HAL
open science

On the computation of the topology of plane curves

Daouda Niang Diatta, Fabrice Rouillier, Marie-Françoise Roy

To cite this version:

Daouda Niang Diatta, Fabrice Rouillier, Marie-Françoise Roy. On the computation of the topology of plane curves. International Symposium on Symbolic and Algebraic Computation, Kobe University, Jul 2014, Kobe, Japan. pp.130-137, 10.1145/2608628.2608670 . hal-00935728v2

HAL Id: hal-00935728

https://hal.science/hal-00935728v2

Submitted on 20 May 2014

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.

On the Computation of the Topology of Plane Curves

Daouda Niang Diatta
Université Assane Seck de Ziguinchor
Senegal

Fabrice Rouillier INRIA
Paris Rocquencourt,
IMJ-Université Paris VI
France

Marie-Françoise Roy
IRMAR, Université 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. Our main result is an algorithm for the computation of the local topology in a neighbourhood of each of the singular points and critical points of the projection wrt the X-axis in $\tilde{O}(d^6\tau + d^7)$ bit operations where $\tilde{O}$ means that we ignore logarithmic factors in d and τ. Compared 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 $\mathcal{C}(P)$ *i.e* a straight-line planar graph isotopic to $\mathcal{C}(P)$ 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 $\mathcal{C}(P)$.

This is a classical problem in algorithmic real algebraic geometry with many applications in Computer Aided Geometric Design. It is extensively studied in the context of symbolic or semi-numerical computation (see for example [1, 2, 3, 6, 9, 10, 11, 14, 15, 16, 17, 18, 20, 25] for recent references). Many 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. The special values are the projection of the X-critical and singular points onto the X-axis, and the *special fibers* are the points of the curve above these special values. Taking additional points between two special values defines some *regular fibers*.

Computing a straight-line planar graph isotopic to $\mathcal{C}(P)$ then essentially amounts to connect the points of a regular fiber to the points of its neighbour special fibers. This operation requires :

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

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. The method used for computing the number of half branches of the curve going to an X-critical or singular point plays a key role in the algorithm. A usual strategy (see [5, 11, 14, 15, 16, 20]), consists in putting the curve in a so-called *generic position*, so that each special fiber contains at most one X-critical or singular point, and identifying this point among the points of the special fiber. An efficient variant of this strategy can be found in [20] with an expected complexity of $\tilde{O}(d^5\tau + d^6)$ bit operations, the probabilistic behavior being due to some gcd computations and to the choice of a direction that separates the X-critical and singular points, which is done at random.

Our results.

We combine new results on the computation of the local topology of the curve in an isolating box of each of its critical points (in a sense to be made precise later in the paper) with efficient sub-algorithms used for computing Cylindrical Algebraic Decompositions from [20].

We essentially obtain two new results:

- The first one (Theorem 1) is a lower bound to measure the deviation of the curve from the vertical axis at a critical point. This bound plays a key role in the complexity analysis of the computation of the local topology of $\mathcal{C}(P)$ inside critical 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 [10].
- The second one is an algorithm for reconstructing the local topology of the curve inside each critical box by connecting its boundary points (see subsection 3.3.4). We build such an algorithm by examining closely the relative position of the boundary points of the critical box with the critical 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 critical box.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
Copyright 20XX ACM X-XXXXX-XX-X/XX/XX ...$15.00.

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.

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.

Our detailed analysis of how far the curve deviates from the vertical axis at an X-critical or singular point is given in Subsection 3.3.3, since it plays a key role in the complexity analysis of the computation of one of the steps of the determination of the local topology of $\mathcal{C}(P)$ inside its critical boxes.

2. BASIC DEFINITIONS AND RESULTS

2.1 Definitions

Let $P \in \mathbb{Z}[X,Y]$ be a square-free polynomial and

$$\mathcal{C}(P) = \{(x,y) \in \mathbb{R}^2 \mid P(x,y) = 0\}$$

be the real algebraic curve defined by P. We also define

$$\mathcal{C}_{\mathbb{C}}(P) = \{(x,y) \in \mathbb{C}^2 \mid P(x,y) = 0\},$$

and

$$D(X) = \mathrm{Res}_Y(P, \partial_Y P)(X), \tag{1}$$

$$S(X) = \mathrm{Res}_Y(P, \partial_X P)(X), \tag{2}$$

and denote by

$$\alpha_1 < \ldots < \alpha_\delta$$

the real roots of D.

A point $(\alpha,\gamma) \in \mathcal{C}(P)$ is called:

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

A point $(\alpha,\gamma) \in \mathcal{C}(P)$ (resp. $\mathcal{C}_{\mathbb{C}}(P)$) is a **critical point** if it is an X-critical or a singular point. We denote by $\mathrm{Crit}(\mathcal{C}(P))$ the set of critical points of $\mathcal{C}(P)$. Note that the X-coordinate of a critical point is a zero of D, and the X-coordinate of a Y-critical point is a zero of S.

Let $\alpha \in \mathbb{R}$. 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

$$\mathrm{SpeFib}(\mathcal{C}(P)) := \{(\alpha,\gamma) \in \mathbb{R}^2, D(\alpha) = P(\alpha,\gamma) = 0\} \tag{3}$$

is the union of the special fibers.

Let $\alpha \in \mathbb{C}$ and

$$\mathrm{Crit}(\alpha) := \#\left\{\gamma \in \mathbb{R} \mid (\alpha,\gamma) \in \mathrm{Crit}(\mathcal{C}_{\mathbb{C}}(P))\right\}.$$

P is in **generic position** if :

- $\forall \alpha \in \mathbb{R}, \mathrm{Crit}(\alpha) \leqslant 1$,
- There is no asymptotic direction of $\mathcal{C}_{\mathbb{C}}(P)$ 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 1 *If $f(X,Y) \in \mathbb{Z}[X,Y]$ has coefficients of bitsize τ and degrees $d_1 = \deg_X(f), d_2 = \deg_Y(f)$ and $(\alpha,\gamma) \in \mathbb{C}^2$,*

$$|f(\alpha,\gamma)| \leqslant (d_1+1)(d_2+1)2^\tau \max(1,|\alpha|)^{d_1} \max(1,|\gamma|)^{d_2}.$$

Proposition 2 *[5] 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 by $q + \tau + \log(p+1)$.*

Definition 1 *Let f be a univariate polynomial with real coefficients. We denote by*

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

Proposition 3 *[5] If f is a univariate polynomial of degree d and bitsize at most τ, then $\Gamma(f) = O(\tau)$ and $\Sigma(f) = \tilde{O}(d\tau)$.*

Proposition 4 *[18] Denoting by δ the number of real roots of D, and $\mathrm{Zer}(D) = \{\alpha_1 < \ldots < \alpha_\delta\}$,*

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

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

2.3 Algorithmic results

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

The definition of the subresultant polynomials can be found, for example, in [5]. The non vanishing subresultant polynomial of smallest index is a gcd of the input polynomials.

Proposition 5 *[5] Let $P \in \mathbb{Z}[Y][X]$ of degree $p \leqslant d$ and $Q \in \mathbb{Z}[X,Y]$ of degree $q < p$, both of bitsize τ. 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 $\tilde{O}(d\tau)$, so with a bit complexity $\tilde{O}(d^5\tau)$. The bitsize of the output is $\tilde{O}(d^5\tau)$.*

Proposition 6 *[13] Let $f, g \in \mathbb{Z}[X]$ 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 7 *[4] 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 λ. The evaluation of f at r can be performed in $\tilde{O}(d(\tau+\lambda))$ and the bitsize of the output $f(r)$ is $\tilde{O}(\tau + d\lambda)$.*

Proposition 8 *([19], see also [21, 22, 23]) 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 such that 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 $\tilde{O}(d^2\tau + d^3 + dL)$ bit operations.

3. COMPUTATION OF THE TOPOLOGY

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.

Lemma 1 *[7] 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 $\tilde{O}(\tau + d)$.*

Then a similar change can be performed to avoid also that the curve contains horizontal lines. So from now on we can suppose that P has the desired properties, and bitsize $\tilde{O}(d + \tau)$.

3.2 Cylindrical algebraic decomposition

We denote by $\lambda(r)$ the bitsize of a rational number. Using the results of [20] (see also [8, 12, 24]) we have the following

Proposition 9 *[20] 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 $\tilde{O}(d^5\tau + d^6)$ for*

- *computing a set of special boxes*

  $$\text{SpeBox} = \{[a_i, b_i] \times [c_{i,j}, d_{i,j}] \mid 1 \le i \le \delta, 1 \le j \le \delta_i\}$$

  isolating the special points $\alpha_i, \gamma_{i,j}$ and such that $[a_i, b_i] \times [c_{i,j}, d_{i,j}] \setminus \{\alpha_i, \gamma_{i,j}\}$ contains no Y-critical point. Moreover, it is possible to ensure

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

  and

  $$\sum_{i=1}^{\delta}\sum_{j=1}^{\delta_i} \lambda(c_{i,j}) = \sum_{i=1}^{\delta}\sum_{j=1}^{\delta} \lambda(d_{i,j}) = \tilde{O}(d^3\tau + d^4). \qquad (5)$$

- *identifying for every $i = 1, \ldots, \delta$, the set $J_i \subset \{1, \ldots, \delta_i\}$ of indices of critical boxes, i.e. special boxes containing a critical point. Denoting by $\alpha_i, \gamma_{i,j}$ the point of the special fiber contained in $[a_i, b_i] \times [c_{i,j}, d_{i,j}]$, this is done by determining the multiplicity of $\gamma_{i,j}$ as a root of $P(\alpha_i, Y)$,*
- *computing the number n_i of real roots of $P(x, Y)$ for $x \in (b_i, a_{i+1})$ as well as n_0, n_δ the number n_i of real roots of $P(x, Y)$ for $x \in (-\infty, a_1)$, $x \in (a_\delta, +\infty)$.*

We now give some details on the method, different from the one given in [20], that we use for determining the 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 2 *Denote by $\mathrm{Sr}_i(X, Y)$ the ith subresultant polynomial of $P(X, Y)$ and $\partial_Y P(X, Y)$ with respect to Y and $\mathrm{sr}_{i,j}(X)$ the coefficient of Y^j in $\mathrm{Sr}_i(X, Y)$ and note that $\mathrm{sr}_{0,0}(X) = D(X)$. We define:*

$$\Phi_0(X) = \frac{D(X)}{\gcd(D(X), D'(X))};$$

$\forall i \in \{1, \ldots, d-1\}$,

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

Proposition 10

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

Proposition 11 *The computation of the polynomials $(D_i(X))_{1 \le i \le d-1}$ 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 coefficients of bitsize $\tilde{O}(d\tau + d^2)$. The sum of their degrees is bounded by $O(d^2)$.*

Proof. Follows from Proposition 6. □

Proposition 12 *Given the polynomials $(D_i(X))_{i \in [1, d-1]}$ computing for every root α of D (see Eq (1)) the degree of $\gcd(P(\alpha, Y), \partial_Y P(\alpha, Y))$ has bit complexity $\tilde{O}(d^5\tau + d^6)$.*

Proof. Use real root isolation for the roots of D_i and refine them to identify which are the roots of D corresponding to a root of D_i. If D_i is of degree d_i the cost is $\tilde{O}(d_i^2(d\tau + d^2) + d_i(d^3\tau + d^4))$. The cost for all i is hence $\tilde{O}(d^5\tau + d^6)$. □

If the curve $\mathcal{C}(P)$ is in general position, i.e. if J_i has at most one element for every $i = 1, \ldots, \delta$, we can compute its topology using the classical method of [14], since there is only one single critical point over a root of D. Otherwise, we compute the local topology of $\mathcal{C}(P)$ inside its critical boxes to reconstruct the topology of the curve $\mathcal{C}(P)$ by the method proposed in the next section.

3.3 Computation of the local topology inside the critical boxes

The computation of the local topology of $\mathcal{C}(P)$ inside the critical boxes is done in Subsection 3.3.4 after we have performed the following 3 steps

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

3.3.1 Isolating horizontal boundary points

We isolate the intersection points of $\mathcal{C}(P)$ with the horizontal boundary of the special boxes.

Proposition 13 *[Boundaries Computation]*

a) *The isolation of the intersection points of $\mathcal{C}(P)$ with the horizontal boundaries of the boxes in* SpeBox *i.e. the real roots of $\{P(X, c_{i,j}) = 0$ and $P(X, d_{i,j}) = 0\}$ costs $\tilde{O}(d^6\tau + d^7)$ bit operations.*

b) *Denoting by $m_{i,j}, m'_{i,j}$ the number of roots of $P(X, c_{i,j})$ and $P(X, d_{i,j})$, and $[u_k^{c_{i,j}}, w_k^{c_{i,j}}], [u_k^{d_{i,j}}, w_k^{d_{i,j}}]$ the isolating intervals of the real roots of $P(X, c_{i,j}), P(X, d_{i,j})$ we have:*

$$\sum_{k=0}^{m_{i,j}} \lambda(u_k^{c_{i,j}}) = \sum_{k=0}^{m_{i,j}} \lambda(w_k^{c_{i,j}}) = \tilde{O}(d(\tau + d\lambda(c_{i,j}))) \quad (6)$$

$$\sum_{k=0}^{m'_{i,j}} \lambda(u_k^{d_{i,j}}) = \sum_{k=0}^{m'_{i,j}} \lambda(w_k^{d_{i,j}}) = \tilde{O}(d(\tau + d\lambda(d_{i,j}))) \quad (7)$$

Proof. We give only the proof for $P(X, c_{i,j})$ since the one for $P(X, d_{i,j})$ is exactly similar.

The polynomial $P(X, c_{i,j})$ is of degree d and of bitsize $\tilde{O}(\tau + d\lambda(c_{i,j}))$. Using Proposition 8 the isolation costs $\tilde{O}(d^2(\tau + d\lambda(c_{i,j})) + d^3)$. Hence the total cost is :

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

So that the total cost is $\tilde{O}(d^6\tau + d^7)$ bit operations, using Eq. (5). Using Proposition 8, the result follows. □

3.3.2 Computing sign of derivatives at horizontal boundary points

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

Proposition 14 *It costs $\tilde{O}(d^6\tau + d^7)$ 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 $x_k \in [u_k^{c_{i,j}}, w_k^{c_{i;j}}]$, $1 \leq k \leq m_{i,j}$ 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 suffices 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 $\mathcal{C}(P)$), we proceed as follows :

1. We compute 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 leads, using Eq (5), to a total cost of $\tilde{O}(d^6\tau + d^7)$ 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 7, costs $\tilde{O}(d(\tau + d\lambda(c_{i,j}) + \lambda(e_\ell)))$. Hence

$$\begin{aligned} & \sum_{i=1}^{\delta}\sum_{j=1}^{\delta'_i}\sum_{\ell=1}^{O(d)} \tilde{O}(d(\tau + d\lambda(c_{i,j}) + \lambda(e_\ell))) \\ = & \sum_{i=1}^{\delta}\sum_{j=1}^{\delta'_i} \tilde{O}(d^2(\tau + d\lambda(c_{i,j}))) \\ = & \tilde{O}(d^6\tau + d^7). \end{aligned}$$

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 in $\tilde{O}(d(\tau + d\lambda(c_{i,j})))$ since its degree is $O(d)$ and its coefficients of bitsize $\tilde{O}((\tau + d\lambda(c_{i,j})))$.

The cost of this refinement process is $\tilde{O}(d^2(\tau + d\lambda(c_{i,j})))$. This leads, using Eq (5), to a total cost of $\tilde{O}(d^6\tau + d^7)$ 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

$$P(X, c_{i,j})\partial_X P(X, c_{i,j})\partial_Y P(X, c_{i,j}).$$

The cost of this refinement process is $\tilde{O}(d^2(\tau + d\lambda(c_{i,j})))$. This leads, using Eq (5), to a total cost of $\tilde{O}(d^6\tau + d^7)$ for the refinement.

4. By ordering the concatenation of the two refined list of isolating intervals one can deduce the signs of

$$\partial_X P(x_k, c_{i,j})\partial_Y P(x_k, c_{i,j}),$$

where $1 \leq i \leq \delta, 1 \leq j \leq \delta'_i, 1 \leq k \leq \epsilon_{i,j}$. 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 $[a_i, b_i] \times [c_{i,j}, d_{i,j}] \in$ SpeBox, $1 \leq i \leq \delta$, $1 \leq j \leq \delta_i$. □

3.3.3 Finding the relative position of the abscissa of horizontal boundary points and critical point

Consider a critical box $[a, b] \times [c, d]$ containing a critical point (α, γ). In order to identify the topology of the curve inside $[a, b] \times [c, d]$, our method requires to know how many roots of $P(X, c)$ (resp. $P(X, d)$) are before and after α on the interval $[a, b]$.

We start by proving Theorem 1, which is a quantitative result on the deviation of the curve from the vertical axis at a critical point and plays a key role in the complexity analysis (Proposition 17). Before stating Theorem 1, we introduce a definition.

Definition 3 *Denote by $\mathcal{C}(P)_k$, $0 \leqslant k \leqslant d$, the points (α, γ) of $\mathcal{C}(P)$ such that*

1. *$\partial_Y^k P(\alpha, \gamma) \neq 0$,*
2. *for every $k' < k$, $\partial_Y^{k'} P(\alpha, \gamma) = 0$.*

Example 1 If (α, γ) is a regular point of $\mathcal{C}(P)$, $(\alpha, \gamma) \in \mathcal{C}(P)_1$.

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

Theorem 1 *Let $(\alpha,\gamma) \in \mathcal{C}(P)_k$. There exist real numbers $A(\alpha,\gamma)$ and $B(\alpha,\gamma)$, such that for every y with $0 < y < B(\alpha,\gamma)$, and every x with $P(\alpha+x,\gamma+y) = 0$, the inequality $|x| > |y|^k |A(\alpha,\gamma)|$ holds. Moreover*

$$-\sum_{(\alpha,\gamma)\in \mathrm{Crit}(\mathcal{C}(P))} \log(|A(\alpha,\gamma)|) = \tilde{O}(d^3\tau + d^4)$$

$$-\sum_{(\alpha,\gamma)\in \mathrm{Crit}(\mathcal{C}(P))} \log(|B(\alpha,\gamma)|) = \tilde{O}(d^3\tau + d^4).$$

The proof of Theorem 1 relies on the following two propositions giving an upper bound and lower bound on the value of specific algebraic numbers.

In the two following propositions, let $P, Q \in \mathbb{Z}[X,Y]$, monic with respect to Y, of degree in each variable dominated by d, and coefficients of bitsizes less than τ. Suppose moreover that P and Q have a finite number of common zeros in $\mathbb{C}^2$. Let

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

Proposition 15 *Consider for each $(\alpha,\gamma) \in Z$, a subset $\mathcal{H}(\alpha,\gamma)$ of at most d^2 elements of $\mathbb{Z}[X,Y]$, each of degree in X, Y dominated by d, and coefficients of bitsizes less than τ. Then*

$$\sum_{(\alpha,\gamma)\in Z} \log\left(\sum_{H\in\mathcal{H}(\alpha,\gamma)} |H(\alpha,\gamma)|\right) = \tilde{O}(d^2\tau)\ .$$

Proof. The claim follows from Proposition 3, Proposition 4 and Proposition 1 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 $O(d^2)$ with coefficients of bitsize $\tilde{O}(d\tau)$. $\square$

Proposition 16 *Let $H_1,\ldots,H_k$, $k \le d$, be elements of $\mathbb{Z}[X,Y]$, monic with respect to Y, of degree in each variable dominated by d, and coefficients of bitsizes less than τ. Let*

$$Z_i = \{(\alpha,\gamma) \in Z \mid \bigwedge_{j=1}^{i-1} H_j(\alpha,\gamma) = 0, H_i(\alpha,\gamma) \neq 0\}.$$

Then

$$-\sum_{i=1}^{k}\sum_{(\alpha,\gamma)\in Z_i} \log(|H_i(\alpha,\gamma)|) = \tilde{O}(d^3\tau + d^4).$$

Proof. We are going to prove that there exists an $E \in \mathbb{Z}$ of bitsize $O(d^3\tau)$ such that

$$\prod_{i=1}^{k}\prod_{(\alpha,\gamma)\in Z_i} H_i(\alpha,\gamma) \geqslant \frac{1}{E}.$$

Let

$$\begin{aligned}
Z' :&= \{(\alpha,\gamma) \in \mathbb{C}^2 \mid P(\alpha,\gamma) = Q(\alpha,\gamma) = 0\},\\
Z'_i &:= \{(\alpha,\gamma) \in Z' \mid \bigwedge_{j=1}^{i-1} H_j(\alpha,\gamma) = 0, H_i(\alpha,\gamma) \neq 0\},\\
W_i^t &:= \{(\alpha,\gamma) \in \mathbb{C}^2 \mid P(\alpha,\gamma) = Q(\alpha,\gamma) + tH_i(\alpha,\gamma)\},\\
W_i^\varepsilon &:= \{(x,y) \in \mathbb{C}'^2 \mid P(x,y) = Q(x,y) + \varepsilon H_i(x,y)\},\\
S_i^\varepsilon(X) &:= \mathrm{Res}_Y(P, Q + \varepsilon H_i),
\end{aligned}$$

where $\mathbb{C}'$ is the field of Puiseux series with coefficients in $\mathbb{C}$. Since W_i^ε is finite and contains no element of Z'_i, there exists $t \in \mathbb{N} \setminus \{0\}$ such that W_i^t is finite and contains no element of Z'_i [5], with t of bit size $O(\log(d))$, using $\deg_\varepsilon(S_i^\varepsilon) \le d$.

Making if necessary a linear change of variable of the form $T = X - sY, Y = Y$, with s an integer of bitsize $O(\log d)$, we can suppose that X separates the elements of $Z'_i \cup W_i^t$ for every $1 \le i \le k$. Let $S_i(X) = \mathrm{Res}_Y(P, Q + tH_i)$, and τ_i a bound on the bitsize of its coefficients. Note that τ_i is in $\tilde{O}(d\tau + d^2)$. There exist polynomials $U_i(X,Y)$ et $V_i(X,Y)$ of degree at most d with respect to Y and at most $O(d^2)$ with respect to X and coefficients of bitsize $\tilde{O}(d\tau + d^2)$ such that

$$S_i(X) = U_i(X,Y)P(X,Y) + V_i(X,Y)(Q + tH_i)(X,Y).$$

Let $(\alpha,\gamma) \in Z'_i$. Since X separates $Z'_i \cup W_i^t$, $S_i(\alpha) \neq 0$. Since $S_i(\alpha) = V_i(\alpha,\gamma)H_i(\alpha,\gamma)$, $V_i(\alpha,\gamma) \neq 0$. We are now going to prove that

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

is bigger than the inverse of a natural number of bitsize $\tilde{O}(d^3\tau + d^4)$. We decompose $R = \mathrm{Res}_Y(P,Q)$ as $R = R_0 \prod_{i=1}^k R_i$, where the zeros of R_i contain the X-projections of Z'_i and denote by d_i the degree of R_i. Since $|\mathrm{Res}_X(R_i, S_i)|$, which is equal to

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

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, taking $L = \max_i(|\operatorname{Lc}_X(S_i)|)$, $\prod_{\alpha\in Z_i} |S_i(\alpha)|$

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

Since $\sum_{i=0}^k d_i = d^2$, $\sum_{i=0}^k \Gamma(R_i) = \Gamma(R) = \tilde{O}(d\tau + d^2)$, $\tau_i = O(d\tau + d^2)$, we obtain $\prod_{i=1}^k \prod_{\alpha\in Z_i} |S_i(\alpha)| \geqslant 2^{-\lambda}$ with $\lambda = O(d^3\tau + d^4)$.

To estimate the products of the $V_i(\alpha,\beta)$, we apply Proposition 1, 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 $\tilde{O}(d\tau + d^2)$, so that $\prod_{(\alpha,\gamma)\in Z_i} |V_i(\alpha,\gamma)|$ is at most

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

Defining $C = \max_i(C_i)$ we obtain, since the $\mathrm{Zer}(R_i)$ are disjoint, that $\prod_{i=1}^k \prod_{(\alpha,\gamma)\in Z_i} |V_i(\alpha,\gamma)|$ is at most

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

Recalling that $\prod_{\alpha\in \mathrm{Zer}(R)} \max(1,|\alpha|)$ is bounded by a natural number of bitsize $\tilde{O}(d\tau+d^2)$ and that $\prod_{(\alpha,\gamma)\in Z} \max(1,|\gamma|)$ is bounded by a natural number of bitsize $\tilde{O}(d^2\tau+d^3)$, and given the degrees of V_i in X,Y, then $\prod_{i=1}^k \prod_{(\alpha,\gamma)\in Z_i} |V_i(\alpha,\gamma)|$ is bounded by a natural number of bitsize $\tilde{O}(d^3\tau+d^4)$ and, finally, $\prod_{i=1}^k \prod_{(\alpha,\gamma)\in Z_i} tH_i(\alpha,\gamma) = \prod_{i=1}^k \frac{\prod_{(\alpha,\gamma)\in Z_i} S_i(\alpha)}{\prod_{(\alpha,\gamma)\in Z_i} V_i(\alpha,\gamma)}$ is bigger than the quotients of two natural numbers of bitsize $\tilde{O}(d^3\tau+d^4)$ and in particular bigger than the inverse of a natural number of bitsize $\tilde{O}(d^3\tau+d^4)$. Since t is of bitsize $O(\ rmlog(d))$ and Z' has at most d^2 elements, the claim follows. $\square$

Proof of Theorem 1. By Taylor formula, for $(\alpha,\gamma)\in \mathcal{C}(P)_k$,

$$P(\alpha+X,\gamma+Y) = \sum_{j=0}^{d} \frac{1}{j!} C_j(\gamma+Y) X^j,$$

with

$$C_0(\gamma+Y) = Y^k \left(\sum_{i=k}^{d} \frac{1}{i!} \partial_Y^i P(\alpha,\gamma) Y^{i-k} \right),$$

and, for $j>0$,

$$C_j(\gamma+Y) = \sum_{i=0}^{d} \frac{1}{i!} \partial_Y^i \partial_X^j P(\alpha,\gamma) Y^i.$$

By Cauchy's root bound [5], for every y with $C_0(\gamma+y)\neq 0$, the smallest positive root of $P(\alpha+X,\gamma+y)$ is at least

$$|C_0(\gamma+y)| \left(\sum_{j=0}^{d} |C_j(\gamma+y)| \right)^{-1}.$$

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

$$\sum_{j=0}^{d} |C_j(\gamma+y)| \leqslant \sum_{j=0}^{d}\sum_{i=0}^{d} \frac{1}{i!} \left| \partial_Y^i \partial_X^j P(\alpha,\gamma) \right|.$$

Let

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

be smaller than the smallest positive root of the univariate polynomial

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

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

$$|C_0(\gamma+y)| > |y|^k \left| \frac{1}{2k!} \partial_Y^k P(\alpha,\gamma) \right|$$

We finally define

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

Taking

$$\mathcal{H}(\alpha,\gamma) = \{\partial_Y^i \partial_X^j P, i=0,\dots,d, j=0,\dots,d\},$$

$$\mathcal{H}_k(\alpha,\gamma) = \{\partial_Y^k P, \frac{2k!}{i!} \partial_Y^k P, i=k+1,\dots,d\},$$

for $(\alpha,\gamma)\in\mathcal{C}(P)_k$ and $H_i = \partial_Y^i P$, $i=1,\dots,d$, and combining Proposition 15 and Proposition 16 we obtain the final estimates on $A(\alpha,\gamma)$ and $B(\alpha,\gamma)$. $\square$

Proposition 17 *It costs $\tilde{O}(d^6\tau+d^7)$ bit operations to compare the abscissa of all the boundary points of the critical boxes with the abscissa of the corresponding critical point.*

Proof. Let

$$c(\alpha,\gamma) = -k\log(|A(\alpha,\gamma)|) - \log(|B(\alpha,\gamma)|).$$

If $(\alpha,\gamma)\in\mathcal{C}(P)_k$, $k>1$, according to Theorem 1 the distance between α and any root of $P(X,c)$ is at least $2^{c(\alpha,\gamma)}$. 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 less than $2^{(c(\alpha,\gamma))}$. Such refinement costs $O(d(c(\alpha,\gamma)))$ for the roots of $P(X,c)$ and $O(d^2(c(\alpha,\gamma)))$ for the roots of D up to $2^{c(\alpha,\gamma)}$. The total cost is again $\tilde{O}(d^6\tau+d^7)$ for all the special boxes by Theorem 1. $\square$

3.3.4 Topology inside a critical box

We prove now that given the information already computed we are able to compute the topology of the curve inside a critical box. We introduce some definitions.

Definition 4 (Monotonic arc) *An arc of $\mathcal{C}(P)$ is a subset of $\mathcal{C}(P)$ homeomorphic to $[0,1]$. 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.*

Proposition 18 *An arc of $\mathcal{C}(P)$ contained in a critical box $[a,b]\times[c,d]$ that does not pass through a critical point (α,γ) is monotonic.*

Denote 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).

Split L_c (resp.L_d) into $L_{c<\alpha}$ and $L_{c>\alpha}$ (resp. $L_{d<\alpha}$ and $L_{d>\alpha}$) which are the points of L_c (resp. L_d) at the left side and the right side of the special fiber $\mathrm{Fib}(\alpha)$.

Given a boundary point (x,y) of $[a,b]\times[c,d]$, there is one and only one arc of $\mathcal{C}(P)$, called a special arc, contained in $[a,b]\times[c,d]$ starting from (x,y), 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 arcs of type 1 having distinct intersection with the horizontal boundary of a critical box do not meet, and that two arcs of type 2 having distinct intersection with the boundary of a critical box meet only at (α,γ).

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

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

Given two lists $L=[x_1,\dots,x_n]$ and $M=[y_1,\dots,y_m]$ we denote their concatenation by $L+M := [x_1,\dots,x_n,y_1,\dots,y_m]$. We denote by SlopeSign the sign of the slope of the tangent line of a point.

The following result holds, as well as similar results for $L_{d,>\alpha}$, $L_{c,<\alpha}$, $L_{c,>\alpha}$.

Proposition 19 *The points of $L_{d<\alpha}$ have the same slope sign. If this sign is $-$, they are contained in an arc of type 2. If this sign is $+$ they are contained in an arc of type 1 and the matching point of $L_{d,<\alpha}[i]$ is $L[i]$, where $L = L_a^{-1} + L_{c,<\alpha}$.*

PROOF. Let (x_1, d) and (x_2, d) be two consecutive points of $L_{d,<\alpha}$ with different slope signs. One of the following conditions necessarily holds:

1. (x_1, d) and (x_2, d) belong to the same connected component of $\mathcal{C}(P)$ inside $[a, b] \times [c, d]$,

2. (x_1, d) and (x_2, d) belong to two differents connected component C_1 and C_2 of $\mathcal{C}(P)$ inside $[a, b] \times [c, d]$

a) C_1 (resp. C_2) has a point above x_2 (resp. x_1), and $C_1 \cap C_2$ contains a point with abscissa in (x_1, x_2),

b) C_1 has a local maximum for x between x_1 and x_2,

c) C_2 has a local minimum for x between x_1 and x_2,

In all these four cases, there is a critical point or a Y-critical point with abscissa in (x_1, x_2). This is a impossible since $(x_1, x_2) \subset (a, \alpha)$ contains no root of D and S. Finally, two consecutive points of $L_{d,<\alpha}$ have same slope signs.

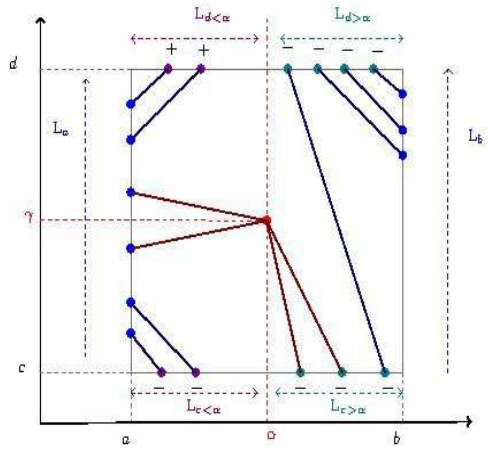
Suppose that the slope sign of the elements of $L_{d,<\alpha}$ is $+$ and take $(x, d) \in L_{d,<\alpha}$. The special arc through (x, d) stays at the left of the line $x = x_1$, since the curve has no local minimum for x_1 at the left of α inside the box. It does not contain (α, γ) and is an arc of type 1. The matching point of $L_{d<\alpha}[i]$ is a point of the boundary to the left of α which does not belong to $L_{d,<\alpha}$: 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 critical 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 obtain a contradiction and the matching point of $L_{d<\alpha}[i]$ is $L[i]$.

Suppose that the slope sign of the elements of $L_{d,<\alpha}$ is $-$. The special arc through $(x, d) \in L_{d,<\alpha}$ stays at the right of the line $x = x_1$, since the curve has no local maximum at the left of α inside the box, so has to contain (α, γ) : it is an arc of type 2. $\square$

We denote by MN the open segment between M and N.

Algorithm 1 Connect
Set `Points` *to* $\{(\alpha, \gamma)\} \cup L_a \cup L_b \cup L_c \cup L_d$ *and initialize* `Arcs` *to the empty list.*
1. Connection at the left of the fiber
Input: L_a, $L_{c,<\alpha}$, $L_{d,<\alpha}$. ***Output:*** *a finite union of points and segments homeomorphic to $\mathcal{C}(P)$ inside $[a, \alpha] \times [c, d]$, and the number ℓ of the segments ending at (α, γ)*
if $\#L_{d,<\alpha} > \#L_a$ *then* $L := L_a^{-1} + L_{c,<\alpha}$, *else* $L := L_a^{-1}$;
if $\mathsf{SlopeSign}(L_{d,<\alpha}[1]) > 0$, *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 $\mathsf{SlopeSign}(L_{c,<\alpha}[1]) < 0$, *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 to` (α, γ) *: For i from 1 to* $\#L$, *add* $L[i]O$ *to Arcs and output* $\ell := \#L$
2.Connection at the right of the fiber.
Input: L_b, $L_{c,>\alpha}$, $L_{d,>\alpha}$. ***Output:****a finite list of points and segments homeomorphic to $\mathcal{C}(P)$ inside $[\alpha, b] \times [c, d]$, and the number r of the segments ending at (α, γ). The process is entirely symmetrical so we do not include it.*



The correctness of Algorithm 1 follows from Proposition 19 and its cost is linear in the total number of the points on the boundary of the box which is bounded by $O(d^4)$.

3.3.5 Final topology

For $\alpha, i, \gamma_{i,j}$ critical, i.e. $j \in J_i$, we denote by $\ell_{i,j}$ (resp. $r_{i,j}$) the number of segments arriving at $(\alpha_i, \gamma_{i,j})$ inside $[a_i, \alpha_i] \times [c_{i,j}, d_{i,j}]$ (resp. $[\alpha_i, b_i] \times [c_{i,j}, d_{i,j}]$). Note that this information has been determined by Algorithm 1. We use the notation of Proposition 9. For $j \notin J_i$, we take $\ell_{i,j} = r_{i,j} = 1$. The topology of $\mathcal{C}(P)$ is encoded by the finite list $n_0, L_1, \ldots, L_\delta, n_\delta$ where L_i is the list $[\ell_{i,j}, r_{i,j}, 1 \leq j \leq \delta_{i,j}]$ and a straight-line planar graphe homeomorphis to $\mathcal{C}(P)$ can be obtained as follows : for each i, $i = 1, \ldots, \delta$

- include the points $A_{i,j} = (2i, j)$ for j from 1 to n_i and $B_{i,j} = (2i - 1, j)$ for j from 1 to δ_j,

- add the open segment $A_{i-1,\ell}B_{i,j}$ (resp. $A_{i,r}B_{i,j}$) if

$$\sum_{k=1}^{j-1} \ell_{i,k} < \ell \leq \sum_{k=1}^{j} \ell_{i,k} (\text{resp.} \sum_{k=1}^{j-1} r_{i,k} < r \leq \sum_{k=1}^{j} r_{i,k}).$$

3.4 Summary

Let us summarize the result we have obtained.

Theorem 2 *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 $\tilde{O}(d^6\tau + d^7)$.*

3.5 Recent results and future work

Recent work [17], currently under peer-review, proposes a deterministic algorithm for computating the topology of an algebraic curve, using only $\tilde{O}(d^5\tau + d^6)$ bit operations. This method is mainly based on a fast algorithm for solving bivariate systems and uses a generic coordinate transformation (which is computed in a deterministic manner).

We plan to investigate in the future the possibility to reach also $\tilde{O}(d^5\tau + d^6)$ bit operations using our approach.

Acknowledgement.

This work was supported by various instititions : AIMS Sénégal, INRIA, Université de Rennes 1 as well as the NLAGA research project. We want to express our gratitude to Michael Sagraloff whose suggestions have helped improving the paper.

4. REFERENCES

[1] Lionel Alberti, Bernard Mourrain: Regularity Criteria for the Topology of Algebraic Curves and Surfaces. IMA Conference on the Mathematics of Surfaces 2007: 1-28

[2] Lionel Alberti, Bernard Mourrain: Visualisation of Implicit Algebraic Curves. Pacific Conference on Computer Graphics and Applications 2007: 303-312

[3] Lionel Alberti, Bernard Mourrain, Julien Wintz: Topology and arrangement computation of semi-algebraic planar curves. Comp. Aided Geom. Des. 25(8): 631-651 (2008)

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

[5] S. Basu, R. Pollack, and M.-F. Roy. Algorithms in Real Algebraic Geometry. Springer, 2nd edition, 2006.

[6] Eric Berberich, Pavel Emeliyanenko, Alexander Kobel, Michael Sagraloff: Exact symbolic-numeric computation of planar algebraic curves. Theor. Comput. Sci. 491: 1-32 (2013)

[7] Yacine Bouzidi, Sylvain Lazard, Marc Pouget, Fabrice Rouillier : Separating Linear Forms for Bivariate Systems, ISSAC, 2013 : 117-124.

[8] W. Dale Brownawell, Chee-Keng Yap: Lower bounds for zero-dimensional projections. ISSAC,2009: 79-86

[9] M. Burr, S.W.Choi, B. Galehouse, Chee Yap. Complete Subdivision Algorithms, II: Isotopic Meshing of Singular Algebraic Curves, ISSAC 2008.

[10] 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

[11] Daouda Niang Diatta, Bernard Mourrain, Olivier Ruatta. On The Computation of the Topology of a Non-Reduced Implicit Space Curve. ISSAC, 2008.

[12] Dimitrios I. Diochnos, Ioannis Z. Emiris, Elias P. Tsigaridas. On the asymptotic and practical complexity of solving bivariate systems over the reals. J. Symb. Comput. 44(7): 818-835 (2009)

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

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

[15] L. Gonzalez-Vega and I. Necula. Efficient topology determination of implicitly defined algebraic plane curves. Comp. Aided Geom. Des. , 19:719–743, 2002.

[16] A. Eigenwillig, M. Kerber, and N. Wolpert. Fast and exact geometric analysis of real algebraic plane curves, ISSAC, 2007 : 151-158.

[17] Alexander Kobel, Michael Sagraloff: Improved Complexity Bounds for Computing with Planar Algebraic Curves. CoRR abs/1401.5690 (2014)

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

[19] Kurt Mehlhorn, Michael Sagraloff, and Pengming. Wang. From Approximate Factorization to Root Isolation. ISSAC, 2013.

[20] Kurt Mehlhorn, Michael Sagraloff, and Pengming. Wang. From Approximate Factorization to Root Isolation with Application to Cylindrical Algebraic Decomposition. To appear in J. Symb. Comput.

[21] Victor Y. Pan: Univariate Polynomials: Nearly Optimal Algorithms for Numerical Factorization and Root-finding. J. Symb. Comput. 33(5): 701-733 (2002)

[22] Victor Y. Pan, Elias P. Tsigaridas: On the boolean complexity of real root refinement. ISSAC 2013: 299-306

[23] Adam W. Strzebonski, Elias P. Tsigaridas: Univariate real root isolation in an extension field. ISSAC 2011: 321-328

[24] Adam W. Strzebonski, Elias P. Tsigaridas: Univariate real root isolation in multiple extension fields. ISSAC 2012: 343-350

[25] Julien Wintz, Bernard Mourrain: A Subdivision Arrangement Algorithm for Semi-Algebraic Curves: An Overview. Pacific Conference on Computer Graphics and Applications 2007: 449-452