic curve and a finite subset  $\mathcal{P} \subset \text{reg}(\mathcal{C})$ . There exists a non-empty Zariski open set  $\mathfrak{A} \subset \text{GL}_n(\mathbb{C})$  such that, for any  $A \in \mathfrak{A}$ ,  $(\mathcal{C}^A, \mathcal{P}^A)$  satisfies (H).*

PROOF. Let  $\mathfrak{A}_1 \subset \text{GL}_n(\mathbb{C})$  be the non-empty Zariski open subset defined in Corollary 2.4 and let  $A \in \mathfrak{A}_1$ . For all  $1 \leq i \leq n$ , the restriction of  $\pi_i$  to  $\mathcal{C}^A$  is a finite morphism, so that  $\mathcal{C}_i^A = \pi_i(\mathcal{C}^A)$  is an algebraic curve. Since  $\mathbb{C}$  is integral over  $\mathbb{Q}$ , the extension  $\mathbb{Q}[\mathcal{C}_i^A] \hookrightarrow \mathbb{Q}[\mathcal{C}^A]$  is integral as well: (H<sub>1</sub>) is satisfied. Applying Corollary 2.4, for  $i = 3$  and  $i = 2$  shows that the curve  $\mathcal{C}^A$  satisfies respectively (H<sub>3</sub>) on the one hand and (H<sub>2</sub>) and (H<sub>4</sub>) on the other.

Let  $\mathbf{A} = (\mathbf{a}_{i,j})_{1 \leq i,j \leq n}$  and  $t$  be new indeterminates, the former ones standing for the entries of a square matrix of size  $n \times n$ . Since  $\mathfrak{A}_1$

is non-empty and Zariski open, there exists a non-zero polynomial  $F \in C[A]$ , such that  $A \in \mathfrak{A}_1$  if  $F(A) \neq 0$ . Besides, according to [9, §4.2] (or [35, §3.2]), there exists a non-zero polynomial  $G \in C[A, t]$  such that, if  $F(A) \neq 0$  and  $G(A, b) \neq 0$  then, for

$$B = \begin{bmatrix} 1 & b & 0 \\ 0 & 1 & 0 \\ 0 & 0 & I_{n-2} \end{bmatrix},$$

the curve  $\mathcal{C}_2^{BA}$  is a plane curve in generic position in the sense of [9, §4.2] and [31, Def 3.3]. In particular,  $\pi_1$  maps no tangent line of any singular point of  $\mathcal{C}_2$  to a point and its restriction of  $\pi_1$  to the finite set  $\mathcal{W}^\circ(\pi_1, \mathcal{C}_2^{BA})$  is injective. Let  $\mathcal{P}_2 = \pi_2(\mathcal{P})$ . As  $\mathcal{P}_2 \cup \text{sing}(\mathcal{C}_2)$  is finite, we can assume that  $\pi_1$  is injective on  $\mathcal{P}_2^{BA} \cup \text{sing}(\mathcal{C}_2^{BA})$  as well. But, for any  $\mathbf{x} \in \mathcal{W}^\circ(\pi_1, \mathcal{C}_2^{BA})$ ,  $\pi_1(\mathbf{x})$  is a point, so that  $\mathbf{x}$  is neither in  $\text{sing}(\mathcal{C}_2^{BA})$  nor  $\mathcal{P}_2^{BA}$ , by genericity of  $\mathcal{C}_2^{BA}$  and item (i) of Corollary 2.4 respectively. Then, let  $b \in C$  such that  $G(\mathbf{A}, b)$  is not zero and let  $B$  be as above. The subset  $\mathfrak{A}_2 \subset \text{GL}_n(C)$  of elements of the form  $BA'$  where  $F(A')G(A', b) \neq 0$  is a non-empty Zariski open subset. Moreover, for any  $A \in \mathfrak{A}_2$ ,  $\mathcal{C}^A$  satisfies (H<sub>5</sub>).

Take  $A \in \mathfrak{A}_1 \cap \mathfrak{A}_2$  and let  $\mathbf{x} \in \mathcal{K}(\pi_1, \mathcal{C}^A) \cup \mathcal{P}^A$  and  $\mathbf{y} = \pi_2(\mathbf{x})$ . Suppose there is  $\mathbf{x}' \in \mathcal{C}^A$  such that  $\mathbf{x}' \neq \mathbf{x}$  and  $\pi_2(\mathbf{x}') = \mathbf{y}$ . By (iii),  $\mathbf{x} \in \mathcal{W}^\circ(\pi_1, \mathcal{C}^A)$  and  $\mathbf{y}$  is a node in  $\text{app}(\mathcal{C}_2^A)$ , with vertical tangent line  $\pi_2(T_{\mathbf{x}}\mathcal{C}^A)$ : this is impossible by above ( $A \in \mathfrak{A}_2$ , so that  $\mathcal{C}_2^A$  is in generic position). Therefore,  $\mathcal{C}^A$  satisfies (H<sub>6</sub>).

We proceed similarly for (H<sub>7</sub>). Let  $A \in \mathfrak{A}_1$ . By (H<sub>1</sub>),  $\mathcal{C}^A$  is in Noether position (for  $\pi_1$ ). Let  $\mathbf{D} = (d_3, \dots, d_n)$  be new variables. By [28, Cor 3.4 & 3.5], there is  $H \in C[\mathbf{A}, \mathbf{D}]$  non-zero such that, if  $F(A) \neq 0$  and  $H(A, \mathbf{d}) \neq 0$ , then the following holds: if  $\mu_{\mathbf{d}} = x_2 + d_3x_3 + \dots + d_nx_n$  is a linear form, then there is  $\mathcal{R} = (\omega, \rho_1, \dots, \rho_n) \subset Q[x_1, v]$  such that  $(\mathcal{R}, x_1, \mu_{\mathbf{d}})$  is a one-dimensional parametrization encoding  $\mathcal{C}^A$ . Let  $\mathbf{d} \in C^{n-1}$  such that  $H(\mathbf{A}, \mathbf{d})$  is not zero and

$$C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & \mathbf{d} \\ 0 & 0 & I_{n-2} \end{bmatrix}.$$

The subset  $\mathfrak{A}_3 \subset \text{GL}_n(C)$  of elements, of the form  $CA'$ , where  $F(A')$  and  $H(A', \mathbf{c})$  are both not zero, is a non-empty Zariski open subset where  $\mathcal{C}^A$  satisfies (H<sub>7</sub>).

Finally, for  $A \in \mathfrak{A} := \mathfrak{A}_1 \cap \mathfrak{A}_2 \cap \mathfrak{A}_3$ ,  $\mathcal{C}^A$  satisfies (H).  $\square$

### 3 DETECT APPARENT SINGULARITIES

We generalize the criterion of [31] used to identify apparent singularities in plane projection of space curve. We keep notations given in Section 1, and **assume for the rest of the document that  $(\mathcal{C}, \mathcal{P})$  satisfies (H)**. We start by an adapted version of [31, Lemma 4.1] (the equivalence relation modulo  $I(\mathcal{C})$  is denoted  $\equiv$ ).

**Lemma 3.1.** *Let  $(\alpha, \beta)$  be a node of  $\mathcal{C}_2$ . There are exactly two power-series  $y_1, y_2 \in C[[x_1 - \alpha]]$  such that for  $i = 1, 2$ , if  $z_i = \frac{\rho_3(x_1, y_i)}{\partial_{x_2} \omega(x_1, y_i)}$  then:*

- (1)  $\omega(x_1, y_i) \equiv 0$  and  $y_i(\alpha) = \beta$  but  $y'_i(\alpha) \neq y'_2(\alpha)$ ;
- (2)  $h(x_1, y_i, z_i) \equiv 0$  for any  $h \in I(\mathcal{C}) \cap Q[x_1, x_2, x_3]$  and  $z_i \in C[[x_1 - \alpha]]$ .

**PROOF.** According to (H<sub>5</sub>) and (H<sub>7</sub>),  $\mathcal{C}_2$  is in generic position in the sense of [35, Def 3.1]. As  $(\alpha, \beta)$  is a node of  $\mathcal{C}_2 = V(\omega)$ , then  $\beta$  is a double root of  $\omega(\alpha, x_2)$  by [35, Prop 2.1 & Thm 3.1]. From the

Puiseux theorem (see e.g. [30, Cor 13.16]), there are exactly two Puiseux series  $y_1, y_2$  of  $\mathcal{C}_2$  at  $(\alpha, \beta)$ . And for  $i = 1, 2$ , from [31, §3.2],  $y_i \in C[[x_1 - \alpha]]$ , hence,  $\omega(x_1, y_i) \equiv 0$  and  $y_i(\alpha) = \beta$ . Besides, as  $(\alpha, \beta)$  is a node, we have  $y'_1(\alpha) \neq y'_2(\alpha)$ . This concludes the proof of assertion (1).

Let  $h \in I(\mathcal{C}) \cap Q[x_1, x_2, x_3]$ . By Euclidean division, there are  $u, r \in Q[x_1, x_2]$  and  $m \geq 0$  such that

$$(\partial_{x_2} \omega)^m \cdot h = u(\partial_{x_2} \omega \cdot x_3 - \rho_3) + r.$$

Since  $I(\mathcal{C}) \cap Q[x_1, x_2] = \langle \omega \rangle$ ,  $\omega$  divides  $r$  in  $Q[x_1, x_2]$ , so that,

$$(\partial_{x_2} \omega(x_1, y_i))^m \cdot h(x_1, y_i, z_i) \equiv 0,$$

for  $i = 1, 2$ . As  $\partial_{x_2} \omega(x_1, y_i)$  cannot be identically zero -  $\mathcal{K}(\pi_1, \mathcal{C}_2)$  is finite by (H<sub>5</sub>),  $h(x_1, y_i, z_i) \equiv 0$ .

Finally, by (H<sub>1</sub>),  $Q[\mathcal{C}_3]$  is integral over  $Q[\mathcal{C}_2]$ , so that there is

$$h_0 \in I(\mathcal{C}_3) = I(\mathcal{C}) \cap Q[x_1, x_2, x_3]$$

monic in  $x_3$ . From above, for  $i = 1, 2$ ,  $h_0(x_1, y_i, z_i) \equiv 0$  and  $z_i$  is integral over  $C[[x_1 - \alpha]]$ . As  $C$  is an algebraically closed field of characteristic 0,  $C[[x_1 - \alpha]]$  is integrally closed [30, Cor 13.15]. Thus, as a fraction,  $z_i \in C[[x_1 - \alpha]]$ .  $\square$

**Proposition 3.2.** *The following assertions are equivalent:*

- (1)  $\mathbf{y} \in \text{app}(\mathcal{C}_2)$ ;
- (2)  $\mathbf{y}$  is a node of  $\mathcal{C}_2$  and

$$(\partial_{x_2}^2 \omega \cdot \partial_{x_1} \rho_3 - \partial_{x_1 x_2}^2 \omega \cdot \partial_{x_2} \rho_3)(\mathbf{y}) \neq 0. \quad (1)$$

**PROOF.** Assume that  $\mathbf{y} = (\alpha, \beta)$  is a node. We first prove that if (1) holds then, there are two distinct points of  $\mathcal{C}$  that project on  $\mathbf{y}$ . By Lemma 3.1, there exist  $y_1, y_2 \in C[[x_1 - \alpha]]$  such that  $y'_1(\alpha) \neq y'_2(\alpha)$  and  $y_i(\alpha) = \beta$  and  $\omega(x_1, y_i) \equiv 0$ , for  $i = 1, 2$ . For  $i = 1, 2$  let  $z_i = \frac{\rho_3(x_1, y_i)}{\partial_{x_2} \omega(x_1, y_i)}$ . By Lemma 3.1,

$$\partial_{x_2} \omega(x_1, y_i) \cdot z_i \equiv \rho_3(x_1, y_i).$$

Since  $z_i \in C[[x_1 - \alpha]]$ , by derivation and evaluation in  $x_1 = \alpha$ ,

$$(\partial_{x_1 x_2}^2 \omega(\mathbf{y}) + y'_i(\alpha) \partial_{x_2}^2 \omega(\mathbf{y})) z_i(\alpha) = \partial_{x_1} \rho_3(\mathbf{y}) + y'_i(\alpha) \partial_{x_2} \rho_3(\mathbf{y}). \quad (2)$$

By Lemma 3.1,  $\omega(x_1, y_i) \equiv 0$ . Differentiating twice and evaluating in  $\alpha$ , we get

$$\partial_{x_1}^2 \omega(\mathbf{y}) + 2y'_i(\alpha) \partial_{x_1 x_2}^2 \omega(\mathbf{y}) + y'_i(\alpha)^2 \partial_{x_2}^2 \omega(\mathbf{y}) = 0.$$

Since  $y'_1(\alpha) \neq y'_2(\alpha)$  by Lemma 3.1, they are simple roots of

$$\partial_{x_1}^2 \omega(\mathbf{y}) + 2U \partial_{x_1 x_2}^2 \omega(\mathbf{y}) + U^2 \partial_{x_2}^2 \omega(\mathbf{y}) \in C[U].$$

Therefore,

$$\partial_{x_1 x_2}^2 \omega(\mathbf{y}) + y'_i(\alpha) \partial_{x_2}^2 \omega(\mathbf{y}) \neq 0. \quad (3)$$

Now let  $H: C \rightarrow C$  such that for all  $t \in C$

$$H(t) = \frac{\partial_{x_1} \rho_3(\mathbf{y}) + t \cdot \partial_{x_2} \rho_3(\mathbf{y})}{\partial_{x_1 x_2}^2 \omega(\mathbf{y}) + t \cdot \partial_{x_2}^2 \omega(\mathbf{y})}.$$

Using (2) and according to (3),  $H(y'_i(\alpha)) = z_i(\alpha)$  for  $i = 1, 2$ . But  $H$  is either bijective or constant, whether (1) respectively holds or not. As  $y'_1(\alpha) \neq y'_2(\alpha)$ , (1) holds if, and only if,  $z_1(\alpha) \neq z_2(\alpha)$ . By Lemma 3.1, (2),  $z_1 = (\alpha, \beta, z_1(\alpha))$  and  $z_2 = (\alpha, \beta, z_2(\alpha))$  are points of  $\mathcal{C}_3$  projecting on  $\mathbf{y}$ . From (H<sub>3</sub>), there are  $\mathbf{x}, \mathbf{x}'$  in  $\mathcal{C}$  that project on resp.  $z_1$  and  $z_2$ . They are distinct if, and only if, (1) holds.

We can now prove the equivalence statement. We just proved that, if  $\mathbf{y}$  is a node and (1) holds then,  $\mathbf{y}$  is the projection of two distinct points, that cannot be singular by (H<sub>5</sub>). Conversely, either  $\mathbf{y}$

is not a node, and we conclude by (H<sub>4</sub>) or, by the above discussion, it is the projection of a point of  $\mathcal{C}$ , with two distinct tangent lines (that project on the ones of  $\mathbf{y}$ ). Hence,  $\mathbf{y}$  is the projection of a singular point and then, not in  $\text{app}(\mathcal{C}_2)$ , by definition.  $\square$

#### 4 CONNECTIVITY RECOVERY

We now investigate the connectivity relation between  $\mathcal{C}_R$  and  $\mathcal{C}_{2,R}$ . The following lemma is partly adapted from [31, Lemma 6.2].

**Lemma 4.1.** *Let  $\mathbf{x} = (x_1, \dots, x_n) \in \mathcal{K}(\pi_1, \mathcal{C})$ , then  $\mathbf{x} \in R^n$  if and only if  $x_1 \in R$ , and  $\mathcal{K}(\pi_1, \mathcal{C}_2) - \text{app}(\mathcal{C}_2) = \pi_2(\mathcal{K}(\pi_1, \mathcal{C}))$ .*

**PROOF.** The second point is a direct consequence of (H<sub>2</sub>), as the non-singular critical points of  $\mathcal{C}$  project to the ones of  $\mathcal{C}_2$ .

Let  $\mathbf{x} \in \mathcal{K}(\pi_1, \mathcal{C})$ , and assume  $x_1 \in R$ . By [35, Prop 3.1], as  $\mathcal{C}$  is in generic position, computing sub-resultant sequences gives a rise to  $\sigma_2 \in \mathcal{Q}[x_1]$  such that  $\mathbf{x}_2 = \sigma_2(\mathbf{x}_1) \in R$ . By (H<sub>6</sub>), the line  $V(x_1 - x_1, x_2 - x_2)$  intersects  $\mathcal{C}$  at exactly one point. Hence, by [20, Thm 3.2], computing a Gröbner basis of the ideal

$$I(\mathcal{C}) + \langle x_1 - x_1, x_2 - x_2 \rangle \subset R[X]$$

with respect to the lexicographic order  $x_1 < \dots < x_n$  gives a rise to  $n - 2$  polynomials  $\sigma_3, \dots, \sigma_n$  such that  $\sigma_i \in R[x_1, \dots, x_{i-1}]$  and  $\sigma_i(x_1, \dots, x_{i-1}) = x_i$ , for  $3 \leq i \leq n$ . Hence, the triangular system formed by the  $\sigma_i$ 's raises polynomials  $\tau_2, \dots, \tau_n \in R[x_1]$  such that  $x_i = \tau_i(x_1)$  for  $i \geq 2$ , thus  $\mathbf{x} \in R^n$ . The converse is straightforward.  $\square$

The following lemma shows that, except at apparent singularities, the real traces of  $\mathcal{C}$  and  $\mathcal{C}_2$  share the same connectivity properties.

**Lemma 4.2.** *The restriction of  $\pi_2$  to  $\mathcal{C}_R - \pi_2^{-1}(\text{app}(\mathcal{C}_2))$  is a s.a. homeomorphism of inverse  $\varphi_2$ , defined on  $\mathcal{C}_{2,R} - \text{app}(\mathcal{C}_2)$  such that*

$$\text{for all } \mathbf{y} \notin \mathcal{K}(\pi_1, \mathcal{C}_2), \quad \varphi_2(\mathbf{y}) = \left( \mathbf{y}, \frac{\rho_3(\mathbf{y})}{\partial_{x_2}\omega(\mathbf{y})}, \dots, \frac{\rho_n(\mathbf{y})}{\partial_{x_2}\omega(\mathbf{y})} \right).$$

**PROOF.** Consider  $\mathbf{y} \in \mathcal{C}_{2,R} - \text{app}(\mathcal{C}_2)$ . As  $\mathcal{C}_2 = V(\omega)$ , either  $\partial_{x_2}\omega(\mathbf{y})$  is non-zero or  $\mathbf{y} \in \mathcal{K}(\pi_1, \mathcal{C}_{2,R}) - \text{app}(\mathcal{C}_2)$ . In the latter case, according to Lemma 4.1

$$\pi_2^{-1}(\mathbf{y}) \cap \mathcal{C} \subset \mathcal{K}(\pi_1, \mathcal{C}_R).$$

By (H<sub>6</sub>) there is a unique  $\mathbf{x} \in \mathcal{K}(\pi_1, \mathcal{C}_R) - \pi_2^{-1}(\text{app}(\mathcal{C}_2))$  such that  $\pi_2(\mathbf{x}) = \mathbf{y}$ . Let  $\varphi_2 : \mathcal{C}_{2,R} - \text{app}(\mathcal{C}_2) \rightarrow R^n$  be defined as:

- ▷ if  $\mathbf{y} \in \mathcal{K}(\pi_1, \mathcal{C}_2) - \text{app}(\mathcal{C}_2)$ , then  $\varphi_2(\mathbf{y})$  is the unique  $\mathbf{x}$  satisfying  $\pi_2(\mathbf{x}) = \mathbf{y}$ ;
- ▷ else  $\varphi_2(\mathbf{y}) = (\mathbf{y}, (\rho_3/\partial_{x_2}\omega)(\mathbf{y}), \dots, (\rho_n/\partial_{x_2}\omega)(\mathbf{y}))$ .

Since its graph is a s.a. set by construction,  $\varphi_2$  is a s.a. map according to [4, §2.5.2]. Moreover, if  $\mathbf{y} \in \mathcal{C}_{2,R} - \text{app}(\mathcal{C}_2)$ , then  $\varphi_2(\mathbf{y})$  is the unique element of  $\mathcal{C}_R - \pi_2^{-1}(\text{app}(\mathcal{C}_2))$  such that  $\pi_2(\varphi_2(\mathbf{y})) = \mathbf{y}$ .

Since  $\partial_{x_2}\omega(\mathbf{y})$  does not vanish on this set,  $\varphi_2$  is continuous on  $\mathcal{C}_{2,R} - \mathcal{K}(\pi_1, \mathcal{C}_2)$ . We prove that it is continuous everywhere. Let  $\mathbf{y} \in \mathcal{K}(\pi_1, \mathcal{C}_{2,R}) - \text{app}(\mathcal{C}_2)$  and suppose there is a s.a. path  $\gamma : [0, 1] \rightarrow \mathcal{C}_{2,R}$ , such that  $\gamma(0) = \mathbf{y}$  and  $\gamma(t) \in \mathcal{C}_{2,R} - \mathcal{K}(\pi_1, \mathcal{C}_2)$ , for all  $t > 0$ . Consider the s.a. path  $\tau : t \in (0, 1] \mapsto \varphi_2(\gamma(t)) \in \mathcal{C}_R$ . Since  $\pi_2$  is a proper map by (H<sub>1</sub>),  $\tau$  is bounded. Thus, by [4, Prop 3.21],  $\tau$  can be continuously extended in  $t = 0$  and by continuity,  $\tau(0) \in \mathcal{C}_R$  and  $\pi_2(\tau(0)) = \pi_2(\varphi_2(\mathbf{y})) = \mathbf{y}$ . Hence, by uniqueness  $\tau(0) = \varphi_2(\mathbf{y})$  and, by [4, Prop 3.6 & 3.20],  $\varphi_2$  is continuous in  $\mathbf{y}$ .

Since  $\mathcal{K}(\pi_1, \mathcal{C}_2)$  is finite, no such path  $\gamma$  exists if, and only if, both  $\mathbf{y}$  and  $\mathbf{x}$  are isolated points so that  $\varphi_2$  is trivially continuous at  $\mathbf{y}$ .

In conclusion,  $\varphi_2$  is a s.a. map, continuous on  $\mathcal{C}_{2,R} - \text{app}(\mathcal{C}_2)$ , of inverse the restriction of  $\pi_2$  to  $\mathcal{C}_R - \pi_2^{-1}(\text{app}(\mathcal{C}_2))$  by Lemma 4.1. Hence, this latter restriction is a s.a. homeomorphism, as stated.  $\square$

It remains to investigate how the connectivity of the real traces of  $\mathcal{C}$  and  $\mathcal{C}_2$  are related close to apparent singularities. Recall that an (ambient) isotopy of  $R^n$  is a continuous map  $\mathcal{H} : R^n \times [0, 1] \rightarrow R^n$  such that  $\mathbf{y} \mapsto \mathcal{H}(\mathbf{y}, 0)$  is the identity map and  $\mathbf{y} \mapsto \mathcal{H}(\mathbf{y}, t)$  is a homeomorphism for  $t \in [0, 1]$ . Then two subsets  $Y$  and  $Z$  of  $R^n$  are isotopy equivalent if there is an isotopy  $\mathcal{H}$  of  $R^n$  such that  $\mathcal{H}(Y, 1) = Z$ .

Recall also that a graph  $\mathcal{G}$  is the data of a set  $\mathcal{V}$  of vertices, together with a set  $\mathcal{E}$  of edges  $\{\mathbf{v}, \mathbf{v}'\}$ , where  $\mathbf{v}, \mathbf{v}' \in \mathcal{V}$ . For any  $\mathbf{y}, \mathbf{y}' \in R^2$ , we will denote by  $[\mathbf{y}, \mathbf{y}']$ , the closed line segment  $\{(1-t)\mathbf{y} + t\mathbf{y}', t \in [0, 1]\}$ . Then, if  $\mathcal{V} \subset R^2$ , we call the piecewise linear curve, denoted  $\mathcal{C}_{\mathcal{G}}$ , associated to  $\mathcal{G}$  the union of  $[\mathbf{v}, \mathbf{v}']$  for all  $\{\mathbf{v}, \mathbf{v}'\} \in \mathcal{E}$ . In the following, we note  $\mathcal{P}_2 = \pi_2(\mathcal{P})$ .

**Definition 4.3.** Let  $\mathcal{G}_2 = (\mathcal{V}_2, \mathcal{E}_2)$  be a graph, with  $\mathcal{V}_2 \subset R^2$ . Then we say that  $\mathcal{G}_2$  is a *real topology graph* of  $(\mathcal{C}_2, \mathcal{P}_2)$  if

- (1)  $\mathcal{C}_{2,R}$  is isotopy equivalent to  $\mathcal{C}_{\mathcal{G}_2}$ ;
- (2) the points of  $\mathcal{K}(\pi_1, \mathcal{C}_{2,R}) \cup \mathcal{P}_{2,R}$  are embedded in  $\mathcal{V}_2$ ;
- (3) no two points of  $\mathcal{K}(\pi_1, \mathcal{C}_{2,R})$  have adjacent vertices in  $\mathcal{G}$ .

For the rest of this section, let  $\mathcal{G}_2$  be a *real topology graph* of  $(\mathcal{C}_2, \mathcal{P}_2)$ ,  $\mathcal{H}$  the induced isotopy and, for  $t \in [0, 1]$ ,  $\mathcal{H}_t : \mathbf{y} \in R^2 \rightarrow \mathcal{H}(\mathbf{y}, t)$ , so that  $\mathcal{H}_1(\mathcal{C}_{\mathcal{G}_2}) = \mathcal{C}_{2,R}$ .

Consider s.a. paths  $\gamma_1, \dots, \gamma_4$  in  $R^2$ , all starting from a unique point  $\mathbf{p} \in R^2$ , and not intersecting each other elsewhere (see Figure 1), so that the  $\gamma_i$ 's can be pairwise associated with respect to their unique *opposite branch at p*: given an orientation of  $R^2$  and a sufficiently small circle centered at  $\mathbf{p}$ , we arrange the  $\gamma_i$ 's around  $\mathbf{p}$  with respect to their unique intersection with this circle [8, Thm 9.3.6]; we then pairwise associate them to the one after next in the above arrangement (it does not depend on the chosen orientation). Up to reindexing, say that  $(\gamma_1, \gamma_3)$  and  $(\gamma_2, \gamma_4)$  are the *unique couples of opposite branches at p*.

The next lemma follows directly from classical results in knots and braids theory, see [10, Prop 1.9-10] for the key arguments.

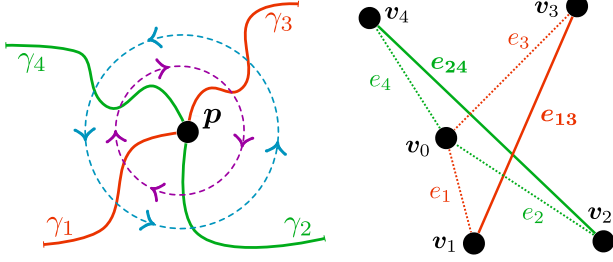
**Lemma 4.4.** *Let the  $\gamma_i$ 's as above, and any isotopy  $\tilde{\mathcal{H}}$  of  $R^2$ . The curves  $(\tilde{\mathcal{H}}_1(\gamma_1), \tilde{\mathcal{H}}_1(\gamma_3))$  and  $(\tilde{\mathcal{H}}_1(\gamma_2), \tilde{\mathcal{H}}_1(\gamma_4))$  do not intersect each other, except at  $\tilde{\mathcal{H}}_1(\mathbf{p})$ . They are the unique couples of opposite branches at this point.*

This property allows us to deduce relations between edges of  $\mathcal{G}_2$ , from relations between the associated branches of  $\mathcal{C}_{2,R}$ .

**Lemma 4.5.** *Let  $\mathbf{y} = (\alpha, \beta) \in \text{app}(\mathcal{C}_{2,R})$ . There are exactly five distinct vertices  $\mathbf{v}_0, \dots, \mathbf{v}_4 \in \mathcal{V}_2$  such that  $\mathcal{H}_1(\mathbf{v}_0) = \mathbf{y}$  and for  $1 \leq i \leq 4$ :*

- (1)  $\{\mathbf{v}_0, \mathbf{v}_i\} \in \mathcal{E}_2$  and  $\mathcal{H}_1(\mathbf{v}_i) \notin \text{app}(\mathcal{C}_2)$ ;
- (2) if  $e_i = [\mathbf{v}_0, \mathbf{v}_i]$ , the  $e_i$ 's do not cross each other except at  $\mathbf{v}_0$ ;
- (3) there exists unique s.a. paths  $\tau_1, \dots, \tau_4$  such that for

$$\tau_i : [0, 1] \rightarrow \mathcal{C}_R, \quad \begin{cases} \pi_2(\tau_i([0, 1])) = \mathcal{H}_1(e_i) \\ \pi_2(\tau_i(0)) = \mathbf{y} \end{cases}$$



**Figure 1:** The left figure illustrates the context of Lemma 4.4 with two possible ordering of the branches; the braid structure appears clearly. On the right, an illustration shows how NodeResolution (Definition 4.6) modifying  $\mathcal{G}_2$  at vertices of  $\mathcal{V}_{\text{app}}$ ; dotted and solid lines representing respective edges of  $\mathcal{G}_2$  and  $\mathcal{G}$ .

- (4) assume that  $(e_1, e_3)$  and  $(e_2, e_4)$  are the two unique couples of opposite edges of  $\mathcal{G}_2$  at  $\mathbf{v}_0$ . Then, there exist  $\mathbf{x}_1 \neq \mathbf{x}_2$  in  $\pi_2^{-1}(\mathbf{y}) \cap \mathcal{C}_R$ , such that  $\mathbf{x}_1 = \tau_1(0) = \tau_3(0)$  and  $\mathbf{x}_2 = \tau_2(0) = \tau_4(0)$ .

PROOF. Let  $\mathbf{v}_0 = \mathcal{H}_1^{-1}(\mathbf{y})$ . As  $\mathbf{y}$  is a node, there are exactly four distinct vertices  $\mathbf{v}_1, \dots, \mathbf{v}_4 \in \mathcal{V}_2$  such that  $\{\mathbf{v}_0, \mathbf{v}_i\} \in \mathcal{E}_2$ , for  $1 \leq i \leq 4$ . Indeed, for  $1 \leq i \leq 4$ , let

$$e_i : t \in [0, 1] \mapsto \mathbf{v}_0 + t(\mathbf{v}_i - \mathbf{v}_0) \in \mathbb{R}^2$$

and  $\gamma_i = \mathcal{H}_1 \circ e_i$ . Then the  $\gamma_i$ 's are the four branches of  $\mathcal{C}_{2,R}$  incident in  $\mathbf{y}$ . Remark that, by the third item of Definition 4.3, none of the  $\mathcal{H}_1(\mathbf{v}_i)$ 's lie in  $\mathcal{K}(\pi_1, \mathcal{C}_{2,R})$ , since  $\mathcal{H}_1(\mathbf{v}_0) = \mathbf{y}$  does. Besides, by the second item, the  $\gamma_i$ 's do not intersect  $\mathcal{K}(\pi_1, \mathcal{C}_2)$ , except in  $\mathbf{y}$ .

In particular, the  $\gamma_i$ 's do not contain points of  $\text{app}(\mathcal{C}_2)$  and intersect each other only at  $\mathbf{y}$ . Hence, by Lemma 4.4, through  $\mathcal{H}_1$ , the  $e_i$ 's intersect each other only at  $\mathbf{v}_0$ .

Besides, let  $i \in \{1, \dots, 4\}$ , and for  $0 < t \leq 1$ , let  $\tau_i(t) = \varphi_2(\gamma_i(t))$ , where  $\varphi_2$  is defined in Lemma 4.2. It is a well-defined s.a. path by the above discussion. Moreover, by Lemma 4.2,  $\tau_i(t) \in \mathcal{C}_R$  and  $\pi_2(\tau(t)) = \gamma(t) = \mathcal{H}_1(e_i(t))$ , for all  $0 < t \leq 1$ . Since  $\pi_2$  is a proper map by (H<sub>1</sub>), [4, Prop 3.21] implies that  $\tau_i$  can be continuously extended in  $t = 0$ . Moreover, by continuity,  $\pi_2(\tau_i(0)) = \mathbf{y}$ .

Finally,  $\mathbf{y}$  being a node, there exist points  $\theta_1 \neq \theta_2$  in  $\mathbb{R}^2$  and  $1 \leq i_1, i_2, i_3, i_4 \leq 4$  such that,

$$\theta_1 = \gamma'_{i_1}(0) = \gamma'_{i_3}(0) \quad \text{and} \quad \theta_2 = \gamma'_{i_2}(0) = \gamma'_{i_4}(0).$$

This means that the branches  $(\gamma_{i_1}, \gamma_{i_3})$  and  $(\gamma_{i_2}, \gamma_{i_4})$  are the two couples of opposite branches of  $\mathcal{C}_2$  at  $\mathbf{y}$ . Then, by Lemma 4.4,  $(e_{i_1}, e_{i_3})$  and  $(e_{i_2}, e_{i_4})$  are the two couples of opposite edges of  $\mathcal{G}_2$  at  $\mathbf{y}$ . For the sake of clarity assume, without loss of generality that  $i_k = k$  for all  $1 \leq k \leq 4$ . By continuity, there exist  $\vartheta_1 \neq \vartheta_2$  in  $\mathbb{R}^n$  such that

$$\vartheta_1 = \tau'_1(0) = \tau'_3(0) \quad \text{and} \quad \vartheta_2 = \tau'_2(0) = \tau'_4(0),$$

and  $\tau_i(0) \in \pi_2^{-1}(\mathbf{y}) \cap \mathcal{C}_R$  for  $1 \leq i \leq 4$ . But as  $\mathbf{y} \in \text{app}(\mathcal{C}_2)$ ,  $\pi_2^{-1}(\mathbf{y}) \cap \mathcal{C}$  contains two distinct non-singular points, of distinct tangent lines, by (H<sub>2</sub>) and (H<sub>4</sub>). Since the  $\tau'_i(0)$ 's are tangent lines of  $\mathcal{C}$ , necessarily,  $\tau_1(0)$  and  $\tau_3(0)$  are equal to one of these points, while  $\tau_2(0)$  and  $\tau_4(0)$  are equal to the other one (if multiple branches converge at a point or the tangent lines differ, it becomes singular).  $\square$

If  $\mathcal{V}_{\text{app}} = \mathcal{H}_1^{-1}(\text{app}(\mathcal{C}_2)) \subset \mathcal{V}_2$  is the subset of apparent nodes, then Lemma 4.5 provides a procedure to compute a new graph  $\mathcal{G}$ , from which we can deduce connectivity queries on  $\mathcal{C}$ .

**Definition 4.6.** Let NodeResolution be the procedure that takes as input  $\mathcal{G}_2$  and  $\mathcal{V}_{\text{app}}$  as above and outputs the graph  $\mathcal{G} = (\mathcal{V}, \mathcal{E})$  as follows (we keep notations of Lemma 4.5).

1. For all  $\mathbf{v} \in \mathcal{V}_{\text{app}}$ , compute the adjacent vertices  $\mathbf{v}_1, \dots, \mathbf{v}_4$  of  $\mathbf{v}$ , indexed such that  $(e_1, e_3)$  and  $(e_2, e_4)$  are opposite edges.
2. Remove  $\mathbf{v}$  from  $\mathcal{V}_2$  and replace the four edges  $(\{\mathbf{v}, \mathbf{v}_k\})_{1 \leq k \leq 4}$  by the two edges  $(\{\mathbf{v}_j, \mathbf{v}_{j+2}\})_{k=1,2}$ , as depicted in Figure 1.

We say that  $\mathbf{v}, \mathbf{v}' \in \mathcal{V}$  are connected in a graph  $\mathcal{G} = (\mathcal{V}, \mathcal{E})$  if there exists an ordered sequence  $(\mathbf{v}_0, \dots, \mathbf{v}_{N+1})$  of vertices in  $\mathcal{V}$  such that  $\mathbf{v}_0 = \mathbf{v}$ ,  $\mathbf{v}_{N+1} = \mathbf{v}'$  and  $\{\mathbf{v}_i, \mathbf{v}_{i+1}\} \in \mathcal{E}$ , for all  $0 \leq i \leq N$ .

**Proposition 4.7.** Let  $\mathcal{G} = (\mathcal{V}, \mathcal{E})$  be the graph output by NodeResolution, on input  $\mathcal{G}_2$  and  $\mathcal{V}_{\text{app}}$ . Then,

- (1)  $\pi_2(\mathcal{P}_R) \subset \mathcal{H}_1(\mathcal{V})$ ;
- (2)  $\mathbf{y}, \mathbf{y}' \in \mathcal{P}_R$  are s.a. connected in  $\mathcal{C}_R$  if, and only if,  $\mathcal{H}_1^{-1}(\pi_2(\mathbf{y}))$  and  $\mathcal{H}_1^{-1}(\pi_2(\mathbf{y}'))$  are connected in  $\mathcal{G}$ .

PROOF. (H<sub>5</sub>) and (H<sub>6</sub>) imply  $\pi_2(\mathcal{P}) \cap \mathcal{H}_1(\mathcal{V}_{\text{app}}) = \emptyset$ . Then  $\mathcal{P}_{2,R} = \pi_2(\mathcal{P}_R)$  as  $\pi_2$  is injective on  $\mathcal{P}$ , and, by definition,  $\mathcal{P}_{2,R} \subset \mathcal{V}$ .

We now deal with the second statement. Let  $\mathbf{x}, \mathbf{x}' \in \mathcal{P}_R$  and

$$\mathbf{v} = \mathcal{H}_1^{-1}(\pi_2(\mathbf{x})) \quad \text{and} \quad \mathbf{v}' = \mathcal{H}_1^{-1}(\pi_2(\mathbf{x}'))$$

in  $\mathcal{V}$ . Assume first that  $\mathbf{v}$  and  $\mathbf{v}'$  are connected in  $\mathcal{G}$ . Then there exist  $\mathbf{v}_1, \dots, \mathbf{v}_N \in \mathcal{V}$  such that, if  $\mathbf{v}_0 = \mathbf{v}$  and  $\mathbf{v}_{N+1} = \mathbf{v}'$ , then  $\{\mathbf{v}_i, \mathbf{v}_{i+1}\} \in \mathcal{E}$  and  $\mathcal{H}_1(\mathbf{v}_i) \notin \text{app}(\mathcal{C}_2)$  for  $0 \leq i \leq N+1$ . Fix  $i \in \{0, \dots, N\}$ . By Lemma 4.2,  $\mathbf{x}_i = \varphi_2(\mathcal{H}_1(\mathbf{v}_i))$  and  $\mathbf{x}_{i+1} = \varphi_2(\mathcal{H}_1(\mathbf{v}_{i+1}))$  are well-defined in  $\mathcal{C}_R$ .

If  $\{\mathbf{v}_i, \mathbf{v}_{i+1}\} \in \mathcal{E}_2$  then,  $\mathcal{H}_1([\mathbf{v}_i, \mathbf{v}_{i+1}]) \cap \text{app}(\mathcal{C}_2) = \emptyset$ , and, by Lemma 4.2,  $\mathbf{x}_i$  and  $\mathbf{x}_{i+1}$  are s.a. connected in  $\mathcal{C}_R$  through  $\varphi_2$ . Otherwise,  $\{\mathbf{v}_i, \mathbf{v}_{i+1}\} \notin \mathcal{E}_2$ , and, by construction of  $\mathcal{G}$ , there exists  $\mathbf{w} \in \mathcal{V}_{\text{app}}$  such that  $\{\mathbf{v}_i, \mathbf{w}\}$  and  $\{\mathbf{w}, \mathbf{v}_{i+1}\}$  are in  $\mathcal{E}_2$ . However, since  $\{\mathbf{v}_i, \mathbf{v}_{i+1}\} \in \mathcal{E}$ , then, according to the construction of  $\mathcal{G}$ ,

$$e_i = [\mathbf{w}, \mathbf{v}_i] \quad \text{and} \quad e_{i+1} = [\mathbf{w}, \mathbf{v}_{i+1}]$$

are opposite edges of  $\mathcal{G}_2$  at  $\mathbf{w}$ . Hence, by items (2) and (3) of Lemma 4.5, there exists a s.a. path  $\tau : [-1, 1] \rightarrow \mathcal{C}_R$  connecting  $\mathbf{x}_i$  to  $\mathbf{x}_{i+1}$ . All in all, by transitivity,  $\mathbf{x}_0 = \mathbf{x}$  and  $\mathbf{x}_{N+1} = \mathbf{x}'$  are s.a. connected in  $\mathcal{C}_R$ , and we are done.

Conversely, suppose that  $\mathbf{x}$  and  $\mathbf{x}'$  are s.a. connected in  $\mathcal{C}_R$  and let  $\tau : [0, 1] \rightarrow \mathcal{C}_R$  be a s.a. path such that  $\tau(0) = \mathbf{x}$  and  $\tau(1) = \mathbf{x}'$ . Let  $\gamma = \pi_2 \circ \tau$ , and

$$\{t_1, \dots, t_N\} = \gamma^{-1}(\mathcal{H}_1(\mathcal{V}_2)) \subset (0, 1)$$

such that  $t_1 < \dots < t_N$ . Let  $t_0 = 0, t_{N+1} = 1$  and for  $0 \leq i \leq N+1$ ,  $\mathbf{v}_i = \mathcal{H}_1^{-1}(\gamma(t_i)) \in \mathcal{V}_2$ . By assumption,  $\{\mathbf{v}_i, \mathbf{v}_{i+1}\} \in \mathcal{E}_2$  for all  $i \in \{0, \dots, N\}$ . Let us prove by induction that for  $0 \leq i \leq N+1$ , either  $\mathbf{v}_i \in \mathcal{V}_{\text{app}}$  or  $\mathbf{v}_i$  is connected to  $\mathbf{v}_0$  in  $\mathcal{G}$ . If  $i = 0$ , there is nothing to prove, so let  $1 \leq i \leq N$  and suppose that the statement holds for all  $0 \leq j < i$ .

Assume  $\mathbf{v}_{i+1} \notin \mathcal{V}_{\text{app}}$ . Then, either  $\mathbf{v}_i \notin \mathcal{V}_{\text{app}}$ , and, by induction hypothesis,  $\mathbf{v}_{i+1}$  and  $\mathbf{v}_0$  are connected, through  $\mathbf{v}_i$ , in  $\mathcal{G}$ . Either  $\mathbf{v}_i \in \mathcal{V}_{\text{app}}$  and, by Lemma 4.5, there are exactly four distinct  $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3, \mathbf{w}_4 \in \mathcal{V} - \mathcal{V}_{\text{app}}$  such that  $\{\mathbf{v}_i, \mathbf{w}_j\} \in \mathcal{E}_2$ , for  $1 \leq j \leq 4$ . Assume, without loss of generality, that  $\mathbf{v}_{i+1} = \mathbf{w}_1$ . Then, there is  $j_1 \in \{2, 3, 4\}$  such that  $\mathbf{v}_{i-1} = \mathbf{w}_{j_1}$ . Using the notation of Lemma 4.5, assume, without loss of generality, that  $e_3 = [\mathbf{v}_i, \mathbf{w}_3]$  is the opposite branch of  $e_1 = [\mathbf{v}_i, \mathbf{w}_1]$  in  $\mathcal{G}_2$  at  $\mathbf{v}_i$ . Then, by items (2) and



(3) of Lemma 4.5, we have  $j_0 = 3$ , since  $\tau([t_{i-1}, t_i])$  is connected to  $\tau([t_i, t_{i+1}])$ . By construction of  $\mathcal{G}$ ,  $\mathbf{w}_1 = \mathbf{v}_{i+1}$  is connected to  $\mathbf{w}_3 = \mathbf{v}_{i-1}$  in  $\mathcal{G}$ , so that, by induction,  $\mathbf{v}_{i+1}$  is connected to  $\mathbf{v}_0$ , through  $\mathbf{v}_{i-1}$ . Hence,  $\mathbf{v} = \mathbf{v}_{N+1}$  and  $\mathbf{v}' = \mathbf{v}_0$  are connected in  $\mathcal{G}$ , proving the converse.  $\square$

Proposition 4.7 also implies that  $\mathcal{G}$  and  $\mathcal{C}_R$  share the same number of s.a. connected components. Therefore, by computing  $\mathcal{G}$ , one can determine this number and answer connectivity queries on  $\mathcal{P}_R$ .

## 5 ALGORITHM

We now provide an algorithm for solving connectivity queries over real algebraic curves, whose different steps correspond sequentially, except for one, to the different sections of this document.

Given a sequence of polynomials defining an algebraic curve, the first step is to perform a linear change of variable, generic enough to ensure assumption (H), and to compute a one-dimensional parametrization encoding it. Answering connectivity queries on the sheared curve is equivalent to do so on the original curve. By [34, Thm 6.18] (or [46, Prop 6.3]), computing such a parametrization has complexity cubic in the degree of the curve, thus bounded by our overall complexity. Besides, according to [46, §J], changing variables in zero and one-dimensional parametrizations has similar complexity. Hence, for the sake of clarity, we omit these two steps.

Following the state of the art of curve topology computation, we consider polynomials with integer coefficients, so that  $\mathbb{Q} = \mathbb{Q}$ ,  $\mathbb{R} = \mathbb{R}$  and  $\mathbb{C} = \mathbb{C}$ . Moreover, we denote by  $\leq_1$  the preorder on points of  $\mathbb{R}^n$  w.r.t. the first coordinate, when they are distinct.

### 5.1 Subroutines

We assume that  $\mathcal{R} = (\omega, \rho_3, \dots, \rho_n)$  has coefficients in  $\mathbb{Z}$  and magnitude  $(\delta, \tau)$ , and consider a zero-dimensional parametrization  $\mathcal{P} = (\lambda, \vartheta_2, \dots, \vartheta_n)$ , with coefficients in  $\mathbb{Z}$  and magnitude  $(\mu, \kappa)$  encoding  $\mathcal{P}$ . Note that  $\mathcal{R}_2 = (\omega, \rho_2)$  and  $\mathcal{P}_2 = (\lambda, \vartheta_2)$  are parametrizations encoding respectively  $\mathcal{C}_2$  and  $\mathcal{P}_2$ . We denote further  $R = \text{Res}_{x_2}(\omega, \partial_{x_2}\omega)$ . Since, by (H<sub>7</sub>),  $\omega$  is monic in  $x_2$ , its roots are exactly the abscissas of  $\mathcal{K}(\pi_1, \mathcal{C}_2)$ . From (H<sub>5</sub>), points of  $\text{app}(\mathcal{C}_2)$  can be identified by their abscissa, which, following Proposition 3.2, can be reduced to gcd computations.

**Proposition 5.1.** *There exists an algorithm `ApparentSingularities` taking as input  $\mathcal{R}$ , as above, and computing a square-free polynomial  $q_{\text{app}} \in \mathbb{Z}[x_1]$ , of magnitude  $(\delta^2, \tilde{O}(\delta^2 + \delta\tau))$  such that*

$$\text{app}(\mathcal{C}_2) = \{(\alpha, \beta) \in \mathcal{K}(\pi_1, \mathcal{C}_2) \mid q_{\text{app}}(\alpha) = 0\},$$

using  $\tilde{O}(\delta^6 + \delta^5\tau)$  bit operations.

**PROOF.** Let  $(\alpha, \beta) \in \mathcal{K}(\pi_1, \mathcal{C}_2)$ . According to [31, Thm 3.2.(ii)], since  $\mathcal{C}$  satisfies (H),  $(\alpha, \beta)$  is a node if, and only if,  $\alpha$  is a double root of  $R$ , i.e. if, and only if,  $\alpha$  is a root of

$$q = \gcd(R^*, R') / \gcd(R^*, R', R''),$$

where  $R^*$  is the square-free part of  $R$ . Moreover, let  $(sr_1, sr_{1,0})$  be the first subresultant sequence of  $(\omega, \partial_{x_2}\omega)$ . By [35, Thm 3.1], if  $q(\alpha) = 0$  then,  $sr_1(\alpha) \neq 0$ , and

$$sr_1(\alpha) \cdot \beta = -sr_{1,0}(\alpha).$$

Let  $A(x_1, x_2)$  be the polynomial on the left-hand side of (1) in Proposition 3.2, and  $u$  be a new indeterminate. Let  $\tilde{A}(x_1, x_2, u)$  be

the homogenization of  $A$  in  $x_2$ , and  $B = \tilde{A}(x_1, -sr_{1,0}, sr_1)$ . Then, from Proposition 3.2, the square-free polynomial

$$q_{\text{app}} = q / \gcd(q, B)$$

vanishes at  $\alpha$  if, and only if,  $(\alpha, \beta) \in \text{app}(\mathcal{C}_2)$ , as required.

We now deal with the quantitative bounds. By [44, Lemma 14],  $R, R^*, sr_1$  and  $sr_{1,0}$  have magnitude  $(\delta^2, \tilde{O}(\delta^2 + \delta\tau))$  and can be computed using  $\tilde{O}(\delta^6 + \delta^5\tau)$  bit operations. Hence, by [49, Cor 11.14] and [44, Lemma 12], computing  $\gcd(R^*, R')$ ,  $\gcd(R^*, R', R'')$  and then  $q$  can be done using  $\tilde{O}(\delta^4 + \delta^3\tau)$  bit operations. Moreover, by [44, Lemma 11],  $q$  has magnitude  $(\delta^2, \tilde{O}(\delta^2 + \delta\tau))$ .

Besides,  $\tilde{A}$  has magnitude  $(O(\delta), \tilde{O}(\tau))$ , so that  $B$  has magnitude

$$(\tilde{O}(\delta^3), \tilde{O}(\delta^3 + \delta^2\tau)).$$

Hence, by [49, Cor 11.14] computing  $\gcd(q, B)$  requires  $\tilde{O}(\delta^6 + \delta^5\tau)$  bit operations. From this, computing  $q_{\text{app}}$  costs  $\tilde{O}(\delta^4 + \delta^3\tau)$  bit operations, by [22, Prop 2.15]. Finally,  $q_{\text{app}}$  has magnitude  $(\delta^2, \tilde{O}(\delta^2 + \delta\tau))$ , by [44, Lemma 11].  $\square$

Suppose now that the polynomial  $q_{\text{app}}$ , from Proposition 5.1, has been computed. We can compute a real topology graph of  $(\mathcal{C}_2, \mathcal{P}_2)$ , while identifying the vertices corresponding to  $\text{app}(\mathcal{C}_2)$  and  $\mathcal{P}_2$ .

**Proposition 5.2.** *There exists an algorithm `Topo2D` taking as input  $\mathcal{R}, \mathcal{P}_2$  and  $q_{\text{app}}$  as above and computing  $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ , a real topology graph of  $(\mathcal{C}_2, \mathcal{P}_2)$ , of size at most  $O(\delta^3 + \delta\mu)$ , using*

$$\tilde{O}(\delta^6 + \delta^5\tau + \mu^6 + \mu^5\kappa)$$

bit operations. It also outputs ordered sequences  $\mathcal{V}_{\text{app}}$  and  $\mathcal{V}_{\mathcal{P}}$ , of elements of  $\mathcal{V}$ , that are in one-to-one correspondence with resp. the points of  $\text{app}(\mathcal{C}_{2, \mathbb{R}})$  and  $\mathcal{P}_{2, \mathbb{R}}$ , ordered with respect to  $\leq_1$ .

**PROOF.** According to [42, Thm 14], and more recently [22, Thm 1.1], there is an algorithm that computes a planar graph  $\mathcal{G}$ , whose associated piecewise linear curve  $\mathcal{C}_{\mathcal{G}}$ , is isotopy equivalent to  $\mathcal{C}_{2, \mathbb{R}}$ , using  $\tilde{O}(\delta^6 + \delta^5\tau)$  bit operations. Under slight modifications, these algorithms can compute the claimed output of `Topo2D`, within the same complexity bounds. For clarity, we only consider the algorithm of [22], that we roughly describe.

Let  $\alpha_1 < \dots < \alpha_N$  be the abscissas of the points of  $\mathcal{K}(\pi_1, \mathcal{C}_{2, \mathbb{R}})$ . They are distinct by (H<sub>5</sub>). [22, Prop 2.24] first computes disjoint isolating intervals for each  $\alpha_i$ . Then, [22, Prop 3.13] isolates the ordinates of the points above each  $\alpha_i$ . This process gives rise to isolating boxes, which stand for vertices in the final graph. The algorithm eventually connects these boxes to separating vertices above regular values in the intervals  $(\alpha_j, \alpha_{j+1})$ . The latter is done by counting the number of incoming left and right branches in each box. For points of  $\mathcal{K}(\pi_1, \mathcal{C}_{2, \mathbb{R}})$ , it is tackled by [22, §4.2-4], while for others it is straightforward (exactly one branch from each side).

The above process computes a graph  $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ , such that  $\mathcal{C}_{\mathcal{G}}$  is isotopy equivalent to  $\mathcal{C}_{2, \mathbb{R}}$ . Remark that  $\mathcal{V}$  contains a subset  $\mathcal{V}_{\mathcal{K}}$  of vertices associated to the unique point of  $\mathcal{K}(\pi_1, \mathcal{C}_{2, \mathbb{R}})$  above the  $\alpha_i$ 's, all separated by vertices associated to regular points. Moreover, by Proposition 5.1,  $\mathcal{V}_{\text{app}}$  is exactly the subset of  $\mathcal{V}_{\mathcal{K}}$ , associated to the  $\alpha_i$ 's where  $q_{\text{app}}$  vanishes. Then, according to [22, Prop 2.24] and Proposition 5.1, one can compute disjoint isolating intervals of the roots of  $R$  and  $q_{\text{app}}$  and identify all common roots, using

$$\tilde{O}(\delta^6 + \delta^5\tau)$$

bit operations. This gives  $\mathcal{V}_{\text{app}}$ .

Hence, it remains to show that introducing vertices for control points  $\mathcal{P}_{2,\mathbb{R}}$  (together with those above and below) can be done in the claimed bound. First, recall that  $\mathcal{D} = (\lambda, \vartheta_2)$  encodes  $\mathcal{P}_2$ . According to [22, Prop 2.24] again, we can compute disjoint isolating intervals for all distinct (by (H<sub>5</sub>)) real roots of  $\lambda$  and  $R$ , using at most

$$\tilde{O}(\delta^6 + \delta^5\tau + \mu^6 + \mu^5\kappa)$$

bit operations. Next, let  $g(x_1, x_2) = \lambda' \cdot x_2 - \vartheta_2$ . It is a bivariate polynomial with magnitude  $(\mu, \kappa)$ . Then, according to [22, Prop 3.14], for each root  $\beta$  of  $\lambda$ , we can compute isolating intervals for all roots  $x_2$  of  $(\omega \cdot g)(\beta, x_2)$ , and identify the unique common roots, within the same complexity bound. This gives  $\mathcal{V}_{\mathcal{D}}$ . Moreover, since  $\mathcal{P} \cap \mathcal{K}(\pi_1, \mathcal{C}_{2,\mathbb{R}}) = \emptyset$ , as seen above, the connection step for the introduced vertices is straightforward, and does not affect the complexity bound.

Finally, since we consider at most  $\delta^2 + \mu$  fibers, each of them containing at most  $\delta$  points then, taking in account the regular separating fibers, we get at most  $O(\delta^3 + \delta\mu)$  vertices and edges.  $\square$

## 5.2 The algorithm

Let `IndConnectComp` be an algorithm taking as input a graph  $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ , and an ordered sequence  $\mathcal{V} = (\mathbf{v}_1, \dots, \mathbf{v}_N)$  of vertices of  $\mathcal{G}$ . It outputs a partition  $I_1, \dots, I_s$  of  $\{1, \dots, N\}$ , grouping the indices of the  $\mathbf{v}_i$ 's lying in the same connected components of  $\mathcal{G}$ . By [19, §22.2], this has a bit complexity linear in the size of  $\mathcal{G}$ .

---

### Algorithm 1 `ConnectCurve`

---

**Input:**  $\mathcal{R} = (\omega, \rho_3, \dots, \rho_n) \subset \mathbb{Z}[x_1, x_2]$  encoding an algebraic curve  $\mathcal{C} \subset \mathbb{C}^n$  and  $\mathcal{P} = (\lambda, \vartheta_2, \dots, \vartheta_n) \subset \mathbb{Z}[x_1]$  encoding points  $\mathbf{p}_1 \preceq_1 \dots \preceq_1 \mathbf{p}_\mu$  of  $\mathcal{C}_{\mathbb{R}}$ , such that  $(\mathcal{C}, \mathcal{P})$  satisfies (H).

**Output:** a partition of  $\{1, \dots, \mu\}$  grouping the indices of the  $\mathbf{p}_i$ 's lying in the same s.a. connected component of  $\mathcal{C}_{\mathbb{R}}$ .

- 1:  $\mathcal{P}_2 \leftarrow (\lambda, \vartheta_2)$ ;
  - 2:  $q_{\text{app}} \leftarrow \text{ApparentSingularities}(\mathcal{R})$
  - 3:  $[\mathcal{G}_2, \mathcal{V}_{\text{app}}, \mathcal{V}_{\mathcal{D}}] \leftarrow \text{Topo2D}(\mathcal{R}, \mathcal{P}_2, q_{\text{app}})$ ;
  - 4:  $\mathcal{G} \leftarrow \text{NodeResolution}(\mathcal{G}_2, \mathcal{V}_{\text{app}})$ ;
  - 5: **return** `IndConnectComp`( $\mathcal{V}_{\mathcal{D}}, \mathcal{G}$ );
- 

Correction, and complexity estimate, of Algorithm 1, follow directly from Propositions 5.1, 5.2 and 4.7. This proves Theorem 1.1.

As mentioned before, the number of connected components of the graph  $\mathcal{G}$  computed equals the number of s.a. connected components of  $\mathcal{C}_{\mathbb{R}}$ . As an extension, for curves given as unions, Algorithm 1 can be applied to each curve, where query points are extended to include pairwise common intersection points. The resulting subsets are then merged based on their shared points.

## REFERENCES

- [1] Lionel Alberti, Bernard Mourrain, and Julien Wintz. 2008. Topology and arrangement computation of semi-algebraic planar curves. *Computer Aided Geometric Design* 25, 8 (2008), 631–651.
- [2] Juan Gerardo Alcázar and J Rafael Sendra. 2005. Computation of the topology of real algebraic space curves. *Journal of Symbolic Computation* 39, 6 (2005), 719–744.
- [3] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. 1999. Computing roadmaps of semi-algebraic sets on a variety. *Journal of the American Mathematical Society* 13, 1 (1999), 55–82.
- [4] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. 2016. *Algorithms in Real Algebraic Geometry* (3 ed.). Springer, Berlin, Heidelberg.
- [5] Saugata Basu and Marie-Françoise Roy. 2014. Divide and conquer roadmap for algebraic sets. *Discrete & Computational Geometry* 52, 2 (2014), 278–343.
- [6] Saugata Basu, Marie-Françoise Roy, Mohab Safey El Din, and Eric Schost. 2014. A baby step–giant step roadmap algorithm for general algebraic sets. *Foundations of Computational Mathematics* 14, 6 (2014), 1117–1172.
- [7] Eric Berberich, Pavel Emeliyanenko, Alexander Kobel, and Michael Sagraloff. 2013. Exact symbolic–numeric computation of planar algebraic curves. *Theoretical Computer Science* 491 (2013), 1–32.
- [8] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy. 1998. *Real algebraic geometry*. Vol. 36. Springer-Verlag Berlin Heidelberg.
- [9] Driss Bouziane and M'hammed El Kahoui. 2002. Computation of the dual of a plane projective curve. *Journal of Symbolic Computation* 34, 2 (2002), 105–117.
- [10] Gerhard Burde and Heiner Zieschang. 2002. *Knots* (2nd revised and extended 2003 ed.). De Gruyter, Berlin, New York. <https://doi.org/doi:10.1515/9783110198034>
- [11] Michael Burr, Sung Woo Choi, Benjamin Galehouse, and Chee K Yap. 2008. Complete subdivision algorithms, II: Isotopic meshing of singular algebraic curves. In *Proceedings of the 21th International Symposium on Symbolic and Algebraic Computation*. 87–94.
- [12] John Canny. 1988. *The complexity of robot motion planning*. MIT press.
- [13] John Canny. 1993. Computing roadmaps of general semi-algebraic sets. *Comput. J.* 36, 5 (1993), 504–514.
- [14] Jose Capco, Mohab Din, Safey El Din, and Josef Schicho. 2020. Robots, computer algebra and eight connected components. In *Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation*. 62–69.
- [15] Jose Capco, Mohab Safey El Din, and Josef Schicho. 2023. Positive dimensional parametric polynomial systems, connectivity queries and applications in robotics. *Journal of Symbolic Computation* 115 (2023), 320–345. <https://doi.org/10.1016/j.jsc.2022.08.008>
- [16] Damien Chablat, Rémi Prébet, Mohab Safey El Din, Durgesh H Salunkhe, and Philippe Wenger. 2022. Deciding cuspidality of manipulators through computer algebra and algorithms in real algebraic geometry. In *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation*. 439–448.
- [17] Jinsan Cheng, Sylvain Lazard, Luis Peñaranda, Marc Pouget, Fabrice Rouillier, and Elias Tsigaridas. 2010. On the topology of real algebraic plane curves. *Mathematics in Computer Science* 4 (2010), 113–137.
- [18] Jin-San Cheng, Kai Jin, and Daniel Lazard. 2013. Certified rational parametric approximation of real algebraic space curves with local generic position method. *Journal of Symbolic Computation* 58 (2013), 18–40.
- [19] Thomas H Cormen, Charles E Leiserson, Ronald L Rivest, and Clifford Stein. 2009. *Introduction to algorithms* (third ed.). MIT press.
- [20] David A. Cox, John Little, and Donal O'Shea. 2015. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra* (4 ed.). Springer Cham.
- [21] Daouda Niang Diatta. 2009. *Calcul effectif de la topologie de courbes et surfaces algébriques réelles*. Ph.D. Dissertation. Université de Limoges.
- [22] Daouda Niang Diatta, Sény Diatta, Fabrice Rouillier, Marie-Françoise Roy, and Michael Sagraloff. 2022. Bounds for polynomials on algebraic numbers and application to curve topology. *Discrete & Computational Geometry* 67, 3 (2022), 631–697.
- [23] Daouda Niang Diatta, Bernard Mourrain, and Olivier Ruatta. 2008. On the computation of the topology of a non-reduced implicit space curve. In *Proceedings of the twenty-first international symposium on Symbolic and algebraic computation*. 47–54.
- [24] Daouda Niang Diatta, Bernard Mourrain, and Olivier Ruatta. 2012. On the isotopic meshing of an algebraic implicit surface. *Journal of Symbolic Computation* 47, 8 (2012), 903–925.
- [25] Daouda Niang Diatta, Fabrice Rouillier, and Marie-Françoise Roy. 2014. On the computation of the topology of plane curves. In *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*. 130–137.
- [26] Dimitrios I. Diochnos, Ioannis Z. Emiris, and Elias P. Tsigaridas. 2007. On the Complexity of Real Solving Bivariate Systems. In *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation* (Waterloo, Ontario, Canada) (ISSAC '07). Association for Computing Machinery, New York, NY, USA, 127–134. <https://doi.org/10.1145/1277548.1277567>
- [27] Dimitrios I. Diochnos, Ioannis Z. Emiris, and Elias P. Tsigaridas. 2009. On the asymptotic and practical complexity of solving bivariate systems over the reals. *Journal of Symbolic Computation* 44, 7 (2009), 818–835.
- [28] Clémence Durvy and Grégoire Lecerf. 2008. A concise proof of the Kronecker polynomial system solver from scratch. *Expositiones Mathematicae* 26, 2 (2008), 101–139.
- [29] Arno Eigenwillig, Michael Kerber, and Nicola Wolpert. 2007. Fast and exact geometric analysis of real algebraic plane curves. In *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation*. 151–158.
- [30] David Eisenbud. 1995. *Commutative Algebra with a View Toward Algebraic Geometry*. Vol. 150. Springer-Verlag, New York.

- [31] M'hammed El Kahoui. 2008. Topology of real algebraic space curves. *Journal of Symbolic Computation* 43, 4 (2008), 235–258.
- [32] E. Fortuna, P. Gianni, and B. Trager. 2009. Generators of the ideal of an algebraic space curve. *Journal of Symbolic Computation* 44, 9 (2009), 1234–1254. <https://doi.org/10.1016/j.jsc.2008.02.014>
- [33] Gregory Gattellier, Abder Labrouzy, Bernard Mourrain, and Jean-Pierre Técourt. 2005. Computing the topology of three-dimensional algebraic curves. *Computational methods for algebraic spline surfaces* (2005), 27–43.
- [34] Nardo Giménez and Guillermo Matera. 2019. On the bit complexity of polynomial system solving. *Journal of Complexity* 51 (2019), 20–67. <https://doi.org/10.1016/j.jco.2018.09.005>
- [35] Laureano González-Vega and M'hammed El Kahoui. 1996. An Improved Upper Complexity Bound for the Topology Computation of a Real Algebraic Plane Curve. *Journal of Complexity* 12, 4 (1996), 527–544. <https://doi.org/10.1006/jcom.1996.0032>
- [36] Robin Hartshorne. 1977. Graduate texts in mathematics. *Algebraic Geometry* 52 (1977).
- [37] Audun Holme and Joel Roberts. 1979. Pinch-points and multiple locus of generic projections of singular varieties. *Advances in Mathematics* 33, 3 (1979), 212–256.
- [38] Md Nazrul Islam and Adrien Poteaux. 2011. Connectivity queries on curves in  $\mathbb{R}^n$ . *ACM Communications in Computer Algebra* 45, 1/2 (2011), 117–118.
- [39] Kai Jin and Jinsan Cheng. 2021. On the complexity of computing the topology of real algebraic space curves. *Journal of Systems Science and Complexity* 34 (2021), 809–826.
- [40] Jeremy Yirmeyahu Kaminski, Alexei Kanel-Belov, and Mina Teicher. 2008. Trisecant Lemma for Non Equidimensional Varieties. *Journal of Mathematical Sciences* 149, 2 (2008), 1087–1097.
- [41] Michael Kerber and Michael Sagraloff. 2012. A worst-case bound for topology computation of algebraic curves. *Journal of Symbolic Computation* 47, 3 (2012), 239–258.
- [42] Alexander Kobel and Michael Sagraloff. 2015. On the complexity of computing with planar algebraic curves. *Journal of Complexity* 31, 2 (2015), 206–236.
- [43] Chen Liang, Bernard Mourrain, and Jean-Pascal Pavone. 2008. Subdivision methods for the topology of 2d and 3d implicit curves. *Geometric modeling and algebraic geometry* (2008), 199–214.
- [44] Kurt Mehlhorn, Michael Sagraloff, and Pengming Wang. 2015. From approximate factorization to root isolation with application to cylindrical algebraic decomposition. *Journal of Symbolic Computation* 66 (2015), 34–69.
- [45] David Mumford. 1995. *Algebraic geometry I: complex projective varieties*. Springer Science & Business Media.
- [46] Mohab Safey El Din and Éric Schost. 2017. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. *Journal of the ACM (JACM)* 63, 6 (2017), 1–37.
- [47] Raimund Seidel and Nicola Wolpert. 2005. On the exact computation of the topology of real algebraic curves. In *Proceedings of the twenty-first annual symposium on Computational geometry*. 107–115.
- [48] Igor Rostislavovich Shafarevich. 2013. *Basic algebraic geometry*. Vol. 1. Springer.
- [49] Joachim von zur Gathen and JÄijrgen Gerhard. 2013. *Modern Computer Algebra* (3 ed.). Cambridge University Press. <https://doi.org/10.1017/CBO9781139856065>