Amortized complexity bounds for polynomials with algebraic coefficients and application to curve topology

D N. Diatta, F. Rouillier, M-F. Roy, M. Sagraloff and S. Diatta

INRIA NANCY GRAND EST

May 25, 2017

Sény DIATTA

Ph.d student of University Assane Seck of Ziguinchor (SENEGAL)

Topic: Computation of the topology of algebraic curves and surfaces.

Supervisors:

- Daouda Niang DIATTA,
- Guillaume MOROZ and
- Marie-Francoise ROY

Area: 196,722 km^2

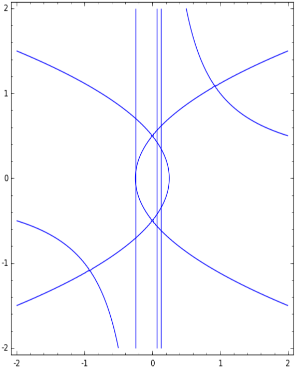
Population: 14,354,690

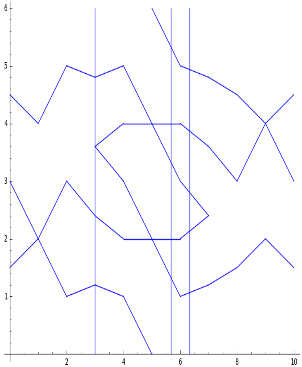
1. Topology of algebraic curves

2. Projection of an analytic surface

Part 1: Topology of algebraic curves

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





$\mathcal{C}(P) = \{(\alpha, \gamma) \in \mathbb{R}^2 | P(\alpha, \gamma) = 0\}$ $\quad \mathrm{Gr}(P) \subset (0, H) \times (0, V)$

Using Generic Position

- An improved upper complexity bound for the topology computation of a real algebraic curve [L. Gonzalez-Vega and M. El Kahoui, 1996] $\longrightarrow \tilde{O}(d^{16}\tau)$.
- From Approximate Factorization to Root Isolation with application to CAD [K. Mehlhorn, M. Sagraloff, P. Wang, 2014] $\longrightarrow \tilde{O}(d^5\tau + d^6)$

Without Generic Position

- On the topology of the planar algebraic curves [J. Cheng, S. Lazard, L. Peneranda, M. Pouget, F. Rouillier and E. Tsigaridas, 2009] $\longrightarrow \tilde{O}(Rd^{22}\tau)$.
- On the Computation of the Topology of Plane curves [D N. Diatta, F. Rouillier and M-F. Roy, 2014]$\longrightarrow \tilde{O}(d^6\tau + d^7)$

Using Generic Position

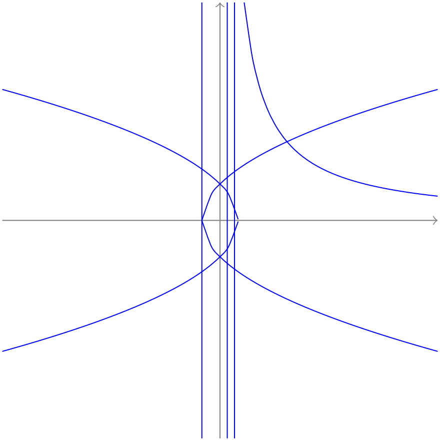
- An improved upper complexity bound for the topology computation of a real algebraic curve [L. Gonzalez-Vega and M. El Kahoui, 1996] $\longrightarrow \tilde{O}(d^{16}\tau)$.
- From Approximate Factorization to Root Isolation with application to CAD [K. Mehlhorn, M. Sagraloff, P. Wang, 2014] $\longrightarrow \tilde{O}(d^5\tau + d^6)$

Without Generic Position

- On the topology of the planar algebraic curves [J. Cheng, S. Lazard, L. Peneranda, M. Pouget, F. Rouillier and E. Tsigaridas, 2009] $\longrightarrow \tilde{O}(Rd^{22}\tau)$.
- On the Computation of the Topology of Plane curves [D N. Diatta, F. Rouillier and M-F. Roy, 2014]$\longrightarrow \tilde{O}(d^6\tau + d^7)$

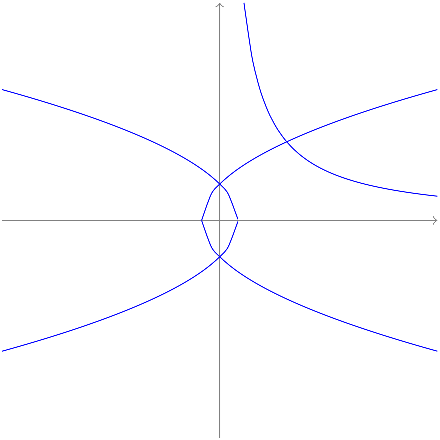
About our Algorithm

We propose a determinist algorithm for computing the topology of curve in $\tilde{O}(d^5\tau + d^6)$ without putting the curve in generic position.



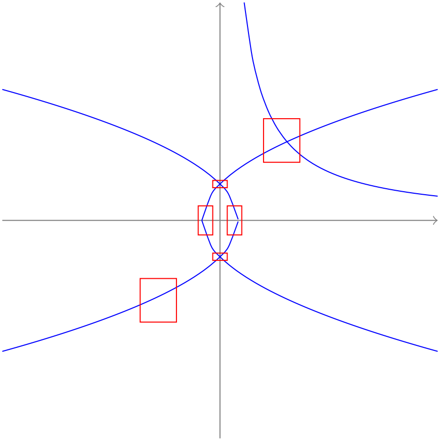
About our Algorithm

We propose a determinist algorithm for computing the topology of curve in $\tilde{O}(d^5\tau + d^6)$ without putting the curve in generic position.



About our Algorithm

We propose a determinist algorithm for computing the topology of curve in $\tilde{O}(d^5\tau + d^6)$ without putting the curve in generic position.



Notations

Let $P(X,Y) = \sum_{i=1}^{d_y} C_i(X)Y^i = C(X)\tilde{P}(X,Y)$,
where $C(X) = \gcd(C_i(X), 1 \leq i \leq d_y)$.
We define

$$D(X) := \mathrm{Res}_Y(\tilde{P}, \partial_Y \tilde{P})(x)$$

and denote $\alpha_1, \ldots, \alpha_\delta$ its real roots. A point (α, γ) of $\mathcal{C}(\tilde{P})$ is called

- a X-critical point if $\partial_Y \tilde{P}(\alpha,\gamma) = 0$
- a singular point if $\partial_X \tilde{P}(\alpha,\gamma) = \partial_Y \tilde{P}(\alpha,\gamma) = 0$.

Definition

Let $f \in \mathbb{Z}[X]$ be a polynomial of degree n. Then, we define: A *well-isolating* interval $\mathcal{I} = (a, b)$ for a real root z of f contains z and no other real root of f and it holds that $|b - a| < \frac{\mathrm{sep}(z,f)}{32n}$

Cylindrical Algebraic Decomposition

Using $\tilde{O}(d^5\tau + d^6)$ bit-operations, we can:

- compute a set of **special boxes**

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

  well-isolating the **special points** $(\alpha_i, \gamma_{i,j})$
- identify the set $J_i \subset \{1, \ldots, \delta_i\}$ of indices of critical boxes and $mult(\gamma_{i,j}, \tilde{P}(\alpha_i, Y)$, for every $i = 1, \ldots, \delta$

Computing adjacency boxes

Theorem

We can describe explicitly two real number A_γ *and* B_γ $(A_\gamma, B_\gamma \leq 1)$*, such that for every* y, $0 \leq y \leq B_\gamma$,

$$|\mathrm{sep}(\bar{P}(X, \gamma + y))| > |y|^{\nu_\gamma/2} |A_\gamma|.$$

Moreover

$$\sum_{S(\gamma)=0} \mu_\gamma |\log A_\gamma| \in O(d^3\tau + d^4), \tag{1}$$

$$\sum_{S(\gamma)=0} \mu_\gamma |\log B_\gamma| \in O(d^3\tau + d^4). \tag{2}$$

Let $S(Y) := \mathrm{Res}_X(\tilde{P}, \partial_X \tilde{P})(Y) \times \mathrm{Res}_X(\tilde{P}, \partial_Y \tilde{P})(Y)$ and γ a real number of $\mu_\gamma := mult(\gamma, S)$ and $\nu(\gamma) := mult(\gamma, \bar{D})$.

Computing adjacency boxes

Let $\mathcal{I}_k = (a'_k, b'_k)$ the well-isolating intervals , for all real roots y_k of S and $\tilde{\sigma} = \tilde{\sigma}_{i,j} \approx \mathrm{sep}(\gamma, \tilde{P}(\alpha, -))$. We now refine (c, d) to a width less than

$$w := w_{i,j} := \frac{1}{8} \cdot \min(\tilde{B}_\gamma, \tilde{\sigma}) \geq \frac{1}{32} \cdot \min(B_\gamma, \mathrm{sep}(\gamma, \tilde{P}(\alpha, -))) \qquad (3)$$

and further extend the interval by w on both sides to obtain an isolating interval (c, d) for γ with $w < \min(\gamma - c, d - \gamma) < \max(\gamma - c, d - \gamma) < 2w$.

$$\sum_{i,j} |\log \tilde{B}_{\gamma_{i,j}}| + |\log \tilde{\sigma}_{i,j}| = \tilde{O}(d^4 + d^3\tau).$$

Lemma

Using $\tilde{O}(d^6 + d^5\tau)$ bit operations, we can compute integers $k_{i,j} \in \{1, \ldots, m\}$ for all x-critical points $(\alpha_i, \gamma_{i,j}) \in \mathrm{Crit}(\mathcal{C}(\tilde{P}))$ with $y_{k_{i,j}} = \gamma_{i,j}$.

Computing adjacency boxes

Let $\mathcal{I}_k = (a'_k, b'_k)$ the well-isolating intervals , for all real roots y_k of S and $\tilde{\sigma} = \tilde{\sigma}_{i,j} \approx \mathrm{sep}(\gamma, \tilde{P}(\alpha, -))$. We now refine (c, d) to a width less than

$$w := w_{i,j} := \frac{1}{8} \cdot \min(\tilde{B}_\gamma, \tilde{\sigma}) \geq \frac{1}{32} \cdot \min(B_\gamma, \mathrm{sep}(\gamma, \tilde{P}(\alpha, -))) \qquad (3)$$

and further extend the interval by w on both sides to obtain an isolating interval (c, d) for γ with $w < \min(\gamma - c, d - \gamma) < \max(\gamma - c, d - \gamma) < 2w$.

$$\sum_{i,j} |\log \tilde{B}_{\gamma_{i,j}}| + |\log \tilde{\sigma}_{i,j}| = \tilde{O}(d^4 + d^3\tau).$$

Lemma

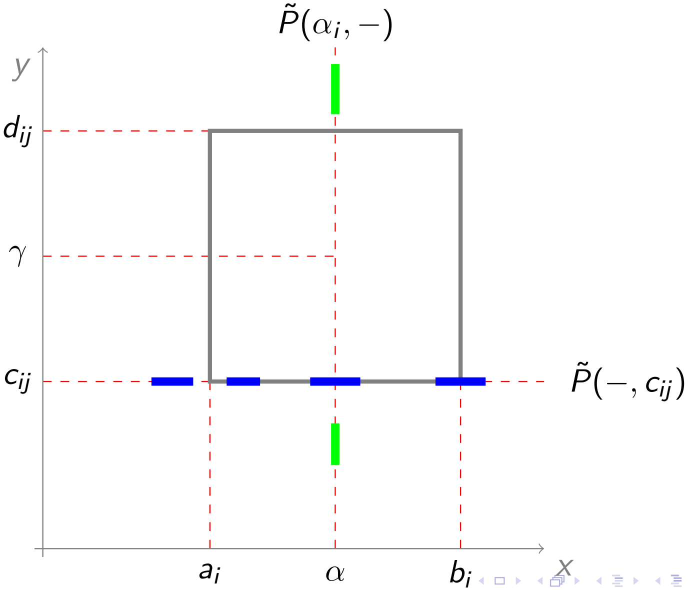
Using $\tilde{O}(d^6 + d^5\tau)$ bit operations, we can compute integers $k_{i,j} \in \{1, \ldots, m\}$ for all x-critical points $(\alpha_i, \gamma_{i,j}) \in \mathrm{Crit}(\mathcal{C}(\tilde{P}))$ with $y_{k_{i,j}} = \gamma_{i,j}$.

Number of roots in the horizontal edges

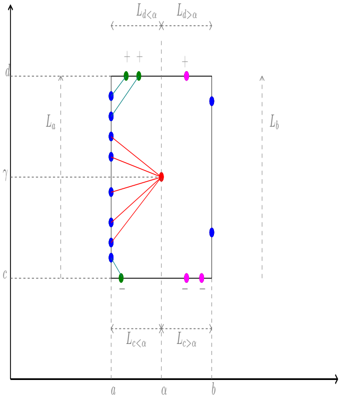
Lemma

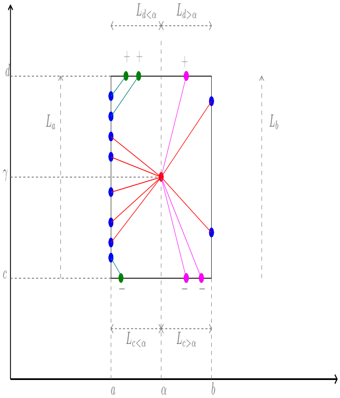
The real roots of all polynomials $\tilde{P}(-, c_{i,j})$ and $\tilde{P}(-, d_{i,j})$ can be isolated in a number of bit operations bounded by $\tilde{O}(d^6 + d^5\tau)$. The separator of each polynomial $\tilde{P}(-, c_{i,j})$ is bounded by $2^{\tilde{O}(d^4+d^3\tau)}$.

Number of roots in the horizontal edges



Topology in critical box





Dealing with vertical asymptotes

$X = \alpha$ is a vertical asymptote *iff* $\deg(\tilde{P}(\alpha, Y)) < d_y = \deg_Y(\tilde{P}(X, Y)$, so $c_{d_Y}(\alpha) = D(\alpha) = 0$.
Let

$$\beta_{+\infty} \in \mathbb{N} \mid \beta_{+\infty} \geq |\alpha|, \forall \alpha \in V_{\mathbb{R}}(\tilde{P}(\alpha, Y))$$

We isolate the real roots of $\tilde{P}(X, \beta_{+\infty}) = 0$, and on each interval $\mathcal{J}_i = (\alpha_i, \alpha_{i+1})$ we compute the numbers $r_i^{+\infty}$ and $\ell_{i+1}^{+\infty}$.
If α_i is not a root of c_{d_y}, $\ell_i^{+\infty} = r_i^{+\infty} = 0$.
The situation at $-\infty$ is entirely similar and we just compute $r_i^{-\infty}$ and $\ell_{i+1}^{-\infty}$.
This can be done in $\tilde{O}(d^5\tau + d^6)$ bit-operations.

Dealing with vertical asymptotes

$X = \alpha$ is a vertical asymptote *iff* $\deg(\tilde{P}(\alpha, Y)) < d_y = \deg_Y(\tilde{P}(X, Y)$, so $c_{d_Y}(\alpha) = D(\alpha) = 0$.
Let

$$\beta_{+\infty} \in \mathbb{N} \mid \beta_{+\infty} \geq |\alpha|, \forall \alpha \in V_{\mathbb{R}}(\tilde{P}(\alpha, Y))$$

We isolate the real roots of $\tilde{P}(X, \beta_{+\infty}) = 0$, and on each interval $\mathcal{J}_i = (\alpha_i, \alpha_{i+1})$ we compute the numbers $r_i^{+\infty}$ and $\ell_{i+1}^{+\infty}$.
If α_i is not a root of c_{d_y}, $\ell_i^{+\infty} = r_i^{+\infty} = 0$.
The situation at $-\infty$ is entirely similar and we just compute $r_i^{-\infty}$ and $\ell_{i+1}^{-\infty}$.
This can be done in $\tilde{O}(d^5\tau + d^6)$ bit-operations.

Topology of $\mathcal{C}(\tilde{P})$

The graph $\mathrm{Gr}(\tilde{P})$ of $\mathcal{C}(\tilde{P})$ is encoded by the finite list

$$\tilde{\mathcal{L}}(\tilde{P}) = [N_0, L_1, \ldots, L_\delta, N_\delta]$$

where

- $L_i = [\delta_i, [\ell_{i,j}, r_{i,j}], 1 \leq j \leq \delta_i]$ for $i = 1, \ldots, \delta$,
- $N_i = [m_i, [r_i^{-\infty}, r_i^{+\infty}], [\ell_{i+1}^{-\infty}, \ell_{i+1}^{+\infty}]$ for $i = 1, \ldots, \delta - 1$,
- $N_0 = [m_0, [\ell_1^{-\infty}, \ell_1^{+\infty}]]$, $N_\delta = [m_\delta, [r_\delta^{-\infty}, r_\delta^{+\infty}]]$.

Adding back vertical lines

$C(X) = \gcd(C_i(X), 1 \leq i \leq d_y)$.
Noting $C^\star(X)$ the square free part of $C(X)$, we set:

- $c_1(X) := \gcd\ (C^\star(X), D_X(X))$ and $c_2(X) :=$quo$(C^\star(X), c_1(X))$,
- $\mathcal{V}_1 := \{(x, y) \in \mathbb{R}^2 | c_1(x) = 0\}$ and $\mathcal{V}_2 := \{(x, y) \in \mathbb{R}^2 | c_2(x) = 0\}$.

Proposition

Adding back the lines in $\mathcal{V}_1$ and $\mathcal{V}_2$ to $\mathcal{C}(\tilde{P})$ has a bit complexity in $\tilde{O}(d^5\tau + d^6)$.

Final topology

The final topology of $\mathcal{C}(P)$ is given by the finite list

$$\mathcal{L}(P) = [N'_0, L'_1, \ldots, L'_\delta, N'_\delta]$$

where

- $L'_i = [\delta_i, w_i, [\ell_{i,j}, r_{i,j}], 1 \leq j \leq \delta_i]$ for $i = 1, \ldots, \delta$,
- $N'_i = [m_i, v_i, [r_i^{-\infty}, r_i^{+\infty}], [\ell_{i+1}^{-\infty}, \ell_{i+1}^{+\infty}]$ for $i = 1, \ldots, \delta - 1$,
- $N'_0 = [m_0, v_0, [\ell_1^{-\infty}, \ell_1^{+\infty}]]$, $N'_\delta = [m_\delta, v_\delta, [r_\delta^{-\infty}, r_\delta^{+\infty}]]$,

$$\mathrm{Gr}(P) = \mathrm{Gr}(\tilde{P}) \cup \bigcup_{\substack{i=1,\ldots,\delta \\ w_i=1}} V_i \cup \bigcup_{\substack{i=0,\ldots,\delta \\ \ell=1,\ldots,v_i}} V_{i,\ell}$$

Part 2: Projection of an analytic surface

Problem

Joint work: G. Moroz, M. Pouget and S. Diatta

Let

$$\mathcal{S}_{P\cap Q} := \{(x,y,z,t) \in \mathbb{R}^4 | P(x,y,z,t) = Q(x,y,z,t) = 0\}$$

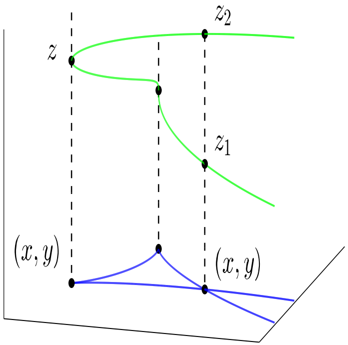
We focus on the problem to describe its projection $\mathcal{S} \subset \mathbb{R}^3$.

Smooth and algebraic surfaces

- Isotopic Implicit Surface Meshing [J.-D. Boissonnat, D. Cohen-Steiner, and G. Vegter, 2008].
- An efficient algorithm for the stratification and triangulation of an algebraic surface [E. Berberich, M. Kerber, and M. Sagraloff, 2009].
- On the isotopic meshing of an algebraic implicit surface [D. N. Diatta, B. Mourrain, and O. Ruatta, 2012].

Projection of analytic curves

- Numeric and Certified Isolation of the Singularities of the Projection of the a smooth Space Curve [R. Imbach, G. Moroz and M. Pouget, 2015]



- singularities of silhouette are isotopic to $x^2 \pm y^{k+1} = 0$
- $(x, y) \in A_1^- \cup A_2^- \Leftrightarrow \ \exists! \ (c, r) \mid S_{\mathcal{B}}(x, y, c, r) = 0$
- Certified drawing with interval arithmetic.

Approach

- Identify the types of singularities that can occur.
- Associate a regular system to each type of singularity ($\tilde{S_{\mathcal{B}}}$).
- Certified drawing using the Newton interval approach.
- Isotopic triangulation to $\mathcal{S}$.
- Implementation of the algorithm.