On the computation of the topology of plane curves

Daouda Niang Diatta, Fabrice Rouillier, Marie-Françoise Roy

On the computation of the topology of plane curves

Daouda Niang Diatta

Université Assane Seck de Ziguinchor, Sénégal

Fabrice Rouillier

INRIA Paris-Rocquencourt, IMJ - Université de Paris VI, France

Marie-Françoise Roy

IRMAR, Université de Rennes I, France

Abstract

Let $P \in \mathbb{Z}[X, Y]$ be a square free polynomial and $\mathcal{C}(P) := \{(\alpha, \beta) \in \mathbb{R}^2, P(\alpha, \beta) = 0\}$ be the real algebraic curve defined by P. We give a deterministic algorithm for the computation of the topology of $\mathcal{C}(P)$ *i.e* a straight-line planar graph isotopic to $\mathcal{C}(P)$. Our main result is the computation of the local topology in a neighbourhood of each of the singular and critical points of the projection wrt the X axis in $\tilde{O}(d^6\tau)$ bit operations where $\tilde{O}$ means that we ignore logarithmic factors in d and τ. Combined to state of the art sub-algorithms used for computing a Cylindrical Algebraic Decomposition, this result avoids a generic shear and gives a deterministic algorithm for the computation of the topology of $\mathcal{C}(P)$ in $\tilde{O}(d^6\tau + d^7)$ bit operations.

1 Introduction

Problem description and related works. Let $P \in \mathbb{Z}[X, Y]$ be a square free polynomial of total degree d and integer coefficients of bitsize bounded by τ and $\mathcal{C}(P) := \{(x, y) \in \mathbb{R}^2, P(x, y) = 0\}$ be the real algebraic curve defined by P. We address the problem of computing the topology of the curve $\mathcal{C}(P)$ *i.e* a straight-line planar graph isotopic to $\mathcal{C}(P)$.

Computing the topology of a real algebraic curve is a classical problem in algorithmic real algebraic geometry and plays an important role in many applications in Computer Aided Geometric Design. It is extensively studied in the context of symbolic computation. Most papers are based on some variant of Cylindrical Decomposition : decompose the X-axis into a finite number of open intervals and points above which the curve has a cylindrical structure. Supposing that there are no vertical asymptotes of vertical lines inside the curve, the special values which are the critical values of the projection onto X and the projections of the singular points define the *special fibers* i.e. the points of the curves above these special values. Taking additional points between two such projections of singular points defines some *regular fibers* as well as a partition of the line (with intervals bounded by the projections of the special and regular fibers).

Computing a straight-line planar graph isotopic to $\mathcal{C}(P)$ then consists essentially in connecting the points of a regular fiber to the points of the next (special) fiber (assuming that the fibers are ordered wrt their projection on the real X axis).

This operation requires :

- computing the special and regular fibers;
- computing the number of branches of the curve that go to each of the points of the special fiber.

The regular fibers can efficiently be obtained by computing the real roots of univariate polynomials with real algebraic coefficients which are square free so that the main difficulty is the computation of the special fibers, which is to compute the real roots of univariate polynomials with real algebraic coefficients which are not square free. This last problem is efficiently solved in [MSW2] in $O(d^5\tau + d^6)$ *expected* bit operations, and $O(d^6\tau + d^7)$ bit operations in the worst case (by simply replacing the expected complexity of the gcd computation of two polynomials by the worst case one - see [GG].

The method used for computing the number of half branches of the curve going to a *special point* plays a key role in the algorithm. A usual strategy, introduced in [GE1] (see [BPR],[GI],[EKW], [DMR], [MSW2]), consists in putting the curve in so call *generic position*, so that each special fiber contains at most one special point (critical or singular), and identifying this point among the points of the special fiber. Having a unique special point per special fiber makes it possible to deduce the number of branches passing through this point instead of computing it explicitly. An efficient variant of this strategy can be found in with an expected complexity in $O(d^5\tau + d^6)$ bit operations, the probabilistic behavior being due to some gcd computations and to the choice of a direction that separate the special points, which is done at random. This approach spoils the study of the complexity in the worst case by a factor up to $O(d^4)$ (the maximum number of non separating directions) as in [GE1].

Our results.

We combine new results on the computation of the local topology of the curve in an isolating box of each of its *special points* (in a sense to be made precise later in the paper) with efficient sub-algorithms used for computing Cylindrical Algebraic Decompositions from [MSW2], mainly the algorithm for isolating and refining the roots on univariate polynomials with approximate coefficients knowing the number of distinct complex roots and its application to the isolation of the roots of $P(\alpha, Y)$, where α is a root of the resultant of P and $\partial_X P$. We essentially obtain two new results:

- The first one (Theorem 33) is a lower bound to measure the deviation of the curve from its tangent at a special point. This bound plays a key role in the complexity analysis of the computation of the local topology of $\mathcal{C}(P)$ inside its special boxes since it permits us to control the sizes of such isolating special boxes. This result is of independent interest and could be used outside the present paper, for example to decrease the complexity of the algorithm from [CLPPRT].
- The second one is an algorithm for reconstructing the local topology of the curve inside each special box by connecting its boundary points (see subsection 3.4). We build such an algorithm by examining closely the relative position of the boundary points of the special box with the special point and by using the signs of the slopes of the tangent lines of $\mathcal{C}(P)$ at the intersection points of $\mathcal{C}(P)$ with the horizontal boundaries of the special box.

We give a *deterministic algorithm* for the computation of the topology of $\mathcal{C}(P)$ and analyze its bit complexity. For a square free polynomial $P \in \mathbb{Z}[X, Y]$ of total degree d and integer coefficients of bitsize bounded by τ, we show that a straight-line planar graph isotopic to $\mathcal{C}(P)$ can be computed with $\tilde{O}(d^6\tau + d^7)$ bit operations using a *deterministic algorithm*. Our algorithm does not require to put the curve in generic position.

Sketch of our algorithm for topology computation. We suppose that the planar algebraic curve $\mathcal{C}(P)$ is defined by a square-free bivariate polynomial $P \in \mathbb{Z}[X, Y]$, of degree d and bitsize bounded by τ.

1. Reduce to the case where the curve does not contain vertical or horizontal lines or vertical asymptotes by a linear change of variable. The cost is $\tilde{O}(d^3\tau + d^4)$ bit operations.
2. Perform the Cylindrical Algebraic Decomposition of the curve with the following steps
    i. compute
    $$D(X) = \mathrm{Res}_Y(P, \partial_X P \partial_Y P)(X), \tag{1}$$
    ii. isolate the real roots of D,
    iii. above each real zero of D, determine the number of complex points of the special fibers defined by $D(X) = P(X, Y) = 0$
    iv. isolate the real roots of the special fibers and define special boxes containing only a special point,
    v. count the number of intersections of the curve with the vertical boundaries of these special boxes.

3. Test whether the curve is in generic position. If so, we combine the results from [MSW2] for computing the local topology at the singular and critical points and use the classical connection from [GE1] to compute the topology.
4. Otherwise, if the curve is not in generic position, we avoid the usual technique which is to enter in a loop calling the same algorithm after changing the direction of projection. We examine closely the situation at the boundary of a special box of the form $[a, b] \times [c, d]$ containing a unique special point (α, γ), and compute the topology of the curve inside the box with the following steps :
   i. isolate the roots on the horizontal sides on the box. The cost is $\tilde{O}(d^6\tau)$ bit operations.
   ii. evaluate the sign of $\partial_X P \partial_Y P$ at these points. The cost is $\tilde{O}(d^6\tau)$ bit operations.
   iii. decide how many roots of $P(X, c)$ are before and after α on the horizontal sides of the box, and similarly for $P(X, d)$. The cost is $\tilde{O}(d^6\tau)$ bit operations.
   iv. use a connection algorithm reconstituting the topology of the curve from the information available on the boundary of the special boxes. The cost is $O(d^4)$ bit operations.

Before going through the detailed description and complexity analysis of each step of our algorithm in Section 3, we recall some definitions and basic complexity results which will be useful along this paper in Section 2, then analyze in details how far the curve deviates from its tangent at a special point in Section 3, since this plays a key role in the complexity analysis of the computation of the local topology of $\mathcal{C}(P)$ inside its special boxes in Section 3.

2 Basic definitions and complexity results

2.1 Definitions

Let $P \in \mathbb{Z}[X, Y]$ be a square-free polynomial and $\mathcal{C}(P) = \{(x, y) \in \mathbb{R}^2: P(x, y) = 0\}$ be the real algebraic curve defined by P.

Definition 1. *[X-critical, Y-critical, Singular points and Regular points.] A point $(\alpha, \gamma) \in \mathcal{C}(P)$ is called:*

- *a X-critical point if $\partial_Y P(\alpha, \gamma) = 0$ and $\partial_X P(\alpha, \gamma) \neq 0$,*
- *a Y-critical point if $\partial_X P(\alpha, \gamma) = 0$ and $\partial_Y P(\alpha, \gamma) \neq 0$,*
- *a singular point if $\partial_X P(\alpha, \gamma) = \partial_Y P(\alpha, \gamma) = 0$,*
- *a regular point if $\partial_X P(\alpha, \gamma) \neq 0$ and $\partial_Y P(\alpha, \gamma) \neq 0$.*

Definition 2. *[Critical point.] A point $(\alpha, \gamma) \in \mathcal{C}(P)$ is a critical point of $\mathcal{C}(P)$ if it is a X-critical or a Y-critical or a singular point of $\mathcal{C}(P)$. We denote by $\mathrm{Crit}(\mathcal{C}(P))$ the set of critical points of $\mathcal{C}(P)$.*

Definition 3. *[Special fiber.] Let $P \in \mathbb{Z}[X, Y]$ be a square-free polynomial and $\alpha \in \mathbb{R}$. We call α-fiber the set*

$$\{(\alpha, \gamma) \in \mathbb{R}^2, P(\alpha, \gamma) = 0\}.$$

A special fiber is an α-fiber for a real root α of D (see Eq (1)).

The set

$$\mathrm{SpeFib}(\mathcal{C}(P)) := \{(\alpha, \gamma) \in \mathbb{R}^2, D(\alpha) = P(\alpha, \gamma) = 0\} \tag{2}$$

is the union of the special fibers.

Definition 4. *[Generic position.] Let $\alpha \in \mathbb{C}$ and $\mathrm{Crit}(\alpha) := \#\{\beta \in \mathbb{C} |\ (\alpha, \beta) \in \mathrm{Crit}(\mathcal{C}(P))\}$. $\mathcal{C}(P)$ is in generic position if :*

1. *$\forall \alpha \in \mathbb{C}, \mathrm{Crit}(\alpha) \leqslant 1$,*
2. *There is no asymptotic direction of $\mathcal{C}(P)$ parallel to the Y-axis.*

2.2 Quantitative results

In our complexity analysis we are going to use some quantitative results on the geometry of the roots. The following result is straightforward.

Proposition 5. *If $f(X,Y)\in\mathbb{Z}[X,Y]$ has coefficients of bitsize τ and $(\alpha,\gamma)\in\mathbb{C}^2$,*

$$|f(\alpha,\gamma)|\leqslant(\deg_X(f)+1)(\deg_Y(f)+1)\,2^{\tau}\max(1,|\alpha|)^{\deg_X(f)}\max(1,|\gamma|)^{\deg_Y(f)}.$$

Notation 6. *We consider a univariate polynomial*

$$f=c_pX^p+\cdots+c_qX^q, p>q, c_qc_p\neq0,$$

with coefficients in $\mathbb{R}$. We denote

$$\begin{aligned} C(f) &= \sum_{q\leq i\leq p}\left|\frac{c_i}{c_p}\right|, \\ c(f) &= |c_q|\left(\sum_{q\leq i\leq p}|c_i|\right)^{-1}. \end{aligned}$$

Proposition 7. *[Cauchy bound][BPR]*
a) The absolute value of any root of f in $\mathbb{C}$ is smaller than $C(f)$.
b) The absolute value of any non-zero root of f in $\mathbb{C}$ is bigger than $c(f)$.

Proposition 8. *[BPR] Let P be a univariate polynomials of degree p and coefficients of bitsize bounded by τ and Q of degree q dividing P. Then the coefficients of Q are of bitsize bounded $q+\tau+\log(p+1)$.*

Definition 9. *Let f be a univariate polynomial with real coefficients. We denote by*

$$\begin{aligned} \mathrm{Zer}(f) &= \{x\in\mathbb{R}|\,f(x)=0\}, \\ \mathrm{Zer}_{\mathbb{C}}(f) &= \{x\in\mathbb{C}|\,f(x)=0\} \\ \mathrm{Zer}_{\mathbb{C}\setminus\mathbb{R}}(f) &= \{x\in\mathbb{C}\setminus\mathbb{R}|\,f(x)=0\} \\ \Gamma(f) &= \log\max\left(1,\max_{\mathrm{Zer}_{\mathbb{C}}(f)}|y|\right), \\ \mathrm{sep}(f,y) &= \min_{z\in\mathrm{Zer}_{\mathbb{C}}(f),z\neq y}|z-y|, \\ \Sigma(f) &= -\sum_{\mathrm{Zer}_{\mathbb{C}}(f)}\log\mathrm{sep}(f,y). \end{aligned}$$

Proposition 10. *[BPR] If f is a univariate polynomial of degree d and bitsize at most τ*

$$\Gamma(f)=\tilde{O}(\tau),$$

$$\Sigma(f)=\tilde{O}(d\tau).$$

Theorem 11. *[KS] Denoting by δ the number of real roots of D, and $\mathrm{Zer}(D)=\{\alpha_1<\ldots<\alpha_\delta\}$,*

$$\sum_{i=1}^{\delta}\Gamma(P(\alpha_i,-))=O(d^2\tau),$$

$$\sum_{i=1}^{\delta}\Sigma(P(\alpha_i,-))=O(d^3\tau).$$

2.3 Algorithmic results

Hereafter we recall some complexity results which will be used in the complexity analysis of our algorithms.

Proposition 12. *[GG] Let $P_1 \in K[X]$ of degree d_1 and $P_2 \in K[X]$ of degree $d_2 < d_1$. The euclidean division of P_1 by P_2 can be computed in $\tilde{O}(d_1)$ arithmetic operations in K*

Proposition 13. *[GG] Let $P_1 \in \mathbb{Z}[X]$ of degree d_1 with coefficients of bitsize bounded by τ and $P_2 \in \mathbb{Z}[X]$ of degree $d_2 < d_1$.*

a) Performing the euclidean division of P_1 by P_2 has a bit complexity $\tilde{O}(d_1 (d_1 - d_2) \tau)$.

b) Deciding whether P_2 divides P_1 has a bit complexity of $\tilde{O}(d_1 (\tau + d_1))$.

The definition of the subresultant polynomials can be found, for example, in [BPR]. The last nonzero subresultant polynomial is a a gcd of the input polynomials.

Proposition 14. *[Subresultant Computation][BPR][GG] Let $P \in K[X]$ of degree $p \leqslant d$ and $Q \in K[X]$ of degree $q < p$.*

The subresultant coefficients of P and Q and a gcd of P and Q can be computed in $O(d)$ arithmetic operations in K.

Proposition 15. *[Bivariate Subresultant Computation][BPR][GG] Let $P \in \mathbb{Z}[Y][X]$ of degree $p \leqslant d$ and $Q \in \mathbb{Z}[Y][X]$ a bivariate polynomial of degree $q < p$, both of bitsize τ.*

The subresultant coefficients of P and Q can be computed in $\tilde{O}(d)$ arithmetic operations between univariate polynomials of degree $O(d^2)$ and of bitsize $O(d\tau)$, so with a bit complexity $\tilde{O}(d^4\tau)$. The bitsize of the output is $O(d^4\tau)$.

The subresultant polynomials of P and Q can be computed in $O(d^2)$ arithmetic operations between univariate polynomials of degree $O(d^2)$ and of bitsize $O(d\tau)$, so with a bit complexity $\tilde{O}(d^5\tau)$. The bitsize of the output is $O(d^5\tau)$.

Proposition 16. *[Univariate gcd Computation][B][GG] Let $P, G \in \mathbb{Z}[X]$ be two polynomials of degree bounded by d and coefficients of bitsize bounded by τ. Computing their gcd has an expected bit complexity of $\tilde{O}(d(\tau + d))$ and a deterministic bit complexity of $\tilde{O}(d^2\tau)$.*

Proposition 17. *[Univariate Polynomial Evaluation][BZ] Let $f \in \mathbb{Z}[X]$ be a polynomial of degree d with coefficients of bitsize bounded by τ and r a rational number of bitsize $\lambda(r)$. The evaluation of f at r can be perform in $\tilde{O}(d(\tau + \lambda(r)))$ and the bitsize of the output $f(r)$ is $\tilde{O}(\tau + d\,\lambda(r))$.*

Proposition 18. *[Root Isolation and Root Refinement][MSW1] Let $f \in \mathbb{Z}[X]$ be a square-free polynomial of degree d with coefficients of bitsize bounded by τ.*

One can compute isolating intervals for the real roots of f using $\tilde{O}(d^2\tau + d^3)$ bit operations and the bitsize of the endpoints of the isolating intervals sums up to $\tilde{O}(d\,\tau)$. Moreover, we can compute isolating intervals of all the roots of f of width 2^{-L} using no more than $\tilde{O}(d^2\,\tau + d^3 + d\,L)$ bit operations.

3 Computation of the topology of $\mathcal{C}(P)$

3.1 Getting rid of vertical lines and vertical asymptotes

In order to avoid unneeded complications in the description of our algorithms, we ensure that the curve admits no vertical asymptotes and no horizontal or vertical lines. So, we give the complexity of shearing the curve so that this condition is fulfilled.

Lemma 19. *[BLPR] We compute $\mathcal{C}(\tilde{P})$, a shear of $\mathcal{C}(P)$ without vertical lines and without vertical asymptotes in $\tilde{O}(d^3\tau + d^4)$ bit operations. Moreover, $\tilde{P}$ is a polynomial of degree d and coefficients of bitsize $\tilde{O}(\tau + d)$.*

Proof. A straightforward way to get rid of the vertical lines and vertical asymptotes is to shear the curve so that the leading coefficient of P with respect to X and with respect to Y is a unit.

One method for doing that is first to compute the leading coefficient $\mathrm{Lc}_Y(Q)$ of the polynomial $Q(S,Y,X)=P(X-sY,Y)$. Noting that $\mathrm{Lc}_Y(Q)$ belongs to $\mathbb{Z}[S]$ and is of degree d, we need to find $s\in\mathbb{Z}$ such that $\mathrm{Lc}_Y(Q)(s)\neq 0$ and finally consider $\tilde{P}=Q(s,X,Y)\in\mathbb{Z}[X,Y]$, whose leading coefficient in Y belongs to $\mathbb{Z}$, instead of $P\in\mathbb{Z}[X,Y]$.

Finding s such that $\mathrm{Lc}_Y(Q)(s)\neq 0$ can be performed after trying $d+1$ values, for example $0,\ldots.,d$. Then it is needed to substitute s in Q. As there are $O(d^2)$ coefficients in Q which are polynomials of degree at most d in S with coefficients of bitsize $\tilde{O}(d+\tau)$, this operation then takes $\tilde{O}(d^3(\tau+d))$ bit operations and the final result is the polynomial $\tilde{P}$ which has coefficients of bitsize $\tilde{O}(\tau+d)$. □

Then a similar change can be performed to avoid also that the curve contains horizontal lines.

3.2 Cylindrical algebraic decomposition

Using the results of [MSW1] and [MSW2] we obtain the following

Proposition 20. *[MSW2] Let $P\in\mathbb{Z}[X,Y]$ be a square-free polynomial of total degree d and integer coefficients of bitsize bounded by τ. Supposing that, for every real root α of D, $\deg(\gcd(P(\alpha,Y)), \partial_Y P(\alpha,Y))$ is known, there is an algorithm with bit complexity $\tilde{O}(d^5\tau+d^6)$ to compute a set of special boxes*

$$\mathrm{SpeBox}=\{[a_i,b_i]\times[c_{i,j},d_{i,j}]|\, i\in[\![1,\delta]\!], j\in[\![1,\delta_{i,j}]\!]\}$$

isolating all the points of the special fibers. Moreover, we have Eq (4) and

$$\sum_{i=1}^{\delta}\sum_{j=1}^{\delta_{i,j}}\lambda(c_{i,j})=\sum_{i=1}^{\delta}\sum_{j=1}^{\delta}\lambda(d_{i,j})=O(d^3\,\tau)\,. \tag{3}$$

Proposition 20 is proved by combining the following results.

Proposition 21. *[MSW1]The computation of δ rational intervals isolating the real roots of D can be performed in $\tilde{O}(d^5\tau+d^6)$ bit operations. The endpoints a_i,b_i of the interval containing the real root α_i are rational numbers and their bitsize $\lambda(a_i),\lambda(b_i)$ satisfies:*

$$\sum_{i=1}^{\delta}\lambda(a_i)=\sum_{i=1}^{\delta}\lambda(b_i)=O(d^3\,\tau), \tag{4}$$

Proposition 22. *[Vertical Boundaries Computation][MSW2] The isolation of the real roots of the following equations:*

$$P(a_i,Y)=0, P(b_i,Y)=0.$$

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

We now give precisions on the method, slightly different from the one given in [MSW2] but altogether already known [D], that we use for determining the exact value of $\deg(\gcd(P(\alpha,Y)), \partial_Y P(\alpha,Y)))$ for a real root α of D. It uses a family of polynomials D_i that we define now.

Definition 23. *We denote by $\mathrm{Sr}_i(X,Y)$ the i^{th} subresultant polynomial of $P(X,Y)$ and $\partial_X P(X,Y)\,\partial_Y P(X,Y)$ and $\mathrm{sr}_{i,j}(X)$ the coefficient of Y^j in $\mathrm{Sr}_i(X,Y)$. Note that $\mathrm{sr}_{00}(X)=D(X)$ (see Eq (1)).We define inductively the following polynomials :*

$$\Phi_0(X)=\frac{\mathrm{sr}_{0,0}(X)}{\gcd(\mathrm{sr}_{0,0}(X),\mathrm{sr}'_{0,0}(X))};$$

$$\forall i\in\{1,\ldots,d-1\},\quad \Phi_i(X)=\gcd(\Phi_{i-1}(X),\mathrm{sr}_{i,i}(X)),\quad D_i(X)=\frac{\Phi_{i-1}(X)}{\Phi_i(X)}.$$

Proposition 24.

$$\deg(\gcd(P(\alpha,Y),\partial_Y P(\alpha,Y)))=i \Longleftrightarrow D_i(\alpha)=0.$$

The following result is a direct consequence of the algorithm described in [BLPR] (and related references), the expected complexity being obtained by replacing the worst case complexity for univariate gcd's by their expected variant (see [GG]).

Proposition 25. *The computation of the sequence $(D_i(X))_{i\in[\![1,d-1]\!]}$ has an expected bit complexity of $\tilde{O}(d^4\tau+d^5)$ and a deterministic bit complexity of $\tilde{O}(d^6\tau+d^7)$. The polynomials $D_i(X)$ have degree bounded by d^2 and coefficients of bitsize $O(d\tau+d^2)$.*

Proposition 26. *Given the polynomials $(D_i(X))_{i\in[\![1,d-1]\!]}$, computing for every root α of D (see Eq (1)),* $\deg(\gcd(P(\alpha,Y)),\partial_Y P(\alpha,Y)))$ *has bit complexity $\tilde{O}(d^5\tau+d^6)$.*

3.3 Checking generic position

We give now a generic position test, improves the one proposed by [GE1].

Proposition 27. *[DMR] The curve $\mathcal{C}(P)$ is in generic position if and only if $\forall k\in\{1,\ldots,d-1\}$, $\forall i\in\{0,\ldots,k-1\}$,*

$$k(k-i)\mathrm{sr}_{k,i}(X)\mathrm{sr}_{k.k}(X)-(i+1)\mathrm{sr}_{k,k-1}(X)\mathrm{sr}_{k,i+1}(X)=0 \bmod D_k(X).$$

This proposition gives immediately a test for checking generic position.

Proposition 28. *Suppose that the sequence $(D_i(X))_{i\in[\![1,d-1]\!]}$ had already been computed. Testing whether the curve is in general position using the preceding proposition has a bit complexity of $\tilde{O}(d^5\tau+d^6)$.*

Proof. We define $P_{k,i}=k\,(k-i)\,\mathrm{sr}_{k,i}(X)\,\mathrm{sr}_{k.k}(X)-(i+1)\,\mathrm{sr}_{k,k-1}(X)\,\mathrm{sr}_{k,i+1}(X)\in\mathbb{Z}[X]$ which has degree in $\tilde{O}(d^2)$ and coefficients of bitsize in $\tilde{O}(d\,\tau)$. The algorithm decides whether D_k divides $P_{k,i}$ using Proposition 13 with bit complexity $\tilde{O}(d^2(\tau d+d^2))$ for each couple (k,i). This leeds to the announced bit complexity. □

If the curve $\mathcal{C}(P)$ is in general position, we can compute its topology using the classical method of [GE1] (see also [BPR]), since there is only one single special point over a root of D. If the curve $\mathcal{C}(P)$ is in general position, we can compute its topology using the classical method of [GE1] (see also [BPR]), since there is only one single special point over a root of D. Otherwise, if the curve is not in generic position, we avoid the usual technique which is to enter in a loop calling the same algorithm after changing the direction of projection. We compute the local topology of $\mathcal{C}(P)$ inside its special boxes to reconstruct the topology of the curve $\mathcal{C}(P)$.

3.4 Computation of the local topology of $\mathcal{C}(P)$ inside its special boxes

At this point, we suppose that all the special boxes are known, i.e. non overlapping boxes that isolate the intersection of the curve with the special fibers, with the bit estimates coming from Proposition 20.

The computation of the local topology of $\mathcal{C}(P)$ inside its special boxes is done by an algorithm we describe in subsection 3.4.4 after we have performed the following 3 steps

- count the intersection points of $\mathcal{C}(P)$ with the horizontal boundaries of the special boxes,
- evaluate the signs of the slopes of the tangent line of $\mathcal{C}(P)$ at the intersection points of $\mathcal{C}(P)$ with the horizontal boundaries of the special boxes
- compare the abscissa of all the intersection points of $\mathcal{C}(P)$ with the horizontal boundaries of the critical boxes with the abscissa of the corresponding special point

3.4.1 Isolating horizontal boundary points

We recall that each special box in SpeBox $:= ([a_i, b_i] \times [c_{i,j}, d_{i,j}])_{i \in [\![1,\delta]\!], j \in [\![1,\delta_i]\!]}$ contains exactly one point of a special fiber of $\mathcal{C}(P)$. For each special box, we will need to isolate the intersection points of $\mathcal{C}(P)$ with the horizontal boundary of the box $[a_i, b_i] \times [c_{i,j}, d_{i,j}]$.

Proposition 29. *[Boundaries Computation]*

a) The isolation of the intersection points of $\mathcal{C}(P)$ with the horizontal boundaries of the boxes in SpeBox*, i.e. isolate the real roots of the following equations:*

$$P(X, c_{i,j}) = 0, P(X, d_{i,j}) = 0.$$

costs $\tilde{O}(d^6 \tau)$ bit operations.

b) If we denote by $\lambda(c_{i,j}), \lambda(d_{i,j})$ the bitsize of the rational numbers $c_{i,j}, d_{i,j}$, and $\zeta_{i,j}, \zeta_{i,j}'$ the number of roots of of $P(X, c_{i,j})$, $P(X, d_{i,j})$, and $[u_k^{c_{i,j}}, w_k^{c_{i,j}}]$, $\left[u_k^{d_{i,j}}, w_k^{d_{i,j}}\right]$ the isolating intervals of the real roots of $P(X, c_{i,j}), P(X, d_{i,j})$) that are computed, we have the following properties:

$$\sum_{k=0}^{\zeta_{i,j}} \lambda(u_k^{c_{i,j}}) = \sum_{k=0}^{\zeta_{i,j}} \lambda(w_k^{c_{i,j}}) = O(d\ (\tau + d\,\lambda(c_{i,j}))) \tag{5}$$

$$\sum_{k=0}^{\zeta_{i,j}'} \lambda\left(u_k^{d_{i,j}}\right) = \sum_{k=0}^{\zeta_{i,j}'} \lambda\left(w_k^{d_{i,j}}\right) = O(d\,(\tau + d\,\lambda(d_{i,j}))) \tag{6}$$

Proof. The polynomials $P(X, c_{i,j})$, $P(X, d_{i,j})$ are of degree d and of bitsize $\tilde{O}(\tau + d\lambda(c_{i,j}))$, $\tilde{O}(\tau + d\lambda(d_{i,j}))$. Using Proposition 18 the isolation costs $\tilde{O}(d^2(\tau + d\lambda(c_{i,j})) + d^3)$, $\tilde{O}(d^2(\tau + d\lambda(d_{i,j})) + d^3))$. Hence the total cost is :

$$\sum_{i=1}^{\delta} \left(\sum_{j=1}^{\delta_i} \tilde{O}(d^2(\tau + d\lambda(c_{i,j})) + d^3) + \sum_{j=1}^{\delta_i'} \tilde{O}(d^2(\tau + d\lambda(d_{i,j})) + d^3) \right)$$

By Proposition 20, we have:

$$\sum_{i=1}^{\delta} \sum_{j=1}^{\delta_i} \lambda(c_{i,j}) = \sum_{i=0}^{\delta} \sum_{j=1}^{\delta_i'} \lambda(d_{i,j}) = O(d^3 \tau).$$

and it appears that the total cost is $\tilde{O}(d^6 \tau)$ bit operations. Using Proposition 18, we obtain the endpoints summation properties. □

3.4.2 Computing sign of derivatives at horizontal boundary points

We also need to evaluate, at each intersection point of $\mathcal{C}(P)$ with the horizontal boundary of a box in SpeBox, the sign of $\partial_X P(X, Y) \partial_Y P(X, Y)$.

Proposition 30. *It costs $\tilde{O}(d^6 \tau)$ bit operations to evaluate the signs of the slopes of the tangent line of $\mathcal{C}(P)$ at the intersection points of $\mathcal{C}(P)$ with the horizontal boundaries of the boxes in* SpeBox*.*

Proof. Let $(x_k, c_{i,j}) \in \mathcal{C}(P)$ with $x_k \in [u_k^{c_{i,j}}, w_k^{c_{i;j}}]$, $k \in [\![1, \zeta_{i,j}]\!]$ the boundary points at the bottom sides of the boxes $[a_i, b_i] \times [c_{i,j}, d_{i,j}] \in$ SpeBox, $i \in [\![1, \delta]\!]$, $j \in [\![1, \delta_i]\!]$.

To evaluate the signs of the slopes of the tangent lines of $\mathcal{C}(P)$ at the regular points $(x_k, c_{i,j})$, it suffice to evaluate the signs of $\partial_X P(X, Y) \partial_Y P(X, Y)$ at these points. Since $\partial_X P(x_k, c_{i,j}) \partial_Y P(x_k, c_{i,j}) \neq 0$ (because $(x_k, c_{i,j})$ is a regular point of $\mathcal{C}(P)$), then the polynomial $P(X, c_{i,j}) \partial_X P(X, c_{i,j}) \partial_Y P(X, c_{i,j})$ is square-free and we can evaluate the sign of $\partial_X P(x_k, c_{i,j}) \partial_Y P(x_k, c_{i,j})$ as follows :

1. We computed the isolating intervals $([e_\ell, f_\ell])_{\ell \in [\![1, O(d)]\!]}$ of the roots of the polynomial $\partial_X P(X, c_{i,j}) \partial_Y P(X, c_{i,j})$ and evaluate the sign of $\partial_X P(X, c_{i,j}) \partial_Y P(X, c_{i,j})$ at the end points of the isolating intervals.

Since the degree of $\partial_X P(X,\ c_{i,j})\partial_Y P(X,\ c_{i,j})$ is $O(d)$ and its coefficients of bitsize $\tilde{O}((\tau + d\lambda(c_{i,j})))$, the cost of the isolation process is $\tilde{O}(d^2(\tau + d\lambda(c_{i,j})))$ and $\sum_{\ell=1}^{O(d)} \lambda(e_\ell) = \sum_{\ell=1}^{O(d)} \lambda(f_\ell) = \tilde{O}(d(\tau + d\lambda(c_{i,j})))$. This leeds, using Eq (3), to a total cost of $\tilde{O}(d^6\tau)$ for the isolation.

The evaluation of $\partial_X P(X, c_{i,j})\partial_Y P(X, c_{i,j})$ at e_ℓ, using Proposition 17, costs $\tilde{O}(d(\tau + d\lambda(c_{i,j}) + \lambda(e_\ell)))$. Hence

$$\sum_{i=1}^{\delta} \sum_{j=1}^{\delta'_i} \sum_{\ell=1}^{O(d)} \tilde{O}(d(\tau + d\lambda(c_{i,j}) + \lambda(e_\ell))) = \sum_{i=1}^{\delta} \sum_{j=1}^{\delta'_i} \tilde{O}(d^2(\tau + d\lambda(c_{i,j}))) = \tilde{O}(d^6\tau)$$

2. We refine the isolating intervals of the roots of $P(X, c_{i,j})$ up to the separation bound of the polynomial $P(X,\ c_{i,j})\partial_X P(X,\ c_{i,j})\partial_Y P(X,\ c_{i,j})$ which is equal to $\tilde{O}(d(\tau + d\lambda(c_{i,j})))$ since its degree is $O(d)$ and its coefficients of bitsize $\tilde{O}((\tau + d\lambda(c_{i,j})))$.

   The cost of the refinement process up to the separation bound $\tilde{O}(d(\tau + d\lambda(c_{i,j})))$ is $\tilde{O}(d^2(\tau + d\lambda(c_{i,j})))$. This leeds, using Eq (3), to a total cost of $\tilde{O}(d^6\tau)$ for the refinement.

3. We refine the isolating intervals of the roots of $\partial_X P(X, c_{i,j})\partial_Y P(X, c_{i,j})$ up to the separation bound of the polynomial $P(X,\ c_{i,j})\partial_X P(X,\ c_{i,j})\partial_Y P(X,\ c_{i,j})$ which is equal to $\tilde{O}(d(\tau + d\lambda(c_{i,j})))$ since its degree is $O(d)$ and its coefficients of bitsize $\tilde{O}((\tau + d\lambda(c_{i,j})))$.

   The cost of the refinement process up to the separation bound $\tilde{O}(d(\tau + d\lambda(c_{i,j})))$ is $\tilde{O}(d^2(\tau + d\lambda(c_{i,j})))$. This leeds, using Eq (3), to a total cost of $\tilde{O}(d^6\tau)$ for the refinement.

4. By ordering the concatenation of the two refined list of isolating intervals one can deduce the signs of $\partial_X P(x_k, c_{i,j})\partial_Y P(x_k, c_{i,j})$, $i \in [\![1, \delta]\!]$, $j \in [\![1, \delta'_i]\!]$, $k \in [\![1, \epsilon_{i,j}]\!]$.

A similar analysis holds for the signs of the slopes of the tangent line of the boundary points at the up sides of the boxes $[a_i, b_i] \times [c_{i,j}, d_{i,j}] \in \mathrm{SpeBox}$, $i \in [\![1, \delta]\!]$, $j \in [\![1, \delta_i]\!]$. □

3.4.3 Finding the relative position of the abscissa of horizontal boundary points and special point

Consider a special box $[a, b] \times [c, d]$ with special point (α, γ). In order to identify the topology of the curve inside $[a, b] \times [c, d]$, the method we are going to use requires to know how many roots of $P(X, c)$ are before and after α on the interval $[a, b]$. The algorithm used for isolating the points in the fibers computes also their multiplicities so that the regular points are well identified and thus there is not further work to be done in order to compute the topology local to their isolation boxes. We thus concentrate on the critical and singular points.

We start by proving Theorem 33, which is a quantitative result on the deviation of the curve from its tangent at a special point and plays a key role in the complexity analysis (Proposition 36). This result is of independent interest and could be used outside the present paper, for example to decrease the complexity of the algorithm from [CLPPRT]. Before stating Theorem 33, we introduce a definition.

Definition 31. *Denote by $\mathcal{C}(P)_k$, $0 \leqslant k \leqslant d$, the points (α, γ) of $\mathcal{C}(P)$ such that*

1. *there exists ℓ such that $\partial_Y^k \partial_X^\ell P(\alpha, \gamma) \neq 0$,*
2. *for every $k' < k$ $\partial_Y^{k'} \partial_X^\ell P(\alpha, \gamma) = 0$,*
3. *for every $\ell' < \ell$ for every k' $\partial_Y^{k'} \partial_X^{\ell}{}' P(\alpha, \gamma) = 0$.*

Example 32.

If (α, γ) is a regular point of $\mathcal{C}(P)$, $(\alpha, \gamma) \in \mathcal{C}(P)_1$.

If (α, γ) is a X-critical point of $\mathcal{C}(P)$, $(\alpha, \gamma) \in \mathcal{C}(P)_2$.

If $(\alpha, \gamma) \in \mathcal{C}(P)_k$, the order of contact of the vertical line through (α, γ) is k.

Theorem 33. *Let $(\alpha, \gamma) \in \mathcal{C}(P)_k$. There exists real numbers $A(\alpha, \gamma)$ and $B(\alpha, \gamma)$, such that for every y, $0 < y < B(\alpha, \gamma)$, and every x, $P(\alpha + x, \gamma + y) = 0$,*

$$|x| > |y|^k\, |A(\alpha, \gamma)|.$$

Moreover

$$-\sum_{(\alpha,\gamma)\in\mathrm{Crit}(\mathcal{C}(P))}\log(|A(\alpha,\gamma)|)=-\sum_{(\alpha,\gamma)\in\mathrm{Crit}(\mathcal{C}(P))}\log(|B(\alpha,\gamma)|)=O(d^3\tau).$$

The proof of Theorem 33 relies on the following two propositions giving an upper bound and lover bound on the value of specific algebraic numbers.

Proposition 34. *Let P, Q, be bivariate polynomials, monic with respect to Y, of degree in each variable dominated by d, and coefficients of bitsizes less than τ. Suppose moreover that the common roots of P and Q in $\mathbb{C}$ are finite.*

Let

$$Z \;=\; \{(\alpha,\gamma)\in\mathbb{R}^2|\,P(\alpha,\gamma)=Q(\alpha,\gamma)=0\}$$

Consider a mapping H from Z to the set of polynomials of degree in each variable dominated by d, and coefficients of bitsizes less than τ, associating to (α,γ) a polynomial $H_{(\alpha,\gamma)}$. Then

$$\sum_{(\alpha,\gamma)\in Z}\log\left(\left|H_{(\alpha,\gamma)}(\alpha,\gamma)\right|\right)\;\leqslant\;\tilde{O}(d^2\tau).$$

Proof. The claim follows from Proposition 10, Proposition 11 and Proposition 5 since α (resp. γ) is the root of $\mathrm{Res}_Y(P,Q)$ (resp. $\mathrm{Res}_X(P,Q)$) which is a polynomial of degree d^2 with coefficients of bitsize $O(d\tau)$. □

Proposition 35. *Let P, Q, H_1, ..., H_k be bivariate polynomials of degree bounded by d and coefficients of bitsize bounded by τ, monic with respect to Y, of degree in each variable dominated by d, and coefficients of bitsizes less than τ. Suppose moreover that the common roots of P and Q in $\mathbb{C}$ are finite.*

Let

$$\begin{aligned}Z &= \{(\alpha,\gamma)\in\mathbb{R}^2|\,P(\alpha,\gamma)=Q(\alpha,\gamma)=0\}\\ Z_i &= \{(\alpha,\gamma)\in Z|\,H_1(\alpha,\gamma)=\ldots=H_{i-1}(\alpha,\gamma)=0,H_i(\alpha,\gamma)\neq 0\}\end{aligned}$$

Then

$$-\sum_{i=1}^{k}\sum_{(\alpha,\gamma)\in Z_i}\log(|H_i(\alpha,\gamma)|)\;\leqslant\;\tilde{O}(d^3\tau)$$

Proof.

We are going to prove that $\displaystyle\prod_{i=1}^{k}\prod_{(\alpha,\gamma)\in Z}H(\alpha,\gamma)\geqslant\frac{1}{E}$ with $E\in\mathbb{Z}$ and E of bitsize $O(d^3\tau)$.

Making if necessary a linear change of variable of the form $T=X-s\,Y,Y=Y$, with s an integer of bitsize $\tilde{O}(1)$, we can suppose that X separates the elements of Z.

Consider $S_i(X)=\mathrm{Res}_Y(Q,H_i)$ and denote by τ_i a bound on the bitsize of its coefficients. Note that τ_i is in $O(d\tau)$ There exist polynomials $U_i(X,Y)$ et $V_i(X,Y)$ of degree at most d with respect to Y and at most d^2 with respect to X and coefficients of bitsize $O(d\tau)$ such that

$$S_i(X)=U_i(X,Y)\,Q(X,Y)+V_i(X,Y)\,H_i(X,Y)$$

Let $(\alpha,\gamma)\in Z_i$. Since $H_i(\alpha,\gamma)\neq 0$ and P and Q are monic in Y then $S_i(\alpha)\neq 0$ and moreover $S_i(\alpha)=V_i(\alpha,\gamma)\,H_i(\alpha,\gamma)$, so that $V_i(\alpha,\gamma)\neq 0$.

We are going to prove that.

$$\prod_{i=1}^{k}\prod_{(\alpha,\beta)\in Z_i}H_i(\alpha,\gamma)=\prod_{i=1}^{k}\frac{\displaystyle\prod_{(\alpha,\gamma)\in Z_i}S_i(\alpha)}{\displaystyle\prod_{(\alpha,\gamma)\in Z_i}V_i(\alpha,\gamma)}$$

is bigger than the inverse of a natural number of bitsize $O(d^3\tau)$.

We decompose $R = \mathrm{Res}_Y(P, Q)$ as $R = R_0 \prod_{i=1}^{k} R_i$, where the zeroes of R_i contain the X-projections of Z_i and denote by d_i the degree of R_i.

Then, since

$$|\mathrm{Res}_X(R_i, S_i)| = \mathrm{lc}_X(R_i)^{\deg(S_i)} \mathrm{lc}_X(S_i)^{d_i} \prod_{(\alpha, \gamma) \in Z_i} |S_i(\alpha)| \prod_{\alpha \in \mathrm{Zer}_{\mathbb{C} \setminus \mathbb{R}}(R_i)} |S_i(\alpha)|$$

is a non zero integer, and, for every $\alpha \in \mathrm{Zer}_{\mathbb{C} \setminus \mathbb{R}}(R_i)$,

$$|S_i(\alpha)| \leqslant (\deg_X (S_i) + 1)\, 2^{\tau_i} \max(1, |\alpha|)^{\deg_X(S_i)},$$

we have

$$\prod_{\alpha \in \mathrm{Zer}_{\mathbb{C} \setminus \mathbb{R}}(R_i)} |S_i(\alpha)| \leqslant (d^2 + 1)^{d_i}\, 2^{\tau_i d_i}\, 2^{\Gamma(R_i) d^2}$$

and

$$\begin{aligned}\prod_{\alpha \in Z_i} |S_i(\alpha)| &\geqslant \frac{1}{\mathrm{lc}_X(R_i)^{\deg(S_i)} \mathrm{lc}_X(S_i)^{d_i} \prod_{\alpha \in \mathrm{Zer}_{\mathbb{C} \setminus \mathbb{R}}(R_i)} |S_i(\alpha)|}\\ &\geqslant \frac{1}{\mathrm{lc}_X(R_{_i})^{d^2} L^{d_i} (d^2 + 1)^{d_i}\, 2^{\tau_i d_i}\, 2^{\Gamma(R_i) d^2}}\end{aligned}$$

where $L = \max_i (|\mathrm{Lc}_X(S_i)|)$.

So that , since $\sum_{i=0}^{k} d_i = d^2$, $\sum_{i=0}^{k} \Gamma(R_i) = \Gamma(R) = O(d\tau)$, $\tau_i = O(d\tau)$,

$$\prod_{i=1}^{k} \prod_{\alpha \in Z_i} |S_i(\alpha)| \;\geqslant\; 2^{-\lambda}$$

with $\lambda = O(d^3\tau)$.

To estimate the products of the $V_i(\alpha,\ \beta)$, we apply Proposition 5, denoting $C_i = (\deg_X\ (V_i) + 1)\ (\deg_Y\ (V_i) + 1)\ 2^{\tau_i'} \in \mathbb{Z}$ where τ_i' is a bound on the bitsize of the coefficients of the V_i of bitsize $\tilde{O}(d\tau)$, so that

$$\prod_{(\alpha, \gamma) \in Z_i} |V_i(\alpha, \gamma)| \leqslant C_i^{d^2} \left(\prod_{\alpha \in \mathrm{Zer}(R_i)} \max(1, |\alpha|) \right)^{\deg_X(V_i)} \left(\prod_{(\alpha, \gamma) \in Z} \max(1, |\gamma|) \right)^{\deg_Y(V_i)}.$$

Defining $C = \max_i (C_i)$ we obtain, since the $\mathrm{Zer}(R_i)$ are disjoint,

$$\prod_{i=1}^{k} \prod_{(\alpha, \gamma) \in Z_i} |V_i(\alpha, \gamma)| \leqslant C^{d^2} \left(\prod_{\alpha \in \mathrm{Zer}(R)} \max(1, |\alpha|) \right)^{d^2} \left(\prod_{(\alpha, \gamma) \in Z} \max(1, |\gamma|) \right)^{d}.$$

Remembering that $\prod_{\alpha \in \mathrm{Zer}(R)} \max(1, |\alpha|)$ is bounded by a natural number of bitsize $\tilde{O}(d\tau)$ and that $\prod_{(\alpha, \gamma) \in Z} \max(1, |\gamma|)$ is bounded by a natural number of bitsize $O(d^2\tau)$, and given the degrees of V_i in X, Y, we get that $\prod_{i=1}^{k} \prod_{(\alpha, \gamma) \in Z_i} |V_i(\alpha, \gamma)|$ is bounded by a natural number of bitsize $\tilde{O}(d^3\tau)$.

Finally,

$$\prod_{i=1}^{k} \prod_{(\alpha, \gamma) \in Z_i} H_i(\alpha, \gamma) = \prod_{i=1}^{k} \frac{\prod_{(\alpha, \gamma) \in Z_i} S_i(\alpha)}{\prod_{(\alpha, \gamma) \in Z_i} V_i(\alpha, \gamma)}$$

is bigger that the quotients of two natural numbers of bitsize $O(d^3\tau)$ and in particular bigger that the inverse of a natural number of bitsize $\tilde{O}(d^3\tau)$. □

Proof. of Theorem 33

By Taylor formula, for $(\alpha,\gamma)\in\mathcal{C}(P)_k$, there exists ℓ such that

$$P(\alpha+X,\gamma+Y)=\sum_{j=\ell}^{d} j!\,C_j(\gamma+Y)X^{j},$$

with

$$C_\ell(\gamma+Y)=Y^k\left(\sum_{i=k}^{d} i!\partial_Y^i\partial_X^\ell P(\alpha,\gamma)\,Y^{i-k}\right).$$

and, for $j>\ell$,

$$C_j(\gamma+Y)=\sum_{i=0}^{d} i!\,\partial_Y^i\partial_X^j P(\alpha,\gamma)\,Y^{i}$$

By Cauchy bound, for every y such that $C_\ell(\gamma+y)\neq 0$, the smallest positive root of $P(\alpha+X,\gamma+y)$ is at least

$$|C_\ell(\gamma+y)|\left(\sum_{j=\ell}^{d}|C_j(\gamma+y)|\right)^{-1}.$$

For every y, $0<y<1$,

$$\sum_{j=\ell}^{d}|C_j(\gamma+y)|\leqslant\sum_{j=\ell}^{d}\sum_{i=0}^{d} i!\left|\partial_Y^i\partial_X^j P(\alpha,\gamma)\right|.$$

Let $B(\alpha,\gamma)$ be smaller that the smallest positive root of the univariate polynomial

$$\sum_{i=k}^{d} i!\,\partial_Y^i\partial_X^\ell P(\alpha,\gamma)\,Y^{i-k}\ -\ \frac{1}{2}k!\partial_Y^k\partial_X^\ell P(\alpha,\gamma),$$

for example

$$B(\alpha,\gamma)\ =\ |\partial_Y^k\partial_X^\ell P(\alpha,\gamma)|\left(|\partial_Y^k\partial_X^\ell P(\alpha,\gamma)|+2\sum_{i=k+1}^{d}\frac{i!}{k!}|\partial_Y^i\partial_X^\ell P(\alpha,\gamma)|\right)^{-1}.$$

For every y, $0<y<B(\alpha,\gamma)$,

$$|C_\ell(\gamma+y)|>|y|^k\left|\frac{1}{2}k!\partial_Y^k\partial_X^\ell P(\alpha,\gamma)\right|$$

We finally define

$$A(\alpha,\gamma)=\left|\frac{1}{2}k!\partial_Y^k\partial_X^\ell P(\alpha,\gamma)\right|\left(\sum_{i=\ell}^{d}\sum_{j=0}^{d} i!\left|\partial_Y^i\partial_X^j P(\alpha,\gamma)\right|\right)^{-1}.$$

Once can then combine Proposition 34 and Proposition 35 to get the final results. □

Let $a(\alpha,\ \gamma)\ =\ \inf\ (\log\ (|A(\alpha,\ \gamma)|),\ \log\ (|a|),\ \log\ (|b|)),\ b(\alpha,\ \gamma)\ =\ \log\ (|B(\alpha,\ \gamma)|)$. If $(\alpha,\gamma)\in\mathcal{C}(P)_1$, according to Proposition 33 the distance between α and any root of $P(X,c)$ is at least $2^{a(\alpha,\gamma)+b(\alpha,\gamma)}$.

The algorithm used for isolating the points in the fibers computes also their multiplicities so that the regular points are well identified and thus there is not further work to be done in order to compute the topology local to their isolation boxes..

Proposition 36. *It costs $\tilde{O}(d^6\tau)$ bit operations to compare the abscissa of all the boundary points of the critical boxes with the abscissa of the corresponding special point.*

Proof. If $(\alpha,\gamma)\in\mathcal{C}(P)_k$, $k>1$, according to Proposition 33 the distance between α and any root of $P(X,c)$ is at least $2^{ka(\alpha,\gamma)+b(\alpha,\gamma)}$. To be able to sort the roots of $P(X,c)$ and the roots of D, we need to refine their isolating intervals up to a width of $2^{k\,a(\alpha,\gamma)+b(\alpha,\gamma)}$. Such refinement costs $O(d\,(k\,a(\alpha,\gamma)+b(\alpha,\gamma)))$ for the roots of $P(X,c)$ and $O(d^2\,(k\,a(\alpha,\gamma)+b(\alpha,\gamma)))$ for the roots of D up to $2^{ka(\alpha,\gamma)+b(\alpha,\gamma)}$. The total cost is again $O(d^6\,\tau)$ for all the special boxes by Theorem 33. □

3.4.4 Topology inside a special box

We prove now that given the information already computed i.e.

- the number of the intersection points of $\mathcal{C}(P)$ with the horizontal boundaries of a special box
- the signs of the slopes of the tangent line of $\mathcal{C}(P)$ at the intersection points of $\mathcal{C}(P)$ with the horizontal boundaries of a special box
- the abscissa of all the intersection points of $\mathcal{C}(P)$ with the horizontal boundary of the special box with the abscissa of the corresponding special point

we are able to compute the topology of the curve inside a special box.

We introduce some definitions.

Definition 37. *[Arc] An arc of $\mathcal{C}(P)$ is a subset of $\mathcal{C}(P)$ homeomorphic to* $[0, 1]$.

Definition 38. *[Monotonic arcs] An arc of $\mathcal{C}(P)$ is monotonic if the polynomial $\partial_X P(X, Y)\, \partial_Y P(X, Y)$ does not vanish at any point of the arc.*

Proof. Inside a special box there is at most one critical point of $\mathcal{C}(P)$. Hence in a special box, the polynomial $\partial_X P(X, Y)\, \partial_Y P(X, Y)$ vanishes only at the critical point (α, γ). So, except the arcs passing through the critical point (α, γ) of the box, all the other arcs of the box are monotonic. □

Proposition 39. *An arc of $\mathcal{C}(P)$ contained in a special box $[a, b] \times [c, d]$ that does not pass through a critical point (α, γ) is monotonic.*

Consider a special box $[a, b] \times [c, d]$ and (α, γ) its special point. We denote respectively by L_a L_b, L_c, L_d the intersection points of $\mathcal{C}(P)$ with the left, right, down and up sides of the box $[a, b] \times [c, d]$. The points inside L_a, L_b (resp. L_c, L_d) are ordered by increasing value of y (resp. x).

We split L_c into $L_{c<\alpha}$ and $L_{c>\alpha}$ where $L_{c<\alpha}$ and $L_{c>\alpha}$ are the points of L_c at the left side and the right side of the critical fiber $\mathrm{Fib}(\alpha)$. Similarly, we split L_d into $L_{d<\alpha}$ and $L_{d>\alpha}$ where $L_{d<\alpha}$ and $L_{d>\alpha}$ are respectively the points of L_d at the left side and the right side of the critical fiber $\mathrm{Fib}(\alpha)$.

Given a boundary point (x, y) of $[a, b] \times [c, d]$, there is one and only one arc of $\mathcal{C}(P)$, contained in $[a, b] \times [c, d]$ starting from (x, y), called a special arc, with exactly one of the following properties

- type 1 : the arc is monotonic and ends at another boundary point, called the matching point of (x, y)
- type 2 : the arc ends at (α, γ)

Note that two special arcs of type 1 having distinct intersection with the boundary of a special box do not meet, and that two special arcs of type 2 having distinct intersection with the boundary of a special box meet only at (α, γ).

Given two boundary points (x, y) and (x', y') of $[a, b] \times [c, d]$, there is at most one special arc of type 1 linking them denoted, when it exists, by $\wideparen{(x, y), (x', y')}$.

Given a boundary point (x, y) of $[a, b] \times [c, d]$, there is at most one special arc of type 2 linking (x, y) to $\alpha, \gamma)$, denoted, when it exists, by $\wideparen{(x, y), (\alpha, \gamma)}$.

Given a list $L = [x_1, \ldots, x_n]$, we denote by

$$L[i] = x_i, L - L[1] = [x_2, \ldots, x_m], L^{-1} := [x_n, \ldots, x_1].$$

Given two lists $L = [x_1, \ldots, x_n]$ and $M = [y_1, \ldots, y_m]$ we denote their concatenation by

$$L + M := [x_1, \ldots, x_n, y_1, \ldots, y_m].$$

We denote by $\mathsf{SlopeSign}$ the function, built from the proof of the Proposition 30, which computes the sign of the slope of the tangent line at the intersection points of $\mathcal{C}(P)$ with the horizontal boundaries of the boxes in SpeBox.

Proposition 40.

1. *The points inside $L_{d<\alpha}$ have the same slope sign. If this slope sign is $+$, the special arcs passing through these points are of type 1. The matching point of $L_{d<\alpha}[i]$ is $L[i]$, where $L=L_a^{-1}+L_{c<\alpha}$. If this slope sign is $-$, the special arcs passing through these points end is of type 2.*

2. *The points inside $L_{c<\alpha}$ have the same slope sign. If this slope sign is $-$, the special arcs passing through these points are of type 1. The matching point of $L_{c<\alpha}[i]$ is $L[i]$, where $L=L_a+L_{d<\alpha}$. If this slope sign is $+$, the special arcs passing through these points end are of type 2.*

3. *The points inside $L_{d>\alpha}$ have the same slope sign. If this slope sign is $-$, the special passing throw these points are of type 1. The matching point of $L_{d>\alpha}[i]$ is $L[i]$, where $L=L_b^{-1}+L_{c>\alpha}$. If this slope sign is $+$, the special arcs passing through these points end are of type 2.*

4. *The points inside $L_{c>\alpha}$ have the same slope sign. If this slope sign is $+$, the special arcs passing throw these points are of type 1. The matching point of $L_{c>\alpha}[i]$ is $L[i]$, where $L=L_b+L_{c>\alpha}$. If this slope sign is $-$, the special arcs passing through these points end are of type 2.*

Proof. Let (x_1,d) and (x_2,d) be two consecutive points of $L_{d<\alpha}$ with different slope signs. One of these four possibilities necessarily hold:

i. (x_1,d) and (x_2,d) belong to the same connected component of $\mathcal{C}(P)$ and there is a special point with abscissa in (x_1,x_2)

ii. (x_1,d) and (x_2,d) do not belong to the same connected component of $\mathcal{C}(P)$

   a) if the connected component C_1 of $\mathcal{C}(P)$ containing (x_1,d) has a point above x_2 and the connected component C_2 of $\mathcal{C}(P)$ containing (x_2,d) has a point above x_1, then C_1 and C_2 have an intersection point with abscissa in (x_1,x_2)

   b) the connected component of $\mathcal{C}(P)$ containing $(x_1,\ d)$ has a local maximum for x between x_1 and x_2,

   c) the connected component of $\mathcal{C}(P)$ containing $(x_1,\ d)$ has a local maximum for x between x_1 and x_2,

In all these four cases, there is a special point with abscissa in $(x_1,\ x_2)$. This is a contradiction since $(x_1,x_2)\subset(a,\alpha)$ contains no root of D.

Finally (x_1,d) and (x_2,d), two consecutive points of $L_{d<\alpha}$ have same slope signs.

If the slope sign of the elements of $L_{d<\alpha}$ is $+$ at (x,d), the special arc through (x,d) stays at the left of the line $x=x_1$, since the curve has no local minimum at the left of x_1 inside the box, so does not contain (α,γ). So it is a special arc of type 1. The matching point of $L_{d<\alpha}[i]$ is a point of the boundary to the left of α and does not belong to $L_{d<\alpha}$, so it is a point of L. Consider the first point of $L_{d<\alpha}[i]$ which is matched to a point $L[j]$ of L with $j>i$. Then $L[i]$ cannot be matched with a point of $L_{d<\alpha}$ since otherwise the special arcs through $L[i]$ and $L[j]$ would have an intersection in the special box. The special path through $L[i]$ cannot be of type 2 since the special arcs through $L[i]$ and $L[j]$ would have an intersection in the special box. So we obtained a contradiction.

If the slope sign is $-$ at (x,d), the special arc through (x,d) stays at the right of the line $x=x_1$, since the curve has no local maximum at the left of x_1 inside the box, so has to contain (α,γ). So it is a special arc of type 2.

We omit the proofs of 2), 3) and 4) which are entirely similar. □

The topology of $\mathcal{C}(P)$ inside the special box $[a,b]\times[c,d]$ depends only on the combinatorial information given by the number of elements of L_a L_b, $L_{c<\alpha}$, $L_{c>\alpha}$,, $L_{d<\alpha}$, $L_{d>\alpha}$ and the SlopeSign function on $L_{c<\alpha}$, $L_{c>\alpha}$, $L_{d<\alpha}$, $L_{d>\alpha}$.

So we can suppose without loss of generality that $[a,b]\times[c,d]=[-1,1]\times[-1,1]$, $(\alpha,\gamma)=(0,0)$ and the points of L_a L_b, $L_{c<\alpha}$, $L_{c>\alpha}$,, $L_{d<\alpha}$, $L_{d>\alpha}$ share the corresponding segments in equal parts. This is necessary to obtain a complexity bound on this part of our algorithm which is independent on τ and does not take into account the bitsize of the rational points defining the isolation intervals

We denote by MN the segment between M and N and by O the point (α,γ).

Algorithm 1

```
Initialize Arcs to the empty list
1. Connection of the points at the left side of the fiber Fib($\alpha$)
Input: $L_a$, $L_{c<\alpha}$, $L_{d<\alpha}$.
Output: a finite list of segments homeomorphic to the topology of $\mathcal{C}(P)$ inside $[a,\alpha]\times[c,d]$
if $\#L_{d<\alpha} > \#L_a$ then $L = L_a^{-1} + L_{c<\alpha}$, else $L := L_a^{-1}$ ;
if SlopeSign$(L_{d<\alpha}[1]) > 0$ then
    • Connection from the corner $(a,d)$
      for $i$ from 1 to $\#L_{d<\alpha}$ add $L[1]\,L_{d<\alpha}[i]$ to Arcs, $L = L - L[1]$;
else $L = L_a + L_{d<\alpha}$
If SlopeSign$(L_{c<\alpha}[1]) < 0$ then
    • Connection from the corner $(a,c)$
      for $i$ from 1 to $\#L_{c<\alpha}$ add $L[1]\,L_{c<\alpha}[i]$ to Arcs, $L = L - L[1]$;
else $L = L + L_{c<\alpha}$
Connection of the remaining points to $(\alpha,\gamma)$
For $i$ from 1 to $\#L$, add $L[i]\,O$ to Arcs;
2. Connection of the points at right side of the fiber Fib($\alpha$).
Input: $L_b$, $L_{c>\alpha}$, $L_{d>\alpha}$.
Output: the topology of $\mathcal{C}(P)$ inside $[\alpha,b]\times[c,d]$
 The process is entirely symmetrical so we do not include it.
```

The correctness of Algorithm 1 follows from Proposition 40.

Example 41. The example illustrates the various situations that can happen: the left hand part of the box has arcs of type 1 from corners (d,a) and (c,a) while the right hand par of the box has arcs of type 1 from corner (d,b) and an arc of type 1 from a point of $L_{d>\alpha}$ to a point of $L_{c>\alpha}$.

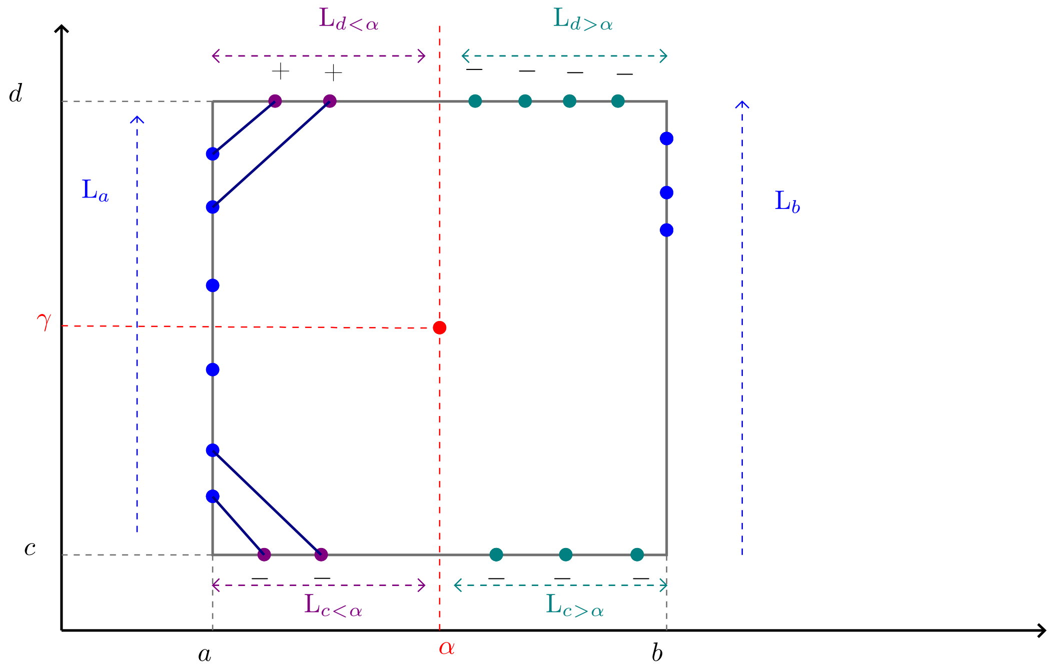

Figure 1. Connection from the corners (a,d) then (a,c).

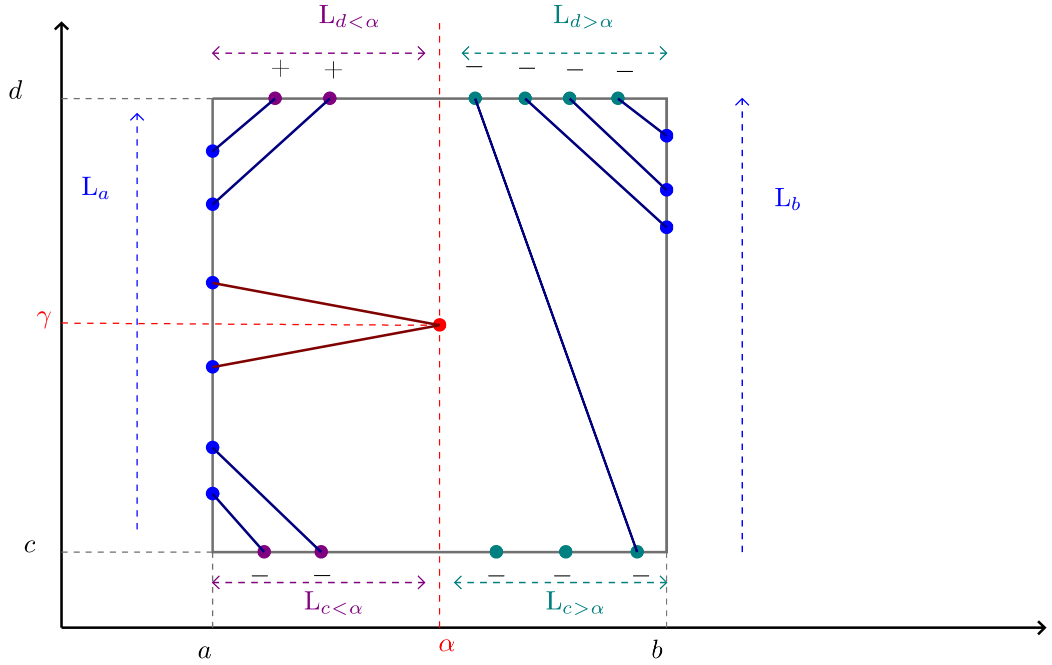

Figure 2. Connection of the remaining points to (α, γ) and Connection from the corner (b, d) (in the example no point are connected from (b, c)).

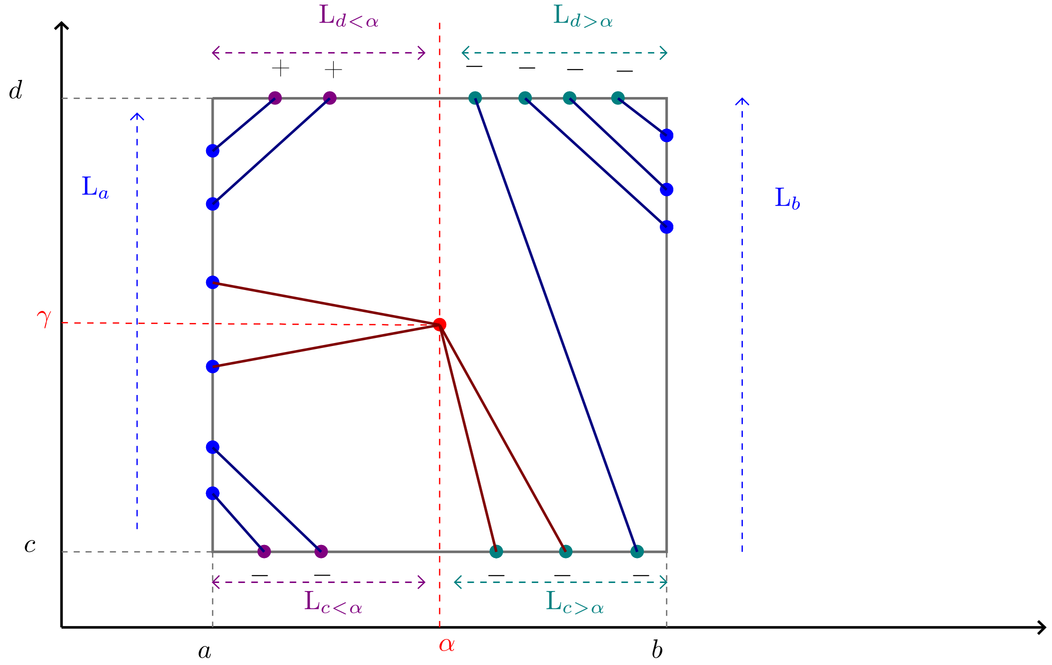

Figure 3. Connection of the remaining points to (α, γ)

The cost of Algorithm 1 is linear in the number of the points on the boundary of the box. The total number of such boundary points is bounded by $O(d^4)$.

4 Summary

Let us summarize the result we have obtained.

Theorem 42. *Let $P \in \mathbb{Z}[X, Y]$ a square free polynomial of total degree d and integer coefficients of bitsize bounded by τ, the algorithm we described computes the topology of $\mathcal{C}(P)$ i.e a straight-line planar graph isotopic to $\mathcal{C}(P)$ with bit complexity $\tilde{O}(d^6\tau + d^7)$. The size of the output is $O(d^4)$.*

Bibliography

[BZ] M. Badrato and A. Zanoni. Long integers and polynomial evaluation with Estrin's scheme. In Proc. SYNACS'11, 39-46, 2011.

[BPR] S. Basu, R. Pollack, and M.-F. Roy. Algorithms in Real Algebraic Geometry, volume 10 of Algorithms and Computation in Mathematics. Springer, 2nd edition, 2006.

[BLPR] Yacine Bouzidi, Sylvain Lazard, Marc Pouget, Fabrice Rouillier : Separating Linear Forms for Bivariate Systems, Proceedings of the 38th International Symposium on International Symposium on Symbolic and Algebraic Computation, ISSAC 2013, ACM, 117–124,2013.

[B] W. S. Brown. On Euclid's Algorithm and the Computation of Polynomial Greatest Common Divisors. J. ACM 18 (1971), pp. 476-504

[CLPPRT] Cheng, J. and Lazard, S. and Penaranda, L. and Pouget, M. and Rouillier, F. and Tsigaridas, E., On the topology of planar algebraic curves, Mathematics in Computer Science, 14(1), pp. 113-137, 2011

[DMR] Daouda Niang Diatta, Bernard Mourrain, Olivier Ruatta. On The Computation of the Topology of a Non-Reduced Implicit Space Curve. International Symposium on Symbolic and Algebraic Computation (ISSAC), 2008.

[GG] J. von zur Gathen and J. Gerhard. Modern computer algebra. Cambridge University Press, Cambridge, 1999.

[GE1] L. Gonzalez-Vega and M. El Kahoui. An improved upper complexity bound for the topology computation of a real algebraic plane curve. Journal of Complexity, 12:527–544, 1996.

[GI] L. Gonzalez-Vega and I. Necula. Efficient topology determination of implicitly defined algebraic plane curves. Computer Aided Geometric Design, 19:719–743, 2002.

[EKW] A. Eigenwillig, M. Kerber, and N. Wolpert. Fast and exact geometric analysis of real algebraic plane curves. In C. W. Brown, editor, Proocedingsa of the 2007 International Symposium on Symbolic and Algebraic Computation (ISSAC 2007), pages 151–158, 2007.

[KS] M. Kerber and M. Sagraloff. A Worst-case Bound for Topology Computation of Algebraic Curves. J. Symb. Comput., 47(3):239–258, 2012.

[MSW1] Kurt Mehlhorn, Michael Sagraloff, and Pengming. Wang. From Approximate Factorization to Root Isolation. In *Proceedings of the 38th international symposium on International symposium on symbolic and algebraic computation*, ISSAC '13. New York, NY, USA, 2013. ACM.

[MSW2] Kurt Mehlhorn, Michael Sagraloff, Pengming Wang: From Approximate Factorization to Root Isolation with Application to Cylindrical Algebraic Decomposition. Preprint (2013)