

Complexite de l'arrangement d'une famille de courbes algébriques planes I et II

basé sur un projet d'article de

Daouda Niang Diatta, Université de Ziguinchor, Sénégal

Sény Diatta, Université de Ziguinchor, Sénégal

Marie-Françoise Roy, IRMAR, Université de Rennes

JGA Roscoff - le 14 octobre 2025

The problem

Compute the arrangement of a finite set of real algebraic plane curves

Input: $P_1, \dots, P_s \in \mathbb{Z}[X, Y]$ (no multiple factor)

Output : a planar graph isotopic to

$\mathcal{Z}(P) := \{(x, y) \in \mathbb{R}^2, P(x, y) = 0\}$, with $P = \prod_{k=1}^s P_k$

by an **exact algorithm of best possible complexity** in terms of the bounded degree d of each P_k and the bounded bitsize τ of their coefficients.

Notation $\tilde{O}$: logarithmic factors in d and τ are not taken into account

Our result

$$\tilde{O}(s^2(d^5\tau + d^6)).$$

Computations made in the initial coordinate system.

Previous results

Compute the arrangement of a finite set of real algebraic plane curves

Best previous result (Ph D of Michael Kerber [1])

$$\tilde{O}(s^2 d^{10} (d + \tau)^2).$$

Basic idea: combinatorial complexity in s^2 (consider two curves together only) + complexity of computation for one curve.

Technical difficulties due to the fact that it is needed to make a change of coordinates.

The base case

Compute the topology of one real algebraic curve

Very classical problem in algorithmic real algebraic geometry

Input: $P \in \mathbb{Z}[X, Y]$ (no multiple factor)

Output : a piecewise linear planar graph isotopic to

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

by an **exact algorithm of best possible complexity** in terms of the bounded degree d of P and the bounded bitzsize τ of its coefficients.

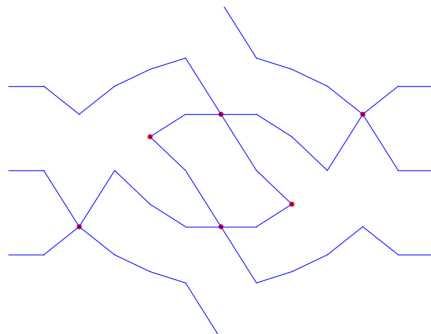
Our result [2]

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

Computations made in the initial coordinate system.

The base case

$$P(X, Y) = (XY - 1)(4Y^2 - 4X - 1)(4Y^2 + 4X - 1),$$



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

Real root isolation on a line

Proposition

Let $R_1, \dots, R_\ell \in \mathbb{Z}[X]$ be non-zero polynomials of magnitude (n, μ) and denote by $Z \subset \mathbb{R}$ the union of the zeroes of the polynomials $R_1, \dots, R_\ell$. Using $\tilde{O}(\ell(n^2\mu + n^3))$ bit operations, one can compute

- (a) for every $x \in Z$, an isolating interval $\mathcal{I}_x = (a_x, b_x) \subset \mathbb{R}$, where a_x and b_x are dyadic numbers,
- (b) for every $x \in Z$, the list of polynomials among $R_1, \dots, R_\ell$ that vanish at x .

Outline proof (a)

Let $\sigma_{i,j}$ be the separator of $R_i \times R_j$, and $\sigma = \min_{i,j}(\sigma_{i,j})$. It is clear that σ is a separator for the set Z . Note that $R_i \times R_j$ is of magnitude $(2n, 2\mu)$ and σ is estimated by $2^{-\tilde{O}(n\mu)}$ (see [3,4]), independent of ℓ .

Refining the isolation intervals of the roots of each R_i up to $\frac{\sigma}{2}$ costs $\tilde{O}(n^3 + n^2\mu)$.

Then, for ℓ polynomials, the total complexity for refining all isolating intervals up to σ is $\tilde{O}(\ell(n^3 + n^2\mu))$.

Outline proof (b)

Since every isolating interval of a point $x \in Z$ is of length less than $\frac{\sigma}{2}$, then the polynomials vanishing at x are those for which one of their isolating interval intersect $\mathcal{I}_x$.

So in case two isolating intervals intersect, and the polynomials have a common root, we simply forget one of them to get the final list of isolating intervals.

Topology of a pair of curves

We now focus on the problem of computing a curve defined by the product of square-free bivariate polynomials. More precisely, the following result is an arrangement of two real curves.

Theorem (Arrangement of two curves)

Let $P_1, P_2 \in \mathbb{Z}[X, Y]$ be two square-free polynomials of magnitudes bounded by (d, τ) . Using a number of bit operations bounded by $\tilde{O}(d^5\tau + d^6)$ one can identify the subset of curve segments and vertices of $\mathcal{Z}(P_1)$ and $\mathcal{Z}(P_2)$ in the planar graph of $\mathcal{Z}(P_1 \times P_2) = \mathcal{Z}(P_1) \cup \mathcal{Z}(P_2)$.

Remark and notations

Note that the graph of $\mathcal{Z}(P_1)$ and the graph of $\mathcal{Z}(P_2)$ can have common curve segments and in this case, $P_1 \times P_2$ is not square-free so that our algorithm in [2] cannot be used directly.

Notations:

Let P_1, P_2 be two polynomials of $\mathbb{Z}[X, Y]$. We set:

$$P_{1 \wedge 2} := \gcd(P_1, P_2), P_{1 \vee 2} := \text{LCM}(P_1, P_2) = \frac{P_1 \times P_2}{P_{1 \wedge 2}}$$

$$\text{and } P_{2 \setminus 1} = \frac{P_2}{P_{1 \wedge 2}}$$

Note that

$$\mathcal{Z}(P_1) \cup \mathcal{Z}(P_{2 \setminus 1}) = \mathcal{Z}(P_1 \times P_2) = \mathcal{Z}(P_{1 \vee 2}),$$

and that $\mathcal{Z}(P_1)$, and $\mathcal{Z}(P_{2 \setminus 1})$ have no edge in common.

Remark and notations

We set $D = \text{Disc}(P_{1 \vee 2})$ as the discriminant of $P_{1 \vee 2}$ with respect the variable Y , and note that

$$D = \text{Disc}(P_{1 \vee 2}) \quad (1)$$

let N the number of real roots of D , denoted by $\alpha_1 < \alpha_2 < \dots < \alpha_N$. We define the square-free part D^* of D

$$D^* = \frac{D}{\gcd(D, D')}$$

and consider its derivative $D^{*'}.$ For each $i = 1, \dots, N - 1$, there are roots of $D^{*'}$ in each interval (α_i, α_{i+1}) and we denote by α'_i the smallest root of $D^{*'}$ bigger than α_i .

Outline proof theorem

Lemma

Let $F_1, F_2 \in \mathbb{Z}[X, Y]$ be two bivariate polynomials of magnitude (d, τ) . Computing the gcd and the gcd free-parts of F_1 and F_2 uses $\tilde{O}(d^4\tau + d^5)$ bit operations.

According to this Lemma and our algorithm in [2], the computation of the graph of $\mathcal{Z}(P_{1 \vee 2})$, $\mathcal{Z}(P_1)$ and $\mathcal{Z}(P_2)$ can be done using $\tilde{O}(d^5\tau + d^6)$ bit operations.

Indeed, $P_{1 \vee 2}$, P_1 and P_2 have their magnitudes respectively bounded by $(2d, d + \tau)$, (d, τ) , (d, τ) .

Outline proof theorem

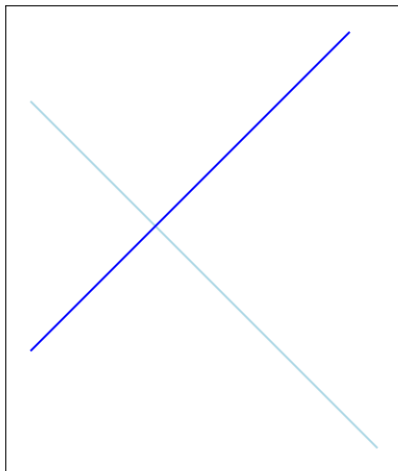
Moreover using [2] , we can output for each α_i which is a zero of D_1 :

- the set $\text{CRITIND}_\ell(1)$ of critical indices of P_1 in the singular fiber defined by α_i ;
- for every $i \in \text{CRITIND}_i(1)$ the number $\text{LEFT}_{i,j}(1)$ of the curve segments of $\mathcal{Z}(P_1)$ ending at $(\alpha_i, \beta_{i,j})$ to the left of α_i ;
- the number $\text{RIGHT}_{i,j}(1)$ of the curve segments of $\mathcal{Z}(P_1)$ ending at $(\alpha_i, \beta_{i,j})$ to the right of α_i .

This is sufficient to identify the graph of $\mathcal{Z}(P_1)$ in $\mathcal{Z}(P_{1 \vee 2})$.

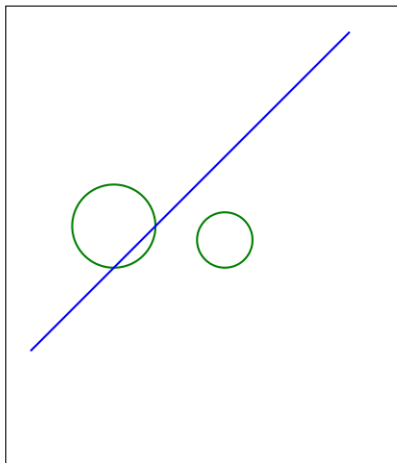
$\mathcal{Z}(P_1)$

$$P_1(X, Y) = (X + Y)(X - Y + 2)$$



$\mathcal{Z}(P_2)$

$$P_2(X, Y) = ((X+4)^2 + (Y-1)^2 - 9)((X-4)^2 + Y^2 - 4)(X - Y + 2)$$



Curves two by two

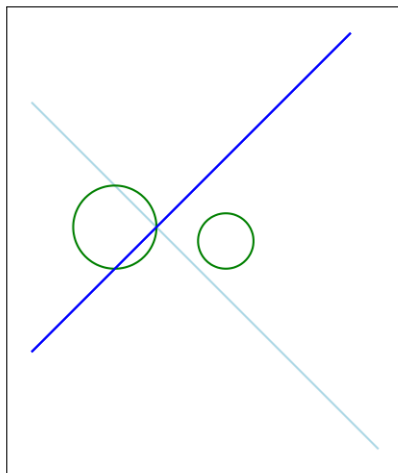


Figure: $\mathcal{Z}(P_1 P_2)$

La description des arrangements

On définit

- un nombre fini $\mathcal{V}$ de points événements de $\mathcal{Z}(P)$,
- un nombre fini $\mathcal{S}$ de segments de courbes sans points X -critiques (ou verticaux) ouverts aux extrémités, qui sont les composantes connexes de $\mathcal{Z}(P) \setminus \mathcal{V}$,
- un nombre fini $\mathcal{C}$ de cellules ouvertes qui sont les composantes connexes de $\mathbb{R}^2 \setminus \mathcal{Z}(P)$.

Chaque segment de $\mathcal{S}$ a deux extrémités dans $\mathcal{V}$ (ou une seule s'il est infini).

Bords orientés

Chaque segment $S \in \mathcal{S}$ a deux copies orientées, S^+ (resp. S^-) est orienté vers la droite (resp. la gauche). Sauf si S est vertical et S^+ (resp. S^-) est orienté vers le haut (resp. le bas).

Le bord orienté de C , $\text{bo}(C)$, est composé de segments orientés et de leurs extrémités : si $S \in \bar{C}$, S^+ (resp. S^-) est dans $\text{bo}(C)$ si C est au dessus (resp. au dessous) de S quand on décrit S vers la droite. Si $S \in \bar{C}$ est vertical, S^+ (resp. S^-) est dans $\text{bo}(C)$ si C est à gauche (resp. à droite) de S quand on décrit S de bas en haut.

Arrangements de droites en position générale

Soient $L_1, \dots, L_s$ des équations affines et $L = L_1 \times \dots \times L_s$ en position générale (pas de répétition, pas de droites parallèles, pas trois droites passant par le même point).

- les événements de $\mathcal{V}$ sont les intersections deux à deux,
- $\mathcal{S}$ est formé des segments de $\mathcal{Z}(L) \setminus \mathcal{V}$,
- $\mathcal{C}$ est formé des composantes connexes de $\mathbb{R}^2 \setminus \mathcal{Z}(L)$,
- chaque segment de $\mathcal{S}$ appartient à une seule droite,
- entre deux événements de $\mathcal{V}$ il y a un seul segment,
- chaque cellule de $\mathcal{C}$ est contractible, et son bord est connexe, le bord orienté est décrit dans le sens trigonométrique,
- chaque cellule de $\mathcal{C}$ est définie par une condition de signe stricte sur la famille $L_1, \dots, L_s$.

Arrangements de droites

- $\#\mathcal{V} = s(s-1)/2 = O(s^2)$,
- $\#\mathcal{S} = O(s^2)$ se montre par récurrence car si on nomme $f(s)$ le nombre de segments avec s droites

$$f(s) = f(s-1) + s - 1 + s,$$

car il y a un nouveau segment pour chaque ancienne droite et s nouveaux segments sur la nouvelle droite,

- $\#\mathcal{C} = O(s^2)$ puisque le nombre de segments orienté est $O(s^2)$ et chaque segment orienté appartient au bord d'une seule cellule.

Si plus de deux droites passent par un point d'intersection, ou s'il y a des droites parallèles, le nombre de segments et de cellules diminue.

Arrangements de courbes algébriques

- les événements de $\mathcal{V}$ sont les intersections deux à deux, et les points X -critiques des différentes courbes
- $\mathcal{S}$ est formé des segments de $\mathcal{Z}(P) \setminus \mathcal{V}$,
- $\mathcal{C}$ est formé des composantes connexes de $\mathbb{R}^2 \setminus \mathcal{Z}(P)$,
- un segment de $\mathcal{S}$ peut appartenir à plusieurs courbes,
- entre deux événements de $\mathcal{V}$ il peut y avoir plusieurs segments,
- il peut y avoir des cellules de $\mathcal{C}$ qui ne sont pas contractibles, ou même dont le bord n'est pas connexe, certaines composantes connexes du bord orienté peuvent ne pas être dans le sens trigonométrique,
- la réalisation d'une condition de signe stricte sur la famille $P_1, \dots, P_s$ peut être formée de plusieurs cellules.

Exemple d'arrangement de courbes algébriques

① $P_1(X, Y) = (X + Y)(X - Y + 2)$

② $P_2(X, Y) =$
 $((X + 4)^2 + (Y - 1)^2 - 9)((X - 4)^2 + Y^2 - 4)(X - Y + 2)$

③ $P_3(X, Y) = ((X + 3)^2 + (Y - 2)^2)((X - 3)^2 + Y^2 - 1)$

④ $P_4(X, Y) = X((X - 10)(Y - 10)^2 - 5)$

⑤ $P_5(X, Y) = (X - 5)^2 + Y^2 - 9$

P_1 et P_2 ont une droite en commun $Y = X + 2$ et P_4 a une ligne verticale $X = 0$ et une asymptote verticale $X = 10$.

Exemple d'arrangement de courbes algébriques

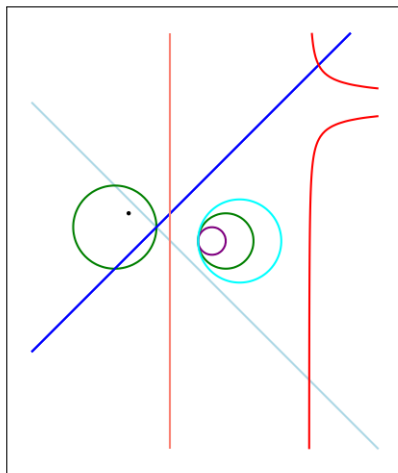


Figure: $\mathcal{Z}(P)$

Exemple d'arrangement de courbes algébriques

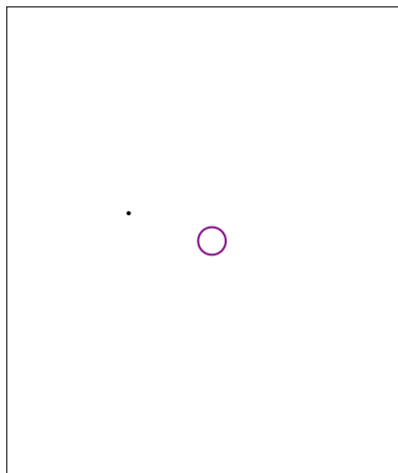


Figure: $\mathcal{Z}(P_3)$, un cercle et un point isolé

Exemple d'arrangement de courbes algébriques

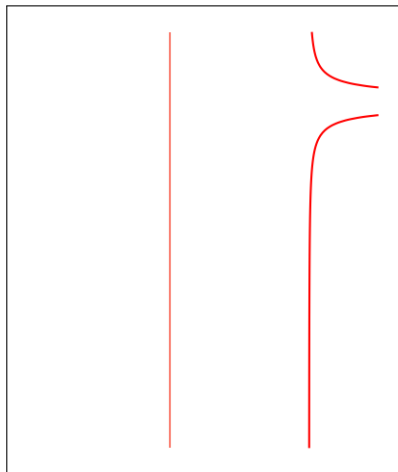


Figure: $\mathcal{Z}(P_4)$, une droite verticale et une asymptote

Exemple d'arrangement de courbes algébriques

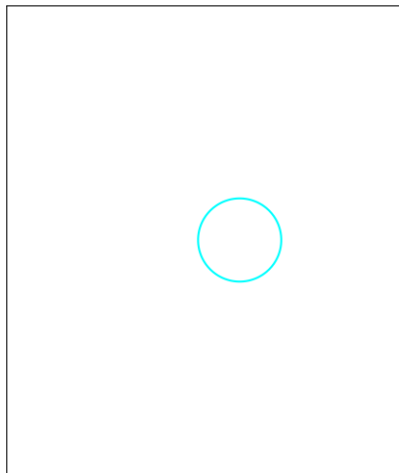


Figure: $\mathcal{Z}(P_5)$, un cercle en plus

Arrangements de courbes algébriques

- $\#\mathcal{V} = O(s^2 d^2)$, par Bezout,
- $\#\mathcal{S} = O(s^2 d^2)$ peut se démontrer en utilisant la caractéristique d'Euler-Poincaré,
- $\#\mathcal{C} = O(s^2 d^2)$ puisque le nombre de segments orienté est $O(s^2 d^2)$ et chaque segment orienté appartient au bord d'une seule cellule.

Caractéristique d'Euler Poincaré

Si $\mathcal{V}(P)$ n'est pas compact, rajouter des points "à l'infini" pour qu'un segment ait toujours deux extrémités.

Définir b_0 le nombre de composantes connexes et b_1 le nombre de boucles (loops) dans un ensemble compact composé d'un nombre fini de points et de segments.

$$b_0 - b_1 = \#V - \#S.$$

Par récurrence sur le nombre de segments. Au départ

$$b_0 = \#V, b_1 = \#S = 0.$$

Rajouter un segment

- si ses extrémités sont dans deux composantes connexes distinctes, b_0 baisse de 1 et b_1 ne change pas.
- sinon b_0 ne change pas et b_1 augmente de 1.

$b_0 + b_1 = 0(s^2 d^2)$ (un peu de théorie de Morse). Si $b_0, b_1, \#V$ sont $0(s^2 d^2)$, $\#S = 0(s^2 d^2)$.

Principe du calcul de l'arrangement

Le calcul de l'arrangement se fait en déplaçant une droite verticale de gauche à droite et en notant les changements dans les segments et les cellules à chaque point événement.

Si deux événements ont la même projection sur l'axe des X , on procède de bas en haut dans la fibre.

On veut conserver la complexité quadratique en s , correspondant au nombres de points, segments et cellules.

Différence avec la CAD

Pour la CAD, même dans le cas des droites le nombre de cellules est $O(s^3)$.

Il y a des points, des segments et des cellules en plus !

Illustration avec trois droites.

Calcul des X -coordonnées des points de $\mathcal{V}$

On isole les racines d'une famille $\mathcal{R}$ de polynômes en une variable, formée de discriminants (X -coordonnées des points critiques d'une courbe) et de résultants: (X -coordonnées des points d'intersection des courbes deux à deux). Attention il peut y avoir des morceaux de courbes en commun, donc un résultant nul.

$$P_{i \wedge j} := \gcd(P_i, P_j), P_{j \setminus i} = \frac{P_j}{P_{i \wedge j}}$$

- $R_{ij} = \text{Res}(P_i, P_{j \setminus i})$,
- $D_i = \text{Disc}(Q_i)$, (Q_i est P_i débarrassé de ses droites verticales)
- V_i in $\mathbb{Z}[X]$ (droites verticales retirées de P_i),
- $L_i = (Q_i)$, in $\mathbb{Z}[X]$ (asymptotes verticales)

Calcul des X - coordonnées des événements de $\mathcal{V}$

Dans notre exemple $\mathcal{R}$ consiste en

$D_1, D_2, D_3, D_4, D_5, V_4, L_4, R_{12}, R_{14}, R_{23}, R_{25}, R_{35}$, et a 12 racines réelles et on considère

- $x_0 = -15$, plus petite que toutes les racines des polynômes de $\mathcal{R}$
- ...
- $x_4 = -1$, racine de D_1, D_2, R_{12} ,
- ...
- $x_6 = 2$, racine de $D_2, D_3, D_5, R_{23}, R_{25}, R_{35}$,
- $x_7 = 4$, racine de D_3 ,
- ...

Courbes deux à deux

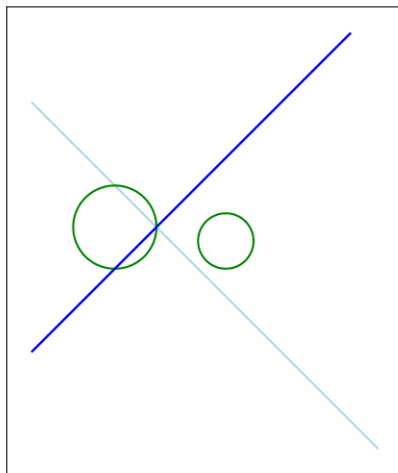


Figure: $\mathcal{Z}(P_1 P_2)$

Aux points de $\mathcal{V}$

Dans l'exemple on a les éléments suivants dans $\mathcal{V}$

- au dessus de x_0 il y a deux événements
 - 1 $v_{0,1}$ crée un segment de P_1 avec P_2 , deux cellules sont créées
 - 2 $v_{0,2}$ crée un segment de P_1 , une nouvelle cellule est créée.
- ...
- au dessus de x_4 , l'événement v_4 est un point spécial: un point d'intersection où P_1 et P_2 s'annulent (mais aussi un point singulier de P_1 et un point critique de P_2), il y a quatre segments se terminant à v_4 , dans l'ordre P_2, P_1 avec P_2, P_1, P_2 et deux segments de courbe commençant à v_4 , le segment de P_1 est sous le segment de P_1 avec P_2 . Trois cellules se ferment et une cellule s'ouvre.
- ...

Calcul des X - coordonnées des points de $\mathcal{V}$

- $x_0 = -15$, plus petite que toutes les racines des polynômes de $\mathcal{R}$
- ...
- $x_4 = -1$, racine de D_1, D_2, R_{12} ,
- ...
- $x_6 = 2$, racine de $D_2, D_3, D_5, R_{23}, R_{25}, R_{35}$,
- $x_7 = 4$, racine de D_3 ,
- ...

Courbes deux à deux

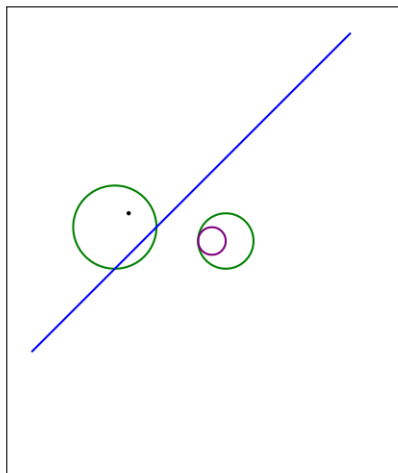


Figure: $\mathcal{Z}(P_2P_3)$

Courbes deux à deux

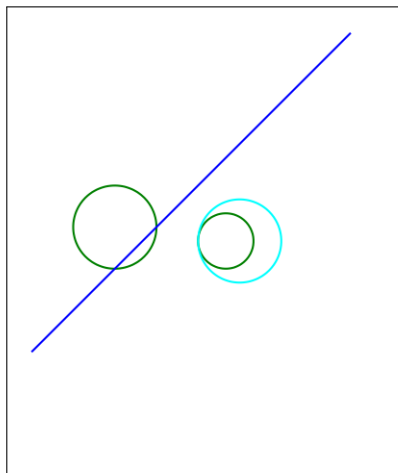


Figure: $\mathcal{Z}(P_2P_5)$

Aux points de $\mathcal{V}$

- ...
- au dessus de x_6 , l'événement v_6 est spécial puisque c'est un point X -critique de P_2 , P_3 et P_5 , il n'y a pas de segment de courbe finissant à v_6 et 6 segments de courbe commençant à v_6 , l'événement v_6 est entre les segments de courbe de P_1 et de P_1 avec P_2 , les six nouveaux segments sont des zeros de $P_5, P_2, P_3, P_3, P_2, P_5$. Cinq nouvelles cellules sont créées.
- au dessus de x_7 , l'événement v_7 est un point critique de P_3 , il y a deux segments de courbe finissant à v_7 et aucun segment de courbe commençant à v_7 , l'événement v_7 est entre les segment de courbe de P_2 créés en v_6 . Une cellule se ferme. Deux cellules fusionnent.

Analyse de complexité

Il faut donner des algorithmes détaillés pour les terminaisons, création de segments de courbes et les les terminaisons, créations ou fusions de cellules, et pour la description du bord de chaque cellule aux événements de V .

L'exemple doit vous avoir convaincu.e que c'est possible.

Calculs de $\mathcal{R}$ et isolation de ses racines les discriminants et résultants sont de degré $O(d^2)$ et de taille $d(\tau + d)$

$$\tilde{O}(s^2(d^5\tau + d^6)).$$

Détermination des changements aux éléments de $\mathcal{V}$: l'examen de la topologie des courbes deux à deux suffit :

$$\tilde{O}(s^2(d^5\tau + d^6)).$$

Analyse de complexité

Il faut faire attention à la gestion des informations. Pour chaque valeur considérée sur l'axe des X , on crée une pile qui décrit la fibre. Si on garde en mémoire toutes ces fibres, l'information est de taille $O(s^3 d^3)$.

Dans le cas linéaire, on modifie localement la fibre aux point de croisement en transposant deux éléments successifs comme dans [5].

Dans le cas algébrique, il n'y a pas que des croisements, il y a aussi des apparitions de segments aux points critiques ... Sans parler des situations où plus de deux courbes se rencontrent ...

- [1] M. Kerber, Geometric Algorithms for Algebraic Curves and Surfaces, PhD, Universität des Saarlandes, Saarbrücken, 2009.
- [2] D. Niang Diatta, S. Diatta, F. Rouillier, M.-F. Roy, M. Sagraloff, Bounds for polynomials on algebraic numbers and application to curve topology, Discrete and Computational Geometry, 67, 631-697, 2022,
- [3] M. Mignotte, Mathematics for Computer Algebra, Springer-Verlag, 1992.
- S. Basu and R. Pollack and M.-F. Roy, Algorithms in real algebraic geometry, Springer-Verlag, 2016, <https://mariefrancoiseroy.pages.math.cnrs.fr/bpr-ed2-posted3v2.html>,
- [5] J. L. Bentley, T. A. Ottmann, "Algorithms for reporting and counting geometric intersections", IEEE Transactions on Computers, C-28 (9): 643–647, (1979)