Topologie de courbes algébriques planes et projection de surfaces analytiques réelles.

Seny Diatta

UNIVERSITÉ ASSANE SECK DE ZIGUINCHOR

UFR SCIENCES ET TECHNOLOGIES
DÉPARTEMENT DE MATHÉMATIQUES

THÈSE

DOMAINE : SCIENCES ET TECHNOLOGIES
MENTION : MATHÉMATIQUES ET APPLICATIONS
SPÉCIALITÉ : MATHÉMATIQUES APPLIQUÉES
OPTION : CALCUL FORMEL

PRESENTÉ PAR :
Sény DIATTA

pour obtenir le grade de
DOCTEUR DE L'UNIVERSITÉ ASSANE SECK DE ZIGUINCHOR

Sujet de thèse :

Topologie de courbes algébriques planes et projection de surfaces analytiques réelles

Jury

Directeurs :	**MC. Daouda Niang Diatta**	UASZ, Sénégal
	CR. Guillaume Moroz	INRIA-Loria Nancy, France
	Pr. Marie-Françoise Roy	Université Rennes 1, France
Président :	**Pr. Oumar Sall**	UASZ, Sénégal
Rapporteurs :	**Pr. Nicolas Delanoue**	LARIS Université d'Angers, France
	Pr. M'hammed El Kahoui	Cadi Ayyad University, Maroc
	Pr. Djiby Sow	UCAD, Sénégal
Examinateur :	**Pr. Salomon Sambou**	UASZ, Sénégal
Date de soutenance :	LE 8 JANVIER 2020	À L'UASZ, SÉNÉGAL

THÈSE PRÉPARÉE DANS LE LABORATOIRE DE MATHÉMATIQUES ET APPLICATIONS (LMA) DE L'UNITÉ DE FORMATION ET DE RECHERCHE (UFR)
SCIENCES ET TECHNOLOGIES DE L'UNIVERSITÉ ASSANE SECK DE ZIGUINCHOR
BP : 523-ZIGUINCHOR-SENEGAL

Topologie de courbes algébriques planes et projection de surfaces analytiques réelles

Résumé.

Cette thèse traite de la représentation topologique d'objets géométriques définis de façon implicite. La résolution de ce type de problème relève du domaine de la **géométrie algorithmique**. Soit $V_{\mathbb{R}}(P)$ une courbe algébrique réelle plane définie comme étant le lieu des zéros d'un polynôme sans facteur carré $P \in \mathbb{Z}[X,Y]$ de magnitude (d,τ). Le premier résultat principal présenté dans ce manuscrit est un algorithme qui calcule un complexe simplicial isotope à $V_{\mathbb{R}}(P)$ sans passer par une mise en position générique de $V_{\mathbb{R}}(P)$ avec seulement $\tilde{O}(d^5\tau + d^6)$ opérations binaires. Il constitue une alternative à l'algorithme de Mehlhorn et al. [33], dont le succès repose sur un processus aléatoire de détermination d'une position générique de $V_{\mathbb{R}}(P)$. La deuxième contribution principale de cette thèse est un algorithme permettant de calculer le graphe des singularités d'une surface analytique réelle $\Omega \subset \mathbb{R}^3$: étant donnée une surface analytique réelle lisse $\mathscr{M}$ définie comme une intersection de deux hypersurfaces réelles dans $\mathbb{R}^4$, la surface Ω est l'image de $\mathscr{M}$ par la projection canonique de $\mathbb{R}^4$ dans $\mathbb{R}^3$. La surface Ω comporte, en général, des singularités. Le calcul du graphe des singularités apparait donc comme un problème sous-jacent dans l'étape de la reconstruction de la topologie globale de Ω.

Mots-clés : Bornes amorties sur les nombres algébriques, Calcul Effectif de la Topologie d'une courbe, Complexité, Projection d'une Surface Analytique Réelle, Graphe des singularités.

Topology of real algebraic curves and projection of real analytic surfaces

Abstract.

The topic of this thesis is related to algorithmic geometry. We focus on the problem to built algorithms that give a representation of the topology for geometric sets defined implicitly. We got two main results : The fisrt one deals with the real algebraic curve. Given a real plan algebraic curve $V_{\mathbb{R}}(P)$ defined as the zero set of a square free polynomial $P \in \mathbb{Z}[X,Y]$ of magnitude (d,τ), our algorithm computes straight planar graph isotopic to $V_{\mathbb{R}}(P)$ using only $\tilde{O}(d^5\tau + d^6)$ bit operations and without putting the curve in generic position. Note that, Mehlhorn et al. [33] deal with the same problem, but their algorithm start by a random process to get a generic position of the curve. The second main result of this thesis is an algorithm that computes the graph of singularites of a real analytic surface $\Omega \subset \mathbb{R}^3$. Let $\mathscr{M}$ be a surface in $\mathbb{R}^4$ defined as the intersection of two hypersurfaces, Ω is then defined as the image of $\mathscr{M}$ by the canonical projection from $\mathbb{R}^4$ to $\mathbb{R}^3$. Usually, the surface Ω is not smooth. We give an algorithm that computes a graph isotopic to the set of singularities of Ω, which is required to reconstruct the whole topology of Ω.

Keys-words : Amortized bounds on algebraic numbers, Real Algebraic curves, Exact Topology Computation, Complexity, projection of Real analytic surfaces, Graph of singularities..

Remerciements

Tout d'abord, je tiens à remercier mes directeurs de thèse pour la confiance et le soutien indéfectible qu'ils n'ont cessé de me manifester afin que cette thèse se déroule dans de bonnes conditions : **Daouda Niang DIATTA, Guillaume Moroz, Marie Salomon SAMBOU et Marie Françoise ROY**.

Je remercie également le Personnel Administratif (PA) de même que le Personnel d'Enseignement et de Recherche (PER) de l'université Assane Seck de Ziguinchor (UASZ) pour avoir toujours oeuvré pour la bon fonctionnement de cette institution.

J'adresse mes remerciements aux responsables du projet **Non-Linear Analysis, Geometry and Applications** (NLAGA) qui, à travers la Fondation SIMONS, ont financé cette thèse. Je remercie, tout particulièrement, les membres du projet NLAGA de l'UASZ pour les moments d'échanges et partages scientifiques entretenus lors des séminaires hebdomadaires.

Le **Fields Institute** de Toronto et l'**IRMAR** de Rennes ne dérogent pas à mes remerciements pour avoir d'une part facilité mon séjour dans leurs laboratoires respectifs. Et d'autre part pour la qualité de la logistique et de la documentation mis à notre disposition. Ce qui a contribué à rendre notre visite très profitable en terme d'acquisition de connaissances nouvelles et de rencontres scientifiques.

Je remercie sincèrement les membres de l'équipe **GAMBLE** du laboratoire INRIA-Loria de Nancy Grand Est pour cette expérience, jusque là unique, dans mon cursus. Je garde toujours à l'esprit cet environnement de travail assez exceptionnel, bâti sous la fondation de la convivialité et de la rigueur scientifique. J'adresse une mention spéciale à mes amis et collègues : **Iordan Iordanov, Charles Dumenil, Eric Biagioli, Georges Krait, Babacar Ben CISSÉ, Mamadou Diogo DIALLO, Mamadou Dian Diallo, Winnie Ossete Ingoba et Souhaibou Sambou**.

Je profite de l'occasion pour exprimer toute ma gratitude à Monsieur **Landing DIÉMÉ** qui, dès le lycée a très tôt cru à mon potentiel intellectuel et scientifique. La confiance et l'assistance que tu m'as accordé ont fini d'installer en moi du courage et de l'abnégation dont le fruit des efforts est synthétisé dans ce rendu qui retrace plus de quatre années de recherches, d'enseignements, d'échanges et de découvertes scientifiques.

Je remercie très chaleureusement mes parents, mes frères et soeurs pour leur soutien infaillible et leurs prières qui ont accompagné toutes ces années d'étude et de recherche.

Enfin, je dédie ce travail à la jeunesse estudiantine du Sénégal qui, dans le soucis quotidien d'être actrice à la reconstruction et au développement de notre cher pays le Sénégal, surmonte des conditions de travail assez précaires. A cette jeunesse, je lui souhaite de retrouver sa voie, qui est celle de ***l'émancipation.***

Table des matières

Introduction

Les questions soulevées dans cette thèse relèvent respectivement des domaines de la géométrie algorithmique et du calcul formel. Il s'agit d'élaborer des algorithmes permettant de calculer une représentation topologiquement correcte d'un objet géométrique défini de façon implicite. L'intérêt suscité par ces problématiques réside à travers les nombreuses applications qui en découlent : nous pouvons citer entre autres le graphisme, la robotique, les conceptions assistées par ordinateurs, la visualisation, etc.

Dans le cas d'une courbe algébrique plane, définie comme étant le lieu des zéros réels d'un polynôme bivarié à coefficients entiers, sans facteur carré et de magnitude (d, τ), calculer sa topologie revient à trouver une structure linéaire par morceaux qui lui est isotope. Le record en terme de complexité, dans ce contexte, est détenu par Mehlhorn et al. [33], qui est de l'ordre de $(d^5\tau + d^6)$ opérations binaires. Toutefois, leur algorithme requiert une mise en position générique de la courbe dont le calcul dépend d'un processus aléatoire. C'est en ce sens que nous proposons un algorithme efficace ayant la même complexité et qui a la particularité d'être effective indépendamment du caractère générique relative à la position de la courbe. Ce qui a pour avantage de faciliter son implémentation sur un ordinateur comparé à celui de Mehlhorn et al. [33]. Notre algorithme, présenté dans Diatta et al. [10], résulte d'un travail collaboratif avec une équipe de chercheurs constituée de D. N. Diatta [1], S. Diatta [2], F. Rouillier [3], M-F. Roy [4] et M. Sagraloff [5].

Le second problème étudié dans cette thèse traite de la représentation topologique de l'image par projection d'une surface analytique réelle lisse de $\mathbb{R}^4$ dans $\mathbb{R}^3$. Il s'agit plus précisément d'un algorithme qui calcule le graphe des singularités de l'image de la surface par cette projection, s'il existe. En effet, lorsque l'image dans $\mathbb{R}^3$ est une surface lisse, alors le graphe est inexistant. Toutefois, il convient de souligner que, le cas de la projection d'une courbe de l'espace $(\mathbb{R}^3)$ dans le plan $(\mathbb{R}^2)$ a été investi par Imbach et al. [21]. Dès lors, il devient donc naturel de s'interroger sur la possibilité de généraliser leur algorithme pour des objets géométriques vivant dans des espaces de dimensions plus grandes. Ainsi, après avoir identifié les différents types de singularités, nous avons proposé un algorithme qui calcule un graphe isotope à la partie singulière de l'image de la surface implicite dans $\mathbb{R}^3$. Les résultats obtenus dans cette deuxième partie émanent de plusieurs séances de travail avec G. Moroz [6] et M. Pouget [7] et ont fait l'objet d'un article publié dans Mathematical Aspects of Computer and Information Sciences (MACIS [8] 2019).

Structure de la thèse. Le plan de ce manuscrit est réparti comme suit :

- **La Première Partie** traite du calcul effectif de la topologie d'une courbe algébrique plane. Elle regroupe les Chapitres 1, 2 et 3.
- **La Deuxième Partie** est dédiée à la projection de surfaces analytiques réelles. Elle est consti-

1. Université Assane Seck de Ziguinchor, Senegal
2. Université Assane Seck de Ziguinchor, Senegal
3. INRIA Paris, IMJ-PRG - Sorbonne Universités, France
4. IRMAR, Université de Rennes I, Campus de Beaulieu, 35042 Rennes CEDEX, France, 33(0)223236020
5. HAW Landshut, Max-Planck-Institut für Informatik, Saarbrücken, Germany
6. INRIA-LORIA, Nancy, France, guillaume.moroz@inria.fr
7. INRIA-LORIA, Nancy, France, marc.pouget@inria.fr
8. http ://macis2019.gtu.edu.tr

tuée des Chapitres 4 et 5.

Première Partie. Le chapitre 1 aborde les algorithmes d'isolation des racines d'un polynôme univarié. La première section constitue essentiellement des rappels sur les prérequis algébriques tels que *la mesure de Mahler, le discriminant, le séparateur et le résultant* d'un polynôme. Elle comporte aussi des résultats déjà connus, qui sont relatifs aux différentes notions citées ci-avant. La deuxième section traite tout particulièrement de l'algorithme d'isolation des racines d'un polynôme proposé par Mehlhorn et al. [33]. En effet, les auteurs détiennent à travers cet article la meilleure borne de complexité connue pour ce problème. L'efficacité de leur algorithme réside dans des techniques nouvelles qui y sont dévoloppées, tout en s'appuyant sur l'algorithme de factorisation de Pan [42] (voir sous-section 1.2.2).

Le chapitre 2 constitue notre contribution originale au problème soulevé dans cette première partie. Nous y traitons du calcul effectif de la topologie d'une courbe algébrique plane. Notre algorithme ne requiert pas une mise en position générique et il est effectif avec une complexité de $\tilde{O}(d^5\tau + d^6)$ opérations binaires. La section 2.1 revient en détails sur la technique utilisée pour calculer le degré d'un polynôme à coefficients algébriques. Ce travail préliminaire nous a permis d'appliquer une Décomposition Cylindrique Algébrique (DCA) efficace (voir section 2.4) de la courbe, tout en restant dans la complexité visée. On peut citer entre autres, le calcul des fibres critiques obtenues en isolant les racines d'un polynôme $P(\alpha, Y)$; où α est racine d'un polynôme univarié. Les détails du calcul effectif du graphe et de l'analyse de la complexité de notre algorithme sont présentés dans la section 2.5 : Il s'agit, tout d'abord, de calculer les boîtes d'isolation des points spéciaux (points singuliers et x-critiques de la courbe). Ensuite, de déterminer des boîtes adjacentes à ces points. Ces deux premières étapes permettent de reconstruire localement la topologie de la courbe autour des points spéciaux. Enfin, nous explicitons la démarche utilisée pour reconstruire la courbe toute entière grâce aux informations collectées précédemment.

Le chapitre 3 constitue une seconde contribution à l'étude quantitative de certains aspects des courbes algébriques. Plus exactement, il s'agit de deux résultats quantitatifs qui permettent d'apprécier la façon dont une courbe algébrique s'écarte de sa tangente verticale en un point x-critique. La section 3.1 est dédiée aux énoncés des théorèmes principaux ainsi que des illustrations à travers des exemples. La section 3.2 comporte des préliminaires utiles. La section 3.3 est dédiée à la démonstration des Théorèmes 3.1 et 3.2.

Deuxième Partie. Elle traite essentiellement de la représentation topologique de l'image, par la projection canonique, de courbes et surfaces analytiques réelles. L'étude des types de singularités (aussi appelées des multigermes) qui apparaissent dans ce contexte relève de la théorie des singularités. Le domaine fut investi en premier par Mather [32], suivi des travaux de Goryunov [19]. L'objectif final étant de faire appel à des méthodes numériques pour visualiser ces objets, nous introduisons dans le chapitre 4 des rappels sur la théorie des singularités et de quelques méthodes numériques.

Le chapitre 5 constitue notre troisième contribution. La projection d'une surface analytique réelle de $\mathbb{R}^4$ dans $\mathbb{R}^3$ comporte généralement une partie singulière. D'après Goryunov [19], pour une surface lisse en position générique, il en résulte trois types de singularités : *cross-cap*, *points triples* et *une courbe de points doubles*. Nous proposons un algorithme permettant de calculer le graphe des singularités de la surface obtenue dans $\mathbb{R}^3$. Après avoir introduit les définitions et les notations de base dans la section 5.1, nous modélisons les différents types de singularités sous forme de solutions régulières de systèmes d'équations (voir section 5.2). La section 5.3 explicite les différentes étapes de notre algorithme.

Première partie

Topologie de courbes algébriques planes

Chapitre 1

Isoler les racines d'un polynôme

Introduction

Les algorithmes d'isolation des racines sont des outils indispensables au calcul de la topologie d'une courbe algébrique. La section 1.1 présente des résultats quantitatifs sur les racines d'un polynôme. La section 1.2 revient sur l'algorithme d'isolation des racines d'un polynôme présenté par Mehlhorn et al. [33]. Les résultats de ce chapitre sont pour la plupart déjà connus.

1.1 Bornes sur les racines de polynômes univariés

1.1.1 Quelques rappels algébriques

Mesure de Mahler et séparateur

Définitions 1.1
Soient

$$f = \sum_{i=0}^{n} a_i \mathrm{X}^i \in \mathbb{C}[\mathrm{X}],$$

un polynôme de degré n et $\mathrm{V}_{\mathbb{C}}(f)$ l'ensemble des différentes racines complexes de f.

- *Le coefficient a_n est appelé le coefficient de tête de f. Il est noté* $\mathrm{LCF}(f) = a_n$. *Donc, le polynôme f peut être réécrit comme suit*

$$f = \mathrm{LCF}(f) \cdot \prod_{z \in \mathrm{V}_{\mathbb{C}}(f)} (\mathrm{X} - z)^{\mu(z)}.$$

- *La* longueur *de f est donnée par la formule*

$$\mathrm{Len}(f) := \sum_{i=0}^{n} |a_i|.$$

- *La* norme *de f est donnée par la formule*

$$\|f\| := \sqrt{\sum_{i=0}^{n} |a_i|^2}.$$

- *La* multiplicité *de z en tant que racine de f, notée ici* $\mathrm{mult}(z, f)$, *est le plus petit indice $i \in \mathbb{N}^*$ tel que $(\mathrm{X} - z)^i$ divise f et $(\mathrm{X} - z)^{i+1}$ ne divise pas f ; i.e*

$$\bigwedge_{i=0}^{\mathrm{mult}(z,f)-1} f^{[i]}(z) = 0 \wedge f^{[\mathrm{mult}(z,f)]}(z) \neq 0.$$

Si z n'est pas une racine de f alors $\mathrm{mult}(z, f) = 0$.

- *La* partie sans facteur carré *de f, notée $f^\star$, est donnée par*

$$f^\star = \mathrm{LCF}(f) \cdot \prod_{z \in \mathrm{V}_{\mathbb{C}}(f)} (\mathrm{X} - z).$$

- *La* mesure de Mahler *de f est définie par*

$$\mathrm{Mea}(f) := |\mathrm{LCF}(f)| \cdot \prod_{z \in \mathrm{V}_{\mathbb{C}}(f)} \max(1, |z|)^{\mu(z)}$$

et $\widehat{\mathrm{Mea}}(f)$ représente la mesure de Mahler de f sans le coefficient de tête

$$\widehat{\mathrm{Mea}}(f) := \prod_{z \in \mathrm{V}_{\mathbb{C}}(f)} \max(1, |z|)^{\mu(z)}.$$

- *Le* séparateur de z, en tant que racine de f, *est défini par*

$$\mathrm{sep}(f, z) := \min_{y \in \mathrm{V}_{\mathbb{C}}(f) \setminus z} |y - z|;$$

et le séparateur du polynôme f *est défini comme étant le minimum des séparateurs des racines du polynôme; i.e*

$$\mathrm{sep}(f) := \min_{z \in \mathrm{V}_{\mathbb{C}}(f)} \mathrm{sep}(f, z)$$

Lemme 1.1
Si $f \in \mathbb{C}[\mathrm{X}]$ est de degré n et $z \in \mathbb{C}$, alors

$$|f(z)| \leq \mathrm{Len}(f) \max(1, |z|)^n.$$

Démonstration
Soit

$$f = \sum_{i=0}^{n} a_i \mathrm{X}^i$$

Pour tout $z \in \mathbb{C}$, on a :

$$|f(z)| \leq \sum_{i=0}^{n} |a_i| \times \max(1, |z|)^n = \mathrm{Len}(f) \max(1, |z|)^n.$$

□

Lemme 1.2 *Basu et al. [4, Lemma 10.10]*
Soient $f \in \mathbb{C}[\mathrm{X}]$ un polynôme de degré n et $z \in \mathbb{C}$. Alors

$$||(\mathrm{X} - z) f(\mathrm{X})|| = ||(\bar{z}\mathrm{X} - 1) f(\mathrm{X})||$$

Démonstration
On a :

$$\begin{aligned} ||(\mathrm{X} - z) f(x)||^2 &= \sum_{j=0}^{n+1} (a_{j-1} - z a_j)(\bar{a}_{j-1} - \bar{z}\bar{a}_j) \\ &= (1 + |z|^2)||f||^2 - \sum_{j=0}^{n} (z a_j \bar{a}_{j-1} + \bar{z}\bar{a}_j a_{j-1}) \end{aligned}$$

avec $a_{-1} = a_{n+1} = 0$, du fait que

$$(a_{j-1} - z a_j)(\bar{a}_{j-1} - \bar{z}\bar{a}_j) = |a_{j-1}|^2 + |z|^2 |a_j|^2 - (z a_j \bar{a}_{j-1} + \bar{z}\bar{a}_j a_{j-1})$$

De la même manière, on a :

$$\begin{aligned}||(\bar{z}\mathrm{X}-1)f(\mathrm{X})||^2 &= \sum_{j=0}^{n+1}(\bar{z}a_{j-1}-a_j)(z\bar{a}_{j-1}-\bar{a}_j)\\ &=(1+|z|^2)||f||^2-\sum_{j=0}^{n}(za_j\bar{a}_{j-1}-\bar{z}\bar{a}_j a_{j-1})\\ ||(\bar{z}\mathrm{X}-1)f(\mathrm{X})||^2 &=||(\mathrm{X}-z)f(\mathrm{X})||^2\\ ||(\bar{z}\mathrm{X}-1)f(\mathrm{X})|| &=||(\bar{z}\mathrm{X}-1)f(\mathrm{X})||\end{aligned}$$

□

Lemme 1.3 *Basu et al. [4, Lemma 2.12]*
Soient $z_1,\dots,z_k$ des éléments appartenant à $\mathbb{C}$ et

$$f=(\mathrm{X}-z_1)\cdots(\mathrm{X}-z_k)=\mathrm{X}^k+\mathrm{C}_1\mathrm{X}^{k-1}+\cdots+\mathrm{C}_k$$

alors

$$\mathrm{C}_i=(-1)^i\sum_{1\le j_1<\cdots<j_i\le k}z_{j_1}\cdots z_{j_i}$$

Démonstration
Il suffit d'identifier les coefficients de X^i de part et d'autre de l'égalité

$$(\mathrm{X}-z_1)\cdots(\mathrm{X}-z_k)=\mathrm{X}^k+\mathrm{C}_1\mathrm{X}^{k-1}+\cdots+\mathrm{C}_k$$

□

Lemme 1.4
Soient $f\in\mathbb{C}[\mathrm{X}]$ de degré n et

$$f^{[k]}:=\frac{f^{(k)}}{k!} \tag{1.1}$$

alors

$$\mathrm{Len}(f^{[k]})<2^n\mathrm{Len}(f)$$

Démonstration
Soient

$$f=\sum_{i=0}^{n}a_i\mathrm{X}^i \qquad \text{et} \qquad f^{(k)}=\sum_{i=0}^{n-k}a_i^{'}\mathrm{X}^{n-k-i}.$$

Pour tout indice $i\in\mathbb{N}$ tel que $0\le i\le n-k$, on a :

$$|a_i^{'}|<n(n-1)\dots(n-k)|a_i|$$

en utilisant le fait que

$$\frac{n(n-1)\dots(n-k)}{k!}<\binom{n}{k}<2^n$$

nous obtenons

$$\frac{1}{k!}\sum_{i=0}^{n-k}|a_i^{'}|<2^n\sum_{i=0}^{n}|a_i|;$$

d'où le résultat.

□

Définition 1.1
Soit $\mathrm{P}(\mathrm{X}) = a_q\mathrm{X}^q + \cdots + a_n\mathrm{X}^n$, *avec* $q \leq n$, *un polynôme univarié de degré* n *à coefficients dans* $\mathbb{C}$, *tel que* $a_q \neq 0$ *et* $a_n \neq 0$. *La borne supérieure (resp. inférieure) de Cauchy du polynôme* P, *notée* $\mathrm{C}(\mathrm{P})$ *(resp.* $c(\mathrm{P})$*), est définie par*

$$\mathrm{C}(\mathrm{P}) = \sum_{q \leq i \leq n} \left| \frac{a_i}{a_n} \right|$$

$$\left(resp.\ c(\mathrm{P}) = \frac{|a_q|}{\sum_{q \leq i \leq n} |a_i|}. \right)$$

Proposition 1.1 *Basu et al. [4]*
Si $z \in \mathbb{C}$ *est une racine de* P,

$$c(\mathrm{P}) \leq |z| \leq \mathrm{C}(\mathrm{P})$$

Résultant et sous-résultant

Dans ce paragraphe, nous introduisons les matrices de *Sylvester* et *Sylvester-Habicht* à partir desquelles nous définirons le *résultant* et *sous-résultants* de deux polynômes (voir Basu et al. [4, section 4.2.1]).

Définition 1.2
Soient $\mathbb{D}$ *un anneau intègre et* $f(\mathrm{X}), g(\mathrm{X})$ *deux polynômes de* $\mathbb{D}[\mathrm{X}]$ *de degrés respectifs* n, n' *par rapport à la variable* X. *Nous supposons que* $n \geq n'$ *et*

$$f = a_n\mathrm{X}^n + \cdots + a_0 \text{ et } g = b_{n'}\mathrm{X}^{n'} + \cdots + b_0$$

La matrice de Sylvester *associée à* f *et* g, *notée* $\mathrm{Syl}(f,g)$ *est la matrice de taille* $(n+n') \times (n+n')$ *obtenue à partir des vecteurs* $\mathrm{X}^{n'-1}f, \ldots, f, \mathrm{X}^{n-1}g, \ldots, g$ *exprimés dans la base* $\mathrm{X}^{n+n'-1}, \mathrm{X}^{n+n'-2}, \ldots, \mathrm{X}, 1$.

$$\mathrm{Syl}(f,g) = \begin{pmatrix}
a_n & a_{n-1} & \cdots & & \cdots & a_0 & 0 & \cdots & 0 \\
0 & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & & & & & & 0 \\
0 & \cdots & 0 & a_n & a_{n-1} & \cdots & \cdots & \cdots & a_0 \\
b_{n'} & b_{n'-1} & \cdots & \cdots & b_0 & 0 & \cdots & \cdots & 0 \\
0 & \ddots & & & & \ddots & \ddots & & \vdots \\
\vdots & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\
\vdots & & \ddots & \ddots & & & & \ddots & 0 \\
0 & \cdots & \cdots & 0 & b_{n'} & b_{n'-1} & \cdots & \cdots & b_0
\end{pmatrix}$$

Soit j *un indice tel que* $0 \leq j \leq \min(n', n-1)$. *La* $j-$*ième matrice de* Sylvester-Habicht *associée aux polynômes* f *et* g, *notée* $\mathrm{SylHa}_j(f,g)$, *est la matrice dont les lignes sont données par les vecteurs* $\mathrm{X}^{n'-j-1}f, \ldots, f, \mathrm{X}^{n-j-1}g, \ldots, g$ *exprimés dans la base* $\mathrm{X}^{n+n'-j-1}, \mathrm{X}^{n+n'j-2}, \ldots, \mathrm{X}, 1$. $\mathrm{SylHa}(f,g)$ *est de taille* $(n+n'-2j) \times (n+n'-j)$

Définition 1.3
Le résultant *de* f *et* g *est l'élément* $\mathrm{Res}(f,g) \in \mathbb{D}$ *défini par*

$$\mathrm{Res}(f,g) = \det(\mathrm{Syl}(f,g))$$

Remarque 1.1

- $\mathrm{Res}(f,g)$ *peut être aussi défini comme étant le déterminant de la matrice transposée, associée à l'application linénaire* $\phi : \mathbb{D}_{<n'} \times \mathbb{D}_{<n} \mapsto \mathbb{D}_{<n+n'}$ *qui, à* u *et* v, *de degrés respectifs au plus* $n'-1$ *et* $n-1$, *associe le polynôme* $uf + vg$.

- *Si* $\mathbb{D}=\mathbb{C}$, $\mathrm{Res}(f,g)=0$ *si et seulement si* $\deg(\mathrm{pgcd}(f,g))>0$, *i.e* f *et* g *admettent au moins une racine commune.*

Définition 1.4
Soit $\mathrm{SylHa}_{j,j}(f,g)$ *la matrice carrée obtenue en prenant les* $(n+n'-2j)$ *premières colonnes de* $\mathrm{SylHa}_j(f,g)$.
Le $k-$*ième* sous-résultant *de* f *et* g, *noté* $\mathrm{sRes}_k(f,g)$, *est le déterminant de* $\mathrm{SylHa}_{j,j}(f,g)$.

Proposition 1.2 *Basu et al. [4]*
Si $\mathbb{D}=\mathbb{C}$ *et* $0\leq k\leq \min(n',n-1)$, *alors* $\deg(\mathrm{pgcd}(f,g))=k$ *si et seulement si*

$$\mathrm{sRes}_0(f,g)=\mathrm{sRes}_1(f,g)=\cdots=\mathrm{sRes}_{k-1}(f,g)=0 \text{ et } \mathrm{sRes}_k(f,g)\neq 0.$$

Définitions 1.2
Soit $\mathbb{D}$ *un anneau intègre,* $f\in\mathbb{D}[X]$ *un polyôme de degré* n *et* $0\leq k\leq n-1$.

- *Le* discriminant *de* f *est l'élément* $\mathrm{Disc}(f)\in\mathbb{D}$ *tel que*

$$\mathrm{LCF}(f)\cdot\mathrm{Disc}(f)=\mathrm{Res}_X(f,f').$$

- *Le* k-ième sous-discriminant *de* f *est l'élément* $sDisc_k(f)\in\mathbb{D}$ *tel que*

$$\mathrm{LCF}(f)\cdot\mathrm{sDisc}_k(f)=\mathrm{sRes}_k(f,f').$$

Proposition 1.3
Si $\mathbb{D}=\mathbb{C}$ *et* $\deg(f)=n$ *et* $z_1,\ldots,z_n$ *sont les racines complexes de* f *alors*

(a)
$$|\mathrm{Disc}(f)|=|\mathrm{LCF}(f)^{2n-2}|\cdot\prod_{i,k:i\neq k}|z_i-z_j|=\mathrm{LCF}(f)^{n-2)}\cdot\prod_i\left|f'(z_i)\right|.$$

(b) k *est le plus petit indice tel que* $\mathrm{sDisc}_k(f)\neq 0$ *si et seulement si* f *admet* $n-k$ *racines distinctes dans* $\mathbb{C}$.

(c)
$$\left|\mathrm{sDisc}_k(f)\right|=\left(\prod_{z\in V_{\mathbb{C}}(f)}\mu(z)\right)\cdot\left|\mathrm{Disc}(f^\star)\right|$$

Remarque 1.2
Les racines de f *n'étant pas nécessairement distinctes, alors* $\mathrm{Disc}(f)=0$ *si et seulement si* f *admet au moins une racine multiple.*

Définition 1.5
Le discriminant généralisé $\mathrm{GDisc}(f)$ *d'un polynôme* f *est l'élément de* $\mathbb{D}$, *défini comme étant le coefficient du terme de plus petit degré en la variable* U *de* $=\mathrm{Res}_X(f,f'+\ldots+U^{i-1}f^{[i]}+\ldots)$. *Si* $\mathbb{D}=\mathbb{C}$,

$$|\mathrm{GDisc}(f)|=|\mathrm{LCF}(f)|^{2n-2}\cdot\prod_{i,j:i\neq j}|z_i-z_j|^{\mu_i\mu_j}=|\mathrm{LCF}(f)|^{n-2}\cdot\prod_{1\leq i\leq n}|f^{[\mu_i]}(z_i)|^{\mu_i},$$

où $z_1,\ldots,z_m$ *désignent les différentes racines complexes de* f *et* μ_i *leurs multiplicités respectives.*
Lorsque toutes les racines sont simples, le discriminant généralisé est égal au discriminant.

Borne de Davenport-Mahler

Définition 1.6 (Notion de grand "O") *Basu et al. [4, Notation 8.2]*
Soient f *et* g *deux applications de* $\mathbb{R}^\ell$ *vers* $\mathbb{R}$ *et* h *une fonction de* $\mathbb{R}$ *dans* $\mathbb{R}$.

- *L'expression "*$f(v)$ *est en* $h(O(g(v)))$*" signifie qu'il existe un entier naturel* b *tel que pour tout* $v\in\mathbb{R}^\ell$, $f(v)\leq h(bg(v))$.

- *L'expression "$f(v)$ est en $h(\tilde{O}(g(v)))$" signifie qu'il existe un entier naturel a tel que pour tout $v \in \mathbb{N}^\ell$, $f(v) \le h(g(v)\log_2(g(v))^a)$.*

Définition 1.7
Un polynôme $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ est de magnitude (n,τ) *si*

$$\deg(f) \le n \text{ et } |a_i| \le 2^\tau \ \forall i = 1,\dots,n.$$

Proposition 1.4 *Eingenwillig [12], Escorcielo and Perrucci [13]*
Soit $f \in C[X]$ un polynôme de degré n ayant m racines complexes distinctes dans $\mathbb{C}$. On a alors :

$$(a) \quad \operatorname{sep}(f) \ge |\operatorname{sDisc}_{n-m}(f)|^{1/2} \operatorname{Mea}(f)^{(1-m)} \frac{\sqrt{3}}{m} m^{-m/2} \left(\frac{1}{3}\right)^{\min(n,2n-2m)/6}, \tag{1.2}$$

$$(b) \quad \prod_{z \in V_{\mathbb{C}}(f)} \operatorname{sep}(z,f) \ge |\operatorname{sDisc}_{n-m}(f)| \operatorname{Mea}(f)^{2(1-m)} \frac{\sqrt{3}^m}{m^{2m}} \left(\frac{1}{3}\right)^{\min(n,2n-2m)/3}. \tag{1.3}$$

Définitions 1.3
Soit $f \in \mathbb{C}[X]$. On définit

$$\begin{aligned}
\operatorname{logLen}(f) &:= \max(1, |\log(\operatorname{Len}(f))|),\\
\operatorname{logMea}(f) &:= \max(1, \log(|\operatorname{LCF}(f)|) + \sum_{z \in V_{\mathbb{C}}(f)} \operatorname{mult}(z,f) \cdot \log(\max(1,|z|))),\\
\widehat{\log\operatorname{Mea}}(f) &:= \max(1, \sum_{z \in V_{\mathbb{C}}(f)} \operatorname{mult}(z,f) \cdot \log(\max(1,|z|))),\\
\operatorname{logsep}(f) &:= \max(1, \sum_{z \in V_{\mathbb{C}}(f)} \operatorname{mult}(z,f) \cdot |\log(\operatorname{sep}(z,f))|),\\
\operatorname{logsep}^\star(f) &:= \operatorname{logsep}(f^\star) = \max(1, \sum_{z \in V_{\mathbb{C}}(f)} |\log(\operatorname{sep}(z,f))|).\\
\widehat{\operatorname{logGDisc}}(f) &:= \max(1, \sum_{z \in V_{\mathbb{C}}(f)} \operatorname{mult}(z,f) |\log(|f^{[\operatorname{mult}(z,f)]}(z)|)|).
\end{aligned}$$

Le terme $\max(1,-)$ qui apparaît dans les définitions précédentes permet de garantir que les quantités correspondantes sont au moins de l'ordre de $O(1)$, ce qui simplifie l'écriture de certaines expressions.

Proposition 1.5 *Basu et al. [4, Proposition 10.8-9]*
Soit $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{C}[X]$, avec $a_n \neq 0$. La norme de f, sa longueur et sa mesure de Mahler sont liées par la relation ci-dessous :

$$2^{-n}\operatorname{Len}(f) \leqslant \operatorname{Mea}(f) \leqslant \|f\|.$$

Par conséquent,

$$\operatorname{logLen}(f) \le \operatorname{logMea}(f) + \deg(f). \tag{1.4}$$

Démonstration
Tout d'abord, montrons que $2^{-n}\operatorname{Len}(f) \leqslant \operatorname{Mea}(f)$. D'après le Lemme 1.3 on a :

$$a_{n-k} = (-1)^k \left(\sum_{1 \le i_1 < \cdots < i_k \le n} z_{i_1} \cdots z_{i_k} \right) a_n$$

$$|a_{n-k}| \le \binom{n}{k} \operatorname{Mea}(f)$$

en prenant la somme de $k = 0$ à n, on obtient :

$$\operatorname{Len}(f) \le \sum_{k=0}^{n} \binom{n}{k} \operatorname{Mea}(f) = 2^n \operatorname{Mea}(f)$$

Ensuite, montrons que $\mathrm{Mea}(f) \leq ||f||$.
Soient $z_1, \ldots, z_k$ les racines de f telles que $|z_i| > 1$, alors

$$\mathrm{Mea}(f) = |a_n| \prod_{i=1}^{k} |z_i|.$$

Soit le polynôme

$$\mathrm{R} = a_n \prod_{i=1}^{k} (\bar{z}_i \mathrm{X} - 1) \prod_{i=k+1}^{p} (\mathrm{X} - z_i) = b_n \mathrm{X}^n + \cdots + b_0$$

Notons que $|b_n| = |a_n \prod_{i=1}^{k} \bar{z}_i| = \mathrm{Mea}(f)$. En appliquant k-fois le Lemme 1.2 à f, nous obtenons la relation suivante

$$||\prod_{i=1}^{k} (\mathrm{X} - z_i) f(x)|| = ||\prod_{i=1}^{k} (\bar{z}_i \mathrm{X} - 1)|| = ||\mathrm{R}||$$

$$||f||^2 = ||\mathrm{R}||^2 \geq |b_n|^2 = \mathrm{Mea}(f)^2$$

$$\mathrm{Mea}(f) \leq ||f||$$

□

Dans ce qui suit, il s'agira de déterminer une borne sur $\mathrm{logsep}(f)$ en fonction de $\log\widehat{\mathrm{Mea}}(f)$, $\mathrm{logLen}(f)$ et $\widehat{\mathrm{logGDisc}}(f)$, et terminer par borner $\mathrm{logsep}(f) + \widehat{\mathrm{logGDisc}}(f)$ lorsque f est sans facteur carré.

Proposition 1.6
Soit $f \in \mathbb{C}[\mathrm{X}]$ un polynôme de degré n.

(a) On a

$$\mathrm{logsep}(f) \in \mathrm{O}(n(n + \mathrm{logLen}(f) + \log\widehat{\mathrm{Mea}}(f)) + \widehat{\mathrm{logGDisc}}(f)) \tag{1.5}$$

(b) Si f est sans facteur carré, alors on a

$$\mathrm{logsep}(f) + \widehat{\mathrm{logGDisc}}(f) \in \tilde{\mathrm{O}}(n(\mathrm{logLen}(f) + \log\widehat{\mathrm{Mea}}(f)) + |\log(|\mathrm{Disc}(f)|)|). \tag{1.6}$$

Le lemme ci-dessous est un résultat intermédiaire qui nous sera utile dans la démonstration de la Proposition 1.6.

Lemme 1.5
Soient S un sous-ensemble non vide de $\mathbb{C}$ et $\phi : \mathrm{S} \mapsto \mathrm{S}$ une application qui, à tout élément $z \in \mathrm{S}$, associe un autre élément $z' \in \mathrm{S}$ qui lui est plus proche; i.e $|z - z'| = \min\{|z - x|,\ \forall x \in \mathrm{S}\}$. Alors, chaque $z' \in \mathrm{S}$ admet au plus 6 préimages par l'application ϕ.

Démonstration
Soient ABCDEF un hexagone de centre O et AOB un triangle de l'hexagone. Si $\mathrm{AB} \geq \max(\mathrm{OA}, \mathrm{OB})$ alors l'angle $\widehat{\mathrm{BOA}}$ est inférieure ou égale à $2\pi/6$. □

Démonstration de la Proposition 1.6
Pour établir la démontration de (a), montrons d'abord que pour toute racine z de f de multiplicité $\mu(z) = \mathrm{mult}(z, f)$,

$$\mathrm{sep}(z, f)^{\mu(z)} > |f^{[\mu(z')]}(z')| \cdot 2^{-n} \cdot \max(1, |z'|)^{-n} \cdot \mathrm{Len}(f)^{-1} \tag{1.7}$$

avec $z' \neq z$ une racine de f telle que $|z - z'| = \min_{x \in \mathrm{V}_{\mathbb{C}-\{z\}}} |z - x|$.
(1.7) découle du calcul ci-dessous :

$$\begin{aligned} |f^{[\mu(z')]}(z')| &= |\mathrm{LCF}(f)| \cdot \prod_{y \in \mathrm{V}_{\mathbb{C}}(f) \setminus \{z'\}} |z' - y|^{\mu(y)} \\ &= \mathrm{sep}(z, f)^{\mu(z)} \cdot |\mathrm{LCF}(f)| \cdot \prod_{y \in \mathrm{V}_{\mathbb{C}}(f) \setminus \{z, z'\}} |z' - y|^{\mu(y)} \\ |f^{[\mu(z')]}(z')| &\leq \mathrm{sep}(z, f)^{\mu(z)} \cdot \mathrm{Mea}(f(\mathrm{X} + z')) \end{aligned}$$

et

$$\mathrm{Mea}(f(X+z')) \le 2^n \cdot \mathrm{Len}(f) \cdot \max(1,|z'|)^n.$$

Soit $\phi : V_{\mathbb{C}}(f) \mapsto V_{\mathbb{C}}(f)$ l'application qui, à une racine z de f associe une racine z' de f qui lui est plus proche. D'après le Lemme 1.5 chaque $z' \in V_{\mathbb{C}}(f)$ admet au plus 6 préimages par l'application ϕ. Nous en concluons que

$$\begin{aligned}
\prod_{z\in V_{\mathbb{C}}(f)} \mathrm{sep}(z,f)^{\mu(z)} &> 2^{-n^2} \cdot \mathrm{Len}(f)^{-n} \cdot \prod_{z\in V_{\mathbb{C}}(f)} \max(1,|\phi(z)|)^{-n} \cdot \prod_{z\in V_{\mathbb{C}}(f)} |f^{[\mu(\phi(z))]}(\phi(z))| \\
&\ge 2^{-n^2} \cdot \mathrm{Len}(f)^{-n} \cdot \prod_{z\in V_{\mathbb{C}}(f)} |\max(1,|z|)|^{-6n} \cdot \prod_{z\in V_{\mathbb{C}}(f)} \min(1,|f^{[\mu(\phi(z))]}(\phi(z))|) \\
\prod_{z\in V_{\mathbb{C}}(f)} \mathrm{sep}(z,f)^{\mu(z)} &\ge 2^{-n^2} \cdot \mathrm{Len}(f)^{-n} \cdot \widehat{\mathrm{Mea}}(f)^{-6n} \cdot \prod_{z\in V_{\mathbb{C}}(f)} \min(1,|f^{[\mu(z)]}(z)|)^6,
\end{aligned}$$

ce qui montre

$$-\sum_{\substack{z\in V_{\mathbb{C}}(f)\\ \mathrm{sep}(z,f)<1}} \mu(z)\cdot\log(\mathrm{sep}(z,f)) \in O(n(n+\log\mathrm{Len}(f)+\log\widehat{\mathrm{Mea}}(f))+\widehat{\log\mathrm{GDisc}}(f)).$$

Il reste à estimer

$$\sum_{\substack{z\in V_{\mathbb{C}}(f)\\ \mathrm{sep}(z,f)\ge 1}} \mu(z)\cdot\log\mathrm{sep}(z,f).$$

En utilisant l'inégalité

$$\mathrm{sep}(z,f) = |z-\phi(z)| \le 2\cdot\max(1,|z|)\cdot\max(1,|\phi(z)|), \tag{1.8}$$

nous montrons que

$$\begin{aligned}
\prod_{\substack{z\in V_{\mathbb{C}}(f)\\ \mathrm{sep}(z,f)\ge 1}} \mathrm{sep}(z,f)^{\mu(z)} &\le 2^n \cdot \widehat{\mathrm{Mea}}(f) \cdot \prod_{z\in V_{\mathbb{C}}(f)} \max(1,|\phi(z)|)^{\mu(z)} \\
&\le 2^n \cdot \widehat{\mathrm{Mea}}(f) \cdot \prod_{z\in V_{\mathbb{C}}(f)} \max(1,|z|)^{6n} \\
\prod_{\substack{z\in V_{\mathbb{C}}(f)\\ \mathrm{sep}(z,f)\ge 1}} \mathrm{sep}(z,f)^{\mu(z)} &\le 2^n \cdot \widehat{\mathrm{Mea}}(f)^{6n+1}
\end{aligned}$$

Finalement

$$\sum_{z:\mathrm{sep}(z,f)>1} \mu(z)\log(\mathrm{sep}(z,f)) \in O(n+\log\widehat{\mathrm{Mea}}(f)). \tag{1.9}$$

Le résultat (b) est obtenu à partir de (1.9) et de la Proposition 1.4 (b). C'est-à-dire :

$$\begin{aligned}
\mathrm{logsep}(f) &= \max(1, -\sum_{z\in V_C(f)} \log(\mathrm{sep}(z,f)) + 2\cdot \sum_{z:\mathrm{sep}(z,f)>1} \log(\mathrm{sep}(z,f))) \\
&\le \log\left(\prod_{z\in V_C(f)} \mathrm{sep}(z,f)^{-1}\right) + O(n\cdot\log\widehat{\mathrm{Mea}}(f)) \\
&\in \tilde{O}(\widehat{\log\mathrm{GDisc}}(f) + n\log\mathrm{Mea}(f)) \\
&\in \tilde{O}(\widehat{\log\mathrm{GDisc}}(f) + n(\log\widehat{\mathrm{Mea}}(f) + \log\mathrm{Len}(f))).
\end{aligned}$$

Il s'agit maintenant de faire une estimation de $\widehat{\log\mathrm{GDisc}}(f)$. D'après le Lemme 1.1, pour tout nombre complexe z, $|f'(z)| \le n\cdot\mathrm{Len}(f)\cdot\max(1,|z|)^n$.
Ce qui signifie que :

$$\sum_{z\in V_C(f):|f'(z)|>1} \log(|f'(z)|) \in \tilde{O}(n(\log\mathrm{Len}(f)) + \log\widehat{\mathrm{Mea}}(f)).$$

Ainsi, on a

$$\begin{aligned}\widehat{\log\mathrm{GDisc}}(f) &= \log(\prod_{z\in \mathrm{V_C}(f)} |f'(z)|^{-1}) + 2\cdot \sum_{z\in \mathrm{V_C}(f):|f'(z)|>1} |\log(|f'(z)|)\\ &= \log(\prod_{z\in \mathrm{V_C}(f)} |f'(z)|^{-1}) + \tilde{\mathrm{O}}(n(\mathrm{logLen}(f) + \log\widehat{\mathrm{Mea}}(f)))\\ &= \log(\frac{|\mathrm{LCF}(f)|^{n-2}}{|\mathrm{Disc}(f)|}) + \tilde{\mathrm{O}}(n(\mathrm{logLen}(f) + \log\widehat{\mathrm{Mea}}(f)))\\ &\in \tilde{\mathrm{O}}(n(\mathrm{logLen}(f) + \log\widehat{\mathrm{Mea}}(f)) + |\log(|\mathrm{Disc}(f)|)|).\end{aligned}$$

□

Lemme 1.6
Si $f \in \mathbb{Z}[X]$ est de magnitude (n,τ) *alors $f^{[k]}$ est de* magnitude $(n,\tau+n)$ *(voir 1.1); où $f^{[k]} = \frac{f^{(k)}}{k!}$.*

Proposition 1.7 *Basu et al. [4]*
Si $f \in \mathbb{Z}[X]$ est de magnitude (n,τ), *alors*

$$2^{\tau-n} \leqslant \mathrm{Mea}(f) \leqslant \sqrt{(n+1)}2^{\tau}. \tag{1.10}$$

Par conséquent,

$$\mathrm{logMea}(f) \in \mathrm{O}(\tau + \log(n)), \tag{1.11}$$

et

$$\log\widehat{\mathrm{Mea}}(f) \in \mathrm{O}(\tau + \log(n)). \tag{1.12}$$

Dans ce paragraphe, il s'agit de déterminer une borne sur $\mathrm{logsep}(f)$ en fonction de la *magnitude* (n,τ) de f. La Proposition 1.6 (a) explicite déjà une borne sur $\mathrm{logsep}(f)$ en fonction du degré n, la longueur $\log\mathrm{Len}(f)$ du polynôme f, des valeurs $\mathrm{logLen}(f)$, $\log\widehat{\mathrm{Mea}}(f)$ et $\widehat{\log\mathrm{GDisc}}(f)$. Sachant que $\mathrm{Len}(f) \leq (n+1)\cdot 2^{\tau}$ et que $\widehat{\mathrm{Mea}}(f) \leq \sqrt{n+1}\cdot 2^{\tau}$ (voir Proposition 1.7 (1.12)). Il s'agit maintenant de trouver une borne sur $\widehat{\log\mathrm{GDisc}}(f)$ en fonction de la *magnitude* (τ,n). Nous établissons un résultat général sur le produit des valeurs absolues d'une famille de polynômes à coefficients entiers évaluées en les racines de f (voir Proposition 1.8). Ce qui permet de déduire une borne sur $\widehat{\log\mathrm{GDisc}}$ en appliquant le résultat général à la suite obtenue en prenant, pour chaque racine z de f, la première dérivée non nulle au point z.

Proposition 1.8
Soient $f \in \mathbb{Z}[X]$ un polynôme de magnitude (n_1,τ_1) *et $(g_i)_{1\leq i\leq m}$ une famille de polynômes appartenant à $\mathbb{C}[X]$ tels que $n_2 = \max_{1\leq i\leq m}(\deg(g_i))$ et dont les coefficients sont bornés en valeur absolue par 2^{τ_2}. Soit $\mu(z) = \mathrm{mult}(z,f)$ la multiplicité de z en tant que racine de f.*

a) Soit $A \subset \mathrm{V}_{\mathbb{C}}(f)$ un sous-ensemble non vide de racines de f et pour tout $z \in A$, soit $i(z) \in \{1,\ldots,m\}$ tel que $g_{i(z)}(z) \neq 0$. Alors,

$$\sum_{z\in A} \mu(z)\log|g_{i(z)}(z)| \in \tilde{\mathrm{O}}(n_1\tau_2 + n_2\tau_1). \tag{1.13}$$

b) Si pour tout $1 \leq i \leq m$, $g_i \in \mathbb{Z}[X]$ et pour toute racine $z \in \mathrm{V}_{\mathbb{C}}(f)$ il existe un indice i tel que $g_i(z) \neq 0$, notons $i(z)$ la plus petite valeur de i telle que $g_i(z) \neq 0$, alors

$$\sum_{z\in \mathrm{V_C}(f)} \mu(z)|\log|g_{i(z)}(z)|| \in \tilde{\mathrm{O}}(n_1\tau_2 + n_2\tau_1). \tag{1.14}$$

La démonstration de la proposition ci-dessus s'appuie sur le Lemme élémentaire ci-dessous.

Lemme 1.7
Soient a,b,c,d quatre nombres réels tels que $a \leq c$ et $b-a \leq d$, alors $a+b \leq 2c+d$.

Démonstration [Proposition 1.8]

a) Pour tout $z \in \mathrm{A}$, on a d'après le Lemme 1.1

$$\left|g_{i(z)}(z)\right| \leq 2^{\tau'_2} \cdot \max(1,|z|)^{n_2}; \tag{1.15}$$

avec τ'_2 défini par $2^{\tau'_2} = (n_2+1)2^{\tau_2}$. En utilisant l'inégalité (1.15), on a

$$\prod_{z\in\mathrm{A}} \left|g_{i(z)}(z)\right|^{\mu(z)} \leq \prod_{z\in\mathrm{A}} 2^{\tau'_2\mu(z)} \cdot \max(1,|z|)^{n_2\mu(z)} \leq \prod_{z\in\mathrm{V}_{\mathbb{C}}(f)} 2^{\tau'_2\mu(z)} \cdot \max(1,|z|)^{n_2\mu(z)}.$$

Sachant que

$$\sum_{z\in\mathrm{A}} \mu(z) \leq n_1, \qquad \widehat{\mathrm{Mea}(f)} \leq 2^{\tau_1+\log n_1} \quad et \quad 2^{\tau'_2} = (n_2+1)2^{\tau_2},$$

on a

$$\prod_{z\in\mathrm{A}} \left|g_{i(z)}(z)\right|^{\mu(z)} \leq 2^{\tau'_2\sum\mu(z)}\widehat{\mathrm{Mea}}(f)^{n_2} \in 2^{\mathrm{O}(n_1\log n_2+n_2\tau_1+n_2\log n_1)}; \tag{1.16}$$

b) Montrons que

$$\prod_{z\in\mathrm{V}_{\mathbb{C}}(f)} \left|g_{i(z)}(z)\right|^{\mu(z)} \in 2^{-\mathrm{O}(\tau_1 n_2)}. \tag{1.17}$$

Posons

$$g(\mathrm{X},\mathrm{U}) = g_1(\mathrm{X}) + \mathrm{U}g_2(\mathrm{X}) + \cdots + \mathrm{U}^{m-1}g_m(\mathrm{X})$$

et considérons

$$\left|\mathrm{Res}_{\mathrm{X}}(f,g)\right| = |\mathrm{LCF}(f)|^{n_2} \cdot \prod_{z\in\mathrm{V}_{\mathbb{C}}(f)} \left|g(z)\right|^{\mu(z)}.$$

On remarque que $\mathrm{Res}_{\mathrm{X}}(f,g)$ est un polynôme en U à coefficients entiers. Le coefficient de son terme de plus bas degré appartient à $\mathbb{Z}\backslash\{0\}$ et vaut

$$|\mathrm{LCF}(f)|^{n_2} \cdot \prod_{z\in\mathrm{V}_{\mathbb{C}}(f)} \left|g_{i(z)}(z)\right|^{\mu(z)}.$$

En particulier, sa valeur absolue est supérieure où égale à 1. Par conséquent,

$$|\mathrm{LCF}(f)|^{n_2} \in 2^{\mathrm{O}(\tau_1 n_2)};$$

D'où on obtient (1.17).

Soit

$$\mathrm{A} = \{z | f(z) = 0, |g_{i(z)}(z)| \geq 1\}.$$

On sait que pout tout $z \in \mathrm{A}$, $\left|g_{i(z)}(z)\right| \geq 1$. D'après (1.16) on a

$$0 \leq \sum_{z\in\mathrm{A}} \mu(z) \cdot \log|g_{i(z)}(z)| \leq c \in \mathrm{O}(n_1\tau_2 + n_2\tau_1 + n_2\log n_1) \tag{1.18}$$

En utilisant (1.17) on montre que

$$\sum_{z\in\mathrm{V}_{\mathbb{C}}(f)} -\mu(z) \cdot \log|g_{i(z)}(z)| \leq d \in \mathrm{O}(n_2\tau_1). \tag{1.19}$$

En appliquant le Lemme 1.7, on montre que

$$\sum_{z\in\mathrm{V}_{\mathbb{C}}(f)} \mu(z)|\log|g_{i(z)}(z)|| \leq 2c + d. \tag{1.20}$$

□

Proposition 1.9
Si $f \in \mathbb{Z}[\mathrm{X}]$ *un polynôme de* magnitude (n,τ), *alors*

(a) $\mathrm{logsep}^{\star}(f) \in \tilde{\mathrm{O}}(n\tau)$.

(b) $\mathrm{logsep}(f) \in \tilde{\mathrm{O}}(n\tau + n^2)$.

Le résultat ci-dessus a été déjà établi dans Kobel and Sagraloff [24]. Il s'agit ici de proposer une démonstration plus simple en s'appuyant sur la Proposition 1.8.

Démonstration

(a) Soit l'application $\phi : \mathrm{V}_{\mathbb{C}}(f) \mapsto \mathrm{V}_{\mathbb{C}}(f)$ qui a chaque racine z de f associe une racine z', telle que $|z - z'| = \min_{x \in \mathrm{V}_{\mathbb{C}}(f)-z} |z - x|$.

D'après l'équation (1.8) et le Lemme 1.5, on a

$$\prod_{z \in \mathrm{V}_{\mathbb{C}}(f)} \mathrm{sep}(z, f) \leq 2^n \cdot \prod_{z \in \mathrm{V}_{\mathbb{C}}(f)} (\max(1, |z|) \cdot \max(1, |\Phi(z)|)) \leq 2^n \cdot \widehat{\mathrm{Mea}}(f)^7.$$

(b) D'après la Proposition 1.6 (a)

$$\mathrm{logsep}(f) \in \mathrm{O}(n(n + \log \mathrm{Len}(f) + \log \widehat{\mathrm{Mea}}(f)) + \widehat{\log \mathrm{GDisc}}(f))$$

On sait que les dérivées de f sont de *magnitudes* bornées par $(n, n+\tau)$. En appliquant la Proposition1.8 b) à la famille des premières dérivées non nulles de f en ses racines, on obtient :

$$\widehat{\log \mathrm{GDisc}}(f) \in \tilde{\mathrm{O}}(n^2 + n\tau).$$

D'après la Proposition 1.7 (1.12) $\log \widehat{\mathrm{Mea}}(f) \in \mathrm{O}(\tau + \log n)$. Le résulat est obtenu en remplaçant $\log \widehat{\mathrm{Mea}}(f), \widehat{\log \mathrm{GDisc}}$ et $\log \mathrm{Len}(f)$ par leurs bornes dans la Proposition 1.6 (a). □

1.2 Algorithme d'isolation des racines d'un polynôme

A présent, nous nous intéressons au calcul des racines d'un polynôme univarié.

1.2.1 Notion de complexité

Définition 1.8

Un algorithme *est une procédure constituée d'une suite finie d'opérations ou d'instructions permettant de résoudre un problème ou d'obtenir un résultat. Il reçoit une* `entrée` *et renvoie une* `sortie` *après avoir exécuté un nombre fini d'opérations. Dans notre contexte, une* `entrée` *est un ensemble de polynômes dont les coefficients appartiennent à* $\mathbb{Z}, \mathbb{C}, \mathbb{Z}[X], \mathbb{C}[X]$ *etc. La taille d'une* `entrée` *est un vecteur d'entiers représentant le degré d'un polynôme et/ou le nombre de variables ou de polynômes, la taille d'une matrice etc.*

Définition 1.9 *Basu et al. [4, section 8.1]*

La complexité *d'un algorithme est une fonction qui associe à la taille v d'une* entrée *une borne sur le nombre d'opérations effectuées par l'algorithme lorsqu'il parcourt toutes les* entrées *de taille v. Toutefois, la complexité d'un algorithme décrite en terme d'opérations arithmétiques ne donne pas souvent une bonne estimation du temps exact de calcul après son implémentation. Ceci est dû à l'accroissement des coefficients dans les opérations intermédiaires; d'où la nécessité de prendre en compte la taille binaires des entrées.*

Proposition 1.10 *Basu et al. [4]*

Soient $f \in \mathbb{Z}[X]$ un polynôme de magnitude (n, τ) *et g un polynôme de degré n_1 tels que g divise f. Alors, g est de* magnitude $(n_1, n_1 + \tau + \log(n+1))$.

Proposition 1.11

Soient $f \in \mathbb{Z}[X]$ et $f_1, f_2 \in \mathbb{Q}[X]$ tels que $f = f_1 f_2$. Alors, il existe deux polynômes $\bar{f}_1, \bar{f}_2 \in \mathbb{Z}[X]$ tels que $\bar{f}_1, \bar{f}_2$ soient proportionnels à f_1, f_2 et $f = \bar{f}_1 \bar{f}_2$.

Proposition 1.12 *Gathen and Gerhard [15]*
Soient $f, g \in \mathbb{Z}[X]$ deux polynômes de magnitudes *respectives (n_1, τ_1) et (n_2, τ_2). Le calcul du* $\mathrm{pgcd}(f, g)$ *a une complexité binaire en*

$$\tilde{O}(\max(n_1, n_2) \cdot (n_1\tau_2 + n_2\tau_1)).$$

Proposition 1.13 *Gathen and Gerhard [15, Exo.* 10.21*]*
Soient $f \in \mathbb{Z}[X]$ un polynôme de magnitude (n, τ) *et $g \in \mathbb{Z}[X]$ un polynôme qui divise f. Alors le calcul du quotient de f par g (f/g) peut s'effectuer avec une complexité en $\tilde{O}(n\tau + n^2)$.*

Proposition 1.14 *Basu and Zell [3], Kerber and Sagraloff [23]*
Soient $f \in \mathbb{Z}[X]$ un polynôme de magnitude (n, τ) *et r un nombre rationnel de taille binaire $\lambda(r)$. Alors, l'évaluation de f au point r peut se faire en $\tilde{O}(n(\tau + \lambda(r)))$ opérations binaires et la taille binaire de la sortie $f(r)$ est en $\tilde{O}(\tau + n\lambda(r))$.*

1.2.2 Factorisation d'un polynôme

Un algorithme de factorisation prend en entrée un polynôme et renvoie une approximation de ses racines, donnant ainsi une expression du polynôme sous la forme d'un produit fini de facteurs.

Définition 1.10

- *Soient $a \in \mathbb{C}$ et un* L *un entier. On dit qu'un nombre Gaussien dyadique de la forme $\tilde{a} = c \cdot 2^{-L-1} + \mathbf{i} \cdot d \cdot 2^{-L-1} \in \mathbb{Q} + \mathbf{i} \cdot \mathbb{Q}$, avec $c, d \in \mathbb{Z}$, est une* L-approximation binaire (absolue) *de a si $|a - \tilde{a}| < 2^{-L}$.*
- *Soit $f = a_0 + \cdots + a_n X^n \in \mathbb{C}[X]$ un polynôme à coefficients complexes et* L *un entier. On dit que le polynôme $\tilde{f} = \tilde{a}_0 + \cdots + \tilde{a}_n X^n$ est une* L-approximation binaire (absolue) *de f si pour tout i, $\tilde{a}_i$ est une* L-approximation binaire (absolue) *de a_i.*

Définition 1.11
Soient $f \in \mathbb{C}[X]$ un polynôme de degré n et z une racine de f. On dit que :

(a) Si $z \in \mathbb{R}$, l'intervalle $\mathscr{I} =]a, b[$, contenant uniquement z en tant que racine de f, est un ***intervalle d'isolation adéquat*** *(well-isolating interval) de z si $|b - a| < \frac{\mathrm{sep}(z,f)}{32n}$.*

(b) Si $z \in \mathbb{C}$, le disque $\mathscr{D}_r(m) = \{z \in \mathbb{C},\ |z - m| \leq r\}$, contenant uniquement z en tant que racine de f, est un disque d'isolation adéquat (well-isolating disk) de z si $r < \frac{\mathrm{sep}(z,f)}{64n}$.

Le Lemme ci-dessous permet d'apprécier la qualité des approximations calculées.

Lemme 1.8 *Mehlhorn et al. [33, Théorème 2] Pan [42]*
Soient $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{C}[X]$ un polynôme de degré n et $z_1, \ldots, z_k$ ses racines distinctes. Si, quelque soit $1 \leq i \leq k$, $|z_i| \leq 1$ alors, pour tout entier naturel $b \geq n \log n$, il est possible de calculer des approximations $\hat{z}_1, \ldots, \hat{z}_n$ des racines de f, telles que

$$\mathrm{Len}\left(f - a_n \prod_{j=1}^{n} (X - \hat{z}_j)\right) \leq 2^{-b}\mathrm{Len}(f); \tag{1.21}$$

en $\tilde{O}(n)$ opérations avec une précision de $\tilde{O}(bn)$ opérations binaires. Le paramètre b permet de contrôler la distance entre les $hatz_i$ et les vraies valeurs z_i.

Remarque 1.3
Toutefois, l'algorithme de Pan s'applique uniquement aux polynômes dont les racines sont contenues dans le disque unité. Pour tout autre polynôme complexe, il faut au préalable procéder à un changement de variable afin de se ramener à la situation précédente. La transformation appliquée dans Mehlhorn et al. [33] consiste à calculer un entier naturel K, tel que $\kappa \leq K < \kappa + 8 \log n$, et de choisir un entier $s := 2^K$ pour définir le polynôme $f_s := P(s \cdot X) = \sum_{i=0}^{n} a_i' X^i$. Les racines $\{\zeta_i = \frac{z_i}{s}\}_{1 \leq i \leq n}$ de f_s sont toutes dans le disque unité $\Delta(0, 1)$. Ce qui permet de déduire une approximation des racines de f à partir de celle de f_s.

Corollaire 1.1
Soit le polynôme $f = a_n X^n + \ldots + a_0 \in \mathbb{C}[X]$, *tel que* $1/4 \le |a_n| \le 1$. *Pour tout entier naturel* $b \ge n \log n$, *on peut calculer des nombres complexes* $\hat{z}_1, \ldots, \hat{z}_n$ *tels que*

$$\mathrm{Len}\left(f - a_n \prod_{j=1}^{n} (X - \hat{z}_j)\right) \le 2^{-b}\mathrm{Len}(f) \tag{1.22}$$

en $\tilde{O}(n^2\kappa + bn)$ *opérations binaires avec* $\kappa := M(\max_i \log(M(z_i)))$. *L'algorithme renvoie les parties réelles et imaginaires des* $\hat{z}_i$ *sous forme de fractions dyadiques* $A \cdot 2^{-B}$ *; où* $A \in \mathbb{Z}$, $B \in \mathbb{N}$ *et* $B = O(b + n\kappa)$.

1.2.3 Algorithme d'isolation

Isoler les racines d'un polynôme univarié consiste à calculer un ensemble de domaines deux à deux disjoints tels que chaque domaine contient exactement une racine du polynôme. Plus précisément, il s'agit d'un ensemble de disques (resp. d'intervalles) d'isolation pour les racines complexes (resp. réelles). La meilleure borne de complexité atteinte dans le cas de ce problème, détenue par Mehlhorn et al. [33], est de $\tilde{O}(n^3 + n^2\tau)$ opérations binaires pour un polynôme complexe de degré n dont les coefficients sont bornés par 2^τ. L'algorithme requiert de connaître le nombre de racines distinctes et un oracle qui permet d'approcher suffisamment les coefficients du polynôme.

La Proposition ci-dessous donne la borne de complexité optimale sur les algorithmes d'isolation des racines d'un polynôme complexe univarié.

Proposition 1.15 *(Mehlhorn et al. [34, Thm. 4]*[1]*)*
Soit $f \in \mathbb{C}[X]$ *un polynôme de degré* n *avec* $1/4 \le \mathrm{LCF}(f) \le 1$. *Si* f *admet exactement* m *racines distinctes alors :*

(a) avec un nombre d'opérations binaires borné par

$$\tilde{O}\left(n \cdot (n^2 + n\,\mathrm{logMea}(f) + \mathrm{logsep}(f) + \widehat{\mathrm{logGDisc}}(f))\right) \tag{1.23}$$

on peut calculer des disques d'isolation adéquats $\mathscr{D}_{r(z)}(m(z), r) \subset C$, *avec des centres dyadiques* $m(z)$ *et des rayons dyadiques* $r(z)$, *pour toutes les racines* $z \in V_{\mathbb{C}}(f)$ *ainsi que leur multiplicités* $\mu(z)$ *respectives. De plus, la somme sur les tailles binaires de tous les* $m(z)$ *et* $r(z)$ *est en* $\tilde{O}(\mathrm{logMea}(f) + \mathrm{logsep}^\star(f))$. *Le calcul d'une* L*-approximation binaire des coefficients du polynôme* f *nécessitera un entier* L *borné par*

$$\tilde{O}\left(n + n\,\mathrm{logMea}(f) + \mathrm{logsep}(f) + \widehat{\mathrm{logGDisc}}(f)\right). \tag{1.24}$$

(b) Soient $V^* \subset V_{\mathbb{C}}(f)$, $\mu_{\max} := \max_{z \in V^*} \mu(z)$, *et* κ *un entier strictement positif. Alors, pour tout* $z \in V^*$, *le disque* $\mathscr{D}_{r(z)}(m(z))$ *peut être réduit à une taille inférieure ou égale à* $2^{-\kappa}$, *tout cela avec*

$$\tilde{O}\left(n \cdot \left(\kappa \cdot \mu_{\max} + n^2 + n\,\mathrm{logMea}(f) + \mathrm{logsep}(f) + \widehat{\mathrm{logGDisc}}(f)\right)\right) \tag{1.25}$$

opérations binaires.[2] *L'oracle requiert en entrée un entier* κ *bornée par*

$$\tilde{O}\left(\kappa \cdot \mu_{\max} + n + n\,\mathrm{logMea}(f) + \mathrm{logsep}(f) + \widehat{\mathrm{logGDisc}}(f)\right). \tag{1.26}$$

pour fournir une κ*-approximation binaire absolue des coefficients du polynôme* f.

1. Voir aussi Becker et al. [5], Mehlhorn et al. [33], Pedersen [44], Pan and Tsigaridas [43], Sagraloff and Mehlhorn [48]

2. Mehlhorn et al. [34, Thm. 4] fournit uniquement une borne sur le raffinement des disques d'isolations adéquats (i.e. pour $V^* = V_C(f)$). Toutefois, la borne s'obtient directement à partir de la preuve du Mehlhorn et al. [34, Theorem. 4]. De plus, le terme supplémemntaire $n\kappa \cdot \max_i \mu_i$ qui apparaît dans Mehlhorn et al. [34, Theorem 4], correspond à la borne sur la taille des précisions requises en entrée. Notons que c'est une faute de frappe et que la vraie borne est meilleure d'un facteur n. Cette erreur est aussi soulignée dans la démonstration du Mehlhorn et al. [34, Theorem 4].

Le Corollaire suivant découle de la Proposition 1.15 et de la Proposition 1.6 (1.6).

Corollaire 1.2
Si $f \in \mathbb{C}[X]$ est un polynôme sans facteur carré de degré n tel que $1/4 \leq \mathrm{LCF}(f) \leq 1$, alors on a les propositions suivantes :

(a) Les bornes obtenues dans (1.23) et (1.24) peuvent être remplacées par[3]

$$\tilde{\mathrm{O}}\left(n(n^2 + n(\log\widehat{\mathrm{Mea}}(f) + \log\mathrm{Len}(f)) + |\log(|\mathrm{Disc}(f)|)|\right)$$

et

$$\tilde{\mathrm{O}}(n(n\log\widehat{\mathrm{Mea}}(f) + n\log\mathrm{Len}(f)) + |\log(|\mathrm{Disc}(f)|)|).$$

(b) Soit $\mathrm{V}^* \subset \mathrm{V}_{\mathbb{C}}(f)$ un sous-ensemble des racines de f et κ un entier strictement positif. Alors, on peut raffiner davantage le disque $\mathscr{D}_{r(z)}(m(z))$ pour toutes les racines $z \in \mathrm{V}^*$ à une taille inférieure ou égale à $2^{-\kappa}$ en

$$\tilde{\mathrm{O}}\left(n \cdot \left(\kappa + n^2 + n(\log\widehat{\mathrm{Mea}}(f) + \log\mathrm{Len}(f)) + |\log(|\mathrm{Disc}(f)|)|\right)\right) \tag{1.27}$$

opérations binaires. Le calcul requiert en entrée un oracle qui lui fournit une κ-approximation de f, avec κ borné par

$$\tilde{\mathrm{O}}\left(\mathrm{L} + n(\log\mathrm{Len}(f)) + \log\widehat{\mathrm{Mea}}(f)) + |\log(|\mathrm{Disc}(f)|)|\right). \tag{1.28}$$

Remarque 1.4

— *Le fait de disposer d'un disque d'isolation adéquat autour de chacune des racines complexes d'un polynôme $f \in \mathrm{R}[X]$ permet entre autre d'en déduire un intervalle d'isolation adéquat pour chaque racine réelle de f. En effet, les racines complexes d'un polynôme à coefficients réels apparaissent par paires de nombres complexes conjugués. Donc leurs disques d'isolation adéquats correspondent à ceux qui intersectent l'axe des abscisses. Ces intersections constituent des intervalles d'isolation pour des racines réelles du polynôme f.*

Toutesfois, lorsque le polynôme est d'emblée identifié comme étant sans facteur carré, il est préférable d'utiliser des méthodes de calcul spécifiquement dédiées au calcul des racines de polynômes réelles. On trouve dans [47] une telle méthode ayant les mêmes bornes que celles ci-dessus. Voir aussi les récents travaux dans [25] où il est proposé une implémentation efficace de cette méthode.

— *L'analyse de la complexité ne prend pas en compte le coût exact du calcul des approximations, qui peut être considérablement grand par rapport au coût de "lecture" des approximations. En particulier, si les coefficients dépendent de nombres algébriques de degrés très élevés.*

Toutefois, il existe un cas particulier concret pour lequel il est possible de calculer des approximations dyadiques de façon efficace.

Proposition 1.16 *Kerber and Sagraloff [23]*
Soient $f \in \mathbb{Z}[X]$ un polynôme de magnitude (n, τ), *$z \in \mathbb{C}$ et L un entier positif. Alors, il est possible de calculer des approximations* dyadiques $\tilde{\beta}_k = b_k \cdot 2^{-\mathrm{L}-1}$ *de $\beta_k := f^{[k]}(z)$ avec $k = 0, \ldots, n$ (voir Équation (1.1)) telles que $b_k \in \mathbb{Z}$ et $|\beta_k - \tilde{\beta}_k| < 2^{-\mathrm{L}}$, en*

$$\tilde{\mathrm{O}}(n(\mathrm{L} + n \cdot \log\max(1, |z|) + \tau))$$

opérations binaires. L'algorithme requiert des L-approximations binaires de f pour $\mathrm{L} = 1, 2, 4, \ldots, \mathrm{L}'$ où L' est de l'ordre de $\tilde{\mathrm{O}}(\mathrm{L} + n \cdot \log\max(1, |z|) + \tau)$.

3. Ce résultat découle directement de 1.6 b).

Cependant, il est préférable de traiter le cas racines réelles à l'aide de la méthode dyadique. En particulier, lorsque le polynôme est identifié comme étant sans facteur carré. On retrouve une méthode similaire dans Sagraloff and Mehlhorn [47] ayant un temps d'exécution du même ordre de grandeur que les bornes ci-dessus. Dans des travaux récents, Kobel et al. [25] présente une implémentation efficace de cette méthode.

La proposition ci-dessous présente des bornes sur le calcul et le raffinement des disques d'isolation. C'est une conséquence immédiate de la proposition 1.15 (appliquée au polynôme $f \cdot \mathrm{LCF}(f)^{-1}$).

Proposition 1.17 *(Mehlhorn et al. [34, Thm. 5][4])*
Soit $f \in \mathbb{Z}[X]$ un polynôme de magnitude (n, τ). *Les instructions ci-dessous peuvent être exécutées en $\tilde{O}(n^2\tau + n^3)$ opérations binaires.*

(a) Calculer un disque d'isolation adéquat $\mathcal{D}_{r(z)}(m(z)) \subset C$ pour toute racine complexe z de f, ayant pour centre dyadique $m(z)$ et rayon dyadique $r(z)$, tel que la somme de toutes les tailles binaires de $m(z)$ et $r(z)$ soit en $\tilde{O}(n\tau)$,

(b) Trouver la multiplicité μ_i de chaque racine z_i de f.

(c) Les disques d'isolation peuvent être raffinés à une taille inférieure ou égale à 2^{-L} en $\tilde{O}(n^2\tau + n^3 + nL)$ opérations binaires[5] ; où L est un entier strictement positif.

Proposition 1.18
Soient $f, g_1, \ldots, g_m \in \mathbb{Z}[X]$ des polynômes de magnitudes *respectives (d, τ), $(d_1, \tau_1), \ldots, (d_m, \tau_m)$ et N, Λ deux entiers strictement positifs tels que $d + d_1 + \cdots + d_m < N$ et $\tau + \tau_1 + \cdots + \tau_m < \Lambda$. Alors les instructions ci-desous peuvent être exécutées en $\tilde{O}(N^2\Lambda + N^3)$ opérations binaires :*

(a) Isoler les racines réelles (complexes) du polynôme f ainsi que celles des polynômes g_i ;

(b) Identifier les racines communes du couple de polynômes (f, g_i), $i = 1, \ldots, m$;

(c) Déterminer le signe de g_i (0, 1 or -1) en les racines réelles de f, pour $i = 1, \ldots, m$.

Démonstration
Supposons que les polynômes $f, g_1, \ldots, g_m \in \mathbb{Z}[X]$ sont sans facteur carré (au cas contraire, il suffit de diviser chaque polynôme par son *pgcd* avec sa première dérivée pour retrouver la partie sans facteur carré). D'après la Proposition 1.12, le calcul des parties sans facteurs carrés des polynômes peut s'effectuer en

$$\tilde{O}(d^2\tau) + \sum_{i=1}^{m} \tilde{O}(d_i^2\tau_i) = \tilde{O}(N^2\Lambda)$$

opérations binaires. De plus, les parties sans facteurs carrés de f et des g_i ont des magnitudes respectivement bornées par $(d, O(d + \tau))$ et $(d_i, O(d_i + \tau_i))$. Donc, pour tout indice i, on peut calculer le polynôme $h_i := \mathrm{pgcd}(f, g_i)$ en

$$\sum_{i=1}^{m} \tilde{O}(\max(d, d_i).(d\tau_i + d d_i + d_i\tau)) = \tilde{O}(N(d\Lambda + N\tau + dN)$$

opérations binaires.

Dans l'étape d'après, il s'agit tout d'abord de calculer des disques d'isolation adéquats pour les racines complexes de f ainsi que celles des polynômes h_i pour tout indice i. Ensuite, de raffiner les disques d'isolation des racines des polynômes h_i à un rayon inférieur ou égale à $\mathrm{sep}(f)/4$. Sachant que $|\log \mathrm{sep}(f)|$ est bornée par $\tilde{O}(N\Lambda)$, ce calcul peut s'effectuer en $\tilde{O}(N^3 + N^2\Lambda)$ opéraions

4. voir aussi Becker et al. [5], Mehlhorn et al. [33], Pedersen [44], Pan and Tsigaridas [43], Sagraloff and Mehlhorn [48]

5. Notons que, contrairement au cas général où les coefficients de f ne sont pas nécesairement des entiers, le facteur additionnel $\max \mu(z)$ n'apparait pas. Ceci est dû au fait qu'avec la complexité donnée on peut tout d'abord calculer la partie sans facteur carré $f^\star$ et travailler avec $f^\star$ pour le raffinement des disques d'isolation.

binaires. Notons que, après le processus de raffinement, chaque disque d'isolation D′ d'une racine h_i intersecte exactement un seul disque d'isolation parmi ceux des racines de f. Ce qui signifie que les disques D et D′ isolent la même racine. Ainsi, afin d'identifier les racines communes à f et g_i, il suffit de déterminer toutes les intersections entre les disques d'isolation des racines de h_i et ceux des racines de f. Pour cela, il s'agira tout d'abord de recenser les parties réelle et complexe du centre de chaque disque d'isolation. Ensuite, d'appliquer une recherche binaire pour déterminer le disque d'isolation de f qui intersecte un disque d'isolation D′ de g_i en effectuant $O(\log n)$ comparaisons entre des nombres ayant une taille binaire de l'ordre de $\tilde{O}(N\Lambda)$. Par conséquent, la compexité globale reste bornée par $\sum_{i=1}^{m} d_i \cdot \tilde{O}(N\Lambda) = \tilde{O}(N^2\Lambda)$.

La détermination du signe se fait par l'évaluation du polynôme g_i aux extrémités de l'intervalle d'isolation de chaque racine réelle z de f non commune à g_i. □

Chapitre 2

Topologie de courbes algébriques

Introduction

Dans ce chapitre, nous traitons du problème qui consiste à calculer la topologie d'une courbe algébrique plane.
Soient $P \in \mathbb{Z}[X,Y]$ un polynôme sans facteur carré de magnitude (d,τ) et considérons la courbe algébrique plane $V_{\mathbb{R}}(P) := \{(\alpha,\beta) \in \mathbb{R}^2,\ P(\alpha,\beta) = 0\}$: c'est-à-dire définie comme étant l'ensemble des zéros réels de P. La topologie de $V_{\mathbb{R}}(P)$ est obtenue par le calcul d'un complexe simplicial (un graphe [1]) isotope à $V_{\mathbb{R}}(P)$. La visualisation des courbes algébriques planes, voire l'acquisition des formes, apparaissent dès lors comme une motivation primaire. Par ailleurs, l'attractivité de ce thème de recherche s'explique aussi à travers ses nombreuses applications pratiques telles que : le calcul d'intersection de surfaces algébriques, le maillage de surfaces algébriques implicites, le calcul de la courbe d'auto-intersection d'une surface paramétrique etc.
Les algorithmes de calcul de la topologie d'une courbe peuvent être classés en deux sous-groupes :

- **Les algorithmes de type balayage.** Ces algorithmes requièrent que la courbe soit en position générique. Le procédé consiste à détecter les endroits où la topologie de la courbe change, par le biais d'un balayage vertical du plan à l'aide d'une droite. On peut citer dans cette catégorie les travaux de Coste and Roy [7], Gonzalez-Vega and Kahoui [17], Diochnos et al. [11], (voir aussi le livre de Basu et al. [4]).

- **Les algorithmes de type subdivision.** Il s'agit d'un découpage du plan par de petits rectangles, appelés boîtes, et de déterminer la topologie de la courbe dans chaque boîte. La difficulté principale se situe dans l'exécution de la deuxième étape pour une boîte qui contient un point singulier de la courbe. Cela est due au fait qu'il faut connaître, au préalable, la structure des singularités. On retrouve dans cette catégorie les travaux de Cheng et al. [6].

L'algorithme que nous présentons dans ce chapitre, calcule la topologie d'une courbe algébrique plane $V_{\mathbb{R}}(P)$ en $\tilde{O}(d^5\tau + d^6)$ opérations binaires. Contrairement aux travaux de Mehlhorn et al. [33], qui détiennent le premier algorithme permettant de résoudre ce problème avec une complexité de $\tilde{O}(d^5\tau + d^6)$, notre algorithme n'impose pas de placer la courbe en position générique. Il constitue ainsi une amélioration des travaux de Diatta et al. [9] dans lequel les auteurs adoptent une démarche similaire mais avec une complexité de $\tilde{O}(d^6\tau + d^7)$.

La section 2.1 comporte des résultats sur l'évaluation de polynômes bivariés à coefficients entiers par des nombres rationnels ou algébriques. Quant-à la la section 2.4, elle est dédiée au calcul du nombre de racines distinctes d'un polynôme à coefficients algébriques. Nous présentons dans la section 2.5 une version améliorée de la CAD en nous appuyant sur les calculs effectués dans les sections 2.4 et 2.1.

1. Un ensemble d'arêtes et de sommets

2.1 Polynômes à coefficients algébriques

La définition ci-dessous est une généralisarion de la définition 1.7 pour les polynômes bivariés.

Définition 2.1
Soient n et τ deux entiers naturels non nuls. Un polynôme $F \in \mathbb{Z}[X,Y]$ est de magnitude (n,τ) s'il est de degré au plus n et que la valeur absolue de chacun de ses coefficients est inférieure ou égale à 2^τ.

2.1.1 Quelques résultats sur les polynômes bivariés

Proposition 2.1
Soit $F(X,Y) \in \mathbb{Z}[X,Y]$ un polynôme bivarié dont la valeur absolue de chaque coefficient est bornée par 2^τ tel que $n_x = \deg_X(F), n_y = \deg_Y(F)$. Si $(z,z') \in \mathbb{C}^2$, alors

$$|F(z,z')| \leqslant (n_x+1)(n_y+1)2^\tau \max(1,|z|)^{n_x} \max(1,|z'|)^{n_y}.$$

La Proposition ci-dessous donne une borne sur l'*évalution approximative bivariée*. C'est une conséquence directe de la Proposition 1.14.

Proposition 2.2 *Kobel and Sagraloff [24]*
Soit $F \in \mathbb{Z}[X,Y]$ un polynôme bivarié de magnitude (n,τ). Pour tout couple $(z,z') \in \mathbb{C}^2$ et tout entier naturel strictement positif $L \in \mathbb{N}_{\geq 1}$, on peut calculer une approximation dyadique $\tilde{F}(z,z') = c \cdot 2^{-L-1}$ de $F(z,z')$, en

$$\tilde{O}(n^2(L + n\cdot(\log\max(1,|z|) + \log\max(1,|z'|)) + \tau))$$

opérations binaires; où $c \in \mathbb{Z}$ et $|F(z,z') - \tilde{F}(z,z')| < 2^{-L}$. Ce calcul requiert en entrée des approximations dyadiques $\tilde{z} = a\cdot 2^{-L'-1}$, $\tilde{z}' = b\cdot 2^{-L'-1}$ de z, z' ; où $a,b \in \mathbb{Z}$, $|z-\tilde{z}| < 2^{-L'}$, $|z'-\tilde{z}'| < 2^{-L'}$ et L' est bornée par $\tilde{O}(L + n\cdot(\log\max(1,|z|) + \log\max(1,|z'|)) + \tau)$.

La proposition ci-dessous donne la complexité de l'évalution exacte d'un polynôme bivarié $F \in \mathbb{Z}[X,Y]$ en un point rationnel (r_1, r_2).

Proposition 2.3
Soit $F \in \mathbb{Z}[X,Y]$ un polynôme bivarié de magnitude (n,τ). Soient $(r_1,r_2) \in \mathbb{Q}^2$ deux nombres rationnels tels que les valeurs absolues des numérateurs et dénominateurs sont inférieures ou égales à 2^λ. Alors, l'évalution de $F(r_1,r_2)$ peut de faire de façon exacte en $\tilde{O}(n^2(\tau+\lambda))$ opérations binaires.

Démonstration
Soit $F = f_0(X) + \cdots + f_n(X)Y^n$ avec $f_i(X) \in \mathbb{Z}[X]$. D'après la Proposition1.14, l'évaluation de $f_i(r_1)$ est en $\tilde{O}(n^2(\tau+\lambda))$ opérations binaires, pour tout $i = 0,\ldots,n$. Supposons que $r_1 = p/q$, où p et q sont deux entiers co-premiers, alors $q^n \cdot f_i(r_1)$ est un entier de taille binaire $O(\tau + n\lambda)$. Le calcul de chaque $q^n \cdot f_i(r_1)$ nécessite $\tilde{O}(\tau + n\lambda)$ opérations binaires. Par conséquent, on peut calculer $q^n \cdot F(r_1,Y) \in \mathbb{Z}[Y]$ avec $\tilde{O}(n^2(\tau+\lambda))$ opérations binaires. Sachant que les coefficients du polynôme $q^n \cdot F(r_1,Y)$ sont des entiers de taille binaire en $O(\tau + n\lambda)$, on en déduit que le calcul $q^n \cdot F(r_1,r_2)$ peut s'effectuer en $\tilde{O}(n^2(\tau+\lambda))$ opérations binaires. □

Proposition 2.4 *Basu et al. [4]*
Soient $F,G \in \mathbb{Z}[X,Y]$ deux polynômes de magnitude (n,τ).

(a) La complexité du calcul des polynômes sous-résultants de F et G par rapport à la variable Y est en $\tilde{O}(n)$ opérations arithmétiques.

(b) Les coefficients sous-résultants de F et G par rapport à la variable Y sont des polynômes en X dont les coefficients ont une taille binaire en $\tilde{O}(n^4\tau)$.

(c) La complexité du calcul des coefficients sous-résultants de F et G est en $\tilde{O}(n^4\tau)$ opérations binaires.

Soient $R \in \mathbb{Z}[X]$ un polynôme de magnitude (N, Λ) et z une racine complexe de R et de multiplicité $\mu(z) := \mathrm{mult}(z, R)$. Soit

$$F(X,Y) = f_{n_y}(X) \cdot Y^{n_y} + \cdots + f_0(X) \in \mathbb{Z}[X,Y]$$

un polynôme bivarié de magnitude (n, τ) tel que $\mathrm{pgcd}(f_0(X), \ldots, f_{n_y}(X)) = k$; où $k \in \mathbb{Z}$. C'est-à-dire que F ne peut pas s'écrire sous la forme d'un produit de deux poynômes $h(X) \times G(X,Y)$ où $h(X) \in Z[X]$ est un polynôme non constant. Par conséquent, la courbe définie par l'équation $F = 0$ ne peut contenir de droites verticales. Pour tout $\ell \leq n_y$, on définit le polynôme

$$F_\ell(X,Y) := f_\ell(X) \cdot Y^\ell + \ldots + f_0(X).$$

Pour toute racine z de R de multiplicité $\mu(z) := \mathrm{mult}(R, z)$, on désigne par $n(z)$ le degré du polynôme $F(z,-) \in Z[Y]$. D'après les hypothèses ci-dessus $0 \leq n(z) \leq n_y$. Donc pour tout $n(z) \neq n_y$, on a $f_{n(z)}(z) \neq 0$ et $f_{n(z)+1}(z) = \cdots = f_{n_y}(z) = 0$. Pour toute racine z' de $F(z,-)$, on note par $\mu(z,z') = \mathrm{mult}(F(z,-), z')$ la multiplicité de z' en tant que racine du polynôme $F(z,-)$.

La proposition suivante donne des bornes de complexité amorties sur la somme des mesures de Mahler des polynômes $F(z,-)$.

Proposition 2.5
Soient $R \in \mathbb{Z}[X]$ *et* $F \in \mathbb{Z}[X,Y]$ *deux polynômes satisfaisant les hypothèses ci-dessus.*
On a alors :

$$\sum_{z \in V_{\mathbb{C}}(R)} \mu(z) \cdot \log \mathrm{Len}(F(z,-)) = \tilde{O}(N\tau + n\Lambda + nN) \tag{2.1}$$

$$\sum_{z \in V_{\mathbb{C}}(R)} \mu(z) \cdot \log \mathrm{Mea}(F(z,-)) = \tilde{O}(N\tau + n\Lambda + nN) \tag{2.2}$$

$$\sum_{z \in V_{\mathbb{C}}(R)} \mu(z) \cdot \log \widehat{\mathrm{Mea}}(F(z,-)) = \tilde{O}(N\tau + n\Lambda + nN). \tag{2.3}$$

Démonstration
Soit $z \in \mathbb{C}$ une racine complexe de R. D'après la Définition 1.3 et la Proposition 1.7, on a

$$2^{-n(z)} \mathrm{Len}(F(z,-)) \leq \mathrm{Mea}(F(z,-)) \leq \|F(z,-)\|$$

On sait que $n(z) \leq n$ et $\sum_{z \in V_{\mathbb{C}}(R)} \mu(z) = N$, donc

$$\sum_{z \in V_{\mathbb{C}}(R)} n(z)\mu(z) \leq nN$$

$$2^{-nN} \leq 2^{-\sum_{z \in V_{\mathbb{C}}(R)} n(z)\mu(z)}.$$

Soit $\ell(z) \in \mathbb{N}$ l'indice tel que

$$|f_{\ell(z)}(z)| = \max_{j=0,\ldots,n_y} |f_j(z)|.$$

Alors, on a

$$|\mathrm{LCF}(F(z,-))| = |f_{n(z)}(z)| \leq \mathrm{Len}(F(z,-)) \leq (n_y+1)|f_{\ell(z)}(z)|$$

$$\|F(z,-)\| \leq \sqrt{n_y+1} \cdot |f_{\ell(z)}(z)|.$$

Par conséquent, on a

$$2^{-n} \prod_{z \in V_{\mathbb{C}}(R)} |f_{n(z)}(z)|^{\mu(z)} \leq \prod_{z \in V_{\mathbb{C}}(R)} \mathrm{Mea}(F(z,-))^{\mu(z)} \leq \sqrt{n_y+1}^N \cdot \prod_{z \in V_{\mathbb{C}}(R)} |f_{\ell(z)}(z)|^{\mu(z)}.$$

Donc

$$\prod_{z \in V_{\mathbb{C}}(R)} |f_{n(z)}(z)|^{\mu(z)} \leq \prod_{z \in V_{\mathbb{C}}(R)} \mathrm{Len}(F(z,-))^{\mu(z)} \leq (n_y+1)^N \cdot \prod_{z \in V_{\mathbb{C}}(R)} |f_{\ell(z)}(z)|^{\mu(z)}$$

On obient les bornes (2.1) et (2.2) en appliquant la Proposition 1.8 au polynôme R et à la famille de polynômes f_j.

Pour démontrer (2.3), il faut noter que

$$\sum_{z\in V_{\mathbb{C}}(R)} \mu(z)|\log|f_{n(z)}(z)|| = \tilde{O}((N\tau + n\Lambda)).$$

Ceci est une conséquence immédiate de la Proposition1.8 appliquée à R et à la famille des f_i et en utilisant (2.2). □

Lemme 2.1
Soient f, g deux polynômes bivariés de degrés respectifs p, q. Soit ϕ l'application de $K_{<p}[X]\times K_{<q}[X]$ dans $K_{<p+q}[X]$ qui à tout (U,V) associe $Uf+Vg$. Alors $\mathrm{Im}(\phi)$ est l'ensemble des multiples, de degré $< p+q$, du plus grand diviseur commun $h = \mathrm{pgcd}(f,g)$ de f et g, et ϕ est de rang $p+q-\deg(h)$.

Démonstration
Notons que, pour tout polynôme m tel que $\deg(m) < \deg(h)$, le couple $(m\cdot g/h, -m\cdot f/h)$ appartient au noyau $\mathrm{Ker}(\phi)$. Réciproquement, pour tout (U,V) appartenant au noyau $\mathrm{Ker}(\phi)$, il existe un polynôme m de degré inférieur à $\deg(h)$ tel que $U = m\cdot g/h$ et $V = -m\cdot f/h$. Ce qui implique que la dimension du $\mathrm{Ker}(\phi)$ est égale à $\deg(h)$ et la dimension de $\mathrm{Im}(\phi)$ est égale à $p+q-\deg(h)$. Par ailleurs, tout élément de $\mathrm{Im}(\phi)$ est un multiple de h, et l'espace vectoriel des multiples de h de degré $< p+q$ est aussi de dimension $p+q-\deg(h)$. Donc $\mathrm{Im}(\phi)$ correspond bien à l'espace des multiples de h, et ϕ est de rang $p+q-\deg(h)$. □

Lemme 2.2
Soient K un corps et $M(X)$ une matrice carrée de taille $n\times n$ à coefficients dans $K[X]$. Si $M(x_0)$ est de rang $n-k$, alors $X = x_0$ est une racine de $\det(M(X))$ et de multiplicité au moins k.

Démonstration
La démontattion de ce lemme s'effectue par récurrence sur k.

Si $k = 0$, le résultat est vrai.

Si $k > 0$, alors $M(x_0)$ n'est pas inversible, et $\det(M(x_0)) = 0$. Soient $m_{i,j}(X)$ le $(i,j)^{ième}$-élément de $M(X)$, et $M_{i,j}(X)$ la matrice de taille $(n-1)\times(n-1)$ obtenue à partir de $M(X)$ en retirant la $i^{ième}$ ligne et la $j^{ième}$ colonne. $M_{i,j}(x_0)$ est de rang $r(x_0) \le n-k$, donc par récurrence x_0 est une racine de $\det(M_{i,j}(X))$ de multiplicité au moins $(n-1)-r(x_0) \ge k-1$. D'après la formule de Jacobi, on a

$$\frac{d}{dX}\det(M(X)) = \sum_{i,j}(-1)^{i+j} m'_{i,j}(X)\det(M_{i,j}(X)).$$

Le résultat est donc obtenu par réccurence puisque, x_0 est une racine de $\det(M(X))$ et de multiplicité au moins $k-1$ en tant que racine de sa dérivée. □

A présent, nous nous intéressons aux multiplicités des racines d'un polynôme $F(z,-)$; où z est une valeur X-critique de F.

Soit F un polynôme bivarié défini comme suit

$$F(X,Y) = f_{n_y}(X)\cdot Y^{n_y} + \cdots + f_0(X) \in \mathbb{C}[X,Y].$$

Désignons par

$$V_{\mathbb{C}}(F) = \{(x,y)\in\mathbb{C}^2 \mid F(x,y) = 0\}.$$

Notons que $V_{\mathbb{C}}(F)$ ne contient pas de droite verticale si et seulement si les polynômes $f_i(X)$, $i = 0,\ldots,n_y$ n'ont pas de facteur commun non trivial (i.e un polynôme non constant).

Proposition 2.6
Soit $F \in \mathbb{C}[X,Y]$ *un polynôme bivarié sans facteur carré, tel que* $V_{\mathbb{C}}(F)$ *ne contient pas de droite verticale. Si l'on désigne par*

$$\mathrm{Crit}(V_{\mathbb{C}}(F)) = \{(x,y) \in \mathbb{C}^2 \mid F(x,y) = \partial_Y F(x,y) = 0\}$$

l'ensemble des points X*-critiques de* F *et par*

$$\mathrm{Crit}(V_{\mathbb{C}}(F))_z = \{z' \in \mathbb{C} \mid F(z,z') = \partial_Y F(z,z') = 0\}$$

la fibre au dessus du point z*, alors pour tout* $z \in \mathbb{C}$*,*

$$\sum_{z' \in \mathrm{Crit}(V_{\mathbb{C}}(F))_z} (\mathrm{mult}(z', F_{n(z)}(z,Y)) - 1) \leq \mathrm{mult}(z, \mathrm{Disc}_Y(F_{n(z)})). \tag{2.4}$$

La démonstration de la Proposition 2.6 s'appuie sur le Lemme ci-dessous.

Lemme 2.3
Soient F *et* G *deux polynômes bivariés. Pour tout* $z \in \mathbb{C}$*, on a*

$$\deg(\gcd(F(z,Y), G(z,Y))) \leq \mathrm{mult}(z, \mathrm{Res}_Y(F,G)). \tag{2.5}$$

La démonstration du Lemme 2.3 découle directement des Lemmes 2.1 et 2.2.
Démonstration Proposition 2.6
Il suffit d'appliquer le Lemme 2.3 avec $F = F_{n(z)}$, $G = \partial_Y F_{n(z)}(X,Y)$ et de prendre en compte le fait que

$$\sum_{z' \in \mathrm{Crit}(V_{\mathbb{C}}(F))_z} (\mathrm{mult}(z', F_{n(z)}(z,Y)) - 1) = \deg(\gcd(F_{n(z)}(z,Y), \partial_Y F_{n(z)}(z,Y))). \tag{2.6}$$

□

Proposition 2.7
Soit $F \in \mathbb{Z}[X,Y]$ *un polynôme sans facteur carré de magnitude* (d,τ) *tel que* $V_{\mathbb{C}}(F)$ *ne comporte pas de droite verticale. Soit* $\mathrm{Crit}(V_{\mathbb{C}}(F))$ *l'ensemble des points* X*-critiques de* F*. Il existe alors un polynôme* $R_Y \in \mathbb{Z}[Y]$ *de magnitude* $(O(d^2), O(d\tau + d^2))$ *tel que : pour tout* $z' \in \mathbb{C}$

$$\sum_{z \mid (z,z') \in \mathrm{Crit}(V_{\mathbb{C}}(F))} (\mathrm{mult}(z', F_{n(z)}(z,Y)) - 1) \leq \mathrm{mult}(z', R_Y). \tag{2.7}$$

En particulier, parmi les racines de R_Y *se trouvent aussi la projection sur l'axe des* Y *des éléments de* $\mathrm{Crit}(V_{\mathbb{C}}(F))$.

Démonstration Proposition 2.7
(a) Tout d'abord, supposons qu'il existe un unique z tel que pour tout $(z,z') \in \mathrm{Crit}(V_{\mathbb{C}}(F))$,

$$\mathrm{mult}(z', F_{n(z)}(z,Y)) > 1$$

et posons

$$\mu = \mathrm{mult}(z', F_{n(z)}(z,Y))$$

la multiplicité de z' en tant que racine du polynôme $F_{n(z)}(z,Y)$.
Soit

$$R(Y) := \mathrm{Res}_X(F, \partial_Y F)(Y) \tag{2.8}$$

on a

$$R(Y) = U(X,Y)F(X,Y) + V(X,Y)\partial_Y F(X,Y). \tag{2.9}$$

En dérivant $1, \ldots, \mu - 2$ fois l'expression (2.8) par rapport à la variable Y d'une part et en utilisant le fait que

$$F(z,z') = \partial_Y F(z,z') = \ldots = \partial_Y^{(\mu-1)} F(z,z') = 0$$

d'autre part, on montre que

$$R(z') = \partial_Y R(F, \partial_Y F)(z') = \ldots = \partial_Y^{(\mu-2)} R(F, \partial_Y F)(z') = 0. \tag{2.10}$$

(b) Il s'agit maintenant de se ramener au cas plus général, en procédant par le changement de variable $Y \leftarrow Y + \epsilon X$, où ϵ est une nouvelle variable, dans cas traité précédemment. On considère le corps des séries de Puiseux algébriques $\mathbb{R}\langle\epsilon\rangle$ [4]. $\mathbb{R}\langle\epsilon\rangle$ est un corps réel clos qui contient le corps de fraction $\mathbb{R}(\epsilon)$. De plus, lorsque ϵ strictement positif et plus petit que tout élément $\mathbb{R}_*^+$, $\mathbb{R}\langle\epsilon\rangle$ est totalement ordonné pour l'ordre 0_+. Posons $\mathbb{C}\langle\epsilon\rangle^2 = \mathbb{R}\langle\epsilon\rangle^2[i]$.

Notons que, à tout point X-critique $(z, z') \in \mathbb{C}^2$ de F, lui correspond un point X-critique $(z, z' - \epsilon z) \in \mathbb{C}\langle\epsilon\rangle^2$ de $\hat{F}(X, Y) := F(X, Y + \epsilon X)$, et que $z'' = z' - \epsilon z$ est une racine de $\hat{F}(z, -)$ de multiplicité $\mu(z, z')$; mais aussi de $\partial_Y^{(i)} \hat{F}(z, z') = \partial_Y^{(i)} F(z, z'')$. De plus, les ordonnées des points X-critiques de $\hat{F}(X, Y)$ sont deux à deux distinctes. Il s'en suit que, d'après (a,) $z' - \epsilon z$ est une racine de $\mathrm{Res}_X(\hat{F}, \partial_Y \hat{F})(Y)$ dont la multiplicité $\nu(z' - \epsilon z)$ vaut au moins $\mu(z, z')$. Donc, on peut écrire

$$\mathrm{Res}_X(\hat{F}, \partial_Y \hat{F})(Y) = A(\epsilon) \hat{R}(Y, \epsilon) B(Y, \epsilon)$$

où $A(\epsilon) \in \mathbb{C}(\epsilon)$, $\hat{R}(Y, \epsilon)$ est un monôme en la variable Y

$$\hat{R}(Y, \epsilon) = \prod_{(z,z') \in \mathrm{Crit}(V_{\mathbb{C}}(F))} (Y - z' + \epsilon z)^{\nu(z' - \epsilon z)} B(Y, \epsilon),$$

avec

$$\mathrm{mult}(z' - \epsilon z, \hat{F}_{n(z)}(z, Y)) - 1 \leq \nu(z' - \epsilon z), \tag{2.11}$$

et $B(Y, \epsilon) \in \mathbb{C}[X, \epsilon]$ tel que $B(Y, 0) \in \mathbb{Z}[X]$ ne soit pas identiquement nul.
Ainsi, en posant

$$\nu(z') = \sum_{z | (z,z') \in \mathrm{Crit}(V_{\mathbb{C}}(F))} \nu(z' - \epsilon z),$$

on a alors

$$R_Y = \hat{R}(Y, 0) = \prod_{z' \in \pi_Y(\mathrm{Crit}(V_{\mathbb{C}}(F)))} (Y - z')^{\nu(z')} B(Y, 0),$$

avec

$$\sum_{z | (z,z') \in \mathrm{Crit}(V_{\mathbb{C}}(F))} (\mathrm{mult}(z', F_{n(z)}(z, Y)) - 1) \leq \nu(z') \leq \mathrm{mult}(z', R_Y). \tag{2.12}$$

En définitive, notons que R_Y est de magnitude $(O(d^2), O(d\tau + d^2))$. □

Remarque 2.1
Si $\deg_X(F) \geq \deg_Y(F)$ *alors*

$$R_Y(Y) = \mathrm{Res}_X(F, \partial_Y F)(Y).$$

En effet, la matrice de Sylvester associée F *et* $\partial_Y F$ *et celle associée à* $\tilde{F}$ *et* $\partial_Y \tilde{F}$ *sont de même taille. Car* $\deg_X(F) = \deg_X(\tilde{F})$. *Toutefois, si* $\deg_X(F) < \deg_Y(F)$, *alors il est possible que*

$$R_Y(Y) \neq \mathrm{Res}_X(F, \partial_Y F)(Y).$$

2.1.2 Degré d'un polynôme à coefficients algébriques

Dans cette sous-section, nous traitons du problème qui consiste à déterminer le degré d'un polynôme $F(X, Y) \in \mathbb{Z}[X, Y]$ évalué en la racine z d'un poynôme univarié $R[X] \in \mathbb{Z}[X]$. Rappelons que R et F sont de magnitudes respectives (N, Λ) et (n, τ), et que $\deg_y(F) = n_y$. Il s'agit donc d'expliquer en détails la méthode utilisée pour déterminer $\deg_Y(F(z, Y))$. Elle s'appuie principalement sur la construction d'une certaine famille de polynômes $R_\ell^\star$ définie ci-dessous. Soient $R^\star$ la partie sans facteurs carrés de R et

$$R^\star_{\leq n_y}(X) := R^\star(X), \tag{2.13}$$

et pour tout $\ell \in \{n_y, \ldots, 1\}$,

$$R^\star_{\leq \ell - 1}(X) := \gcd(R^\star_{\leq \ell}(X), \tilde{f}_\ell(X)), \quad R^\star_{\ell - 1}(X) := \frac{R^\star_{\leq \ell}(X)}{R^\star_{\leq \ell - 1}(X)}. \tag{2.14}$$

Proposition 2.8
Soit $z \in \mathbb{C}$ une racine de R. *Pour tout entier $\ell \in [\![0, n_y]\!]$, on a*

$$\deg_{\mathrm{Y}}(\mathrm{F}(z,\mathrm{Y})) \leq \ell \Longleftrightarrow \mathrm{R}^{\star}_{\leq \ell}(z) = 0.$$

$$\deg_{\mathrm{Y}}(\mathrm{F}(z,\mathrm{Y})) = \ell \Longleftrightarrow \mathrm{R}^{\star}_{\ell}(z) = 0.$$

Démonstration
La démonstration se fait par récurrence sur le degré n_y du polynôme $\mathrm{F}(z,\mathrm{Y})$.
Commençons par montrer la première équivalence.
Pour $\ell = n_y$,

$$\deg_{\mathrm{Y}}(\mathrm{F}(z,\mathrm{Y})) \leq n_y \Leftrightarrow \mathrm{R}^{\star}_{\leq n_y}(z) = 0.$$

Pour $\ell = n_y - 1$,
si

$$\deg_{\mathrm{Y}}(\mathrm{F}(z,\mathrm{Y})) \leq n_y - 1 \text{ alors } \tilde{f}_{n_y}(z) = 0$$

Puisque z est une racine de $\mathrm{R}^{\star}_{\leq n_y} := \mathrm{R}^{\star}$,
donc

$$\mathrm{pgcd}\left(\mathrm{R}^{\star}_{\leq n_y}, \tilde{f}_{n_y}\right)(z) = 0$$

$$\mathrm{R}^{\star}_{\leq n_y - 1}(z) = 0$$

Inversement,
si

$$\mathrm{R}^{\star}_{\leq n_y - 1}(z) = 0 \Rightarrow \tilde{f}_{n_y}(z) = 0$$

donc

$$\deg_{\mathrm{Y}}(\mathrm{F}(z,\mathrm{Y})) \leq n_y - 1.$$

Supposons que, pour tout k tel que $0 \leq k < n_y$,

$$\deg_{\mathrm{Y}}(\mathrm{F}(z,\mathrm{Y})) \leq k \Longleftrightarrow \mathrm{R}^{\star}_{\leq k}(z) = 0.$$

si

$$\deg_{\mathrm{Y}}(\mathrm{F}(z,\mathrm{Y})) \leq k - 1 \text{ alors } \tilde{f}_{n_y}(z) = \ldots = \tilde{f}_{k}(z) = 0.$$

Puisque z est une racine de $\mathrm{R}^{\star}_{\leq n_y}$,
donc

$$\mathrm{pgcd}\left(\mathrm{R}^{\star}_{\leq n_y}, \tilde{f}_{n_y}, \ldots, \tilde{f}_{k}\right)(z) = 0;$$

d'où

$$\mathrm{R}^{\star}_{\leq k-1}(z) = 0.$$

Inversement,

$$\mathrm{R}^{\star}_{\leq k-1}(z) = 0 \Rightarrow \tilde{f}_{n_y}(z) = \ldots = \tilde{f}_{k}(z) = 0;$$

donc

$$\deg_{\mathrm{Y}}(\mathrm{F}(z,\mathrm{Y})) \leq k - 1.$$

La deuxième équivalence de la proposition ci-dessus se démontre presque de la même manière.
Pour $\ell = n_y$,
on a

$$\deg_{\mathrm{Y}}(\mathrm{F}(z,\mathrm{Y})) = n_y \Longleftrightarrow \mathrm{R}^{\star}_{n_y}(z) = 0.$$

En effet, si $\deg_{\mathrm{Y}}(\mathrm{F}(z,\mathrm{Y})) = n_y$ alors $\tilde{f}_{n_y+1}(z) = 0$. Par conséquent, $\mathrm{R}^{\star}_{\leq n_y+1}(z) = 0$ et $\mathrm{R}^{\star}_{n_y}(z) = 0$.
A présent, supposons que, pour tout k tel que $1 \leq k < n_y$,

$$\deg_{\mathrm{Y}}(\mathrm{F}(z,\mathrm{Y})) = k \Longleftrightarrow \mathrm{R}^{\star}_{k}(z) = 0.$$

Si

$$\deg_y(\mathrm{F}(z,\mathrm{Y})) = k-1 \text{ alors } \tilde{f}_{n_y}(z) = \ldots = \tilde{f}_k(z) = 0 \text{ et } \tilde{f}_{k-1}(z) \neq 0.$$

On déduit de la première relation de la Proposition que

$$\mathrm{R}^\star_{\leq k}(z) = 0 \qquad \text{et} \qquad \operatorname{pgcd}\left(\mathrm{R}^\star_{\leq k}, \tilde{f}_{k-1}\right)(z) \neq 0;$$

ce qui entraine que

$$\mathrm{R}^\star_{k-1}(z) = 0.$$

Réciproquement,
si

$$\mathrm{R}^\star_{k-1}(z) = 0 \text{ alors } \mathrm{R}^\star_{\leq k}(z) = 0 \text{ et } \mathrm{R}^\star_{\leq k-1}(z) \neq 0;$$

d'après la définition 2.14.
Donc

$$\operatorname{pgcd}\left(\mathrm{R}^\star_{\leq k}, \tilde{f}_{n_y}, \ldots, \tilde{f}_{k-1}\right)(z) \neq 0.$$

Puisque par récurrence $\tilde{f}_{n_y}(z) = \ldots = \tilde{f}_k(z) = 0$,
alors

$$\tilde{f}_{k-1}(z) \neq 0;$$

d'où

$$\deg_{\mathrm{Y}}(\mathrm{F}(z,\mathrm{Y})) = k-1.$$

□

Proposition 2.9
Soit $\mathrm{R}(\mathrm{X}) \in \mathbb{Z}[\mathrm{X}]$ *un polynôme de magnitude* (N, Λ) *et* $\mathrm{F}(\mathrm{X},\mathrm{Y}) \in \mathbb{Z}[\mathrm{X},\mathrm{Y}]$ *de magnitude* (n_1, τ_1)*, tels que l'ensemble*

$$\mathrm{Z} = \{(z,z') \in \mathbb{C}^2 \mid \mathrm{R}(z) = \mathrm{F}(z,z') = 0\}$$

soit de cardinal fini. Soient $\mathrm{G}_1, \ldots, \mathrm{G}_m \in \mathbb{C}[\mathrm{X},\mathrm{Y}]$ *des polynômes de degrés bornés par* n_2 *et dont les coefficients sont tous de module inférieur ou égal à* 2^{τ_2}*, et désignons par* $\mu(z) := \mathrm{mult}(z,\mathrm{R})$ *la multiplicité de* z *en tant que racine de* R.

(a) Soit $\mathrm{A} \subset \mathrm{Z}$ *le sous-ensemble de* Z *tel que, pour tout* $(z,z') \in \mathrm{A}$*, il existe un indice* $i(z,z') \in \{1,\ldots,m\}$ *pour lequel* $\mathrm{G}_{i(z,z')}(z,z') \neq 0$*. Alors, on a :*

$$\sum_{z \in \mathrm{V}_{\mathbb{C}}(\mathrm{R})} \mu(z) \sum_{z' \in \mathrm{A}_z} \log|\mathrm{G}_{i(z,z')}(z,z')| \in \tilde{\mathrm{O}}((\tau_2 n_1 + \tau_1 n_2)\mathrm{N} + (\Lambda + \mathrm{N}) n_1 n_2). \tag{2.15}$$

avec

$$\mathrm{A}_z := \{z' \in \mathbb{C} \mid (z,z') \in \mathrm{A}\}.$$

(b) Soient $\mathrm{G}_1, \ldots, \mathrm{G}_m \in \mathbb{Z}[\mathrm{X},\mathrm{Y}]$ *des polynômes à coefficients entiers tels que, pour tout* $(z,z') \in \mathrm{Z}$*, il existe un indice* i *pour lequel* $\mathrm{G}_i(z,z') \neq 0$*. Si* $i(z,z')$ *est le plus petit indice* i *tel que* $\mathrm{G}_i(z,z') \neq 0$*, alors on a :*

$$\sum_{z \in \mathrm{V}_{\mathbb{C}}(\mathrm{R})} \mu(z) \sum_{z' \in \mathrm{Z}_z} |\log|\mathrm{G}_{i(z,z')}(z,z')|| \in \tilde{\mathrm{O}}((\tau_2 n_1 + \tau_1 n_2)\mathrm{N} + (\Lambda + \mathrm{N}) n_1 n_2), \tag{2.16}$$

avec

$$\mathrm{Z}_z := \{z' \in \mathbb{C} \mid \mathrm{F}(z,z') = 0\}.$$

Démonstration
a) D'après la Proposition 3.3, on a :

$$|\mathrm{G}_{i(z,z')}(z,z')| \leq 2^{\tau'_2} \max(1,|z|)^{n_2} \max(1,|z'|)^{n_2},$$

avec $\tau_2' := \lceil \log((n_2+1)^2 2^{\tau_2}) \rceil \in O(\tau_2 + \log n_2)$.
Notons que

$$\prod_{(z,z')\in A} 2^{\tau_2' \mu(z)} \leq \prod_{z\in V_{\mathbb{C}}(R)} 2^{\tau_2' n_1 \mu(z)} \in 2^{O((\tau_2+\log n_2) n_1 N)} \tag{2.17}$$

et

$$\prod_{(z,z')\in A} \max(1,|z|)^{\mu(z) n_2} \leq \prod_{z\in V_{\mathbb{C}}(R)} \max(1,|z|)^{\mu(z) n_1 n_2} \tag{2.18}$$

$$\leq \widehat{\mathrm{Mea}}(R)^{n_1 n_2} \in 2^{O((\Lambda+\log N) n_1 n_2)}. \tag{2.19}$$

Sachant que

$$\prod_{(z,z')\in A} \max(1,|z'|)^{\mu(z)} \leq \prod_{z\in V_{\mathbb{C}}(R)} \widehat{\mathrm{Mea}}(F(z,-))^{\mu(z)} \tag{2.20}$$

et en appliquant les Propositions 2.5 et 1.8, on obtient

$$\prod_{(z,z')\in A} \max(1,|z'|)^{\mu(z) n_2} \in 2^{\tilde{O}((\tau_1 N + \Lambda n_1 + n_1 N) n_2)}. \tag{2.21}$$

Donc

$$\prod_{(z,z')\in A} |G_{i(z,z')}(z,z')|^{\mu(z)} \in 2^{\tilde{O}((\tau_2 n_1 + \tau_1 n_2) N + (\Lambda+N) n_1 n_2)} \tag{2.22}$$

en prenant le logarithme de part et d'autre, on établit que

$$\sum_{(z,z')\in A} \mu(z) \log |G_{i(z,z')}(z,z')| \in \tilde{O}((\tau_2 n_1 + \tau_1 n_2) N + (\Lambda+N) n_1 n_2). \tag{2.23}$$

b) Tout d'abord, montrons que

$$\prod_{(z,z')\in Z} |G_{i(z,z')}(z,z')|^{\mu(z)} \geq \frac{1}{E''}$$

avec E'' un entier naturel de taille $O(\Lambda n_1 n_2 + \tau_1 n_2 N)$.

Soit

$$F(X,Y) := f_{n_y}(X) Y^{n_y} + \ldots + f_0(X),$$

avec $n_y = \deg_Y(F) \leq n_1$, et $R^\star$ la partie sans facteurs carrés de R.

Soit $(R_\ell^\star(X))_{\ell\in[\![1,n_y]\!]}$ une suite finie de polynômes définie comme dans les équations (2.13) et (2.14), telle que

$$\deg(F(z,Y) = \ell \Longleftrightarrow R_\ell^\star(z) = 0.$$

Soient les polynômes

$$\Psi_{\ell,>1}(X) := \mathrm{pgcd}(R', R_\ell^\star), \qquad \Psi_{\ell,1}(X) := \frac{R_\ell^\star}{\Psi_{\ell,>1}(X)}$$

et pour tout $i \in \{1,\ldots,N\}$.

$$\Psi_{\ell,>i}(X) := \mathrm{pgcd}(\Psi_{\ell,i-1}(X), R^{(i)}(X)), \quad \Psi_{\ell,i}(X) := \frac{\Psi_{\ell,>i-1}(X)}{\Psi_{\ell,>i}(X)}.$$

Remarque 2.2

— *Si* $\deg(F(z,Y)) = \ell$, *alors* z *est une racine de* R *et de multiplicité* μ *si et seulement si* $\Psi_{\ell,\mu}(z) = 0$

—

$$R^\star = \prod \Psi_{\ell,\mu} \tag{2.24}$$

$$R = \prod \Psi_{\ell,\mu}^{\mu}. \tag{2.25}$$

Soient

$$F_\ell(X,Y) := f_\ell(X)Y^\ell + \ldots + f_0(X),$$

$$Z_{\ell,\mu} := \{(z,z') \in Z \mid \Psi_{\ell,\mu}(z) = 0\},$$

$$G = G_1 + UG_2 + \ldots + U^{m-1}G_m$$

et

$$A_{\ell,\mu}(U) := \mathrm{Res}_X(\mathrm{Res}_Y(F_\ell, G), \Psi_{\ell,\mu}) \in \mathbb{Z}[U].$$

Soient

$$Q_\ell(U,X) := \mathrm{Res}_Y(F_\ell, G)$$

et

$$Q_\ell(U,z) = f_\ell(z)^{O(n_2)} \prod_{z' \in Z_{\ell,\mu,z}} G(z,z').$$

Soit le polynôme

$$A_{\ell,\mu}(U) = \mathrm{LCF}(\Psi_{\ell,\mu})^{\delta - n_2 n_\ell} \prod_{z \mid \Psi_{\ell,\mu}(z)=0} f_\ell(z)^{O(n_2)} \prod_{(z,z') \in Z_{\ell,\mu}} G(z,z'),$$

où $\delta \leq n_1 n_2$ est le degré du polynôme $Q(U,X)$ par rapport à la variable X et n_ℓ celui du polynôme f_ℓ par rapport à la variable X.
Le coefficient du monôme de plus bas degré de $A_{\ell,\mu}(U)$ par rapport à la variable U est un entier non nul et vaut

$$\mathrm{LCF}(\Psi_{\ell,\mu})^{\delta - n_2 n_\ell} \mathrm{Res}_X(f_\ell, \Psi_{\ell,\mu})^{n_2} \prod_{(z,z') \in Z_{\ell,\mu}} G_{i(z,z')}(z,z').$$

Sachant que

$$\delta - n_2 n_\ell \in O(n_1 n_2), \qquad \prod_{\ell,\mu} \mathrm{LCF}\left(\Psi_{\ell,\mu}^\mu\right) = \mathrm{LCF}(R) \in 2^{O(\Lambda)}$$

et

$$\prod_{\ell,\mu} \mathrm{Res}_X(f_\ell, \Psi_{\ell,\mu}^\mu) = \mathrm{Res}_X(f_\ell, R) \in 2^{O(\tau_1 N + \Lambda n_1)},$$

on en déduit que

$$\prod_{(z,z') \in Z} |G_{i(z,z')}(z,z')|^{\mu(z)} \geq \frac{1}{E''} \tag{2.26}$$

avec $E'' := \mathrm{LCF}(R)^{n_1 n_2} \mathrm{Res}_X(f_\ell, R)^{n_2} \in 2^{O(\Lambda n_1 n_2 + \tau_1 n_2 N)}$.

On montre bien que

$$\sum_{z \in V_{\mathbb{C}}(R)} -\mu(z) \sum_{z' \in Z_z} \log|G_{i(z,z')}(z,z')| \leq b \in O(\Lambda n_1 n_2 + \tau_1 n_2 N) \tag{2.27}$$

avec $b = \log E''$.

Posons $\bar{Z} = \{(z,z') \in Z,\ |G_i(z,z')| \geq 1\}$. En utilisant (2.22), (2.27) et le Lemme 1.7, on établit que

$$\sum_{z \in V_{\mathbb{C}}(R)} \mu(z) \sum_{z' \in Z_z} |\log|G_{i(z,z')}(z,z')|| \leq 2a + b \tag{2.28}$$

avec a défini dans (2.23). Donc

$$\sum_{z \in V_{\mathbb{C}}(R)} \mu(z) \sum_{z' \in Z_z} |\log|G_{i(z,z')}(z,z)|| \in \tilde{O}((\tau_2 n_1 + \tau_1 n_2)N + (\Lambda + N) n_1 n_2) \tag{2.29}$$

□

Le théorème ci-dessous donne des bornes de compexité amorties sur la somme des mesures de Mahler des polynômes $F(z_i,-)$ et des séparateurs de ses racines $z_{i,j}$ ainsi que les valeurs absolues de ses premières dérivées non nulles en les racines $z_{i,j}$.

Dans la suite de ce manuscrit, nous noterons par

$$F^{[k]} = \frac{\partial_Y^k F}{k!} \tag{2.30}$$

la dérivée k-ième de F par rapport à la variable Y divisée par factorielle k.

Théorème 2.1
Soient $R \in \mathbb{Z}[X]$ *et* $F \in \mathbb{Z}[X,Y]$ *deux polynômes définis comme dans la Proposition 2.9, où* $\mu(z) := \mathrm{mult}(z,R)$. *Alors, on a*

(a) $\sum_{z\in V_{\mathbb{C}}(R)} \mu(z)\cdot \widehat{\log \mathrm{GDisc}}(F(z,-)) \in \tilde{O}(n(N\tau + n\Lambda + Nn))$.

(b) $\sum_{z\in V_{\mathbb{C}}(R)} \mu(z)\cdot \mathrm{logsep}(F(z,-)) \in \tilde{O}(n(N\tau + n\Lambda + Nn))$.

Démonstration
(a) est une conséquence immédiate de la Proposition 2.9 appliquée à R et à la famille $F^{[i(z,z')]}$ de magnitudes respectives (N,Λ) et $(n, n+\tau)$.
(b) D'après la Proposition 1.6

$$\mathrm{logsep}(f) + \widehat{\log \mathrm{GDisc}}(f) \in \tilde{O}(n(\mathrm{logLen}(f) + \widehat{\log \mathrm{Mea}}(f)) + |\log(|\mathrm{Disc}(f)|)|).$$

On démontre (b) en utilisant les bornes amorties suivantes déjà établies :
d'après le Théorème 2.1(a),

$$\sum_{z\in V_{\mathbb{C}}(R)} \mu(z)\cdot \widehat{\log \mathrm{GDisc}}(F(z,-)) \in \tilde{O}(n(N\tau + n\Lambda + Nn));$$

d'après la Proposition 2.5 (2.1),

$$\sum_{z\in V_{\mathbb{C}}(R)} \mu(z)\cdot \log \mathrm{Len}(F(z,-)) = \tilde{O}(N\tau + n\Lambda + nN),$$

et à partir de l'équation (2.3) toujours dans la même proposition 2.5,

$$\sum_{z\in V_{\mathbb{C}}(R)} \mu(z)\cdot \widehat{\log \mathrm{Mea}}(F(z,-)) = \tilde{O}(N\tau + n\Lambda + nN).$$

□

A présent, nous allons expliciter la technique adoptée dans la détermination de

$$\deg_Y(\mathrm{pgcd}(F(z,Y)), \partial_Y(F(z,Y))),$$

où z est une racine de R ; avec comme objectif final la démonstration de la proposition ci-dessous :

Proposition 2.10
Pour toute racine $z \in \mathbb{C}$ *de* R, *la complexité du calcul de* $\deg(F(z,Y))$ *et* $\deg(\mathrm{pgcd}(F(z,Y), \partial_Y(F(z,Y))$ *vaut*

$$\tilde{O}(N^2\Lambda + N^3 + n^5\tau + n^6).$$

Nous commençons par faire une estimation de la complexité du calcul des polynômes $R_\ell^\star$ définis dans les équations (2.13) et (2.14).

Proposition 2.11
La complexité du calcul des polynômes

$$(\mathrm{R}^\star_\ell(\mathrm{X}))_{\ell\in[\![1,n_y]\!]}$$

nécessite $\tilde{\mathrm{O}}(\max(n,\mathrm{N})(n\mathrm{N}+n\Lambda+\mathrm{N}\tau)+n^3\tau+n^4)$ *opérations binaires.*

Démonstration
On sait que la magnitude du polynôme $\mathrm{R}^\star$ est bornée par $(\mathrm{N},\Lambda+\mathrm{N})$, et $f_{n_y}(\mathrm{X})$ est de degré maximal n et taille binaire $\mathrm{O}(\tau)$. D'après la Proposition 1.12, on peut calculer le $\mathrm{pgcd}(\mathrm{R}^\star, f_{n_y})$ avec $\tilde{\mathrm{O}}(\max(n,\mathrm{N})(n\mathrm{N}+n\Lambda+\mathrm{N}\tau))$ opérations binaires. Sachant que, pour tout $\ell\in[0,n_y-1]$, $\deg(\mathrm{R}^\star_{\leq\ell})\leq n$ et que la taille binaire des coefficients du polynôme $\mathrm{R}^\star_{\leq\ell}$ vaut au plus $n+\tau$, la complexité du calcul de tous les $(\mathrm{R}^\star_{\leq\ell})_{\ell\in[0,n_y-1]}$ est en $\mathrm{O}(n^3\tau+n^4)$.

Il reste à analyser la complexité du calcul de $\mathrm{R}^\star_\ell$ tout en prenant en compte la division exacte de $\mathrm{R}^\star_{\leq\ell}$ par $\mathrm{R}^\star_{\leq\ell-1}$. Cette tâche requiert $\mathrm{O}(\mathrm{N}\Lambda+\mathrm{N}^2)$ opérations binaires pour $\ell=n_y$ et $\mathrm{O}(n\tau+n^2)$ opérations binaires pour chaque $\ell<n_y$. □

La démonstration de la Proposition 2.10 qui est proposée dans ce manuscrit s'appuie sur une famille de polynômes $\mathrm{R}^\star_{\ell,k}$ que nous allons définir ci-après. Pour tout entier positif $\ell\leq n_y$, on définit le polynôme

$$\mathrm{F}_\ell := \sum_{i=0}^{\ell} f_i(\mathrm{X})\mathrm{Y}^i.$$

On note par $\mathrm{sDisc}_{\ell,k}(\mathrm{X})$ le k-ième sous-discriminant de F_ℓ vu comme un polynôme en la variable Y. On définit :

$$\mathrm{R}^\star_{\ell,\geq 0}(\mathrm{X}) := \mathrm{R}^\star_\ell,$$

et pour tout $k\in\{0,\ldots,\ell-1\}$,

$$\mathrm{R}^\star_{\ell,\geq k+1}(\mathrm{X}) := \mathrm{pgcd}\left(\mathrm{R}^\star_{\ell,\geq k}(\mathrm{X}), \mathrm{sDisc}_{\ell,k}(\mathrm{X})\right), \quad \mathrm{R}^\star_{\ell,k}(\mathrm{X}) := \frac{\mathrm{R}^\star_{\ell,\geq k}(\mathrm{X})}{\mathrm{R}^\star_{\ell,\geq k+1}(\mathrm{X})}. \tag{2.31}$$

Proposition 2.12
Soient $z\in\mathbb{C}$ *et* $\ell\in[\![1,n_y]\!]$ *tels que* $\deg_{\mathrm{Y}}(\mathrm{F}(z,\mathrm{Y}))=\ell$ *(i.e.* $\mathrm{R}^\star_\ell(z)=0$*), alors on a*

$$\deg_{\mathrm{Y}}\left(\mathrm{pgcd}\left(\mathrm{F}_\ell(z,\mathrm{Y}),\partial_{\mathrm{Y}}\mathrm{F}_\ell(z,\mathrm{Y})\right)\right)\geq k \Longleftrightarrow \mathrm{R}^\star_{\ell,\geq k}(z)=0.$$

$$\deg_{\mathrm{Y}}\left(\mathrm{pgcd}\left(\mathrm{F}_\ell(z,\mathrm{Y}),\partial_{\mathrm{Y}}\mathrm{F}_\ell(z,\mathrm{Y})\right)\right)= k \Longleftrightarrow \mathrm{R}^\star_{\ell,k}(z)=0.$$

Démonstration
La démonstration se fait par récurrence sur le degré du pgcd.
Pour $k=1$,
si

$$\deg_{\mathrm{Y}}\left(\mathrm{pgcd}\left(\mathrm{F}_\ell(z,\mathrm{Y}),\partial_y\mathrm{F}_\ell(z,\mathrm{Y})\right)\right)\geq 1 \Rightarrow \mathrm{sDisc}_{\ell,1}(z)=0$$

puisque z est une racine de $\mathrm{R}^*_{\ell,\geq 0}$, donc d'après la Définition (2.31)

$$\mathrm{R}^*_{\ell,\geq 1}(z)=0;$$

en particulier, si

$$\deg_{\mathrm{Y}}(\mathrm{pgcd}(\mathrm{F}_\ell(z,\mathrm{Y}),\partial_y\mathrm{F}_\ell(z,\mathrm{Y})))=1\Rightarrow \mathrm{sDisc}_{\ell,1}(z)=0 et \mathrm{sDisc}_{\ell,2}(z)\neq 0$$

$$\mathrm{R}^*_{\ell,1}(z)=0.$$

Inversement,
si

$$\mathrm{R}^*_{\ell,\geq 1}(z)=0 \text{ alors par définition } \mathrm{sDisc}_{\ell,1}(z)=0$$

$$\deg_{\mathrm{Y}}(\mathrm{pgcd}(\mathrm{F}_\ell(z,\mathrm{Y}),\partial_y\mathrm{F}_\ell(z,\mathrm{Y}))\geq 1;$$

en particulier,

$$\mathrm{R}^*_{\ell,1}(z)=0 \text{ entraine par définition } \mathrm{R}^*_{\ell,\geq 0}(z)=0 \text{ et } \mathrm{R}^*_{\ell,\geq 1}(z)\neq 0$$

$$\mathrm{sDisc}_{\ell,1}(z)=0 \text{ et } \mathrm{sDisc}_{\ell,2}(z)\neq 0$$

$$\deg_{\mathrm{Y}}(\mathrm{pgcd}(\mathrm{F}_\ell(z,\mathrm{Y}),\partial_y\mathrm{F}_\ell(z,\mathrm{Y})))=1.$$

Admettons que la proposition est vraie à l'ordre k et vérifions la à l'ordre suivant.

$$\deg_{\mathrm{Y}}(\mathrm{pgcd}(\mathrm{F}_\ell(z,\mathrm{Y}),\partial_y\mathrm{F}_\ell(z,\mathrm{Y})))\geq k+1\Rightarrow \mathrm{sDisc}_{\ell,1}(z)=\ldots=\mathrm{sDisc}_{\ell,k+1}(z)=0$$

par ailleurs,

$$\mathrm{R}^\star_{\ell,\geq 0}(z)=\ldots=\mathrm{R}^\star_{\ell,\geq k}(z)=0$$

par récurrence du fait que la proposition reste vraie à l'ordre k.

$$\mathrm{R}^\star_{\ell,\geq k+1}(z)=\mathrm{pgcd}(\mathrm{R}^\star_{\ell,\geq k},\mathrm{sDisc}_{\ell,k})(z)=0;$$

en particulier,
si

$$\deg_{\mathrm{Y}}(\mathrm{pgcd}(\mathrm{F}_\ell(z,\mathrm{Y}),\partial_y\mathrm{F}_\ell(z,\mathrm{Y})))=k+1,$$

alors

$$\mathrm{sDisc}_{\ell,1}(z)=\ldots=\mathrm{sDisc}_{\ell,k+1}(z)=0 \text{ et } \mathrm{sDisc}_{\ell,k+2}(z)\neq 0$$

par construction des polynômes $\mathrm{R}^\star_{\ell,\geq k}$ (2.31), on a

$$\mathrm{R}^\star_{\ell,\geq k+1}(z)=0 \text{ et } \mathrm{R}^\star_{\ell,\geq k+2}(z)\neq 0;$$

d'où

$$\mathrm{R}^\star_{\ell,k+1}(z)=0.$$

Inversement,

$$\mathrm{R}^\star_{\ell,\geq k+1}(z)=0$$

entraine par définition que

$$\mathrm{R}^\star_{\ell,\geq k}(z)=\mathrm{sDisc}_{\ell,k}(z)=0$$

$$\deg_{\mathrm{Y}}(\mathrm{pgcd}(\mathrm{F}_\ell(z,\mathrm{Y}),\partial_y\mathrm{F}_\ell(z,\mathrm{Y})))\geq k+1;$$

en particulier,

$$\mathrm{R}^\star_{\ell,k+1}(z)=0\Rightarrow \mathrm{R}^\star_{\ell,\geq k+1}(z)=0 \text{ et } \mathrm{R}^\star_{\ell,\geq k+2}(z)\neq 0$$

or, d'une part $\mathrm{R}^\star_{\ell,\geq k+1}(z)=0$ entraine par récurrence que

$$\mathrm{sDisc}_{\ell,k}(z)=\ldots=\mathrm{sDisc}_{\ell,1}(z)=0;$$

d'autre part $\mathrm{R}^\star_{\ell,\geq k+2}(z)\neq 0$ implique que

$$\mathrm{sDisc}_{\ell,k+1}(z)\neq 0;$$

d'où

$$\deg_{\mathrm{Y}}(\mathrm{pgcd}(\mathrm{F}_\ell(z,\mathrm{Y}),\partial_y\mathrm{F}_\ell(z,\mathrm{Y})))=k+1.$$

□

Proposition 2.13
La complexité du calcul des polynômes

$$\big(\mathrm{sDisc}_{\ell,k}(\mathrm{X})\big)_{\ell\in[\![1,n_y]\!],k\in[\![0,\ell-1]\!]}$$

est en $\tilde{\mathrm{O}}(n^5\tau)$ *opérations binaires.*

Démonstration
Notons qu'il y a $n_y \leq n$ listes de polynômes sous-résultants à calculer. D'après la Proposition 2.4 la complixité est en $\tilde{O}(n^5\tau)$ opérations binaires. □

Proposition 2.14
La complexité du calcul des polynômes $\left(R^\star_{\ell,k}(X)\right)_{\ell\in[\![1,n_y]\!],k\in[\![0,\ell-1]\!]}$ *est en*

$$\tilde{O}(\max(N,n^2)(Nn^2+N n\tau+n^2\Lambda)+n^5\tau+n^6)$$

opérations binaires

Démonstration
Soient $\varphi_{\ell,k}$ le degré du polynôme $R^\star_{\ell,\geq k}$ et $\tau_{\ell,k}$ la taille binaire maximale des coefficients de $R^\star_{\ell,\geq k}$. Notons que les racines de $R^\star_{n_y,0}$ correspondent en réalité aux racines z de R telles que

$$\deg_Y(F(z,Y))=n_y, \quad \text{et } \deg_Y\left(\operatorname{pgcd}(F(z,Y),\partial_Y F(z,Y))\right)=0.$$

D'aprés les Propositions 1.12 et 1.13, la complexité de calcul du polynôme $R^\star_{n_y,0}$ est en

$$\tilde{O}(\max(N,n^2)(Nn^2+N n\tau+n^2\Lambda)$$

opérations binaires. Or, d'après la Proposition 2.6, on sait que toute racine de $R^\star_{n_y,\geq k}$ pour $k>0$ est aussi une racine de $\mathrm{Disc}_Y(F)$ de multiplicité supérieure ou égale à k. Par conséquent, $\left(R^\star_{n_y,\geq k}\right)^k$ divise $\mathrm{Disc}_Y(F)$. Donc

$$\varphi_{n_y,k}\leqslant\frac{n(2n-1)}{k}, \quad \text{et } \sum_{k=1}^{n_y}\varphi_{n_y,k}\in\tilde{O}(n^2).$$

En appliquant la Proposition 1.5 (1.4), on montre que $\tau_{n_y,k}\leqslant \mathrm{logMea}(R^\star_{n_y,\geq k})+\varphi_{n_y,k}$. En tenant compte du fait que $\left(R^\star_{n_y,\geq k}\right)^k$ divise $\mathrm{Disc}_Y(F)$ et que la mesure de Mahler est multiplicative, on montre aussi que

$$\sum_{k=1}^{n_y}\mathrm{logMea}(R^\star_{n_y,\geq k})\leqslant\mathrm{logMea}(\mathrm{Disc}_Y(F))\in\tilde{O}(n\tau).$$

Donc

$$\sum_{k=1}^{n_y}\tau_{n_y,\geq k}\in\tilde{O}(n^2+n\tau).$$

Par ailleurs, pour tout $\ell\in[\![1,n_y-1]\!]$, $R^\star_{\ell,\geq k}$ est un diviseur de $R^\star_\ell$. Donc

$$\sum_{k=0}^{\ell}\varphi_{\ell,k}\leq(\ell+1)\cdot\deg\left(R^\star_\ell\right);$$

$$\sum_{\ell=1}^{n_y-1}\deg\left(R^\star_\ell\right)\leq n_y\leq n$$

et

$$\sum_{\ell=1}^{n_y-1}\sum_{k=0}^{\ell}\varphi_{\ell,k}\in\tilde{O}(n^2).$$

En appliquant la Proposition 1.5 (1.4) on montre que $\tau_{\ell,k}\leqslant\mathrm{logMea}(R^\star_{\ell,\geq k})+\varphi_{\ell,k}$. Sachant que $R^\star_{\ell,\geq k}$ est un diviseur de $R^\star_\ell$, qui lui divise f_ℓ, et que

$$\sum_{k=0}^{\ell}\mathrm{logMea}(R^\star_{\ell,\geq k})\leqslant\mathrm{logMea}(f_\ell)\in\tilde{O}(\tau),$$

on en déduit que

$$\sum_{\ell=1}^{n_y-1}\sum_{k=0}^{\ell}\tau_{\ell,k}\in\tilde{O}(n^2+n\tau).$$

Donc

$$\sum_{k=1}^{n_y}\varphi_{n_y,k}+\sum_{\ell=1}^{n_y-1}\sum_{k=0}^{\ell}\varphi_{\ell,k}\in\tilde{O}(n^2)$$

$$\sum_{k=1}^{n_y-1}\tau_{n_y,k}+\sum_{\ell=1}^{n_y-1}\sum_{k=0}^{\ell}\tau_{n_y,k}\in\tilde{O}(n^2+n\tau).$$

D'après la Proposition 1.12, la complexité du calcul de $R^{\star}_{\ell,\geq k+1}(X)=\operatorname{pgcd}\left(R^{\star}_{\ell,\geq k}(X),\operatorname{sDisc}_{\ell,k}(X)\right)$ pour $(\ell,k)\neq(n_y,0)$ est en

$$\tilde{O}\left(\max(\varphi_{\ell,k}+n^2)(n^2\tau_{\ell,k}+\varphi_{\ell,k}n\tau)\right)$$

opérations binaires. Ainsi, calculer tous les polynômes $R_{\ell,\geq k}$ requiert

$$\tilde{O}\left(\max(N,n^2)(Nn^2+Nn\tau+n^2\Lambda)+n^5\tau+n^6\right)$$

opérations binaires.

La démonstration s'achève par l'analyse de la complexité du calcul des $R^{\star}_{\ell,k}$ en prenant compte la division exacte de $R^{\star}_{\ell,\geq k}$ par $R^{\star}_{\ell,\geq k+1}$. Cette tâche nécessite $O(N\Lambda+N^2)$ opérations binaires lorsque $(\ell,k)=(n_y,0)$, $O(n^2\tau+n^3)$ opérations binaires pour tout (n_y,k) tel que $k\neq 0$, et $O(n\tau+n^2)$ opérations binaires pour tout (ℓ,k) tel que $\ell<n_y$.

□

Démonstration Proposition 2.10
Il s'agit tout d'abord d'identifier les racines communes à $R^{\star}_{\ell,0}$ et R, ce qui nécessite $\tilde{O}(N^2\Lambda+N^3)$ opérations binaires. Ensuite, une fois que les polynômes $R^{\star}_{\ell,k}$ ont été calculés, pour tout $(k,\ell)\neq(n_y,0)$, il s'agira d'isoler leurs racines et d'identifier celles qui sont communes au polynôme D. D'après la Proposition 1.18 cette tâche requiert $\tilde{O}(n^5\tau+n^6)$ opérations binaires. □

Le théorème ci-dessous donne une borne sur la compexité du calcul des racines des polynômes $F(z,-)$, où z est une racine du polynôme R. Ce résultat est une conséquence de la Proposition 1.15, qui représente la meilleure borne de complexité pour l'isolation des racines d'un polynôme univarié à coefficients complexes.

Théorème 2.2
Soient $R\in\mathbb{Z}[X]$ *un polynôme de magnitude* (N,Λ) *et* $F\in\mathbb{Z}[X,Y]$ *un polynôme de magnitude* (n,τ). *Si, pour toute racine* z *de* R, *les entiers naturels* $n(z)=\deg(F(z,-))$ *et* $k(z)=\deg\left(\operatorname{pgcd}(F(z,-),\partial_Y F(z,-))\right)$ *sont connus*[2], *alors :*

(a) Avec une complexité en

$$\tilde{O}(N^3+N^2\Lambda+n\cdot\max(n^2,N)\cdot(N\tau+n\Lambda+nN))$$

opérations binaires, on peut calculer

(a1) des disques d'isolation adéquats $\mathcal{D}_{z,z'}\subset\mathbb{C}$ *pour toutes les racines complexes* z' *des polynômes* $F(z,-)$ *; de plus la somme de toutes les tailles binaires des rayons et des centres des disques* $\mathcal{D}_{z,z'}$ *est bornée par* $\tilde{O}(n(N\tau+n\Lambda+nN))$,

(a2) la multiplicité $\mu(z,z')$ *de chaque racine complexe* z' *du polynôme* $F(z,-)$, *et*

2. Notons que, d'après la Proposition 2.14, les entiers naturels $n(z)$ et $k(z)$ peuvent être calculés avec $\tilde{O}(N^2\Lambda+N^3+n^5\tau+n^6)$ opérations binaires. Par conséquent, le polynôme $F(z,-)$ admet $m(z)=n(z)-k(z)$ racines distinctes.

(a3) une approximation dyadique $\tilde{\sigma}_{z,z'}$ *des séparateurs* $\mathrm{sep}(z', \mathrm{F}(z,-))$ *telle que*

$$\frac{1}{2} \cdot \mathrm{sep}(z', \mathrm{F}(z,-)) < \tilde{\sigma}_{z,z'} < 2 \cdot \mathrm{sep}(z', \mathrm{F}(z,-))$$

pour toutes les racines z *(resp.* z' *) de* R *(resp.* $\mathrm{F}(z,-)$*).*

(b) Soient le sous-ensemble $\mathrm{V} \subset \{(z,z') \in \mathbb{C}^2 : \mathrm{R}(z) = 0 \text{ et } \mathrm{F}(z,z') = 0\}$ *de* $\mathbb{C}^2$ *et* κ *un entier naturel strictement positif. Alors, pour tout* $(z,z') \in \mathrm{V}$*, son disque d'isolation* $\mathscr{D}_{z,z'}$ *peut être rétréci sur un rayon inférieur ou égal à* $2^{-\kappa}$ *avec pas plus de*

$$\tilde{\mathrm{O}}\left(\mathrm{N}^3 + \mathrm{N}^2\Lambda + n \cdot \max(n^2, \mathrm{N}) \cdot (\mathrm{N}\tau + n\Lambda + n\mathrm{N}) + \kappa \cdot (\mathrm{N} \cdot \mu + n^2 \cdot \sum_{z \in \pi_X(\mathrm{V})} \mu_z)\right)$$

opérations binaires; où $\mu_z := \max_{(z,z') \in \mathrm{V}} \mu(z', \mathrm{F}(z,-)))$ *et* $\mu := \max_{z \in \pi_X(\mathrm{V})} \mu_z$.

(c) En particulier, si $\mu(z,z') = 1$*, pour tout* $(z,z') \in \mathrm{V}$ *alors on peut raffiner les disques* $\mathscr{D}_{z,z'}$ *avec*

$$\tilde{\mathrm{O}}\left(\mathrm{N}^3 + \mathrm{N}^2\Lambda + n \cdot \max(n^2, \mathrm{N}) \cdot (\mathrm{N}\tau + n\Lambda + n\mathrm{N}) + \kappa \cdot (\mathrm{N} \cdot \mu + n^2 \cdot \mathrm{card}(\pi_X(\mathrm{V})\right)$$

opérations binaires

Démonstration
Soient z une racine complexe de R, $\tau_z \in \mathbb{Z}$ tel que $2^{-\tau_z - 2} < \mathrm{LCF}(\mathrm{F}(z,-)) \leq 2^{-\tau_z}$, et $\mathrm{F}_z := 2^{\tau_z} \cdot \mathrm{F}(z,-)$. Notons que, sous ces hypothèses, les polynômes F_z et $\mathrm{F}(z,-)$ ont les mêmes racines et la valeur absolue du coefficient de tête de F_z reste comprise entre 1/4 et 1. D'après la Proposition 1.15, on peut calculer des disques d'isolation adéquats $\mathscr{D}_{z,z'}$ pour toutes les racines de F_z (il en de même pour les racines de $\mathrm{F}(z,-)$) ainsi que leurs multiplicités $\mu(z,z')$ respectives avec au plus

$$\tilde{\mathrm{O}}(n(n^2 + n \cdot \mathrm{logMea}(\mathrm{F}_z) + \mathrm{logsep}(\mathrm{F}_z) + \widehat{\mathrm{logGDisc}}(\mathrm{F}_z))), \tag{2.32}$$

opérations binaires. Dans la suite, nous aurons besoin d'une approximation de F_z avec une précision absolue, bornée par

$$\rho_z \in \tilde{\mathrm{O}}(n(n^2 + n \cdot \mathrm{logMea}(\mathrm{F}_z) + \widehat{\mathrm{logGDisc}}(\mathrm{F}_z))). \tag{2.33}$$

D'après la Proposition 2.5 et le Théoreme 2.1, on montre que la somme, sur toutes les racines z de R, de la borne (2.32) vaut

$$\tilde{\mathrm{O}}(n^2 \cdot (\mathrm{N}\tau + n\Lambda + n\mathrm{N})),$$

et la somme, sur tous les $z \in \mathrm{V}_{\mathbb{C}}(\mathrm{R})$, de la borne (2.33) pour la précision d'entrée vaut

$$\sum_{z \in \mathrm{V}_{\mathbb{C}}(\mathrm{R})} \rho_z \in \tilde{\mathrm{O}}(n \cdot (\mathrm{N}\tau + n\Lambda + n\mathrm{N})).$$

Ainsi, il reste à démontrer qu'on peut calculer des approximations suffisamment bonnes des polynômes F_z avec pas plus de $\tilde{\mathrm{O}}(n^2 \cdot (\mathrm{N}\tau + n\Lambda + n\mathrm{N}))$ opérations binaires. Le calcul d'une ρ_z-approximation binaire de F_z nécessite tout d'abord de trouver un entier τ_z, tel que $2^{-\tau_z - 2} < \mathrm{LCF}(\mathrm{F}(z,-)) \leq 2^{-\tau_z}$ et calculer une $(\rho_z + \tau_z)$-approximation binaire de $\mathrm{F}(z,-)$. Ensuite, multiplier les coefficients du polynôme approximant $\mathrm{F}(z,-)$ par τ_z bites. Commençons par analyser la complexité du calcul de l'entier τ_z. D'après la Proposition 1.16 a), on peut calculer une approximation $\tilde{c}_z$ de $c_z := |\mathrm{LCF}(\mathrm{F}(z,-))|$, telle que $|c_z - \tilde{c}_z| < 2^{-\mathrm{L}}$, avec $\tilde{\mathrm{O}}(n(\mathrm{L} + n\log\max(1,|z|)) + \tau)$ opérations binaires. L'algorithme prend en entrée une $\tilde{\mathrm{O}}(\mathrm{L} + n\log\max(1,|z|) + \tau)$-approximation binaire de z. Ainsi, en choisissant successivement $\mathrm{L} = 2, 4, 8, \ldots$, on arrive à calculer τ_z avec un entier naturel L de taille

$$\mathrm{L}_z \in \mathrm{O}\left(|\log|\mathrm{LCF}(\mathrm{F}(z,-))|| + \tau + n + n\log\max(1,|z|)\right),$$

tel que le coût d'évaluation reste borné par $\tilde{O}(nL_z)$ opérations binaires. En prenant la somme de cette borne sur tous les z et en appliquant la Proposition 2.9 (b) (avec $G_i = f_{n_y-i}$, la suite des coefficients de $F \in \mathbb{Z}[X][Y]$), on montre que

$$\begin{aligned}\sum_{z\in V_{\mathbb{C}}(R)} \tilde{O}(nL_z) &= n\cdot\tilde{O}\left(\sum_{z\in V_{\mathbb{C}}(R)} (|\log|\mathrm{LCF}(F(z,-))|| + \tau + n + n\log\max(1,|z|))\right)\\ &= \tilde{O}\left(n^2(N\tau + n\Lambda + Nn)\right)\end{aligned}$$

Notons que l'analyse de la complexité ci-dessus implique aussi que

$$\sum_{z\in V_{\mathbb{C}(R)}} \tau_z \in \tilde{O}\left(n(N\tau + n\Lambda + nN)\right).$$

L'estimation de la complexité du calcul des approximations suffisamment bonnes de $F(z,-)$ est obtenue à l'aide de la Proposition 1.16 a). Donc la complexité d'une $(\rho_z+\tau_z)$-approximation binaire de $F(z,-)$ est en au plus $\tilde{O}(n^2(\tau + n + n\log\max(1,|z|) + \rho_z + \tau_z))$ opérations binaires pour une $\tilde{O}(\tau + n + n\log\max(1,|z|) + \rho_z + \tau_z)$-approximation binaire de z. En prenant la somme de cette borne sur toutes les racines z de R, on obtient

$$\begin{aligned}&\tilde{O}\left(n^2N(\tau+n) + n^3\sum_{z\in V_{\mathbb{C}}(R)} \log\max(1,|z|) + n^2\sum_{z\in V_{\mathbb{C}}(R)} (\rho_z+\tau_z)\right)\\ &= n^3\cdot\tilde{O}\left(N\tau + n\Lambda + nN\right)\end{aligned}$$

A présent, nous allons déterminer une borne sur la complexité du calcul des approximations suffisamment bonnes des racines du polynôme R. Notons que, pour toute racine z de R, le réel $\tau + n + n\log\max(1,|z|) + \rho_z + \tau_z$ est borné par $\tilde{O}(n\cdot(N\tau + n\Lambda + nN))$. En effet, la borne précédente s'applique à la somme de tous les termes. Donc il suffit de calculer des approximations pour toutes les racines de R avec une précision absolue de taille $\tilde{O}(n\cdot(N\tau + n\Lambda + nN))$. D'après la Proposition 1.17, la complecité du calcul des disques d'isolation adéquats correspondants est bornée par $\tilde{O}(N^3 + N^2\Lambda + nN(N\tau + n\Lambda + nN))$. La borne sur la somme de toutes les tailles binaires des centres et des rayons des disques $D_{z,z'}$ découle directement de la Proposition 2.5 et du Théorème 2.1.
Ce qui met fin à la démonstration des assertions (a1) et (a2).
Pour l'assertion (a3), notons que

$$\frac{\min_{z''\neq z' : F(z,z'')=0} |m_{z,z'} - m_{z,z''}|}{\mathrm{sep}(z', F(z,-))} \in]1-1/32\ ,\ 1+1/32[;$$

où $m_{z,z'}$ représente le centre de $\mathscr{D}_{z,z'}$. Ainsi, les approximations $\tilde{\sigma}_{z,z'}$, satisfaisant les propriétés requises, peuvent être directement obtenues à partir des distances qui séparent les centres $m_{z,z'}$ des disques. En effet, la somme de toutes les tailles binaires des centres $m_{z,z'}$ est bornée par

$$\tilde{O}(\sum_{z\in V_{\mathbb{C}}(R)} \mathrm{logMea}(F_z) + \mathrm{logsep}^*(F_z)) \in \tilde{O}(n(N\tau + n\,\mathrm{logMea} + Nn)).$$

Il reste à établir la complexité du procéssus de raffinement des disques $\mathscr{D}_{z,z'}$ qui consiste à réduire les disques à une taille inférieure ou égale à $2^{-\kappa}$, pour tout $(z,z') \in V$. D'après la Proposition 1.17 (c), pour un z fixé, on peut raffiner tous les disques $\mathscr{D}_{z,z'}$ en

$$\tilde{O}(n(L\cdot\mu_z + n^2\cdot\mathrm{logMea}(F_z) + n\widehat{\mathrm{logGDisc}}(F_z) + n^3))$$

opérations binaires. La somme sur toutes les racines z de R est de l'ordre de

$$\tilde{O}(n^2(N\tau + n\Lambda + Nn) + nL\cdot\sum_{z\in V_{\mathbb{C}}(R)} \mu_z).$$

La précision d'entrée ρ_z requise pour approcher le polynôme F_z est en

$$\rho_z \in \tilde{O}(L\cdot\mu + n\cdot\mathrm{logMea}(F_z) + \widehat{\mathrm{logGDisc}}(F_z) + n^2).$$

Les mêmes arguments nous permettent d'en déduire que le calcul des approximations suffisamment bonnes pour les polynômes F_z peut s'effectuer en

$$\tilde{O}(n^3 \cdot (N\tau + n\Lambda + Nn) + L(N\mu + n^2 \cdot \sum_{z \in V_C(R)} \mu_z)$$

opérations binaires. □

Remarque 2.3
Au vu des deux derniers points du Théorème 2.2, il n'est pas toujours facile de raffiner les disques d'isolation d'un polynôme bivarié. En particulier, lorsque $\mu(z, z') > 1$ *est grand.*

Cependant, il est possible d'adapter les algorithmes dédiés à ce calcul afin de les rendre plus effectifs et efficaces. Il s'agit d'utiliser les bornes amorties sur la taille du séparateur. En effet, dans certains cas de figures, les racines peuvent être assez proches les unes des autres. Si toutefois le nombre de paires de racines deux à deux proches est minime et que l'on dispose d'un test pas cher permettant d'identifier les calculs nécessaires et suffisantes à effectuer.

Une telle situation apparaît dans le Théorème 2.3 mais aussi dans les Propositions 2.17 et 2.18 qui constituent des résultats clés à la démonstration du Théorème 2.4.

Théorème 2.3
Soient $R \in \mathbb{Z}[X]$ *un polynôme de magnitude* (N, Λ), $F, G \in \mathbb{Z}[X, Y]$ *deux polynômes de magnitude* (n, τ), *et* $H := F \times G$. *Avec un nombre d'opérations binaires borné par*

$$\tilde{O}\left(N^3 + N^2\Lambda + n^5\tau + n^6 + n \cdot \max(n^2, N) \cdot (N\tau + n\Lambda + nN)\right)$$

on peut effectuer les calculs suivant pour toutes les racines complexes z *de* R *:*

(a) calculer des disques d'isolation adéquats $\mathscr{D}_{z,z'}$ *pour toutes les racines complexes* z' *du polynôme* $H(z, -)$ *ainsi que leurs multiplicités* $\mu(z, z') = \mathrm{mult}(z', H(z, -))$ *correspondantes.*

(b) pour toute racine z' *de* $H(z, -)$, *déterminer si* z' *est une racine de* $F(z, -)$, $G(z, -)$, *ou une racine commune aux deux polynômes. Si* z *et* z' *sont des nombres réels, on peut déterminer le signe de* $F(z, z')$ *et* $G(z, z')$.

Démonstration
Le point (a) découle directement du Lemme 2.14 et du Théorème 2.2, sachant que H est de magnitude $\big(O(n), O(\log n + \tau)\big)$. Nous pouvons supposer que, pour toutes les racines complexes z de R, nous avons déjà calculé

— des disques d'isolation adéquats $\mathscr{D}^F_{z,z''}$ et $\mathscr{D}^G_{z,z'''}$ pour toutes les racines complexes z'' et z''' des polynômes $F(z, -)$ et $G(z, -)$ respectivement ;

— les multiplicités respectives $\mathrm{mult}(z'', F(z, -))$ et $\mathrm{mult}(z''', G(z, -))$;

— les degrés des polynômes $F(z, -)$ et $G(z, -)$, et

— les signes des coefficients dominants des polynômes $F(z, -)$ et $G(z, -)$ lorsque z est une racine réelle de R.

Pour le (b), nous allons raffiner chaque disque $\mathscr{D}^F_{z,z''}$ jusqu'à ce qu'il n'intersecte qu'un seul disque $\mathscr{D}_{z,z'}$. Si c'est le cas, alors cela signifie que $z' = z''$. De plus, z' est aussi une racine de $G(z, -)$ si et seulement si $\mu(z, z') > \mathrm{mult}(z'', F(z, -))$ puisque $\mathrm{mult}(z', F(z, -)) + \mathrm{mult}(z', G(z, -)) = \mu(z, z')$. Donc, pour chaque racine z' de $H(z, -)$, nous connaissons sa multiplicité en tant que racine de $F(z, -)$ et $G(z, -)$. Lorsque nous nous restreignons au racines réelles de R, alors nous pouvons directement en déduire le signe de $F(z, z')$ (respectivement $G(z, z')$) en la racine réelle z' de $H(z, -)$, qui n'est pas une racine de $F(z, -)$ (respectivement $G(z, -)$). C'est-à-dire, à partir du signe du coefficient dominant de $F(z, -)$ (respectivement $G(z, -)$) et de son degré, nous connaissons son signe en $\pm\infty$, et plus exactement le polynôme change de signe en les racines de H qui sont aussi racines de $F(z, -)$ (respectivement $G(z, -)$) de multiplicité impaire.

Il reste à majorer le coût du raffinement des disques $\mathscr{D}^{\mathrm{F}}_{z,z''}$. Soit $\mathrm{V} \subset \mathrm{C}^2$ défini par $\mathrm{R}(z) = \mathrm{F}(z,z'') = 0$ et V^1_z l'ensemble de tous les $z'' \in \mathbb{C}$ avec $(z,z'') \in \mathrm{V}$. Le raffinement est offectué suivant les valeurs croissantes de $\ell = 1,2,3,\ldots$: dans le ℓ-ième tour, pour tout $z'' \in \mathrm{V}^\ell_z$, les disques d'isolation $\mathscr{D}^{\mathrm{F}}_{z,z''}$ sont raffinés à une taille inférieure ou égale à 2^{-2^ℓ}. Si $\mathscr{D}^{\mathrm{F}}_{z,z''}$ intersecte au plus un disque d'isolation adéquat $\mathscr{D}_{z,z'}$ d'une racine du polynôme $\mathrm{H}(z,-)$ alors nous savons que $z' = z''$. Après avoir traité tous les points de V^ℓ_z, nous définissons $\mathrm{V}^{\ell+1}_z$ comme étant l'ensemble des valeurs z'' appartenant à V^ℓ_z pour lesquelles leur disques d'isolation intersectent au moins deux disques d'isolation adéquats de racines de $\mathrm{H}(z,-)$. C'est-à-dire que, l'ensemble V^ℓ_z est constitué des $z'' \in \mathrm{V}^1_z$ qui ne correspondent à aucune z' de $\mathrm{H}(z,-)$ avec $z' = z''$ après le ℓ-ième tour de raffinement. Dans ce cas, nous exécutons un $(\ell+1)^{\text{ième}}$ tour de raffinement. Le processus est interrompu dès que V^ℓ_z est vide pour tous les z, au quel cas, chaque racine de $\mathrm{F}(z,-) = 0$ s'identifie à une racine de $\mathrm{H}(z,-)$. Notons que, pour chaque couple (z,z''),l'identification aboutit avec succès au $\ell_{z,z''}$ième tour de raffinement, où $2^{\ell_{z,z''}}$ est borné par $\mathrm{O}\left(|\log \mathrm{sep}(z'', \mathrm{H}(z,-))|\right)$. Le Théorème 2.1 permet de conclure que $|\log \mathrm{sep}\left(z'', \mathrm{H}(z,-)\right)|$ est borné par $\tilde{\mathrm{O}}\left(n(\mathrm{N}\tau + n\Lambda + n\mathrm{N})\right)$; d'où le résulat après κ tours avec

$$\kappa = \max_{(z,z'')} \left(\ell_{z,z^{\mathrm{n}}} + 1\right) \in \mathrm{O}\left(\log(n(\mathrm{N}\tau + n\Lambda + n\mathrm{N}))\right).$$

D'après le Théorème 2.2, le coût de raffinement des disques $\mathscr{D}^{\mathrm{F}}_{z,z''}$ pour tous les $z, \mathrm{R}(z) = 0$ et $z'' \in \mathrm{V}^\ell_z$ à une taille inférieure ou égale à 2^{-2^ℓ} est borné par

$$\sum_{\ell=1}^{\kappa} \tilde{\mathrm{O}}\left(\mathrm{N}^3 + \mathrm{N}^2\Lambda + n\max(n^2,\mathrm{N})(\mathrm{N}\tau + n\Lambda + n\mathrm{N}) + 2^\ell(\mathrm{N}\mu^{[\ell]} + n^2 \sum_{z \in \mathrm{C}:\mathrm{R}(z)=0} \mu^{[\ell]}_z)\right)$$

opérations binaires, avec

$$\mu^{[\ell]}_z := \begin{cases} \max_{z'' \in \mathrm{V}^\ell_z} \mathrm{mult}\left(z'', \mathrm{F}(z,-)\right) & \text{si } \mathrm{V}^\ell_z \neq \emptyset \\ 0 & \text{sinon.} \end{cases}$$

et

$$\mu^{[\ell]} := \max_{z:\mathrm{R}(z)=0} \mu^{[\ell]}_z.$$

Sachant que κ est borné par $\mathrm{O}\left(\log(n(\mathrm{N}\tau + n\Lambda + n\mathrm{N}))\right)$, on parvient à borner la somme

$$\sum_{\ell=1}^{\kappa} 2^\ell \cdot \left(\mathrm{N} \cdot \mu^{[\ell]} + n^2 \cdot \sum_{z \in \mathrm{C}:\mathrm{R}(z)=0} \mu^{[\ell]}_z\right). \tag{2.34}$$

Si $\mathrm{V}^\ell_z \neq \emptyset$, soit $z''_{\ell,z} \in \mathrm{V}^\ell_z$ tel que $\mathrm{mult}\left(z''_{\ell,z}, \mathrm{F}(z,-)\right) = \mu^{[\ell]}_z$, et soit $z''_\ell \in \mathrm{V}^\ell_{z_\ell}$ un point appartenant à V_ℓ avec $\mathrm{mult}\left(z''_\ell, \mathrm{F}(z_\ell,-)\right) = \mu^{[\ell]}$. En d'autres termes, $z''_{\ell,z} \in \mathrm{V}^\ell_z$ maximise la multiplicité dans la fibre, et (z_ℓ, z''_ℓ) est un point appartenant à V qui maximise la multiplicité sur toutes les fibres. Par conséquent, la somme dans (2.34) peut être réécrite comme suit

$$\mathrm{N} \cdot \sum_{\ell=1}^{\kappa} \mu(z''_\ell, \mathrm{F}(z_\ell,-)) \cdot 2^\ell + n^2 \cdot \sum_{\ell=1}^{\kappa} \sum_{z \in \mathrm{C}:\mathrm{R}(z)=0} \mu(z''_{\ell,z}, \mathrm{F}(z,-)) \cdot 2^\ell.$$

Notons qu'une paire (z,z') telle que $z'' \in \mathrm{V}^e ll_z$ peut apparaître au plus κ fois dans chacune des sommes ci-dessus. De plus, $z'' \notin \mathrm{V}^\ell_z$ pour $\ell > \ell_{z,z''}$ avec $2^{\ell_{z,z''}} \in \mathrm{O}\left(|\log \mathrm{sep}(z'', \mathrm{H}(z,-))|\right)$. Donc, la somme ci-dessus est bornée par

$$\mathrm{O}\left(\kappa \cdot (n^2 + \mathrm{N}) \cdot \sum_{(z,z'') \in \mathrm{V}} \mu(z'', \mathrm{F}(z,-)) \cdot |\log \mathrm{sep}(z'', \mathrm{H}(z,-))|\right) \tag{2.35}$$

Sachant que $\mu\left(z'', \mathrm{F}(z,-)\right) \leq \mu\left(z'', \mathrm{H}(z,-)\right)$ et que V est un sous-ensemble de l'ensemble des paires $(z,z') \in \mathrm{C}^2$ telles que $\mathrm{R}(z) = \mathrm{H}(z,z') = 0$, le Théorème 2.1 permet ainsi de conclure que (2.35) est majorée par

$$\tilde{\mathrm{O}}\left(n \cdot (n^2 + \mathrm{N}) \cdot (\mathrm{N}\tau + n\Lambda + n\mathrm{N})\right).$$

□

Remarque 2.4
Les considérations ci-dessus ont permis d'élaborer un algorithme qui résout un système de polynômes bivariés avec une complexité presque égale à la complexité optimale connue pour ce type de problème.

Corollaire 2.1
Soient $F, G \in \mathbb{Z}[X,Y]$ *des polynômes co-premiers de magnitude* (n,τ). *La complexité du calcul des domaines d'isolation pour toutes les solutions complexes du système* $F = G = 0$ *est en* $\tilde{O}(d^5\tau + d^6)$ *opérations binaires.*

Démonstration
Soit $R = \mathrm{Res}_X(F,G)$ le polynôme résultant de F et G, qui peut être calculé en $\tilde{O}(d^5 + d^4\tau)$ opérations binaires. Pour toute solution commune $(x_0, y_0) \in \mathbb{C}$ de $F = G = 0$, x_0 est une racine de R; par conséquent y_0 est une racine commune de $F(x_0,-)$ et $G(x_0,-)$. Inversement, toute racine commune y_0 de $F(x_0,-)$ et $G(x_0,-)$, le couple (x_0,y_0) est une solution du système $F = G = 0$. D'après le Théorème 2.3, il est possible calculer toutes les racines communes de $F(z,-)$ et $G(z,-)$ pour toute racine complexe z de R avec $\tilde{O}(d^5\tau + d^6)$ opérations binaires. □

2.2 Retrait des droites verticales de la courbe

Soient $P \in \mathbb{Z}[X,Y]$ un polynôme sans facteur carré de magnitude (d,τ) et

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

la courbe algébrique réelle définie par P,

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

la courbe complexe correspondante.

Soit

$$P(X,Y) = c(X) \cdot \tilde{P}(X,Y) \tag{2.36}$$

une décomposition de $P(X,Y)$, où $c(X) \in \mathbb{Z}[X]$ et $\tilde{P}(X,Y) \in \mathbb{Z}[X,Y]$, telle que pour tout $z \in \mathbb{C}$, $\tilde{P}(z,Y)$ ne soit jamais identiquement nul. Géométriquement, cette décompositon distingue les droites verticales de $\mathscr{C}_{\mathbb{C}}(P)$ du reste de la courbe $\mathscr{C}_{\mathbb{C}}(\tilde{P})$, i.e la partie qui ne contient aucune droite verticale.

Proposition 2.15
La complexité du calcul de $c(X)$ *et* $\tilde{P}(X,Y)$ *est de l'ordre de* $\tilde{O}(n^4 + n^3\tau)$ *opérations binaires. Les polynômes* $\tilde{P}(X,Y)$ *et* $c(X)$ *sont de magnitude au plus* $\big(n, \tau + n + \log(n+1)\big)$.

Démonstration
Soit $P(X,Y) := c_{d_y}(X)Y^{d_y} + \ldots + c_0(X)$, avec $d_y = \deg_Y(P) \le d$. Soit $c(X)$ le pgcd de tous les coefficients $c_i(X)$ de P. Tout d'abord, nous calculons le polynôme $c(X)$ pour ensuite exprimer $P(X,Y)$ sous la forme $P(X,Y) = c(X)\tilde{P}(X,Y)$ afin de retirer les droites verticales du reste des solutions de l'équation $P(X,Y) = 0$. La complexité du calcul de $c(X)$ et $\tilde{P}(X,Y)$ ainsi que la borne supérieure sur leur magnitude découlent des Propositions 1.10 et 1.12. □

A présent, nous allons étudier les solutions de l'équation $\tilde{P}(X,Y) = 0$, qui est une courbe ne comportant aucune droite verticale. Nous supposons que $\deg_X(\tilde{P}(X,Y)) > 0$, sans quoi la courbe $\mathscr{C}(\tilde{P})$ n'est qu'un nombre fini de droites horizontales et sa topologie est assez simple à décrire (voir les détails dans la section 2.5.2). La section 2.5.2 explicite aussi la technique utilisée pour rajouter les droites verticales dans $\mathscr{C}(\tilde{P})$ aboutissant à la reconstruction de la topologie globale de $\mathscr{C}(P)$.

Tout d'abord, nous considérons les définitions suivantes

$$\begin{aligned} D_X(X) &:= \mathrm{Disc}_Y(\tilde{P})(X), && (2.37)\\ D_Y(Y) &:= \mathrm{Disc}_X(\tilde{P})(Y), && (2.38)\\ S_X(X) &= D_X(X)\cdot \mathrm{Res}_Y(\tilde{P},\partial_X\tilde{P})(X), && (2.39)\\ S_Y(Y) &:= D_Y(Y)\cdot \mathrm{Res}_X(\tilde{P},\partial_Y\tilde{P})(Y),, && (2.40)\\ T_X(X) &:= S_X\cdot (S_X^\star)', && (2.41)\\ T_Y(Y) &:= S_Y\cdot (S_Y^\star)'. && (2.42) \end{aligned}$$

où $(S_X^\star)'$ et $(S_X^\star)'$ désignent respectivement les dérivées des parties sans facteurs carrés de S_X et S_Y.

Lemme 2.4 *Les polynômes* $D_X, D_Y, S_X, S_Y, T_X, T_Y$ *sont tous de magnitude* $\big(O(d^2), O(d\tau + d^2)\big)$ *et peuvent être calculés en* $\tilde{O}(d^4\tau + d^5)$ *opérations binaires.*

Démonstration . La démonstration de Lemme est obtenue à partir des Propositions 1.12 et 2.4. □

Nous désignons par

$$\alpha_1 < \ldots < \alpha_N \tag{2.43}$$

les racines réelles de $D_X(X)$. Un point $(\alpha,\beta) \in \mathscr{C}(\tilde{P})$ est dit :

— X-*critique* si $\partial_Y\tilde{P}(\alpha,\beta) = 0$,
— Y-*critique* si $\partial_X\tilde{P}(\alpha,\beta) = 0$,
— *singulier* si $\partial_X\tilde{P}(\alpha,\beta) = \partial_Y\tilde{P}(\alpha,\beta) = 0$,
— *régulier* si $\partial_Y\tilde{P}(\alpha,\beta) \neq 0$ et $\partial_X\tilde{P}(\alpha,\beta) \neq 0$.

Soit $\mathrm{Crit}(\mathscr{C}(\tilde{P}))$ l'ensemble des points X-critiques de la courbe $\mathscr{C}(\tilde{P})$. Notons que, tout point singulier $\mathscr{C}(\tilde{P})$ est aussi X-critique et Y-critique ; l'abscisse (resp l'ordonnée) d'un point X-critique est racine de D_X (resp. S_Y), et l'ordonnée (resp. l'abscisse) d'un point Y-critique est une racine de D_Y (resp. S_X).

Nous désignerons aussi par

$$\xi_1 < \ldots < \xi_{N'}, \tag{2.44}$$

les racines réelles de $(S_X^\star)'(X)$, et $\xi_0 = -C(T_X)$, $\xi_{N'+1} = C(T_X)$ (comme dans la Notation 1.1), tels que ξ_0 (resp. $\xi_{N'+1}$) soit plus petit (resp. plus grand) que toutes les racines réelles de S_X et $(S_X^\star)'$. Notons que ξ_0 et $\xi_{N'+1}$ sont des nombres rationnels de taille binaire $\tilde{O}(d\tau + d^2)$.

Pour tout $i = 1,\ldots,N$, on notera par α_i^- et α_i^+ les éléments appartenant à

$$\{\xi_0, \xi_1, \ldots, \xi_{N'}, \xi_{N'+1}\}$$

tels que $\alpha_i \in]\alpha_i^-, \alpha_i^+[$.

Notons que pour tout intervalle $]\alpha_i^-, \alpha_i^+[$, α_i y est la seule racine de D_X et S_X.

Sur l'axe des ordonnées,

$$\gamma_1 < \ldots < \gamma_M,$$

désignent les racines de $S_Y(Y)$,

$$\eta_1 < \ldots < \eta_{M'}, \tag{2.45}$$

désignent les racines réelles de $(S_Y^\star)'(Y)$, et $\eta_0 = -C(T_Y)$, $\eta_{M'+1} = C(T_Y)$ (d'après la Notation 1.1), tels que η_0 (resp. $\eta_{M'+1}$ soit plus petit (resp. plus grand) que toutes les racines réelles de S_Y et $(S_Y^\star)'$. Notons que η_0 et $\eta_{M'+1}$ sont des nombres rationnels de taille binaire $O(d\tau + d^2)$.

Pour tout $k = 1,\ldots,M$, on désigne par γ_k^- et γ_k^+ les éléments de

$$\{\eta_0, \eta_1, \ldots, \eta_{M'}, \eta_{M'+1}\}$$

tels que $\gamma_k \in]\gamma_k^-, \gamma_k^+[$.

Pour tout $i = 1,\ldots,N$, on désigne par

$$\beta_{i,1} < \ldots < \beta_{i,m(i)} \tag{2.46}$$

les racines réelles de $P(\alpha_i, Y)$. Pour tout point X-critique $(\alpha_i, \beta_{i,j})$, on peut voir que $\beta_{i,j}$ est une racine de S_Y et on définit $k(i,j)$ comme étant l'indice tel que $\gamma_{k(i,j)} = \beta_{i,j}$.

2.3 Structures des boîtes adjacentes

La boîte adjacente associée au point singulier $(\alpha,\beta) = (\alpha_i, \beta_{i,j})$ est définie par $[\alpha^-,\alpha^+]\times[\gamma^-,\gamma^+]$ avec $\alpha^- = \alpha_i^-, \alpha^+ = \alpha_i^+$ et $\gamma^- = \gamma^-_{k(i,j)}, \gamma^+ = \gamma^+_{k(i,j)}$.

L'objectif, ici, est d'expliquer le processus de détermination des nombres LEFT et RIGHT de segments qui arrivent respectivement à gauche et à droite du point (α,β), par rapport à la verticale, en comptant uniquement les points d'intersection de $\mathscr{C}(P)$ avec des parties spécifiques du bord de la boîte adjacente.

Notation 2.1

- *Soit* L_{α^-} *(resp.* L_{α^+}*) la liste ordonnée des points d'intersection de* $\mathscr{C}(P)$ *avec* $\{\alpha^-\}\times]\gamma^-,\gamma^+[$ *(resp.* $\{\alpha^+\}\times]\gamma^-,\gamma^+[$*); où* $\{\alpha^-\}\times]\gamma^-,\gamma^+[$ *et* $\{\alpha^+\}\times]\gamma^-,\gamma^+[$ *sont respectivement les côtés gauche et droite de la boîte* $[\alpha^-,\alpha^+]\times[\gamma^-,\gamma^+]$.
- *Soit* $L_\alpha^{<\beta}$ *(resp.* $L_\alpha^{>\beta}$*) la liste ordonnée des points d'intersection de* $\mathscr{C}(P)$ *avec* $\{\alpha\}\times]\gamma^-,\beta[$ *(resp.* $\{\alpha\}\times]\beta,\gamma^+[$*) Nous considérons que les points sont ordonnés suivant l'ordre croissant de y dans toutes ces listes.*
- *Soit* L_{γ^-} *(resp.* L_{γ^+}*) l'ensemble des points d'intersections de* $\mathscr{C}(P)$ *avec* $]\alpha^-,\alpha^+[\times\{\gamma^-\}$ *(resp.* $]\alpha^-,\alpha^+[\times\{\gamma^+\}$*); où* $]\alpha^-,\alpha^+[\times\{\gamma^-\}$ *et* $]\alpha^-,\alpha^+[\times\{\gamma^+\}$*) sont les côtés inférieur et supérieur de la boîte* $[\alpha^-,\alpha^+]\times[\gamma^-,\gamma^+]$.
- *Soit* $L_{\gamma^-}^{<\alpha}$, $L_{\gamma^-}^{>\alpha}$ *(resp.* $L_{\gamma^+}^{<\alpha}$, $L_{\gamma^+}^{>\alpha}$*) l'ensemble des points de* L_{γ^-} *(resp.* L_{γ^+}*) qui sont à l'intérieur de* $]\alpha^-,\alpha[\times\{\gamma^-\}$, $]\alpha,\alpha^+[\times\{\gamma^-\}$ *(resp.* $]\alpha^-,\alpha[\times\{\gamma^+\}$, $]\alpha,\alpha^+[\times\{\gamma^+\}$*). Les ensembles* L_{γ^-}, L_{γ^+} *sont ordonnés de façon croissante par rapport à x.*
- *On définit* $L_{\gamma^-}^{=\alpha^-}$ *(resp.* $L_{\gamma^-}^{=\alpha}$, $L_{\gamma^-}^{=\alpha^+}$*) comme étant l'ensemble vide si* $P(\alpha^-,\gamma^-)\neq 0$ *(resp.* $P(\alpha,\gamma^-)\neq 0$, $P(\alpha^+,\gamma^-)\neq 0$*) et* $\{(\alpha^-,\gamma^-)\}$ *(resp.* $\{(\alpha,\gamma^-)\}$, $\{(\alpha^+,\gamma^-)\}$*) au cas contraire.*
- *On définit* $L_{\gamma^+}^{=\alpha^-}$ *(resp.* $L_{\gamma^+}^{=\alpha}$, $L_{\gamma^+}^{=\alpha^+}$*) comme étant l'ensemble vide si* $P(\alpha^-,\gamma^+)\neq 0$ *(resp.* $P(\alpha,\gamma^+)\neq 0$, $P(\alpha^+,\gamma^+)\neq 0$*) et* $\{(\alpha^-,\gamma^+)\}$ *(resp.* $\{(\alpha,\gamma^+)\}$, $\{(\alpha^+,\gamma^+)\}$*) au cas contraire.*

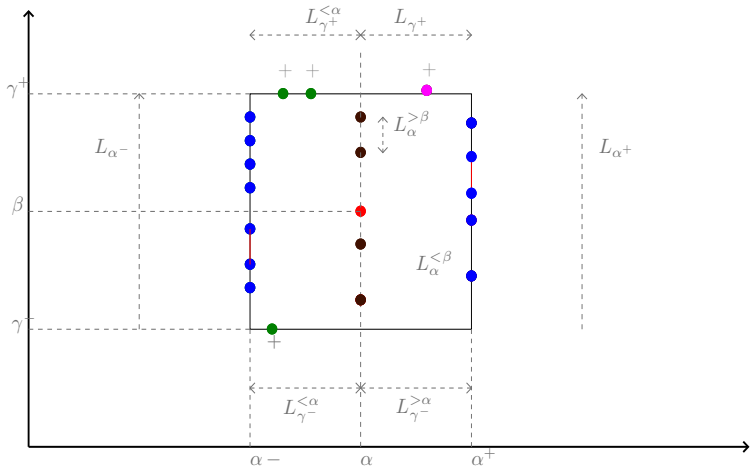


FIGURE 2.1 – Illustration des notations

Soit (x,y) un point bord de $[\alpha^-,\alpha[\times[\gamma^-,\gamma^+]\cap\mathscr{C}(\tilde{P})$ (resp. $]\alpha,\alpha^+]\times[\gamma^-,\gamma^+]\cap\mathscr{C}(\tilde{P})$). Il existe un seul et unique arc, appelé **arc spécial**, et qui satisfait exactement une des propriétés ci-dessous :

— **type 1 :** l'arc qui connecte (x,y) à un autre point du bord $[\alpha^-,\alpha[\times[\gamma^-,\gamma^+]$ (resp. $]\alpha,\alpha^+]\times[\gamma^-,\gamma^+]$), appelé le **point correspondant** (matching point) de (x,y) ;

— **type 2 :** l'arc qui connecte (x,y) à un point régulier de la fibre spéciale, appelé le **point correspondant** de (x,y) ;

— **type 3 :** l'arc connecte (x,y) à (α,β), appelé le **point correspondant** de (x,y).

Remarque 2.5 *Un arc de type 1 ou 2 n'intersecte aucun autre arc, tandis qu'un arc de type 3 croise d'autres arcs du même type au point* (α,β).

Pour toute liste $L=[x_1,\dots,x_n]$, on définit

$$L[i]=x_i,\quad L\setminus L[1]=[x_2,\dots,x_m],\quad \bar{L}:=[x_n,\dots,x_1].$$

Etant données deux listes $L=[x_1,\dots,x_n]$ et $M=[y_1,\dots,y_m]$, la **concaténation** de L et M, notée L+M, est donnée par

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

On note $\mathrm{Pente}(\tilde{P})(X,Y)$ la fraction rationnelle définie par

$$\mathrm{Pente}(\tilde{P})(X,Y)=-\frac{\partial_X\tilde{P}(X,Y)}{\partial_Y\tilde{P}(X,Y)}.$$

La **pente** de la tangente à la courbe $\mathscr{C}(\tilde{P})$ au point régulier (x,y) est donnée par la formule suivante

$$\mathrm{Pente}(\tilde{P})(x,y)=-\frac{\partial_X\tilde{P}(x,y)}{\partial_Y\tilde{P}(x,y)}.$$

Notons que, en tout point (x,y) appartenant à $\mathscr{C}_{\mathbb{R}}(\tilde{P})\cap[\alpha^-,\alpha^+]\times[\gamma^-,\gamma^+]\setminus\{(\alpha,\beta)\}$, $\mathrm{Pente}(\tilde{P})(x,y)$ est bien définie et non nulle, sauf si la droite horizontale $Y=\beta$ appartient à la courbe.

Proposition 2.16

a) a.1) si $L^{>\beta}_{=\alpha^-}+L^{=\alpha^-}_{\gamma^+}+L^{<\alpha}_{\gamma^+}+L^{=\alpha}_{\gamma^+}+\bar{L}^{>\beta}_{\alpha}\neq[]$, *les pentes sont du même signe sur tous ces points. Soit* σ^+ *le signe de la pente sur ces points ;*

a.2) si $\sigma^+>0$ *alors, pour* $i=1,\dots\#L^+$, $\mathrm{Match}(L^+[i])=L'^+[i]$ *avec* $L^+=L^{<\alpha}_{\gamma^+}+L^{=\alpha}_{\gamma^+}+\bar{L}^{>\beta}_{\alpha}$ *et* $L'^+=\bar{L}_{\alpha^-}+L^{=\alpha^-}_{\gamma^-}+L^{<\alpha}_{\gamma^-}$;

a.3) si $\sigma^+<0$ *alors, pour tout* $i=1,\dots\#L^+$, $\mathrm{Match}(L^+[i])=L'^+[i]$ *avec* $L^+=\bar{L}^{>\beta}_{\alpha}$ *et* $L'^+=\bar{L}^{<\alpha}_{\gamma^+}+L^{=\alpha^-}_{\gamma^+}+\bar{L}^{>\beta}_{\alpha^-}$.

b) b.1) Si $\bar{L}^{<\beta}_{=\alpha^-}+L^{=\alpha^-}_{\gamma^-}+L^{<\alpha}_{\gamma^-}+L^{=\alpha}_{\gamma^-}+L^{<\beta}_{\alpha}\neq[]$ *alors la pente est du même signe sur tous ces points. Soit* σ^- *le signe de la pente sur ces points ;*

b.2) si $\sigma^->0$ *alors, pour tout* $i=1,\dots\#L^-$, $\mathrm{Match}(L^-[i])=L'^-[i]$ *avec* $L^-=L^{<\beta}_{\alpha}$ *et* $L'^-=\bar{L}^{<\alpha}_{\gamma^-}+L^{=\alpha^-}_{\gamma^-}+L^{<\beta}_{\alpha^-}$;

b.3) si $\sigma^-<0$ *alors, pour touti* $=1,\dots\#L^-$, $\mathrm{Match}(L^-[i])=L'^-[i]$ *avec* $L^-=L^{<\alpha}_{\gamma^-}+L^{=\alpha}_{\gamma^-}+L^{<\beta}_{\alpha}$ *et* $L'^-=L_{\alpha^-}+L^{=\alpha^-}_{\gamma^-}+L^{<\alpha}_{\gamma^-}$.

c) c.1) Si $L^{>\beta}_{\alpha^+}+L^{=\alpha^+}_{\gamma^+}+\bar{L}^{>\alpha}_{\gamma^+}+L^{=\alpha}_{\gamma^+}+\bar{L}^{>\beta}_{\alpha}\neq[]$ *alors la pente est du même signe sur tous ces points. Soit* τ^+ *le signe de la pente sur ces points ;*

c.2) si $\tau^+>0$ *alors, pour tout* $i=1,\dots\#M^+$, $\mathrm{Match}(M^+[i])=M'^+[i]$ *avec* $M^+=\bar{L}^{>\beta}_{\alpha}$ *et* $M'^+=L^{>\alpha}_{\gamma^+}+L^{=\alpha^+}_{\gamma^+}+\bar{L}^{>\beta}_{\alpha^+}$;

c.3) si $\tau^+<0$ *alors, pour tout* $i=1,\dots\#M^+$, $\mathrm{Match}(M^+[i])=M'^+[i]$ *avec* $M^+=\bar{L}^{>\alpha}_{\gamma^+}+L^{=\alpha}_{\gamma^+}+\bar{L}^{>\beta}_{\alpha}$ *et* $M'^+=\bar{L}_{\alpha^+}+L^{=\alpha^+}_{\gamma^-}+\bar{L}^{>\alpha}_{\gamma^-}$.

d) d.1) Si $\bar{L}^{<\beta}_{\alpha^+}+L^{=\alpha^+}_{\gamma^-}+\bar{L}^{>\alpha}_{\gamma^-}+L^{=\alpha}_{\gamma^-}+L^{<\beta}_{\alpha}\neq[]$ *alors la pente est du même signe en tous ces points. Soit* τ^- *le signe de la pente sur ces points ;*

d.2) *si* $\tau^- > 0$ *alors, pour tout* $i = 1, \ldots \#M^-$, $\text{Match}(M^-[i]) = M'^-[i]$ *avec* $M^- = \bar{L}^{>\alpha}_{\gamma^-} + L^{=\alpha}_{\gamma^-} + L^{<\beta}_{\alpha}$ *et* $M'^- = L_{\alpha^+} + L^{=\alpha^+}_{\gamma^-} + \bar{L}^{>\alpha}_{\gamma^-}$.

d.3) *si* $\tau^- < 0$ *alors, pour tout* $i = 1, \ldots \#M^-$, $\text{Match}(M^-[i]) = M'^-[i]$ *avec* $M^- = L^{<\beta}_{\alpha}$ *et* $M'^- = L^{>\alpha}_{\gamma^-} + L^{=\alpha^+}_{\gamma^-} + L^{<\beta}_{\alpha^+}$.

Démonstration

a.1) Supposons que $L^{=\alpha^-}_{\gamma^+} + L^{<\alpha}_{\gamma^+} + L^{=\alpha}_{\gamma^+}$ admet au moins deux points (x_2, γ^+), (x_1, γ^+) avec $x_1 < x_2$, dont les signes de la pente sont opposés. Désignons par C_1 et C_2 les composantes connexes de $\mathscr{C}_{\mathbb{R}}(\tilde{P})$ dans le cylindre $[\alpha^-, \alpha[\times\mathbb{R}$ telles que $(x_1, \gamma^+) \in \bar{C}_1$ et $(x_2, \gamma^+) \in \bar{C}_2$. Puisque l'intervalle $[\alpha^-, \alpha[$ ne continent aucune racine du polynôme S_X, donc C_1 et C_2 sont des graphes de deux fonctions monotones semi-algébriques φ_1 et φ_2 définies sur $[\alpha^-, \alpha)$. Les fonctions φ_1 et φ_2 ont des limites positives au point α, donc le signe de la limite de $\varphi_1 - \varphi_2$ est bien défini au point α. Le signe de $\varphi_1(x_1) - \varphi_2(x_1)$ et le signe de la limite de $\varphi_1 - \varphi_2$ lorsque x tend vers x_2 sont contraires, donc pour tout $x \in (x_1, \alpha)$, $\varphi_1(x) = \varphi_2(x)$; ce qui est impossible car un tel point est nécessairement un point singulier de la courbe $\mathscr{C}_{\mathbb{R}}(\tilde{P})$ dans la cylindre $[\alpha^-, \alpha[\times\mathbb{R}$.

Supposons que $L^{>\beta}_{\alpha}$ (resp. $L^{>\beta}_{\alpha^-}$) admet au moins deux points (α, y_1) et (α, y_2) (resp. (α^-, y_1) et (α^-, y_2)), avec $y_1 < y_2$, dont les signes de la pente sont opposés. Désignons par C'_1 et C'_2 les composantes connexes de $\mathscr{C}_{\mathbb{R}}(\tilde{P})$ dans le cylindre $\mathbb{R}\times]\beta, \gamma^+[$. Puisque $(\beta, \gamma^+]$ ne contient aucune racine de S_Y, donc C'_1 et C'_2 sont des graphes de deux fonctions monotones semi-algébriques ψ_1 et ψ_2 définies sur $]\beta, \gamma^+]$. Les signes de $\psi_1 - \psi_2$ aux points y_1 et y_2 sont contraires , donc pour tout $y \in]y_1, y_2[$, $\psi_1(y) = \psi_2(y)$; ce qui est impossible car un tel point est nécessairement un point singulier de la courbe $V_{\mathbb{R}}(\tilde{P})$ restreinte au cylindre $R\times]\beta, \gamma^+]$.

En définitive, supposons que $L^{=\alpha^-}_{\gamma^+} + L^{<\alpha}_{\gamma^+} + L^{=\alpha}_{\gamma^+} \neq []$ et $L^{>\beta}_{\alpha} \neq []$ (resp. $L^{>\beta}_{\alpha^-} \neq []$), et soit (α, y) le premier point dans la liste $\bar{L}^{>\beta}_{\alpha}$ (resp. $L^{>\beta}_{\alpha^-} \neq []$).

(i) Supposons que la pente est de signe négatif (resp. positif) au point (α, y), et de signe positif en tous les points de la liste $L^{=\alpha^-}_{\gamma^+} + L^{<\alpha}_{\gamma^+} + L^{=\alpha}_{\gamma^+}$. Soit (x, γ^+) le dernier (resp. premier) point dans la liste $L^{<\alpha}_{\gamma^+} + L^{=\alpha}_{\gamma^+}$. Désignons par C'_1 et C'_2 les composantes connexes de la $\mathscr{C}_{\mathbb{R}}(\tilde{P})$ dans le cylindre $\mathbb{R}\times]\beta, \gamma^+]$ telles que $(\alpha, y) \in \bar{C}_1$ et $(x, \gamma^+) \in \bar{C}_2$. Puisque $]\beta, \gamma^+]$ ne contient aucune racine de S_Y, C'_1 (resp. C'_2) est le graphe d'une fonction semi-algébrique ψ_1 (resp. ψ_2) définie, continue et croissante sur $]\beta, \gamma^+]$. Le point (x, γ^+) n'est pas le correspondant de (α, y) car ces deux points ont des pentes de signes contraires; donc la limite de φ_1 au point γ^+ est strictement inférieure à x. La limite de $\psi_1 - \psi_2$ au point β (resp. γ^+) est de signe positif (resp. négatif). Elle est positive (resp. négative) au point y_2 (resp. y_1), donc $\psi_1(y) = \psi_2(y)$ pour tout $y \in]\beta, \gamma^+]$: ce qui est impossible car il s'agirait d'un point singulier de $V_{\mathbb{R}}(\tilde{P})$ appartenant à $R\times]\beta, \gamma^+[$.

(ii) A présent, supposons que la pente au point (α, y) est de signe positif et que les pentes au niveau des points de l'ensemble $L^{=\alpha^-}_{\gamma^+} + L^{<\alpha}_{\gamma^+} + L^{=\alpha}_{\gamma^+}$ sont toutes positives.

Notons que le cas de figure $\tilde{P}(\alpha, \gamma^+) = 0$ (resp.$\tilde{P}(\alpha^-, \gamma^+) = 0$) est impossible d'après (i) (en utilisant la symétrie par rapport à la droite $X = \alpha$).

Par conséquent, il existe un point (x, γ^+) appartenant à $L^{=\alpha^-}_{\gamma^+} + L^{<\alpha}_{\gamma^+}$. Soient C_1 (resp. C_2) la composante connexe de $V_{\mathbb{R}}(\tilde{P})$ dans $[\alpha^-, \alpha[\times R$ telle que $(x, \gamma^+) \in \bar{C}_1$ (resp. $(\alpha, y) \in \bar{C}_2$). Compte tenu du fait que $[\alpha^-, \alpha[$ ne contient aucune racine du polynôme S_X, alors C_1 (resp. C_2) est le graphe d'une fonction semi-algébrique, continue, croissante (resp. décroissante) φ_1 (resp. φ_2) définie sur $[\alpha^-, \alpha[$. Le point (α, y) n'est pas le correspondant de (x, γ^+). Car les signes de la pente en ces points sont contraires; c'est-à-dire que la limite de φ_2 au point α est strictement inférieure à y. Donc la limite de $\varphi_1 - \varphi_2$ au point α^- (resp. α) est négative (resp. positive). Par conséquent, pour toute valeur $x \in]\alpha^-, \alpha[$, $\varphi_1(x) = \varphi_2(x)$: ce qui est impossible; car ce point doit nécessairement être un point singulier de $V_{\mathbb{R}}(\tilde{P})$ dans $[\alpha^-, \alpha[\times R$.

a.2) Le correspondant de $L^+[i]$ est un point qui se situe sur le bord gauche α et il n'appartient pas à la liste L. Car le polynôme S_Y ne s'annule pas sur l'intervalle $]\beta, \gamma^+]$: c'est donc un point de de

la liste $L'^{+} = \bar{L}_{\alpha^-} + L_{\gamma^-}^{=\alpha} + L_{\gamma^-}^{<\alpha}$. On considère le premier point dans la liste $L^+[i]$ à qui on fait correspondre un point $L'^{+}\left[j\right]$ de la liste L' avec $j > i$. Ce qui signifie que $L'^{+}[i]$ ne peut pas correspondre avec un point de L^+. Car cela aurait pour conséquence que les arcs passant par $L^+[i]$ et $L^+\left[j\right]$ aller s'intersecter dans la boîte adjacente : Ce qui est impossible car un tel point devrait être nécessairement un point singulier de $V_{\mathbb{R}}(\tilde{P})$ distinct du point $\alpha,\beta)$ à l'intérieur de la boîte adjacente. Ce qui signifie que, $L'^{+}[i]$ est le point correspondant de $L^+[i]$.

a.3) Le correspondant de $L^+[i]$ est un point qui se situe sur le bord gauche de α et il n'appartient pas à L. Car le polynôme S_X ne s'annule pas sur l'intervalle $[\alpha^+,\alpha[$ et son ordonnée est plus grande que celle de $L^+[i]$: c'est un point de L'^{+}. On considère le premier point de la liste $L^+[i]$ à qui on fait correspondre un point $L'^{+}\left[j\right]$ de la liste L' avec $j > i$. Donc $L'^{+}[i]$, dont l'ordonnée est au moins égale à celle de $L^+[i]$, ne peut être un correspondant d'un point de L_α en ayant une ordonnée plus petite que que celle de $L^+[i]$. Car cela signifierait que les arcs passant par $L^+[i]$ et $L^+\left[j\right]$ s'intersectent dans la boîte adjacente. Ce qui signifie que $L'^{+}[i]$ est le correspondant du point $L^+[i]$. □

Notation 2.2

Désignons par σ^- *et* σ^+ *les signes de* $\text{Pente}(\tilde{P})(L_{\gamma^-}^{<\alpha}[1])$ *et de* $\text{Pente}(\tilde{P})(L_{\gamma^+}^{<\alpha}[1])$ *et par* τ^- *et* τ^+ *les signes de* $\text{Pente}(\tilde{P})(L_{\gamma^-}^{>\alpha}[1])$ *et* $\text{Pente}(\tilde{P})(L_{\gamma^+}^{>\alpha}[1])$. *Par convention, nous considérons que* σ^- *(resp.* σ^+, τ^-, τ^+*) est strictement positif lorsque* $L_{\gamma^-}^{<\alpha}$ *(resp.* $L_{\gamma^+}^{<\alpha}$, $L_{\gamma^-}^{>\alpha}$, $L_{\gamma^+}^{>\alpha}$*) est vide.*

Algorithm 1 Nombre de segments arrivant sur un point critique

1. Nombre de segments qui arrivent à gauche

Input : $\#L_{\alpha^-}$,$\#L_{\gamma^-}^{=\alpha^-}$, $\#L_{\gamma^-}^{<\alpha}$, $\#L_{\gamma^-}^{=\alpha}$, $\#L_{\gamma^+}^{=\alpha^-}$, $\#L_{\gamma^+}^{<\alpha}$, $\#L_{\gamma^+}^{=\alpha}$, $\#L_{\alpha}^{>\beta}$, $\#L_{\alpha}^{<\beta}$, σ^- et σ^+

Output : Le nombre LEFT de segments qui s'arrêtent au point (α,β) à gauche de α

— **Si** $\sigma^+ > 0$ et $\sigma^- > 0$ **alors**

$$\text{LEFT} = \#L_{\alpha^-} - (\#L_{\gamma^+}^{<\alpha} + \#L_{\gamma^+}^{=\alpha}) + \#L_{\gamma^-}^{<\alpha} + \#L_{\gamma^-}^{=\alpha^-} - (\#L_{\alpha}^{>\beta} + \#L_{\alpha}^{<\beta}) \tag{2.47}$$

— **Si** $\sigma^+ > 0$ et $\sigma^- < 0$ **alors**

$$\text{LEFT} = \#L_{\alpha^-} - (\#L_{\gamma^+}^{<\alpha} + \#L_{\gamma^+}^{=\alpha}) - (\#L_{\gamma^-}^{<\alpha} + \#L_{\gamma^-}^{=\alpha}) - (\#L_{\alpha}^{>\beta} + \#L_{\alpha}^{<\beta}) \tag{2.48}$$

— **Si** $\sigma^+ < 0$ et $\sigma^- > 0$ **alors**

$$\text{LEFT} = \#L_{\alpha^-} + \#L_{\gamma^+}^{<\alpha} + \#L_{\gamma^+}^{=\alpha^-} + \#L_{\gamma^-}^{<\alpha} + \#L_{\gamma^-}^{=\alpha^-} - (\#L_{\alpha}^{>\beta} + \#L_{\alpha}^{<\beta}) \tag{2.49}$$

— **Si** $\sigma^+ < 0$ et $\sigma^- < 0$ **alors**

$$\text{LEFT} = \#L_{\alpha^-} + \#L_{\gamma^+}^{<\alpha} + \#L_{\gamma^+}^{=\alpha^-} - (\#L_{\gamma^-}^{<\alpha} + \#L_{\gamma^-}^{=\alpha}) - (\#L_{\alpha}^{>\beta} + \#L_{\alpha}^{<\beta}) \tag{2.50}$$

2. Nombre de segments qui arrivent à droite

Input : $\#L_{\alpha^+}$,$\#L_{\gamma^-}^{=\alpha^+}$, $\#L_{\gamma^-}^{>\alpha}$, $\#L_{\gamma^-}^{=\alpha}$, $\#L_{\gamma^+}^{=\alpha^+}$, $\#L_{\gamma^+}^{>\alpha}$, $\#L_{\gamma^+}^{=\alpha}$, $\#L_{\alpha}^{>\beta}$, $\#L_{\alpha}^{<\beta}$, σ^- et σ^+

Output : le nombre RIGHT de segments qui s'arrêtent au point (α,β) à droite de α.

— **Si** $\tau^+ < 0$ et $\tau^- < 0$ **alors**

$$\text{RIGHT} = \#L_{\alpha^+} - (\#L_{\gamma^+}^{>\alpha} + \#L_{\gamma^+}^{=\alpha}) + \#L_{\gamma^-}^{>\alpha} + \#L_{\gamma^-}^{=\alpha^+} - (\#L_{\alpha}^{>\beta} + \#L_{\alpha}^{<\beta}) \tag{2.51}$$

— **Si** $\tau^+ < 0$ et $\tau^- > 0$ **alors**

$$\text{RIGHT} = \#L_{\alpha^+} - (\#L_{\gamma^+}^{>\alpha} + \#L_{\gamma^+}^{=\alpha}) - (\#L_{\gamma^-}^{>\alpha} + \#L_{\gamma^-}^{=\alpha}) - (\#L_{\alpha}^{>\beta} + \#L_{\alpha}^{<\beta}) \tag{2.52}$$

— **Si** $\tau^+ > 0$ et $\tau^- < 0$ **alors**

$$\text{RIGHT} = \#L_{\alpha^+} + \#L_{\gamma^+}^{>\alpha} + \#L_{\gamma^+}^{=\alpha^+} + \#L_{\gamma^-}^{>\alpha} + \#L_{\gamma^-}^{=\alpha^+} - (\#L_{\alpha}^{>\beta} + \#L_{\alpha}^{<\beta}) \tag{2.53}$$

— **Si** $\tau^+ > 0$ et $\tau^- > 0$ **alors**

$$\text{RIGHT} = \#L_{\alpha^+} + \#L_{\gamma^+}^{>\alpha} + \#L_{\gamma^+}^{=\alpha^+} - (\#L_{\gamma^-}^{>\alpha} + \#L_{\gamma^-}^{=\alpha}) - (\#L_{\alpha}^{>\beta} + \#L_{\alpha}^{<\beta}) \tag{2.54}$$

Correction de l'Algorithme 1

La correction de l'Algorithme 1 découle de la Proposition 2.16. En effet, soient N_1 (resp. N_2, N_3) le nombre d'arcs de **type 1** (resp. **2,3**) dans $[\alpha^-,\alpha[\times[\gamma^-,\gamma^+]$, notons que $\text{LEFT} = N_3$, $N_2 = \#L_{\alpha}^{<\beta} + \#L_{\alpha}^{<\beta}$. Posons $N = 2N_1 + 2N_2 + N_3$.

(i) Si $\sigma^+ > 0$ et $\sigma^- > 0$

$$N = \#L_{\alpha^-} + \#L_{\gamma^+}^{<\alpha} + \#L_{\gamma^+}^{=\alpha} + \#L_{\gamma^-}^{<\alpha} + \#L_{\gamma^-}^{=\alpha^-} + \#L_{\alpha}^{>\beta} + \#L_{\alpha}^{<\beta}.$$

De plus, tous les points de la liste $L_{\gamma^-} \setminus \text{Match}(L^-)$ sont connectés par un arc au point (α,β). Et là fin, les points de la liste $L_{\alpha} \setminus \text{Match}(L^+)$ sont aussi connectés à (α,β).

(ii) Si $\sigma^+ > 0$ et $\sigma^- < 0$

$$N = \#L_{\alpha^-} + \#L_{\gamma^+}^{<\alpha} + \#L_{\gamma^+}^{=\alpha} + \#L_{\gamma^-}^{<\alpha} + \#L_{\gamma^-}^{=\alpha} + \#L_{\alpha}^{>\beta} + \#L_{\alpha}^{<\beta}.$$

L'ordonnée de chaque point de la liste Match($L_{\alpha^-}^{>\beta}$) (resp. Match($L_{\alpha^-}^{<\beta}$)) est plus grand (petit) que β et Match($L_{\alpha^-}^{>\beta}$) = $L_{\gamma^+}^{<\alpha} + L_{\gamma^+}^{=\alpha} + L_{\alpha}^{>\beta}$) (resp. Match($L_{\alpha^-}^{<\beta}$) = $L_{\gamma^-}^{<\alpha} + L_{\gamma^-}^{=\alpha} + L_{\alpha}^{<\beta}$)). Donc

— si $P(\alpha^-,\beta) = 0$ alors LEFT = 1, ce qui correspond à une droite horizontale $Y = \beta$ de la courbe $\mathscr{C}_{\mathbb{R}}(\tilde{P})$

— si $P(\alpha^-,\beta) \neq 0$ alors LEFT = 0.

(iii) si $\sigma^+ < 0$ et $\sigma^- > 0$

$$N = \#L_{\alpha^-} + \#L_{\gamma^+}^{<\alpha} + \#L_{\gamma^+}^{=\alpha^-} + \#L_{\gamma^-}^{<\alpha} + \#L_{\gamma^-}^{=\alpha^-} + \#L_{\alpha}^{>\beta} + \#L_{\alpha}^{<\beta}.$$

De plus, tous les points de la liste $L_{\gamma^+} \setminus \text{Match}(L^+)$ (resp. $L_{\gamma^-} \setminus \text{Match}(L^-)$) sont connectés à (α,β). Et au final, les points de la liste$L_\alpha \setminus (\text{Match}(L^+) \cup \text{Match}(L^-))$ sont connectés à (α,β).

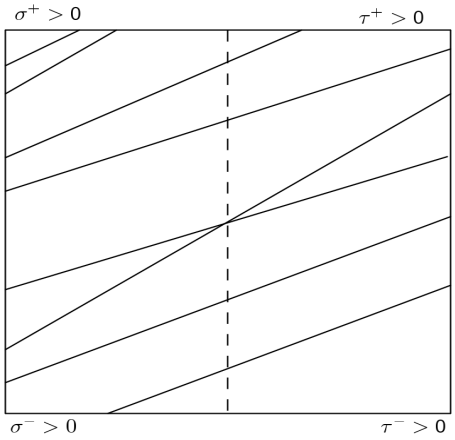
(iv) Si $\sigma^+ < 0$ et $\sigma^- < 0$

$$N = \#L_{\alpha^-} + \#L_{\gamma^+}^{<\alpha} + \#L_{\gamma^+}^{=\alpha^-} + (\#L_{\gamma^-}^{<\alpha} + \#L_{\gamma^-}^{=\alpha}) + \#L_{\alpha}^{>\beta} + \#L_{\alpha}^{<\beta}.$$

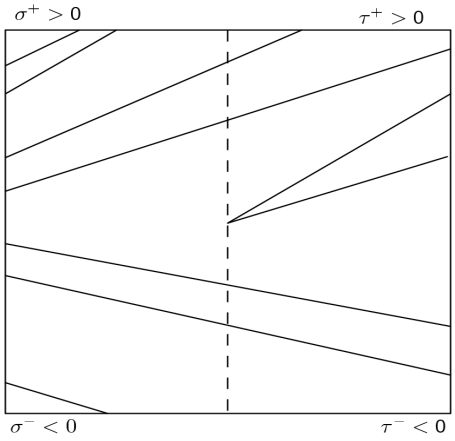
De plus, tous les points de la liste $L_{\gamma^+} \setminus \text{Match}(L^+)$ sont connectés à (α,β). Au final, les points de la liste $L_\alpha \setminus \text{Match}(L^-)$ sont aussi conncetés à (α,β).

Le certificat sur l'exactitude du calcul de RIGHT par le biais de l' Algorithme 1 se démontre de la même manière. □

Exemple 2.1 *Dans le cas de la figure 2.1, le côté gauche est caractérisé par :* $\sigma^+ > 0$, $\sigma^- > 0$, $\#L_{\alpha^-} = 7$,$\#L_{\gamma^-}^{=\alpha^-} = 0$, $\#L_{\gamma^-}^{<\alpha} = 1$, $\#L_{\gamma^-}^{=\alpha} = 0$, $\#L_{\gamma^+}^{=\alpha^-} = 0$, $\#L_{\gamma^+}^{<\alpha} = 2$, $\#L_{\gamma^+}^{=\alpha} = 0$, $\#L_{\alpha}^{>\beta} = 2$, $\#L_{\alpha}^{<\beta} = 2$. *En appliquant la formule (2.49) on trouve* LEFT = 2. *Le côté droite est caractérisé par :* $\tau^+ > 0$, $\tau^- > 0$ *(par convention),* $\#L_{\alpha^+} = 5$, $\#L_{\gamma^-}^{=\alpha^+} = 0$, $\#L_{\gamma^-}^{>\alpha} = 0$, $\#L_{\gamma^-}^{=\alpha} = 0$, $\#L_{\gamma^+}^{=\alpha^+} = 0$, $\#L_{\gamma^+}^{>\alpha} = 1$, $\#L_{\gamma^+}^{=\alpha} = 0$, $\#L_{\alpha}^{>\beta} = 2$, $\#L_{\alpha}^{<\beta} = 0$. *D'après la formule (2.53) on a* RIGHT = 2. *Cet exemple est illustré dans la figure ci-dessous.*



Tout en restant sur le cas de la figure 2.1, on suppose que sur le côté gauche : $\sigma^+ > 0$, $\sigma^- > 0$. *Donc, d'après la formule (2.48)* LEFT = 0. *On a sur le côté droite :* $\tau^+ > 0$, $\tau^- > 0$ *(par convention),* $\#L_{\alpha^+} = 5$, $\#L_{\gamma^-}^{=\alpha^+} = 0$, $\#L_{\gamma^-}^{>\alpha} = 0$, $\#L_{\gamma^-}^{=\alpha} = 0$, $\#L_{\gamma^+}^{=\alpha^+} = 0$, $\#L_{\gamma^+}^{>\alpha} = 1$, $\#L_{\gamma^+}^{=\alpha} = 0$, $\#L_{\alpha}^{>\beta} = 2$, $\#L_{\alpha}^{<\beta} = 0$. *Donc, d'après la formule (2.53)* RIGHT = 2. *L'image ci-dessous est une illustration de la situation précédente.*



2.4 Raffinement de la Décomposition Cylindrique Algébrique

Nous rappelons d'abord la définition générale de la décomposition cylindrique algébrique.

Définition 2.2 *Basu et al. [4, Def. 5.1]*
*Une **décomposition cylindrique algébrique** de $\mathbb{R}^n$ est une suite finie d'ensembles $\mathscr{P}_1,\ldots,\mathscr{P}_n$ telle que, pour tout $1 \le i \le n$, $\mathscr{P}_i$ est une partition de $\mathbb{R}^i$ en des sous-ensembles semi-algébriques, appelés **cellules de niveau i**, qui satisfont les propriétés suivantes :*

- *Toute cellule $C \in \mathscr{P}_1$ est soit un point ou un intervalle.*
- *Pour tout $1 \le i \le n$ et tout $C \in \mathscr{P}_i$, il existe des fonctions semi-algébriques continues*

$$F_{C,1} < \cdots < F_{C,\ell_C} : C \to \mathbb{R}$$

telles que le cylindre $C \times \mathbb{R} \subset \mathbb{R}^{i+1}$ soit l'union disjointe de cellules de $\mathscr{P}_{i+1}$ qui sont :

— *soit le **graphe** d'une des fonctions $F_{C,j}$, pour $j = 1,\ldots,\ell_C$:*

$$\{(a_1,\ldots,a_j,a_{j+1}) \in C \times \mathbb{R} \mid a + j + 1 = F_{C,j}(a_1,\ldots,a_j)\},$$

— *ou une bande du cylindre délimitée (en haut et en bas) par les **graphes** des fonctions $F_{C,j}$ et $F_{C,j+1}$, lorsque $j = 0,\ldots,\ell_C$, $F_{C,0} = -\infty$ et $F_{C,\ell_C+1} = +\infty$:*

$$\{(a_1,\ldots,a_j,a_{j+1}) \in C \times \mathbb{R} \mid F_{C,j}(a_1,\ldots,a_j) < x_{j+1} < F_{c,j+1}(a_1,\ldots,a_j)\}.$$

Dans la suite de cette section, pour tout $i = 1,\ldots,N$, nous désignons par

$$\eta^-_{i,1} < \ldots < \eta^-_{i,m_i} (\text{resp.} \eta^+_{i,1} < \ldots < \eta^+_{i,m_i}) \tag{2.55}$$

les racines réelles de $P(\alpha_i^-, Y)$ (resp. $P(\alpha_i^+, Y)$).

Pour chaque $k = 1,\ldots,M$, nous désignons par

$$\xi^-_{k,1} < \ldots < \xi^-_{k,n_k} (\text{resp.} \xi^+_{k,1} < \ldots < \xi^+_{k,n_k}) \tag{2.56}$$

les racines réelles du polynôme $P(X, \gamma_k^-)$ (resp. $P(X, \gamma_k^+)$).

Le Théorème 2.4 (Décomposition Cylindrique Algébrique améliorée) donne

(a) une décomposition cylindrique de $\tilde{P}$ mais aussi des informations supplémemtaires concernant sa projection par rapport à l'axe des abscisses ;

(b) une décomposition cylindrique partielle $\tilde{P}$ mais aussi des informations concernant sa projection par rapport à l'axe des ordonnées ;

(c) un raffinement des calculs précédents qui garantit la compatibilité entre (a) et (b).

Théorème 2.4
Les calculs ci-dessous peuvent être effectués avec une complicité en $\tilde{O}(d^5\tau + d^6)$ *opérations binaires :*

(a) (a.1) Calcul des intervalles dyadiques $I_i, I_{i,j}$ *pour* $1 \le i \le N, 1 \le j \le m_i$, *où* I_i *(resp* $I_{i,j}$*) est un intervalle d'isolation adéquat de* α_i *(resp.* $\beta_{i,j}$*), en tant que racine de* D_X *et* T_X *(resp.* $\tilde{P}(\alpha_i, Y)$*);*

(a.2) Calcul de $\deg\big(\tilde{P}(\alpha_i, Y)\big)$ *et de* $\deg\big(\mathrm{pgcd}\big(\tilde{P}(\alpha_i, Y), \partial_Y\tilde{P}(\alpha_i, Y)\big)\big)$ *quelque soit* $1 \le i \le N$*;*

(a.3) Calcul de la multiplicité $\mathrm{mult}(\beta_{i,j}, \tilde{P}(\alpha_i, -))$ *de* $\beta_{i,j}$ *en tant que racine de* $\tilde{P}(\alpha_i, Y)$ *quelque soit* $1 \le i \le N, 1 \le j \le m_i$ *et de l'ensemble* $\mathrm{CRIT}_i \subset \{1, \ldots, m_i\}$ *des indices des points* X*-critiques au dessus de* α_i*. De plus, si* $j \notin \mathrm{CRIT}_i$ *alors* $I_{i,j}$ *est un intervalle d'isolation adéquat de* $\beta_{i,j}$ *en tant que racine de*

$$\tilde{P}(\alpha_i, Y) \cdot \partial_X\tilde{P}(\alpha_i, Y) \cdot \partial_Y\tilde{P}(\alpha_i, Y).$$

(a.4) Calcul des intervalles dyadiques $I_i^-, I_{i,j}^-$, *(resp.* $I_i^+, I_{i,j}^+$*) pour tout* $1 \le i \le N, 1 \le j \le m_i^-$ *(resp.* $j \le m_i^+$*) où* I_i^- *(resp* I_i^+ *) est un intervalle d'isolation adéquat pour* α_i^- *(resp.* α_i^+*) en tant que racine de* T_X*, et* $I_{i,j}^-$ *(resp.* $I_{i,j}^+$ *) est un intervalle d'isolation adéquat de* $\eta_{i,j}^-$ *(resp.* $\eta_{i,j}^+$*) en tant que racine de*

$$\tilde{P}(\alpha_i^-, Y) \cdot \partial_X\tilde{P}(\alpha_i^-, Y) \cdot \partial_Y\tilde{P}(\alpha_i^-, Y) \quad \big(\text{resp. } \tilde{P}(\alpha_i^+, Y) \cdot \partial_X\tilde{P}(\alpha_i^+, Y) \cdot \partial_Y\tilde{P}(\alpha_i^+, Y)\big).$$

(b) Pour tout $k = 1, \ldots, M$*, calculer un intervalle dyadique* J_k*, qui est en fait un intervalle d'isolation adéquat de* γ_k *en tant que racine de* T_Y*, et pour tout point* X*-critique* $(\alpha_i, \beta_{i,j})$*, déterminer l'indice* $k(i,j)$ *tel que* $\beta_{i,j} = \gamma_{k(i,j)}$*.*

(c) (c.1) Pour tout $1 \le k \le M, 1 \le \ell \le n_k^-$ *(resp.* $\ell \le n_k^+$*), calculer des intervalles dyadiques* $J_k^-, J_{k,\ell}^-$ *(resp.* $J_k^+, J_{k,\ell}^+$*); où* J_k^- *(resp.* J_k^+*) est un intervalle d'isolation adéquat de* γ_k^- *(resp.* γ_k^+*) en tant que racine de* T_Y *et* $J_{k,\ell}^-$ *(resp.* $J_{k,\ell}^+$*) intervalle d'isolation de* $\xi_{k,\ell}^-$ *(resp.* $\xi_{k,\ell}^+$*) en tant que racine de*

$$\tilde{P}(X, \gamma_k^-) \cdot \partial_X\tilde{P}(X, \gamma_k^-) \cdot \partial_Y\tilde{P}(X, \gamma_k^-) \quad \big(\text{resp. } \tilde{P}(X, \gamma_k^+) \cdot \partial_X\tilde{P}(X, \gamma_k^+) \cdot \partial_Y\tilde{P}(X, \gamma_k^+)\big).$$

(c.2) Pour tout $i = 1, \ldots, N$, $j \in \mathrm{CRIT}_i$*, garantir que les intervalles dyadiques* $J_{k(i,j),\ell}^-$ *pour* $\ell = 1, \ldots, n_{k(i,j),\ell}^-$ *(resp.*$J_{k(i,j),\ell}^+$ *pour* $\ell = 1, \ldots, n_{k(i,j),\ell}^+$*) contiennent au plus un des points* α_i^-*,* α_i *ou* α_i^+*.*

(c.3) Pour tout $i = 1, \ldots, N$, $j \in \mathrm{CRIT}_i$*, garantir que les intervalles dyadiques* $I_{i,j'}^-$ *pour* $j' = 1, \ldots, m_i^-$ *(resp.* $I_{i,j'}^+$ *pour* $j' = 1, \ldots, m_i^+$*) contiennent au plus un des points* $\gamma_{k(i,j)}^-$ *ou* $\gamma_{k(i,j)}^+$*.*

De plus,

$$\sum_{i=1}^{N} \lambda(I_i) = \sum_{i=1}^{N} \lambda(I_i^-) = \sum_{i=1}^{N} \lambda(I_i^+) \in \tilde{O}(d^3\tau + d^4), \tag{2.57}$$

$$\sum_{i=1}^{N}\sum_{j=1}^{m_i} \lambda(I_{i,j}) = \sum_{i=1}^{N}\sum_{j=1}^{m_i^-} \lambda(I_{i,j}^-) = \sum_{i=1}^{N}\sum_{j=1}^{m_i^+} \lambda(I_{i,j}^+) \in \tilde{O}(d^3\tau + d^4). \tag{2.58}$$

$$\sum_{k=1}^{M} \lambda(J_k) = \sum_{k=1}^{M} \lambda(J_k^-) = \sum_{k=1}^{M} \lambda(J_k^+) \in \tilde{O}(d^3\tau + d^4). \tag{2.59}$$

$$\sum_{k=1}^{M}\sum_{\ell=1}^{n_k^-} \lambda(J_{k,\ell}^-) = \sum_{k=1}^{M}\sum_{\ell=1}^{n_k^+} \lambda(J_{k,\ell}^+) = \in \tilde{O}(d^3\tau + d^4). \tag{2.60}$$

Remarque 2.6
Notons que le Théorème 2.4 (c1) n'explicite pas si $\xi^+_{k,\ell} < \alpha^-_i$, $\xi^+_{k,\ell} = \alpha^-_i$ *ou* $\xi^+_{k,\ell} = \alpha^-_i$ *lorsque* $J^+_{k(i,j),\ell}$ *contient* α^-_i. *En effet, le signe de* $\tilde{P}(\alpha_i, \gamma^-_k)$ *reste inconnu. Cependant, il est possible d'obtenir cette information en faisant des calculs exacts, mais cette instruction étant très couteuse, elle dépasse la borne de complexité visée dans cet algorithme qui est de l'ordre de* $\tilde{O}(d^5\tau + d^6)$ *opérations binaires.*

La même remarque s'impose pour les cas (c1) et (c2)).

Démonstration
Pour les assertions (a1), (a2) et (a3), notons tout d'abord que d'après les Propositions 1.12 et 2.4, la complexité du calcul de T_X est de $\tilde{O}(d^4\tau + d^5)$ opérations binaires. De plus, les polynômes T_X, D_X et la partie sans facteur carré de leurs dérivées respectives(i.e T'^*_X et D'^*_X) sont tous de magnitudes $(N, \lambda) = \big(O(d^2), \tilde{O}(d\tau + d^2)\big)$. En appliquant les Propositions 1.17 et 1.18, on peut calculer des intervalles d'isolation adéquats pour toutes les racines réelles de T_X, tout en identifiant parmi elles les racines réelles de D_X, avec une complexité en $\tilde{O}(d^5\tau + d^6)$ opérations binaires. D'après la Proposition 2.10 (avec $R := D_X$ et $F := \tilde{P}(X, Y)$), pour tout $i \in [\![1, N]\!]$, on peut calculer $\deg\big(\tilde{P}(\alpha_i, Y)\big)$ ainsi que $\deg\big(\mathrm{pgcd}\big(\tilde{P}(\alpha_i, Y), \partial_Y\tilde{P}(\alpha_i, Y)\big)\big)$ avec $\tilde{O}(d^5\tau + d^6)$ opérations binaires. Le Théorème 2.2 stipule que, pour tout $i \in [\![1, N]\!]$, la complexité du calcul des intervalles d'isolation adéquats pour toutes les racines des polynômes $\tilde{P}(\alpha_i, Y)$ ainsi que leurs multiplicités correspondantes est en $\tilde{O}(d^5\tau + d^6)$ opérations binaires. A toute racine $\beta_{i,j}$ de multiplicité au moins deux correspond un point X-critique $(\alpha_i, \beta_{i,j})$ de l'ensemble $\mathrm{CRITIND}_i$ pour $i \in [\![1 \dots N]\!]$. En appliquant le Théorème 2.3 avec

$$H = \tilde{P}(X, Y) \cdot \partial_X\tilde{P}(X, Y) \cdot \partial_Y\tilde{P}(X, Y),$$

on obtient des *intervalles d'isolation adéquats* pour les racines simples du polynôme

$$\tilde{P}(\alpha_i, Y) \cdot \partial_X\tilde{P}(\alpha_i, Y) \cdot \partial_Y\tilde{P}(\alpha_i, Y),$$

tout en identifiant, pour tout $i = 1, \dots, N$, les racines spéciales de $\tilde{P}(\alpha_i, Y)$. Finalement, la borne sur la somme des tailles des intervalles $I_i, I_{i,j}$ est obtenue grâce aux Théorèmes 2.2 et 2.3. Ce qui met fin à la démonstration des assertions (a1), (a2) et (a3).

Pour (a4), d'après les Propositions 1.17 et 1.18, nous pouvons calculer des intervalles d'isolation adéquats pour toutes les racines réelles de T_X et identifier parmi ces racines celles de D_X avec une complexité en $\tilde{O}(d^5\tau + d^6)$ opérations binaires. D'après la Proposition 2.10 (où $R := (T^\star_X)'$ et $F := \tilde{P}(X, Y)$), on peut déterminer $\deg\tilde{P}(\xi_i, Y)$ avec la même complexité. En définitive, d'une part le Théorème 2.2 nous permet de conclure qu'avec au plus $\tilde{O}(d^5\tau + d^6)$ opérations binaires nous pouvons calculer des intervalles d'isolations adéquats pour toutes les racines réelles des polynômes

$$\tilde{P}(\xi_i, Y) \cdot \partial_X\tilde{P}(\xi_i, Y) \cdot \partial_Y\tilde{P}(\xi_i, Y);$$

d'autre part, le Théorème 2.3 garantit que, pour tout $i = 1, \dots, N'$, nous pouvons identifier les racines de $\tilde{P}(\xi_i, Y)$. Dès lors, il ne reste plus qu'à calculer des intervalles d'isolation pour les racines des polynômes

$$\tilde{P}(\xi_0, Y) \cdot \partial_X\tilde{P}(\xi_0, Y) \cdot \partial_Y\tilde{P}(\xi_0, Y),$$

et

$$\tilde{P}(\xi'_N, Y) \cdot \partial_X\tilde{P}(\xi'_N, Y) \cdot \partial_Y\tilde{P}(\xi'_N, Y).$$

Il devient alors facile d'identifier α^-_i et α^+_i, aussi bien que les intervalles $I^-_i, I^-_{i,j'}, I^+_i, I^+_{i,j'}$, à partir des résulats obtenus dans les calculs précédents. La borne sur la somme des tailles binaires des intervalles $I^-_i, I^-_{i,j'}, I^+_i, I^+_{i,j'}$ est donnée par le Théorème 2.2 (a1) et le Théorème 2.3.

La démonstartion du (b) est similaire à celle de (a4). Il suffit de permuter les rôles de X et Y. Dans la partie (c.1), d'après le Lemme 2.4, le calcul de T_Y est de l'ordre de $\tilde{O}(d^4\tau + d^5)$, et d'après les Propositions 1.17 et 1.18 le calcul des J_k, $k = 1, \dots, M$ requiert au plus $\tilde{O}(d^5\tau + d^6)$ opérations binaires; puisque T_Y est de magnitude $\big(O(d^2), O(d\tau + d^2)\big)$. La détermination des indices $k(i, j)$ pour $i = 1, \dots, N$, $j \in \mathrm{CRITIND}_i$ découle de la Proposition 2.17.

Les parties (c.2), (c.3) découlent de la Proposition 2.18. □

Proposition 2.17
Le calcul des entiers $k(i,j) \in \{1,\dots,m\}$, pour tous les points X*-critiques* $(\alpha_i, \beta_{i,j}) \in \mathrm{Crit}(V_{\mathbb{R}}(\tilde{P}))$ *tels que* $\gamma_{k(i,j)} = \beta_{i,j}$, *coûte* $\tilde{O}(d^5\tau + d^6)$ *opérations binaires.*

Démonstration
Soit $V_i^1 := \textsc{CritInd}_i$. Pour calculer les nombres $k(i,j)$ de chaque $\beta_{i,j}$), $j \in \textsc{CritInd}_i$, nous procédons par une suite d'énumération indexée par $\ell = 1,2,3,\dots$. Au $\ell^{\text{ième}}$ tour, nous raffinons les intervalles d'isolations pour tous les indices i et toutes les racines $\beta_{i,j}$ avec $j \in V_i^\ell$ à une taille inférieure à 2^{-2^ℓ}. Si l'intervalle d'isolation concerné $I_{i,j}$ intersecte au plus un autre intervalle d'isolation J_k pour les racines de $\mathrm{Res}_X(\tilde{P}, \partial_Y\tilde{P})$, nous savons que $k = k(i,j)$. Après avoir traité tous les éléments V_i^ℓ, on définit $V_i^{\ell+1}$ comme étant l'ensemble de tous les indices critiques appartenant à V_i^ℓ dont un intervalle d'isolation $I_{i,j}$ de $\beta_{i,j}$ intersecte au moins deux intervalles de J_k. C'est-à-dire, V_i^ℓ regroupe tous les indices critiques dont $k(i,j)$ reste inconnu après le $\ell^{\text{ième}}$ tour. Dans ce cas, nous passons au $(\ell+1)^{\text{ième}}$ tour. Nous nous arrêtons dès que V_i^ℓ est vide pour chaque $i = 1,\dots,N$, auquel cas $k(i,j)$ a été déterminé pour tous les points critiques.

On utilise le polynôme R_Y définit dans la Proposition 2.7, avec $F = \tilde{P}$, tout se rappelant que parmi les racines de R_Y se trouve les des points Y-critiques de $\tilde{P}$. A noter que, pour tout point critique $(\alpha_i, \beta_{i,j})$, nous aboutissons à un succès au $\ell_{i,j}^{\text{ième}}$ tour, où $2^{\ell_{i,j}}$ est borné par $O\left(\left|\log\left(\mathrm{sep}\left(\beta_{i,j}, T_Y R_Y\right)\right)\right|\right)$. Ce qui signifie que, pour tout $\ell > \ell_{i,j}$, $j \notin V_i^\ell$.

Le coût du test, qui consiste à vérifier si l'intervalle $I_{i,j}$ intersecte ou pas avec exactement un seul intervalle d'isolation J_k, est borné par $\tilde{O}\left(d^3\tau + d^4\right)$ opérations binaires à chaque tour. En effet, nous avons uniquement besoin de $O(\log(d))$ comparaisons entre les points les extremités des intervalles qui apparaissent. Chaque comparaison est réalisée avec une précision bornée par $\tilde{O}(d^3\tau + d^4)$, en l'utilisant cela à partir des bornes amorties sur le séparateur des racines (Proposition 1.9)

$$O\left(\left|\log\left(\mathrm{sep}\left(\beta_{i,j}, T_Y R_Y\right)\right)\right|\right) \in O(d^3\tau + d^4).$$

Sachant qu'il a au plus $O(d^2)$ points critiques, le coût total des comparaisons est alors bornée par $\tilde{O}(d^5\tau + d^6)$.

A présent, il ne reste plus quà faire une estimation du coût de raffinement des intervalles $I_{i,j}$, pour tout i,j, à une largeur inférieure à $2^{-2^{\ell_{i,j}}}$. En utilisant encore $O(|\log(\mathrm{sep}(\beta_{i,j}, T_Y R_Y))|) \in O(d^3\tau + d^4)$ opérations, nous obtenons un succès au bout de κ tours avec

$$\kappa = \max_{i,j} \ell_{i,j} + 1 \in O(\log(d^4 + d^3\tau)). \tag{2.61}$$

D'après le Théorème 2.2, le coût est borné par

$$\sum_{\ell=1}^{\kappa} \tilde{O}\left(d^5\tau + d^6 + 2^\ell d^2 \cdot \sum_{i=1}^{N} \mu_i^{[\ell]}\right) \in \tilde{O}\left(d^5\tau + d^6\right) + \tilde{O}\left(d^2 \cdot \sum_{\ell} 2^\ell \cdot \sum_{i=1}^{N} \mu_i^{[\ell]}\right),$$

où

$$\mu_i^{[\ell]} := \begin{cases} \max_{j \in V_i^\ell} \mu(\beta_{i,j}, \tilde{P}(\alpha_i, -)) & \text{si } V_z^\ell \neq \emptyset \\ 0 & \text{sinon.} \end{cases}$$

Ainsi, il suffit de montrer que

$$\sum_{\ell=1}^{\kappa} 2^\ell \cdot \sum_{i=1}^{N} \mu_i^{[\ell]} \in \tilde{O}(d^3\tau + d^4).$$

Si $V_i^\ell \neq \emptyset$, soit $j_i^{[\ell]} \in V_i^\ell$ tel que $\mu(\beta_{i,j_i^{[\ell]}}, \tilde{P}(\alpha_i, -)) = \mu_i^{[\ell]}$. En d'autres termes, $j_i^{[\ell]}$ est l'indice critique dans V_i^ℓ au dessus de α_i ayant la plus grande multiplité dans la fibre. Dans ce cas, nous pouvons écrire

$$\sum_{\ell=1}^{\kappa} 2^\ell \cdot \sum_{i=1}^{N} \mu_i^{[\ell]} = \sum_{\ell=1}^{\kappa} 2^\ell \sum_{i, V_i^\ell \neq \emptyset} \mu(\beta_{i,j_i^{[\ell]}}, \tilde{P}(\alpha_i, -))$$

Évidemment, chaque point critique $(\alpha_i,\beta_{i,j})$ apparaît au plus $\kappa \in O(\log(d^3\tau + d^4))$ fois dans la somme précédente. De plus, sachant que $(\alpha_i,\beta_{i,j}) \notin V_\kappa$ et $2^{\ell_{i,j}} \in O(|\log(\mathrm{sep}(\beta_{i,j}, T_Y R_Y))|)$, il s'en suit que

$$\sum_{\ell=1}^{\kappa} 2^\ell \sum_{i=1}^{N} \sum_{j\in V_i^\ell} \mu\left(\beta_{i,j}, \tilde{P}(\alpha_i,-)\right) \in \tilde{O}\left(\sum_{i=1}^{N} \sum_{j\in \mathrm{CritInd}_i} \mu(\beta_{i,j}, \tilde{P}(\alpha_i,-)) \cdot |\log(\mathrm{sep}(\beta_{i,j}, T_Y R_Y))|\right).$$

Sachant que

$$\sum_{\ell=1}^{\kappa} 2^\ell \sum_{i, V_i^\ell \neq \emptyset} \mu(\beta_{i,j_i^{[\ell]}}, \tilde{P}(\alpha_i,-)) \leq \sum_{\ell=1}^{\kappa} 2^\ell \sum_{i=1}^{N} \sum_{j\in V_i^\ell} \mu(\beta_{i,j}, \tilde{P}(\alpha_i,-)),$$

nous avons

$$\sum_{\ell=1}^{\kappa} 2^\ell \sum_{i, V_i^\ell \neq \emptyset} \mu(\beta_{i,j_i^{[\ell]}}, \tilde{P}(\alpha_i,-)) \in \tilde{O}(\sum_{i=1}^{N} \sum_{j\in \mathrm{CritInd}_i} \mu(\beta_{i,j}, \tilde{P}(\alpha_i,-)) \cdot |\log(\mathrm{sep}(\beta_{i,j}, T_Y R_Y))|).$$

D'après la Proposition 2.7, pour toute valeur fixe $\beta_{i,j}$,

$$\sum_{(\alpha_i,\beta_{i,j}):\beta_{i,j}=\gamma} (\mathrm{mult}(\beta_{i,j}, \tilde{P}(\alpha_i,-)) - 1) \leq \mathrm{mult}(\gamma, R_Y)).$$

Sachant que $\mathrm{mult}(\beta_{i,j}, \tilde{P}(\alpha_i,-)) \leq 2\cdot(\mathrm{mult}(\beta_{i,j}, \tilde{P}(\alpha_i,-)) - 1)$, nous pouvons conclure que

$$\sum_{(i,j):\beta_{i,j}=\gamma} \mathrm{mult}(\beta_{i,j}, \tilde{P}(\alpha_i,-)) \leq 2\cdot \mathrm{mult}(\gamma, T_Y R_Y).$$

En définitive, d'àprès la Proposition 1.9

$$\sum_{\ell=1}^{\kappa} 2^\ell \sum_{i=1}^{N} \mu_i^{[\ell]} \in \tilde{O}(\mathrm{logsep}(T_Y R_Y)) \in \tilde{O}(d^3\tau + d^4).$$

□

Pour chauqe indice fixé i, nous désignons par

$$\mathrm{CritInd}_i := \{k \in \{1,\ldots,M\} : (\alpha_i, \gamma_k) \in \mathrm{Crit}(\mathscr{C})\}.$$

l'ensemble des *indices critiques au dessus de i*. De la même manière, pour tout indice fixé k, nous désignons par

$$\mathrm{CritInd}_k := \{i \in \{1,\ldots,N\} : (\alpha_i, \gamma_k) \in \mathrm{Crit}(\mathscr{C})\}.$$

l'ensemble des *indices critiques au niveau k*.

Proposition 2.18
Avec $\tilde{O}(d^5\tau + d^6)$ *opérations binaires, et sans modifier les estimations (2.57), (2.58), (2.59) et (2.60),*

(a) on peut raffiner tous les intervalles $I^-_{i,j'}$ *(resp.* $I^+_{i,j'}$*) de sorte que, si* $I^-_{i,j'}$ *(resp.* $I^+_{i,j'}$*) intersecte un intervalle* J^+_k *(resp.* J^-_k*) pour un certain indice* $k \in \mathrm{CritPl}_i$*, alors il contient* J^+_k *(resp.* J^-_k*) et n'intersecte pas* J^-_k *(resp.* J^+_k*).*

(b) on peut raffiner tous les intervalles $J^-_{k,\ell}$ *(resp.* $J^+_{k,\ell}$*) de sorte que, si* $J^-_{k,\ell}$ *(resp.* $J^+_{k,\ell}$*) intersecte un intervalle* I^+_i *(resp.* I_i *; resp.* I^-_i*) pour* $i \in \mathrm{CritPl}^k$*, alors il contient* I^+_i *(resp.* I_i *; resp.* I^-_i*) et n'intersecte pas* I_i *et* I^-_i *(resp.* I^+_i *et* I^-_i *; resp.* I_i *et* I^+_i*).*

Démonstration
Nous traitons de façon détaillée le cas des intervalles $I^-_{i,j'}$ qui constitue la première moitié de (a). Soit $I^-_{i,j'}$ les intervalles calculés dans le Théorème 2.4. Dans ce qui suit, nous nous restreignons à l'ensemble V^1 de tous les indices (i,j') appelés *bad pairs* tels que l'intervalle $I^-_{i,j'}$ intersecte deux intervalles J^-_k et J^+_k, et nous désignerons par V^1_i l'ensemble des indices correspondants au dessus

de i. Soit ϕ l'application qui à tout *bad pair* (i,j') associe un indice arbitraire k (il peut exister plus d'un tel indice) tel que $I^-_{i,j'}$ intersecte les intervalles J^-_k et J^+_k et que par ailleurs $\gamma^+_k - \gamma^-_k$ soit minimal avec cette propriété. Il en résulte que la taille de la préimage de chaque k est bornée par CRITPL_k. A savoir, pour un indice i fixé, il peut y avoir au plus un intervalle $I^-_{i,j'}$ qui intersecte deux autres intervalles J^-_k et J^+_k. Par conséquent,

$$|\Phi^{-1}(k)| \leq |\text{CRITPL}_k| \leq \mu(\gamma_k, S_Y) \leq \mu(\gamma_k, T_Y),$$

ce qui implique davantage que V^1 contient au plus $O(d^2)$ éléments. A noter qu'une paire (i,j') ne peut devenir *bad* que si la largeur l'intervalle correspondant $I^-_{i,j'}$ est plus petit que $\frac{1}{2}\cdot \text{sep}(\gamma_k, T_Y)$; puisque la distance entre les intervalles J^-_k et J^+_k vaut au moins $\frac{1}{2}\cdot\min(|\gamma^+_k - \gamma^-_k|) \leq \frac{1}{2}\cdot\text{sep}(\gamma^-_k, T_Y)$. Ainsi, afin de certifier que l'intervalle $I^-_{i,j'}$ n'intersecte pas J^-_k et J^+_k, il suffit de raffiner les intervalles $I^-_{i,j'}$ avec $(i,j') \in V_1$ à une largeur inférieure à $\frac{1}{2}\cdot\text{sep}(\gamma^-_k, T_Y)$.

Pour cela, nous procédons tout d'abord par une suite d'énumération indexée par $\ell = 1,2,3,\ldots$, au cours de laquelle, au $\ell^{\text{ième}}$ tour, nous raffinons tous les intervalles $I^-_{i,j'}$ avec $(i,j') \in V^\ell_i$ à une largeur plus petite que 2^{-2^ℓ}. Ensuite, on retire toutes les paires (i,j') de V^ℓ_i qui ne sont plus *bad* pur obtenir l'ensemble $V^{\ell+1}_i$. En d'autres termes , $V^{\ell+1}_i$ regroupe toutes les paires dont les intervalles $I^-_{i,j'}$ intersectent chacun deux intervalles J^-_k et J^+_k au sortir du $\ell^{\text{ième}}$ tour. Dès lors, nous passons au $(\ell+1)^{\text{ième}}$ tour. Le processus est interrompu dès que tous les ensembles V^ℓ_i sont vides, auquel cas, chaque intervalle $I^-_{i,j'}$ satisfait la condition.

A noter que l'intervalle $I^-_{i,j'}$ est retiré après $\ell_{i,j'}$ tours, avec $2^{\ell_{i,j'}}$ borné par $O(|\log(\text{sep}(\gamma_{\phi((i,j'))}, T_Y))|)$. C'est-à-dire, pour tout $\ell > \ell_{i,j'}$, $j' \notin V^\ell_i$. Ce qui implique que le séparateur de chaque racine contenue dans $\phi(V_\ell)$ est inférieure à $2^{1+2^{-\ell}}$. En outre, notons qu'à partir des bornes amorties sur les séparateur des racines (Proposition 1.9)

$$O(|\log(\text{sep}(\gamma_{\phi((i,j'))}, T_Y))|) \in O(d^3\tau + d^4),$$

donc le coût du test consistant à vérifier si $j' \in V^\ell_i$ est borné par $\tilde{O}(d^3\tau + d^4)$ opérations binaires à chaque tour; puisque nous avons juste besoin de considérer $O(\log(d))$ comparaisons entre les extrémités des intervalles correspondants concernés. Chaque comparaison est réalisée avec une précision bornée par $\tilde{O}(d^3\tau + d^4)$. Sachant qu'il y a au plus $O(d^2)$ éléments dans chaque V, le coût total des comparaisons est bornée par $\tilde{O}(d^5\tau + d^6)$.

A présent, il reste à faire une estimation du coût de raffinement des intervalles $I^-_{i,j'}$, pour tout $(i,j') \in V$, à une largeur plus que $2^{-2^{\ell_{i,j'}}}$. Sachant que $O(|\log(\text{sep}(\gamma_{\phi((i,j'))}, T_Y))|) \in O(d^3\tau + d^4)$,

$$\kappa = \max_{i,j'} \ell_{i,j'} + 1 \in O(\log(d^3\tau + d^4)).$$

D'après le Théorème 2.2, le coût est borné par

$$\sum_{\ell=1}^{\kappa} \tilde{O}(d^5\tau + d^6 + 2^\ell d^2 \cdot \lambda_\ell) \in \tilde{O}(d^5\tau + d^6) + \tilde{O}(d^2 \cdot \sum_\ell 2^\ell \cdot |\{i \mid V^\ell_i \neq \emptyset\}|,$$

Ainsi, il suffit de montrer que

$$\sum_{\ell=1}^{\kappa} 2^\ell \cdot |\{i \mid V^\ell_i \neq \emptyset\}| \in \tilde{O}(d^4 + d^3\tau),$$

ou de façon alternative que

$$\sum_{\ell=1}^{\kappa} \sum_{k:\log(\text{sep}(\gamma_k, T_Y)) < 2^{1-2^\ell}} \mu(\gamma_k, T_Y) \cdot |\log(\text{sep}(\gamma_k, T_Y))| \in \tilde{O}(d^3\tau + d^4). \tag{2.62}$$

Sachant que chaque racine γ_k a au plus $\mu(\gamma_k, T_Y)$ préimages sous l'application ϕ et que $\phi(V^\ell_i)$ contient uniquement des racines γ_k dont le séparateur est plus petit que $2\cdot 2^{1-2^\ell}$. Par ailleurs $\kappa \in$

$O(\log(d^3\tau+d^4))$ et $\sum_{k=1}^{M}\mu(\gamma_k,T_Y)\cdot|\log(\mathrm{sep}(\gamma_k,T_Y))|\in\tilde{O}(d^3\tau+d^4)$; d'où l'on conclue que l'inégalité (2.62) est vérifiée.

Le cas des intervalles $I^+_{i,j'}$ qui est la seconde moitié de (a) est totalement identique. Nous admettons aussi la démonstration du (b) qui est similaire au (a). Il s'agira de permuter les rôles de X et Y, en commençant par le premier cas α_i^-,α_i pour terminer par le second cas α_i,α_i^+. □

A présent, nous allons voir comment traiter les asymptotes verticales.

Les asymptotes verticales apparaissent en des valeurs de α où $\deg(\tilde{P}(\alpha,Y))<d_y=\deg_Y(\tilde{P})$, donc uniquement aux racines de $c_{d_y}(X)$ qui sont aussi des racines de D_X. Les indices $i=1,\ldots,N$ tels que $c_{d_y}(\alpha_i)=0$ font partie des informations obtenues en sortie à travers le Théorème 2.4.

En ce qui concerne les asymptotes verticales à $-\infty$, il suffit d'isoler les racines de $\tilde{P}(X,\gamma_1^-)=0$ et de lire les signes de la pente en les racines de $\tilde{P}(X,\gamma_1^-)=0$. Ce travail peut être fait avec $\tilde{O}(d^4\tau+d^5)$ opérations binaire. En effet, $\tilde{P}(X,\gamma_1^-)$ est un polynôme dont la magnitude est bornée par $(d,O(d^2\tau+d^3))$. Par ailleurs, nous faisons aussi une comparaison entre les racines de $\tilde{P}(X,\gamma_1^-)$ et celles de D_X. A noter que les polynômes $\tilde{P}(X,\gamma_1^-)$ et D_X n'ont aucune racine commune. Sachant que les séparateurs de $\tilde{P}(X,\gamma_1^-)$ et D_X sont tous les deux bornés par $2^{\tilde{O}(d^3\tau+d^4)}$, donc d'après la Proposition 1.17, la comparaison coûtera au plus $\tilde{O}(d^5\tau+d^6)$ opérations binaires.

Sur chaque intervalle $]\alpha_i,\alpha_{i+1}[$, $i=1,\ldots,N$ délimitée par les racines de D_X, on désigne par $\mathrm{RIGHT}_{i,0}$ le nombre de racines de $\tilde{P}(X,\gamma_1^-)=0$ tel que le signe de la pente est >0 et par $\mathrm{LEFT}_{i+1,0}$ le nombre de racines de $\tilde{P}(X,\gamma_1^-)=0$ tel que le signe de la pente est <0. On désignera aussi par $\mathrm{RIGHT}_{N,0}$ le nombre de racines de $\tilde{P}(X,\gamma_1^-)=0$ tel que le signe de la pente est >0 sur $(\alpha_N,+\infty)$ et par $\mathrm{LEFT}_{1,0}$ le nombre de racines de $\tilde{P}(X,\gamma_M^+)=0$ tel que le signe de la pente est <0 sur $(-\infty,\alpha_1)$.

A noter que toutes les racines de $\tilde{P}(X,\gamma_1^-)=0$ sur (α_i,α_{i+1}) dont le signe de la pente est positif sont plus grand que toutes les racines de $\tilde{P}(X,\gamma_1^-)=0$ sur I_i dont le signe de la pente est négatif.De plus, si α_i n'est pas une racine de c_{d_y}, alors $\mathrm{LEFT}_{1,0}=\mathrm{RIGHT}_{1,0}=0$.

La situation à $+\infty$ est totalement similaire. Soient RIGHT_{i,m_i+1} le nombre de racines de $\tilde{P}(X,\gamma_M^+)=0$ sur (α_i,α_{i+1}) dont le signe de la pente est >0 et $\mathrm{LEFT}_{i+1,m_{i+1}+1}$ le nombre de racines de $\tilde{P}(X,\gamma_M^+)=0$ on (α_i,α_{i+1}) dont le signe de la pente est <0. Nous désignons par RIGHT_{N,m_N+1} le nombre de racines de $\tilde{P}(X,\gamma_M^+)=0$ dont le signe de la pente est <0 sur l'intervalle $]\alpha_N,+\infty[$ et par LEFT_{1,m_1+1} le nombre de racines de $\tilde{P}(X,\gamma_M^+)=0$ dont le signe de la pente est >0 sur l'intervalle $]-\infty,\alpha_1[$.

Finalement, nous avons la résulat suivant.

Proposition 2.19
Le nombre de branches asymptotiques qui tendent vers $-\infty$ (resp $+\infty$) à gauche de α_i est $\mathrm{LEFT}_{i,0}$ *(resp.* LEFT_{i,m_i+1}*) et le nombre de branches asymptotiques qui tendent vers $-\infty$ (resp $+\infty$) à droite de α_i est* $\mathrm{RIGHT}_{i,0}$ *(resp.* RIGHT_{i,m_i+1}*). La complexité du calcul de ces nombres est bornée par* $\tilde{O}(d^5\tau+d^6)$.

2.5 Calcul effectif de la topologie d'une courbe algébrique

2.5.1 Topologie des boîtes adjacentes

Dans cette section, l'objectif est de déterminer, pour chaque boîte adjacente d'un point critique $(\alpha_i,\beta_{i,j})$, les nombres de segments $\mathrm{LEFT}_{i,j}$ et $\mathrm{RIGHT}_{i,j}$ arrivant respectivement à gauche et à droite de $(\alpha_i,\beta_{i,j})$ à l'aide de l'Algorithme 1.

On considère la boîte adjacente $[\alpha^-,\alpha^+]\times[\gamma^-,\gamma^+]$ associée au point singulier $(\alpha,\beta)=(\alpha_i,\beta_{i,j})$, avec $\alpha^-=\alpha_i^-,\alpha^+=\alpha_i^+$ et $\gamma^-=\gamma^-_{k(i,j)},\gamma^+=\gamma^+_{k(i,j)}$, où α^-,α,α^+ et γ^-,γ^+ sont donnés par des intervalles dyadiques $]a^-,a'^-[,]a,a'[,]a^+,a'^+[$ et $]c^-,c'^-[,]c^+,c'^+[$. Posons $\mathrm{LEFT}=\mathrm{LEFT}_{i,j}$ et $\mathrm{RIGHT}=\mathrm{RIGHT}_{i,j}$.

Nous pouvons remarquer que, au niveau du coin (α^-,γ^+) de la boîte, le signe de $\tilde{P}(\alpha^-,\gamma^+)$ est inconnu lorsque l'intervalle d'isolation $]x,x'[$ de ξ (en tant que racine du polynôme $\tilde{P}(X,\gamma^+)$) contient α^- et que l'intervalle d'isolation $]y,y'[$ de η (en tant que racine du polynôme $\tilde{P}(\alpha^-,Y)$) contient γ^+. Car nous ne savons pas si $\xi<\alpha^-$, $\xi=\alpha^-$ ou $\xi>\alpha^-$ (respectivement $\eta<\gamma^+$, $\eta=\gamma^+$

ou $\eta > \gamma^+$). Évidemment, on peut aussi tirer cette information en faisant des calculs exacts, ce qui dépassera largement les bornes de complexité escomptées. Ainsi, nous introduisons la définition suivante afin de traiter de pareilles ambiguïtés.

Définition 2.3
Le coin (α^-, γ^+) *est dit* **ambigu** *lorsque l'intervalle d'isolation* $]x, x'[$ *d'une racine* ξ *de* $\tilde{P}(X, \gamma^+)$ *contient* α^- *et que l'intervalle d'isolation* $]y, y'[$ *d'une racine* η *de* $\tilde{P}(\alpha^-, Y)$ *contient* γ^+. *Nous admettons la même définition pour les coins* (α^-, γ^-), (α^+, γ^-), (α^+, γ^+).

De la même manière, un midpoint (α, γ^+) *est dit* **ambigu** *lorsque l'intervalle d'isolation* $]x, x'[$ *d'une racine* ξ *de* $\tilde{P}(X, \gamma^+)$ *contient* α *et que l'intervalle d'isolation* $]y, y'[$ *d'une racine* η *de* $\tilde{P}(\alpha, Y)$ *contient* γ^+ . *Nous admettons la même définition pour le midpoint* (α, γ^-).

Au niveau d'un coin ambigu (α^-, γ^+), il est impossible de connaître la cardinalité des ensembles $L_{\gamma^+}^{<\alpha} \cap [x, x']$, $L_{\gamma^+}^{=\alpha} \cap [x, x']$ et $L_{\alpha^-} \cap [y, y']$; puisqu'on ignore si $\sigma \in L_{\gamma^+}^{<\alpha}$ (respectivement $\eta \in L_{<\alpha^-}$. Toutefois, en faisant une étude au cas par cas, on arrive aux résultats suivants :

— SIi$\sigma^+ > 0$ (avec $\partial_X \tilde{P}(\alpha^-, \gamma^+) > 0$ et $\partial_Y \tilde{P}(\alpha^-, \gamma^+) < 0$) alors $\tilde{P}(x, \gamma^+) < 0$ et $\tilde{P}(x', \gamma^+) > 0$ tant que $\tilde{P}(\alpha^-, y) > 0$ et $\tilde{P}(\alpha^-, y') < 0$.

— Si $\tilde{P}(\alpha^-, \gamma^+) > 0$, alors $\xi < \alpha^-$ et $\eta > \gamma^+$. Donc

$$\#L_{\gamma^+}^{<\alpha} \cap [x, x'] = \#L_{\alpha^-} \cap [y, y'] = 0$$

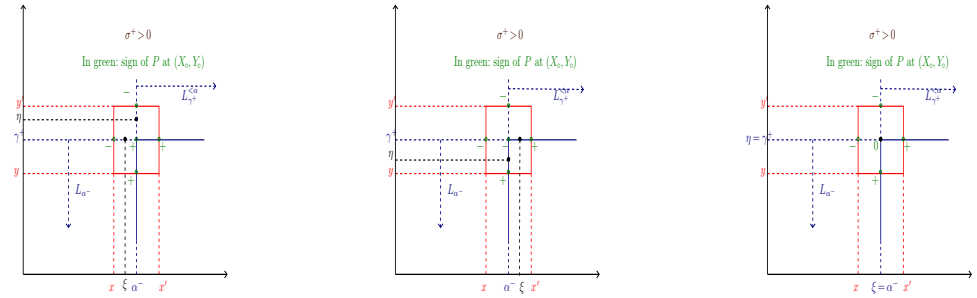
— Si $\tilde{P}(\alpha^-, \gamma^+) < 0$, alors $\xi > \alpha^-$ et $\eta < \gamma^+$. Donc

$$\#L_{\gamma^+}^{<\alpha} \cap [x, x'] = \#L_{\alpha^-} \cap [y, y'] = 1,$$

— Si $\tilde{P}(\alpha^-, \gamma^+) = 0$, alors $\xi = \alpha^-$ et $\eta = \gamma^+$. Donc

$$\#L_{\gamma^+}^{<\alpha} \cap [x, x'] = \#L_{\alpha^-} \cap [y, y'] = 0$$

$\tilde{P}(\alpha^-, \gamma^+) > 0$ $\tilde{P}(\alpha^-, \gamma^+) < 0$ $\tilde{P}(\alpha^-, \gamma^+) = 0$



Ainsi, dans tous ces cas de figures lorsque $\sigma^+ > 0$ (avec $\partial_X \tilde{P}(\alpha^-, \gamma^+) > 0$ et $\partial_Y \tilde{P}(\alpha^-, \gamma^+) < 0$), on voit obtient toujours

$$\#L_{\gamma^+}^{<\alpha} \cap [x, x'] - \#L_{\alpha^-} \cap [y, y'] = 0.$$

— Si $\sigma^+ < 0$ (avec $\partial_X \tilde{P}(\alpha^-, \gamma^+) > 0$ et $\partial_Y \tilde{P}(\alpha^-, \gamma^+) > 0$), alors $\tilde{P}(x, \gamma^+) < 0$ et $\tilde{P}(x', \gamma^+) > 0$ tant que $\tilde{P}(\alpha^-, y) < 0$ et $\tilde{P}(\alpha^-, y') > 0$.

— Si $\tilde{P}(\alpha^-, \gamma^+) > 0$, alors $\xi < \gamma^-$ et $\eta < \alpha^+$. Donc

$$\#L_{\gamma^+}^{<\alpha} \cap [x, x'] = \#L_{\gamma^+}^{=\alpha^-} \cap [x, x'] = 0, \#L_{\alpha^-} \cap [y, y'] = 1$$

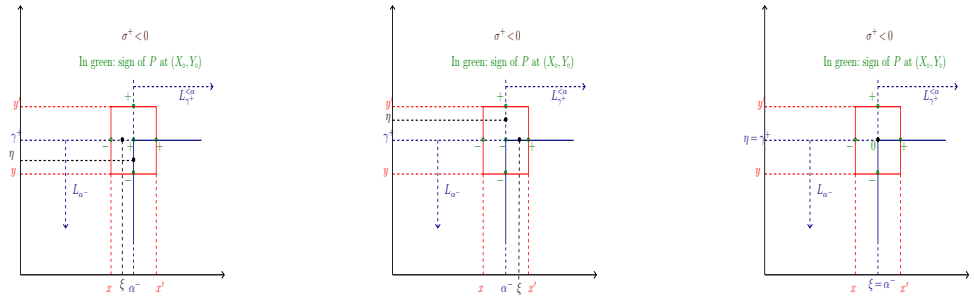
— Si $\tilde{P}(\alpha^-, \gamma^+) < 0$, alors $\xi > \gamma^-$ et $\eta > \alpha^+$. Donc

$$\#L_{\gamma^+}^{<\alpha} \cap [x, x'] = 1, \#L_{\alpha^-} \cap [y, y'] = \#L_{\gamma^+}^{=\alpha^-} \cap [x, x'] = 0$$

— Si $\tilde{P}(\alpha^-, \gamma^+) = 0$ alors $\xi = \alpha^-$ et $\eta = \gamma^+$. Donc

$$\#L_{\gamma^+}^{<\alpha} \cap [x, x'] = \#L_{\alpha^-} \cap [y, y'] = 0, \#L_{\gamma^+}^{=\alpha^-} \cap [x, x'] = 1$$

$\tilde{P}(\alpha^-,\gamma^+)>0$ $\tilde{P}(\alpha^-,\gamma^+)<0$ $,\tilde{P}(\alpha^-,\gamma^+)=0$



Finalement, dans ces différents cas de figures, lorsque $\sigma^+<0$ (avec $\partial_X\tilde{P}(\alpha^-,\gamma^+)>0$ et $\partial_Y\tilde{P}(\alpha^-,\gamma^+)>0$), on voit que

$$\#L_{\gamma^+}^{<\alpha}\cap[x,x']+\#L_{\alpha^-}\cap[y,y']+\#L_{\alpha^-}\cap[y,y']=1.$$

— Les détails concernant les cas où $\sigma^+>0$ avec $\partial_X\tilde{P}(\alpha^-,\gamma^+)<0$ et $\partial_Y\tilde{P}(\alpha^-,\gamma^+)>0$ (resp. $\sigma^+<0$ avec $\partial_X\tilde{P}(\alpha^-,\gamma^+)<0$ et $\partial_Y\tilde{P}(\alpha^-,\gamma^+)<0$) sont entièrement similaires.

En définitive, dans toutes les situations, la conclusion est la suivante

— Si $\sigma^+>0$ alors

$$\#L_{\alpha^-}\cap[y,y']-\#L_{\gamma^+}^{<\alpha}\cap[x,x']=0$$

— Si $\sigma^-<0$ alors

$$\#L_{\alpha^-}\cap[y,y']+\#L_{\gamma^+}^{<\alpha}\cap[x,x']+\#L_{\gamma^+}^{=\alpha}\cap[x,x']=1$$

Ce qui signifie que le signe de $\tilde{P}(\alpha^-,\gamma^+)$ n'a aucune influence sur le nombre LEFT renvoyé par les formules dans l'Algorithme 1.

A présent nous allons analyser la situation au tour d'un midpoint ambigu (α,γ^+).

— Si $\sigma^+>0$ avec $\partial_X\tilde{P}(\alpha,\gamma^+)>0$ et $\partial_Y\tilde{P}(\alpha,\gamma^+)<0$, alors $\tilde{P}(x,\gamma^+)<0$ et $\tilde{P}(x',\gamma^+)>0$ tant que $\tilde{P}(\alpha,y)>0$ et $\tilde{P}(\alpha,y')<0$.

  — Si $\tilde{P}(\alpha,\gamma^+)>0$, alors $\xi<\alpha$ et $\eta>\gamma^+$. Donc

  $$\#L_{\gamma^+}^{<\alpha}\cap[x,x']=1,\#L_{\gamma^+}^{=\alpha}\cap[x,x']=\#L_{\alpha}^{>\beta}\cap[y,y']=0$$

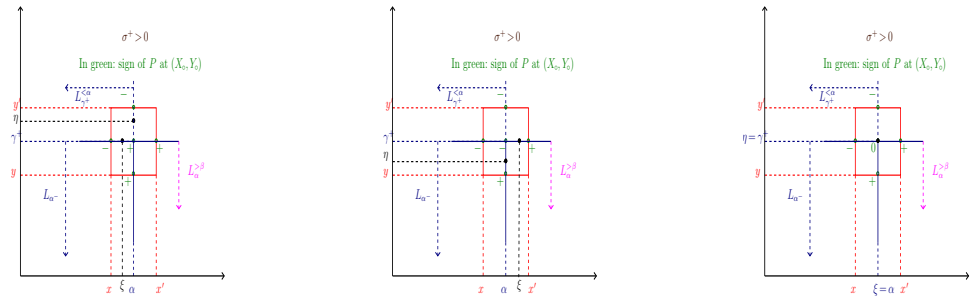
  — Si $\tilde{P}(\alpha,\gamma^+)<0$, alors $\xi>\alpha$ et $\eta<\gamma^+$. Donc

  $$\#L_{\gamma^+}^{<\alpha}\cap[x,x']=\#L_{\gamma^+}^{=\alpha}\cap[x,x']=0,\#L_{\alpha}^{>\beta}\cap[y,y']=1$$

  — Si $\tilde{P}(\alpha,\gamma^+)=0$, alors $\xi=\alpha$ et $\eta=\gamma^+$. Donc

  $$\#L_{\gamma^+}^{<\alpha}\cap[x,x']=0,\#L_{\gamma^+}^{=\alpha}\cap[x,x']=1,\#L_{\alpha}^{>\beta}\cap[y,y']=0$$

$\tilde{P}(\alpha,\gamma^+)>0$ $\tilde{P}(\alpha,\gamma^+)<0$ $\tilde{P}(\alpha,\gamma^+)=0$



Dans les différents cas de figures, si $\sigma^+>0$ (avec $\partial_X\tilde{P}(\alpha^-,\gamma^+)>0$ and $\partial_Y\tilde{P}(\alpha^-,\gamma^+)<0$) alors

$$-\#L_{\gamma^+}^{<\alpha}\cap[x,x']-\#L_{\gamma^+}^{=\alpha}\cap[x,x']-\#L_{\alpha}^{>\beta}\cap[y,y']=-1.$$

— Si $\sigma^+ < 0$ avec $\partial_X \tilde{P}(\alpha, \gamma^+) > 0$ et $\partial_Y \tilde{P}(\alpha, \gamma^+) > 0$, alors $\tilde{P}(x, \gamma^+) < 0$ et $\tilde{P}(x', \gamma^+) > 0$ tant que $\tilde{P}(\alpha, y) < 0$ et $\tilde{P}(\alpha, y') > 0$.

— Si $\tilde{P}(\alpha, \gamma^+) > 0$, alors la racine ξ est à gauche de α et la racine η est sous γ^+. Donc

$$\#L_{\gamma^+}^{<\alpha} \cap [x, x'] = 1, \#L_{\alpha}^{>\beta} \cap [y, y'] = 1$$

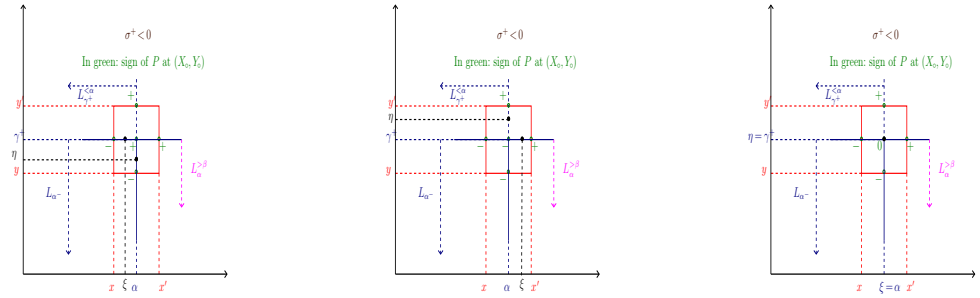
— Si $\tilde{P}(\alpha, \gamma^+) < 0$, alors la racine ξ est à droite de α et la racine η est au dessus de γ^+. Donc

$$\#L_{\gamma^+}^{<\alpha} \cap [x, x'] = 0, \#L_{\alpha}^{>\beta} \cap [y, y'] = 0$$

— Si $\tilde{P}(\alpha, \gamma^+) = 0$ alors $\xi = \alpha$ alors $\eta = \gamma^+$. Donc

$$\#L_{\gamma^+}^{<\alpha} \cap [x, x'] = \#L_{\alpha}^{>\beta} \cap [y, y'] = 0$$

$\tilde{P}(\alpha, \gamma^+) > 0$ $\tilde{P}(\alpha, \gamma^+) < 0$ $\tilde{P}(\alpha, \gamma^+) = 0$



Dans ces différents cas de figures, lorsque $\sigma^+ < 0$ (avec $\partial_X \tilde{P}(\alpha^-, \gamma^+) > 0$ et $\partial_Y \tilde{P}(\alpha^-, \gamma^+) > 0$),

$$\#L_{\gamma^+}^{<\alpha} \cap [x, x'] - \#L_{\alpha}^{>\beta} \cap [y, y'] = 0.$$

— Les détails concernant les cas $\sigma^+ > 0$ avec $\partial_X \tilde{P}(\alpha, \gamma^+) < 0$ et $\partial_Y \tilde{P}(\alpha, \gamma^+) > 0$ (respectivement $\sigma^+ < 0$ avec $\partial_X \tilde{P}(\alpha, \gamma^+) < 0$ et $\partial_Y \tilde{P}(\alpha, \gamma^+) < 0$) sont similaires.

En somme, pour toutes ces différentes situations, la conclusion est la suivante

— Si $\sigma^+ > 0$ alors

$$-\#L_{\gamma^+}^{<\alpha} \cap [x, x'] - \#L_{\gamma^+}^{=\alpha} \cap [x, x'] - \#L_{\alpha}^{>\beta} \cap [y, y'] = -1$$

— Si $\sigma^+ < 0$ alors

$$\#L_{\gamma^+}^{<\alpha} \cap [x, x'] - \#L_{\alpha}^{>\beta} \cap [y, y'] = 0$$

Ce qui signifie que le signe de $\tilde{P}(\alpha, \gamma^+)$ n'a aucune influence sur le nombre LEFT renvoyé par les formules dans l'Algorithme 1).

Les analyses pour les autres coins ambigus et les midpoints ambigus sont similaires. Nous pouvons donc conclure par une proposition comme suit :

Proposition 2.20
Le signe de P *en un coin ambigu ou un midpoint ambigu n'a aucune influence sur les nombres* LEFT *et* RIGHT.

Par conséquent, il est possible de considérer arbitrairement que $\tilde{P}$ est nul sur tous les coins ambigus ainsi qu'au niveau des midpoints ; ce qui nous permet de déterminer les nombres

$$\#L_{\alpha^-}, \#L_{\gamma^-}^{=\alpha^-}, \#L_{\gamma^-}^{<\alpha}, \#L_{\gamma^-}^{=\alpha}, \#L_{\gamma^+}^{=\alpha^-}, \#L_{\gamma^+}^{<\alpha}, \#L_{\gamma^+}^{=\alpha}, \#L_{\alpha}^{>\beta}, \#L_{\alpha}^{<\beta}$$

à partir desquels nous pouvons calculer la valeur exacte de LEFT par les formules dans l'Algorithme 1. La démarche est similaire pour RIGHT.

Proposition 2.21
Pour tout i, j, $i = 1, \ldots, N$, $j \in \text{RIGHT}_i$, *nous pouvons calculer* $\text{LEFT}_{i,j}$ *et* $\text{RIGHT}_{i,j}$ *avec une complexité en* $\tilde{O}(d^5\tau + d^6)$ *opérations binaires.*

2.5.2 Reconstruction de la topologie globale

Rappelons que, pour tout point critique $(\alpha_i, \beta_{i,j})$, i.e. $j \in \mathbf{C}_i$, $\text{LEFT}_{i,j}$ (resp. $\text{RIGHT}_{i,j}$) désigne, comme défini dans la section précédente, le nombre de segments qui arrivent à $(\alpha_i, \beta_{i,j})$ et qui sont à l'intérieur de la boîte $[a_i, \alpha_i] \times [c_{i,j}, d_{i,j}]$ (resp. $[\alpha_i, b_i] \times [c_{i,j}, d_{i,j}]$). Notons aussi que cette information a été déterminée grâce à la Proposition 2.21 avec une complexité en $\tilde{O}(d^5\tau + d^6)$ opérations binaires. Pour $j \notin \mathscr{C}_i$, nous choisirons $\text{LEFT}_{i,j} = \text{RIGHT}_{i,j} = 1$. De la même manière, nous désignons par $\text{LEFT}_{i,0}$ (resp. $\text{RIGHT}_{i,0}$) le nombre $\ell_i^{-\infty}$ (resp $\ell_i^{-\infty}$) de branches verticales qui tendent vers $-\infty$ à gauche (resp. à droite) de α_i et par LEFT_{i,m_i+1} (resp. RIGHT_{i,m_i+1}) le nombre branches verticales qui tendent vers $+\infty$ à gauche (resp. à droite) de α_i. Ces valeurs ont été déterminées grâce à la Proposition 2.19.

La topologie de la courbe $\mathscr{C}(\tilde{P})$ est représentée par une liste finie de valeurs

$$\tilde{\mathscr{L}}(\tilde{P}) = [m'_0, L_1, \ldots, L_N, m'_N]$$

avec

- $L_i = [m_i, [[\text{LEFT}_{i,j}, \text{RIGHT}_{i,j}], 0 \le j \le m_i + 1]]$ où $i = 1, \ldots, N$,

En particulier, si $\deg_X(\tilde{P}(X,Y)) = 0$ et $\mathscr{C}(\tilde{P})$ est un ensemble fini de m droites alors m est obtenu en calculant le nombre de racines réelles de $\text{pgcd}(\tilde{P}(X,Y), \text{LCF}_X(\tilde{P}(X,Y))$ qui est un polynôme en Y. La topologie de $\mathscr{C}(\tilde{P})$ est représentée par $\tilde{\mathscr{L}}(\tilde{P}) = [m]$.

Exemple 2.2 *Soit le polynôme bivarié*

$$P(X,Y) = (4X+1)(8X-1)(16X-1)(XY-1)(4Y^2-4X-1)(4Y^2+4X-1),$$

donc

$$\tilde{P}(X,Y) = (XY-1)(4Y^2-4X-1)(4Y^2+4X-1).$$

On a

$$D_X = -2^{28}X^4\,(4X-1)\,(1+4X)\left(4-X^2+4X^3\right)^2\left(-4+X^2+4X^3\right)^2,$$

$4-X^2+4X^3$ *(resp.* $-4+X^2+4X^3$*) admet une seule racine réelle appartenant à l'intervalle* $[-1,-1/2]$ *(resp. à* $[1/2,1]$*) donc* $N = 5$. *La topologie de la courbe* $\mathscr{C}(\tilde{P})$*, i.e sans les droites verticales, est représentée par la liste*

$$\tilde{\mathscr{L}}(\tilde{P}) = [3, L_1, 3, L_2, 5, L_3, 5, L_4, 3, L_5, 3]$$

avec

- $L_1 = [2, [[0,0], [2,2], [1,1], [0,0]]]$
- $L_2 = [4, [[0,0], [1,1], [1,1], [0,2], [1,1], [0,0]]]$
- $L_3 = [2, [[1,0], [2,2], [2,2], [0,1]]]$
- $L_4 = [4, [[0,0], [1,1], [2,0], [1,1], [1,1], [0,0]]]$
- $L_5 = [2, [[0,0], [1,1], [2,2], [0,0]]]$

On construit un graphe linéaire par morceaux $\widetilde{\text{Gr}}(\tilde{P})$ en dimension 2 comme suit

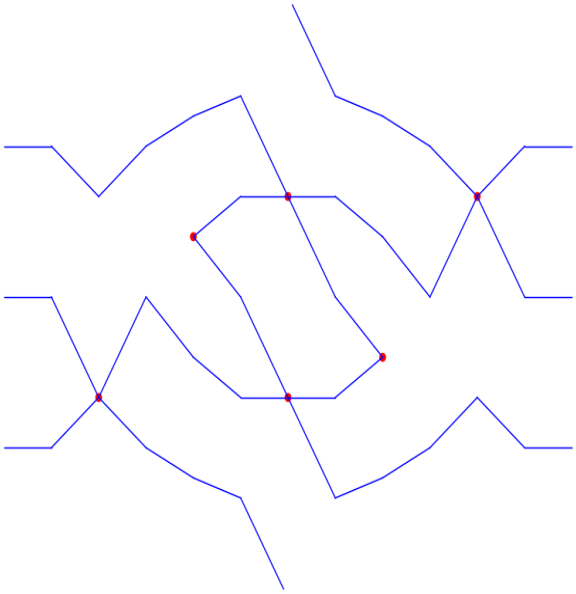
— soit $d' = \max(\max_{i=0,\ldots,N} m'_i, \max_{i=1,\ldots,N} m_i))$,

— pour tout $i = 0, \ldots, N$ et $j = 1, \ldots, m'_i$, introduire les points

$$I_{i,j} = \left(2i+1, \frac{j(d'+1)}{m'_i+1}\right)$$

— pour tout $i = 1, \ldots, N$ et $j = 0, \ldots, m_j + 1$, introduire les points

$$P_{i,j} = \left(2i, \frac{j(d'+1)}{m_i+1}\right)$$



— pour tout $j = 1, \ldots, m'_0$, introduire les points

$$\mathrm{P}_{-\infty,j} = \left(0, \frac{j(d'+1)}{m'_0+1}\right)$$

ainsi que les points

$$\mathrm{P}_{+\infty,j} = \left(2(\mathrm{N}+1), \frac{j(d'+1)}{m'_\mathrm{N}+1}\right)$$

pour tout $j = 1, \ldots, m'_\mathrm{N}$,

— Pour $i = 1, \ldots, \mathrm{N}$, si

$$\sum_{k=0}^{j-1} \mathrm{LEFT}_{i,k} < \ell \leq \sum_{k=0}^{j} \mathrm{LEFT}_{i,k} (\text{resp. } \sum_{k=0}^{j-1} \mathrm{RIGHT}_{i,k} < r \leq \sum_{k=0}^{j} \mathrm{RIGHT}_{i,k})$$

alors ajouter le segment $\mathrm{I}_{i-1,\ell}\mathrm{P}_{i,j}$ (resp. $\mathrm{P}_{i,j}\mathrm{I}_{i,r}$)

— pour $j = 1, \ldots, m'_0$, ajouter les segments $\mathrm{P}_{-\infty,j}\mathrm{I}_{0,j}$ et pour $j = 1, \ldots, m'_\mathrm{N}$, ajouter les segments $\mathrm{I}_{\mathrm{N},j}\mathrm{P}_{\infty,j}$.

Proposition 2.22
$\widetilde{\mathrm{Gr}}(\tilde{\mathrm{P}}) \subset (0, 2\mathrm{N}) \times (0, d'+1)$ *est homémorphe à* $\mathscr{C}(\tilde{\mathrm{P}}) \subset \mathbb{R}^2$.

En définitive, nous allons reconstruire la courbe $\mathscr{C}(\mathrm{P})$ en rajoutant les droites verticales qui ont été enlevées afin de faciliter le calcul de $\mathscr{C}(\tilde{\mathrm{P}})$. Pour rappel, $c(\mathrm{X})$ désigne le pgcd de tous les coefficients $c_i(\mathrm{X})$ de $\mathrm{P}(\mathrm{X},\mathrm{Y})$ vu comme un élément de $\mathbb{Z}[\mathrm{X}][\mathrm{Y}]$. Soit $c^\star(\mathrm{X})$ la partie sans facteur carré de $c(\mathrm{X})$.

Posons :

— $c_1(\mathrm{X}) := \mathrm{pgcd}(c^\star(\mathrm{X}), \mathrm{D}_\mathrm{X}(\mathrm{X}))$ et $c_2(\mathrm{X}) := \mathrm{quo}(c^\star(\mathrm{X}), c_1(\mathrm{X}))$,

— $\mathscr{V}_1 := \{(x,y) \in \mathbb{R}^2 | c_1(x) = 0\}$ et $\mathscr{V}_2 := \{(x,y) \in \mathbb{R}^2 | c_2(x) = 0\}$.

$\mathscr{V}_1$ est le sous-ensemble des droites verticales de $\mathscr{C}(\mathrm{P})$ passant par les valeurs critiques de $\mathscr{C}(\tilde{\mathrm{P}})$ tandis que $\mathscr{V}_2$ est le sous-ensemble de celles qui passent entre les valeurs critiques de $\mathscr{C}(\tilde{\mathrm{P}})$. D'après les Propositions 1.12 et 1.13, la complexité du calcul de $c_1(\mathrm{X})$ et $c_2(\mathrm{X})$ est respectivement en $\tilde{\mathrm{O}}(d^4\tau + d^5)$ et $\tilde{\mathrm{O}}(d\tau + d^2)$ opérations binaires. Afin de rajouter les droites appartenant à $\mathscr{V}_1$ dans $\mathscr{C}(\tilde{\mathrm{P}})$, il est nécessaire d'identifier les racines de réelles de $c_1(\mathrm{X})$ qui sont aussi racines de $\mathrm{D}_\mathrm{X}(\mathrm{X})$, i.e. pouvoir dire si oui ou non une droite verticale $\mathrm{X} = \alpha_i$ appartient à $\mathscr{C}(\mathrm{P})$. Une telle identification requiert

une complexité binaire en $\tilde{O}(d^5\tau + d^6)$; d'après la Proposition 1.18. Pour rajouter les droites de $\mathcal{V}_2$ dans $\mathscr{C}(\tilde{P})$, il suffit de compter le nombre de racines réelles de $c_2(X)$ sur l'intervalle $\mathscr{I}_i$. D'après la Proposition 1.18, cela requiert $\tilde{O}(d^5\tau + d^6)$ opérations binaires.

Proposition 2.23
Soit $P \in \mathbb{Z}[X,Y]$ *un polynôme sans facteur carré de magnitude* (s,τ). *L'instruction qui consiste à rajouter les droites verticales de* $\mathscr{C}(P)$ *dans* $\mathscr{C}(\tilde{P})$ *a une complexité en* $\tilde{O}(d^5\tau + d^6)$.

Nous obtenons une description combinatoire complète de la topologie de $\mathscr{C}(P)$ à travers la liste finie de valeurs

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

où

- $L'_i = [[m_i, w_i], [[\ell_{i,j}, r_{i,j}], 0 \le j \le m_i + 1]]$ pour $i = 1, \ldots, \delta$,
- $N'_i = [m'_i, v_i]$ pour $i = 0, \ldots, \delta$,

avec $w_i = 1$ si pour tout $i = 1, \ldots, \delta$, la droite $X = \alpha_i$ appartient à $\mathscr{C}(P)$ sinon $w_i = 0$; pour $i = 1, \ldots, \delta - 1$, v_i désigne le nombre de droites verticales $X = x$ telles que $\alpha_i < x < \alpha_{i+1}$ et v_0 (resp. v_δ) désigne le nombre de droites verticales $X = x$ avec $x < \alpha_1$ (resp. $x > \alpha_\delta$). En définitive, le graphe planaire linéaire par morceaux $Gr(P)$ est défini par

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

où V_i est le segment vertical défini par l'équation $X = 2i, 0 < Y < d' + 1$ et pour $i = 0, \ldots, \delta, \ell = 1, \ldots, v_i$, $V_{i,\ell}$ est le segment vertical défini par l'équation

$$X = 2i + \frac{2\ell}{v_i + 1}, 0 < Y < d' + 1.$$

On a donc la proposition suivante.

Proposition 2.24
$Gr(P) \subset (0, 2\delta) \times (0, d' + 1)$ *est homéomorphe à* $\mathscr{C}(P) \subset \mathbb{R}^2$.

Exemple 2.3
Dans la suite de l'Exemple 2.2, nous avons trois droites verticales définies par les équations ci-dessous

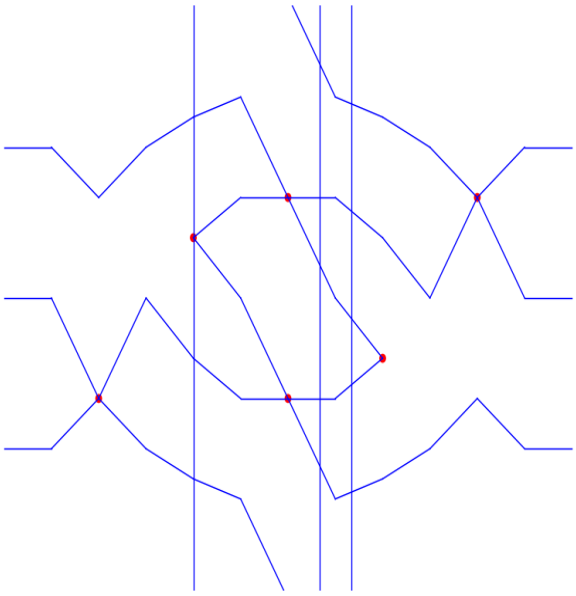
$$X = \frac{-1}{4}, X = \frac{1}{8}, X = \frac{1}{16}$$

Nous obtenons la liste

$$\mathscr{L}(P) = [N'_0, L'_1, N'_1, L'_2, N'_2, L'_3, N'_3, L'_4, N'_4, L'_5, N'_5]$$

avec

- $N'_0 = [3, 0]$
- $L_1 = [[2, 0], [[0, 0], [2, 2], [1, 1], [0, 0]]]$
- $N_1 = [3, 0]$
- $L_2 = [[4, 1], [[0, 0], [1, 1], [1, 1], [0, 2], [1, 1], [0, 0]]]$
- $N_2 = [5, 0]$
- $L_3 = [[2, 0], [[1, 0], [2, 2], [2, 2], [0, 1]]]$
- $N_3 = [5, 2]$
- $L_4 = [[4, 0], [[0, 0], [1, 1], [2, 0], [1, 1], [1, 1], [0, 0]]]$
- $N_4 = [3, 0]$
- $L_5 = [[2, 0], [[0, 0], [1, 1], [2, 2], [0, 0]]]$
- $N_5 = [3, 0]$



Chapitre 3

Déviation d'une courbe algébrique par rapport à sa tangente verticale

Introduction

Soit $P \in \mathbb{Z}[X,Y]$ un polynôme bivarié, sans facteur carré et de magnitude (d,τ). On désigne par $V_{\mathbb{R}}(P) := \{(\alpha,\gamma) \in \mathbb{R}^2 \mid P(\alpha,\gamma) = 0\}$ la courbe algébrique réelle définie comme étant l'ensemble des solutions réelles de l'équation $P(x,y) = 0$. Nous supposons que $V_{\mathbb{R}}(P)$ ne contient pas de droite verticale . Dans ce chapitre, nous établissons deux résultats quantitatifs :

— Le **Théorème 3.1** donne une borne sur la variation du sépateur du polynôme $P(X,y)$;

— Le **Théorème 3.2** est une analyse de la déviation de la courbe $V_{\mathbb{R}}(P)$, autour d'un point X-critique, par rapport à la tangente verticale en ce point lorsque y varie le long de la direction Y.

Nous introduisons, tout d'abord, dans la section 3.1 les énoncés et des illustrations, à travers des exemples, des théorèmes principaux. Ensuite, la section 3.2 donne quelques résultats préliminaires. Enfin, la section 3.3 est dédiée à la démonstration des théorèmes principaux.

3.1 Définitions et notations

Les définitions sur la *multiplicité*, le *séparateur* et le *résultant* écrites dans le chapitre 1 restent valables tout au long de ce chapitre. On considère aussi les polynômes $f^{[i]}$, $D_Y(Y)$ et $S_Y(Y)$ définis respectivement par les équations (1.1), (2.38) et (2.40).

Définition 3.1 *[Formule de Taylor]*
Soit $f \in \mathbb{C}[X]$, un polynôme de degré n. La formule de Taylor devient

$$f(\alpha + X) = \sum_{i=0}^{n} f^{[i]}(\alpha) X^i$$

Définition 3.2
Soient

$$\Delta_i = \frac{\partial_Y^i P}{i!},$$

$d > i \geq 1$ *et* $\Delta = \Delta_1 \cdot \partial_X P$. *Soit*

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

$$Z_\gamma = \{\alpha \in \mathbb{C} \mid (\alpha,\gamma) \in Z\}$$

Notation 3.1
Si $(\alpha,\gamma)\in Z$, *l'ordre de contact* $\nu(\alpha,\gamma)$ *de la droite verticale passant par* (α,γ) *avec la courbe* $V_{\mathbb{R}}(P)$ *est l'indice* $i\in\mathbb{N}$ *tel que*

$$\bigwedge_{j=1}^{i-1}\Delta_j(\alpha,\gamma)=0,\Delta_i(\alpha,\gamma)\neq 0.$$

L'objectif principal dans ce chapitre est de démontrer les théorèmes suivants.

Théorème 3.1
Soit γ *une racine commune aux polynômes* S_Y *et* D_Y *de multiplicités respectives* $\mu(\gamma)$ *et* $\nu(\gamma)$. *Il existe deux nombres réels* $A(\gamma)\leq 1$ *et* $B(\gamma)\leq 1$ [1], *tels que pour tout* y, $0<|y|<B(\gamma)$,

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

De plus,

$$\sum_{S_Y(\gamma)=0}\mu(\gamma)|\log A(\gamma)|\in O(d^3\tau+d^4), \tag{3.1}$$

$$\sum_{S_Y(\gamma)=0}\mu(\gamma)|\log B(\gamma)|\in O(d^3\tau+d^4). \tag{3.2}$$

Exemple 3.1
Soit le polynôme bivarié $P(X,Y)=Y^3-Y^2+X^2$, *alors*

$$D_Y(Y)=4(Y-1)Y^2,$$

La valeur $\gamma=1$ *est une racine de* D_Y *de multiplicité* $\nu(1)=1$. *D'après le Théorème 3.1, il existe un nombre réel* $A(1)\leq 1$ *et un nombre réel* $B(1)\leq 1$, *tels que pour tout* y *vérifiant* y, $0<|y|<B(1)$,

$$|\mathrm{sep}(P(X,1+y))|>A(1)\cdot|y|^{1/2}.$$

On peut choisir $A(1)=1,B(1)=3/10$ *comme illustré dans la Figure 3.1.*

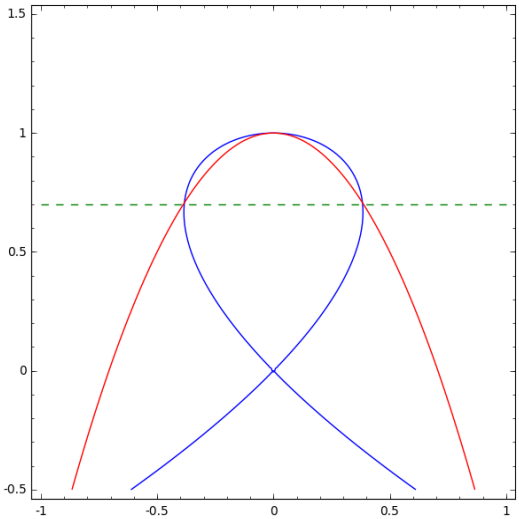


FIGURE 3.1 – **Illustration de l'Exemple 3.1**

1. Ces nombres sont déterminés dans (3.20) et (3.8))

Théorème 3.2
Soit $(\alpha,\gamma) \in Z$. *Il existe deux nombres réels* $A(\alpha,\gamma)$ *et* $B(\alpha,\gamma)$ [2], *tels que pour tout* y, $0 < y < B(\alpha,\gamma)$, *et tout* x, $P(\alpha+x,\gamma+y)=0$,

$$|x| > |y|^{\nu(\alpha,\gamma)} A(\alpha,\gamma).$$

De plus,

$$\sum_{\gamma | S_Y(\gamma)=0} \mu(\gamma) \sum_{\alpha \in Z_\gamma} |\log A(\alpha,\gamma)| \in \tilde{O}(d^3\tau + d^4), \tag{3.3}$$

$$\sum_{\gamma | S_Y(\gamma)=0} \mu(\gamma) \sum_{\alpha \in Z_\gamma} |\log B(\alpha,\gamma)| \in \tilde{O}(d^3\tau + d^4), \tag{3.4}$$

Exemple 3.2

Soit le polynôme bivarié

$$P(X,Y) = Y^3 - Y^2 + X^2.$$

On a alors

$$\Delta_1(X,Y) = 3Y^2 - 2Y \quad donc \quad \Delta_1(0,0) = 0$$

$$\Delta_2(X,Y) = Y - \frac{1}{3} \quad donc \quad \Delta_2(0,0) \neq 0$$

Ce qui signifie que l'ordre de contact de la courbe par rapport à l'axe Y à l'origine vaut $\nu(0,0) = 2$.

D'après le Théorème 3.2, il existe deux nombres réels $A(0,0)$ *et* $B(0,0)$ *tels que, tout* y *vérifiant* $0 < y < B(0,0)$, *et tout* x *tel que* $P(x,y) = 0$,

$$|x| > A(0,0) \cdot y^2.$$

On peut choisir $A(0,0) = 1, B(0,0) = 3/5$ *comme illustré dans la Figure 3.2.*

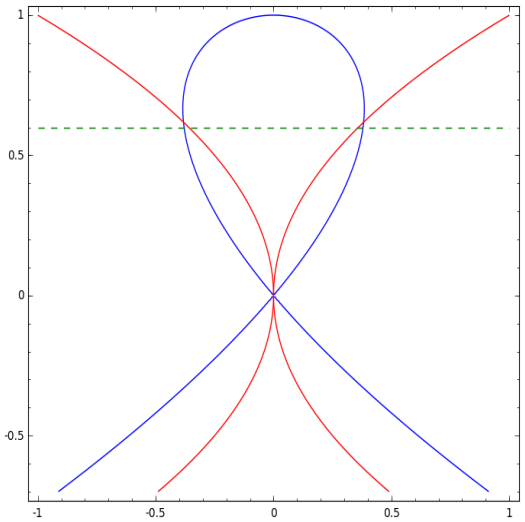


FIGURE 3.2 – **Illustration de l'Exemple 3.2**

La suite de chapitre est dédiée à la démonstration des Théorèmes 3.1 et 3.2. Tout d'abord, nous introduisons quelques résultats préliminaires sur les polynômes, nécessaires aux démonstrations des théorèmes cités ci-avant.

2. Ces nombres sont déterminés dans (3.23) et (3.15))

3.2 Quelques résultats préliminaires

Proposition 3.1 *Basu et al. [4, Proposition 10.22]*
Soit $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{C}[X]$, *with* $a_n \neq 0$.

$$\operatorname{sep}(f) \geq (n\sqrt{3})^{-1} n^{-\frac{n}{2}} |\operatorname{Disc}(f)|^{\frac{1}{2}} ||f||^{1-n}$$

La Proposition ci-dessous est un résultat essentiel dans la démontration du Théorème 3.1.

Proposition 3.2
Soit γ *une racine des polynômes* S_Y *et* D_Y *de multiplicités respectives* $\mu(\gamma)$ *et* $\nu(\gamma)$. *Il existe alors deux nombres réels* $\bar{A}(\gamma) \leq 1$ *et* $B(\gamma) \leq 1$ [3], *tels que pour tout* y, $0 < y < B(\gamma)$,

$$|D_{\nu(\gamma)}(\gamma + y)| > |y|^{\nu(\gamma)} |\bar{A}(\gamma)|.$$

De plus,

$$\sum_{S_Y(\gamma)=0} \mu(\gamma) |\log \bar{A}(\gamma)| \in O(d^3\tau + d^4), \tag{3.5}$$

$$\sum_{S_Y(\gamma)=0} \mu(\gamma) |\log B(\gamma)| \in O(d^3\tau + d^4). \tag{3.6}$$

Démonstration de la Proposition 3.2
Posons $\delta' = \deg(D_Y)$.

En appliquant la formule de Taylor au polynôme D_Y au point γ, on obtient :

$$D_Y(\gamma + Y) = \sum_{k=0}^{\delta'} D_k(\gamma) Y^k$$

Soit γ une racine de D_Y de multiplicité $\nu(\gamma)$.
Alors

$$\forall k < \nu(\gamma),\ D_k(\gamma) = 0 \ \text{ et } D_{\nu(\gamma)}(\gamma) \neq 0$$

Donc

$$D_Y(\gamma + Y) = D_{\nu(\gamma)}(\gamma) Y^{\nu(\gamma)} + \sum_{k=\nu(\gamma)+1}^{\delta'} D_k(\gamma) Y^k.$$

Posons

$$\bar{A}(\gamma) = \frac{D_{\nu(\gamma)}(\gamma)}{2} \tag{3.7}$$

et

$$B(\gamma) = \frac{\left|D_{\nu(\gamma)}(\gamma)\right|}{\left|D_{\nu(\gamma)}(\gamma)\right| + 2\sum_{\nu(\gamma)+1 \leq k \leq \delta'} \left|D_k(\gamma)\right|} \tag{3.8}$$

donc (voir Notation(1.1 et Proposition 1.1) $B(\gamma)$ est plus petit que la valeur absolue de la plus petite racine de

$$D(Y) = D_Y(\gamma + Y) - \bar{A}(\gamma) Y^{\nu(\gamma)};$$

d'où

$$\forall y, 0 < y < B(\gamma), \left|D_Y(\gamma + y)\right| > \left|\bar{A}(\gamma)\right| \cdot \left|y\right|^{\nu(\gamma)}.$$

A présent, nous allons analyser les tailles binaires de $\bar{A}(\gamma)$ et $B(\gamma)$.
a) L'estimation de la taille binaire de $\bar{A}(\gamma)$ découle directement de la Proposition1.8.
b) Concernant la taille binaire de $B(\gamma)$, il est clair que $0 < B(\gamma) \leq 1$. Nous commençons par une estimation du dénominateur

$$N(\gamma) = \left|D_{\nu(\gamma)}(\gamma)\right| + \sum_{k=\nu(\gamma)+1}^{\delta'} 2\left|D_k(\gamma)\right|.$$

3. voir les équations (3.7) et (3.8))

D'après la Proposition 1.8

$$\prod_{\gamma|S_Y(\gamma)=0} N(\gamma)^{\mu(\gamma)} \geq \prod_{\gamma|S_Y(\gamma)=0} |D_{v(\gamma)}(\gamma)|^{\mu(\gamma)} \geq \frac{1}{E} \tag{3.9}$$

avec $E \in 2^{O(d^3\tau)}$.

Soit l'ensemble

$$A' = \{\gamma | S_Y(\gamma) = 0, N(\gamma) \geq 1\}.$$

En appliquant la Proposition 1.8 a), on note que pour tout indice $i \in \mathbb{N}$, le polynôme D_i est de magnitude inférieure ou égale à $(d^2, O(d\tau + d^2)$.
En appliquant la Proposition 1.8 b) à la suite de polynômes $(D_i)_{1\leq i\leq \delta'}$; on obtient

$$\sum_{\gamma|S_Y(\gamma)=0} \mu(\gamma) \left|\log\left|D_{v(\gamma)}(\gamma)\right|\right| \in O(d^3\tau + d^4). \tag{3.10}$$

De plus, pour toute racine γ de S_Y, il existe un polynôme $D_{k(\gamma)}$, avec

$$|D_{k(\gamma)}(\gamma)| = \max\{|D_i(\gamma)|, 1 \leq i \leq \delta'\}.$$

Aussi, pour tout γ tel que $S_Y(\gamma) = 0$,

$$N(\gamma) \leq (2\delta' + 1)|D_{k(\gamma)}(\gamma)|$$

alors,

$$\prod_{\gamma|S_Y(\gamma)=0} N(\gamma)^{\mu(\gamma)} \leq \prod_{\gamma|S_Y(\gamma)=0} (2\delta' + 1)|D_{k(\gamma)}(\gamma)|.$$

En appliquant la Proposition 1.8 b) à la suite de polynômes $(D_{k(\gamma)})_{\{\gamma|S_Y(\gamma)=0\}}$; on obtient

$$\sum_{\gamma|S_Y(\gamma)=0} \mu(\gamma) \left(\log(2\delta' + 1) + \left|\log\left|D_{k(\gamma)}(\gamma)\right|\right|\right) \in \tilde{O}(d^3\tau + d^4) \tag{3.11}$$

avec

$$\prod_{\gamma|S_Y(\gamma)=0} (2\delta' + 1)^{\mu(\gamma)} \in 2^{\tilde{O}(d^2)}.$$

En utilisant l'équation (3.9)

$$\sum_{\gamma|S_Y(\gamma)=0} \mu(\gamma) \left|\log N(\gamma)\right| \in O(d^3\tau + d^4).$$

Finalement, on obtient

$$\begin{aligned} \sum_{\gamma|S_Y(\gamma)=0} \mu(\gamma) \left|\log B(\gamma)\right| &= \sum_{\gamma|S_Y(\gamma)=0} \mu(\gamma) \left|\log \bar{A}(\gamma) - \log N(\gamma)\right| \\ &\leq \sum_{\gamma|S_Y(\gamma)=0} \mu(\gamma)(\left|\log \bar{A}(\gamma)\right| + \left|\log N(\gamma)\right|) \\ &\in O(d^3\tau + d^4). \end{aligned}$$

□

Proposition 3.3
Si $f(X,Y) \in \mathbb{Z}[X,Y]$ *a des coefficients de taille binaire* τ *et de degrés* $d_1 = \deg_X(f), d_2 = \deg_Y(f)$ *et* $(\alpha, \gamma) \in \mathbb{C}^2$, *alors*

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

La Proposition ci-dessous est aussi un résultat essentiel dans la démonstration du Théorème 3.2.

Proposition 3.4
Pour tout $(\alpha,\gamma)\in Z$, *il existe deux nombres réels* $\bar{A}(\alpha,\gamma)$ *et* $B(\alpha,\gamma)$ [4], *tels que pour tout* y, $0<y<B(\alpha,\gamma)$

$$|P(\alpha,\gamma+y)|>|y|^{\nu(\alpha,\gamma)}|\bar{A}(\alpha,\gamma)|.$$

De plus,

$$\sum_{\gamma|S_Y(\gamma)=0}\mu(\gamma)\sum_{\alpha\in Z_\gamma}|\log\bar{A}(\alpha,\gamma)|\in\tilde{O}(d^3\tau+d^4), \tag{3.12}$$

$$\sum_{\gamma|S_Y(\gamma)=0}\mu(\gamma)\sum_{\alpha\in Z_\gamma}|\log B(\alpha,\gamma)|\in\tilde{O}(d^3\tau+d^4), \tag{3.13}$$

Démonstration
En appliquant la formule de Taylor, on obtient

$$P(\alpha,\gamma+Y)=\Delta_{\nu(\alpha,\gamma)}(\alpha,\gamma)Y^{\nu(\alpha,\gamma)}+\sum_{k=\nu(\alpha,\gamma)+1}^{d}\Delta_k(\alpha,\gamma)Y^k.$$

Posons

$$\bar{A}(\alpha,\gamma)=\frac{|\Delta_{\nu(\alpha,\gamma)}(\alpha,\gamma)|}{2} \tag{3.14}$$

et

$$B(\alpha,\gamma)=\frac{|\Delta_{\nu(\alpha,\gamma)}(\alpha,\gamma)|}{|\Delta_{\nu(\alpha,\gamma)}(\alpha,\gamma)|+2\sum_{k=\nu(\alpha,\gamma)+1}^{d}|\Delta_k(\alpha,\gamma)|}. \tag{3.15}$$

Donc (voir Notation 1.1 et Proposition 1.1) $B(\alpha,\gamma)\le 1$ est plus petit que la racine de plus petite valeur absolue du polynôme

$$P(\alpha,Y)-\bar{A}(\alpha,\gamma)Y^{\nu(\alpha,\gamma)};$$

d'où

$$\forall\, y, 0<y<B(\alpha,\gamma), \left|P(\alpha,\gamma+y)\right|>\bar{A}(\alpha,\gamma)\cdot\left|y\right|^{\nu(\alpha,\gamma)}.$$

Nous allons maintenant donner des estimations de $\bar{A}(\alpha,\gamma)$ et $B(\alpha,\gamma)$.
a) D'après la définition de $\bar{A}(\alpha,\gamma)$ et la Proposition 2.9, on a

$$\sum_{\gamma|S_Y(\gamma)=0}\mu(\gamma)\sum_{\alpha\in Z_\gamma}|\log\bar{A}(\alpha,\gamma)|\in\tilde{O}(d^3\tau+d^4). \tag{3.16}$$

b) Nous pouvons maintenant estimer

$$B(\alpha,\gamma)=\frac{|\Delta_{\nu(\alpha,\gamma)}(\alpha,\gamma)|}{|\Delta_{\nu(\alpha,\gamma)}(\alpha,\gamma)|+2\sum_{k=\nu(\alpha,\gamma)+1}^{d}|\Delta_k(\alpha,\gamma)|},$$

plus particulièrement son dénominateur

$$N(\alpha,\gamma)=|\Delta_{\nu(\alpha,\gamma)}(\alpha,\gamma)|+2\sum_{k=\nu(\alpha,\gamma)+1}^{d}|\Delta_k(\alpha,\gamma)|.$$

D'après la Proposition 2.9,

$$\prod_{(\alpha,\gamma)\in Z}N(\alpha,\gamma)^{\mu(\gamma)}\ge\prod_{(\alpha,\gamma)\in Z}|\Delta_{\nu(\alpha,\gamma)}(\alpha,\gamma)|^{\mu(\gamma)}\ge\frac{1}{E''} \tag{3.17}$$

avec $E''\in 2^{O(d^3\tau+d^4)}$.

4. voir les équations (3.14) et (3.15))

Notons que les polynômes Δ_k, avec $0 \le k \le d$, sont de degré inférieur ou égal à d et des coefficients de tailles binaires de l'ordre de $O(d+\tau)$.
En appliquant la Proposition 2.9 b) à la suite de polynômes $(\Delta_{\nu(\alpha,\gamma)})_{\{(\alpha,\gamma)\in Z\}}$; on obtient

$$\sum_{\gamma|S_Y(\gamma)=0} \mu(\gamma) \sum_{\alpha\in Z_\gamma} \left|\log|\Delta_{\nu(\alpha,\gamma)}(\alpha,\gamma)|\right| \in \tilde{O}(d^3\tau + d^4). \tag{3.18}$$

A présent, nous donnons une majoration de $N(\alpha,\gamma)$. Pour tout $(\alpha,\gamma)\in Z$, il existe un polynôme $\Delta_{k(\alpha,\gamma)}$ tel que

$$\left|\Delta_{k(\alpha,\gamma)}(\alpha,\gamma)\right| = \max\{|\Delta_k(\alpha,\gamma)|, 0 \le k \le d\}.$$

Puisque

$$N(\alpha,\gamma) \le (2d+1)\left|\Delta_{k(\alpha,\gamma)}(\alpha,\gamma)\right|,$$

alors

$$\prod_{(\alpha,\gamma)\in Z} N(\alpha,\gamma)^{\mu(\gamma)} \le \prod_{(\alpha,\gamma)\in Z} \left((2d+1)\left|\Delta_{k(\alpha,\gamma)}(\alpha,\gamma)\right|\right)^{\mu(\gamma)}.$$

En appliquant la Proposition 2.9 b) à la suite de polynômes $(\Delta_{k(\alpha,\gamma)})_{\{(\alpha,\gamma)\in Z\}}$; on obtient

$$\sum_{\gamma|S_Y(\gamma)=0} \mu(\gamma \sum_{\alpha\in Z_\gamma}) \log(2d+1) + \left|\log\left|\Delta_{k(\alpha,\gamma)}(\alpha,\gamma)\right|\right| \in \tilde{O}(d^3\tau + d^4). \tag{3.19}$$

avec

$$\prod_{(\alpha,\gamma)\in Z} (2d+1)^{\mu(\gamma)} \in 2^{\tilde{O}(d^3)}.$$

Dès lors, en utilisant d'une part les équations (3.18) et 3.19, on montre que

$$\sum_{S_Y(\gamma)=0} \mu(\gamma) \sum_{\alpha\in Z_\gamma} \left|\log N(\alpha,\gamma)\right| \in \tilde{O}(d^3\tau + d^4);$$

et d'autre part l'équation (3.17) et le Lemme1.7, on montre que

$$\sum_{S_Y(\gamma)=0} \mu(\gamma) \sum_{\alpha\in Z_\gamma} \left|\log N(\alpha,\gamma)\right| \in \tilde{O}(d^3\tau + d^4).$$

Ainsi, en utilisant l'équation(3.16), on a

$$\begin{aligned}
\sum_{\gamma|S_Y(\gamma)=0} \mu(\gamma) \sum_{\alpha\in Z_\gamma} \left|\log B(\alpha,\gamma)\right| &= \sum_{\gamma|S_Y(\gamma)=0} \mu(\gamma) \sum_{\alpha\in Z_\gamma} \left|\log \bar{A}(\alpha,\gamma) - \log N(\alpha,\gamma)\right| \\
&\le \sum_{\gamma|S_Y(\gamma)=0} \mu(\gamma) \sum_{\alpha\in Z_\gamma} \left(\left|\log \bar{A}(\alpha,\gamma)\right| + \left|\log N(\alpha,\gamma)\right|\right) \\
&\in \tilde{O}(d^3\tau + d^4).
\end{aligned}$$

□

3.3 Démonstration des théorèmes

Cette section est dédiée à la démonstration des Théorèmes 3.1 et 3.2.

Étant donné un polynôme $R(X) \in \mathbb{C}[X]$ et un nombre $\alpha \in \mathbb{C}$, on désigne par $\text{mult}(\alpha, R(X))$ la multiplicité de α en tant que racine du polynôme $R(X)$, i.e. l'indice $i \in \mathbb{N}$ tel que $(X-\alpha)^i$ divise $R(X)$ et $(X-\alpha)^{i+1}$ ne divise pas $R(X)$. Si α n'est pas une racine $R(X)$, $\text{mult}(\alpha, P(X)) = 0$. If $R(\alpha) = 0$,

$$\mu = \text{mult}(\alpha, R(X)) \iff \bigwedge_{i=0}^{\mu-1} R^{(i)}(\alpha) = 0 \wedge R^{(\mu)}(\alpha) \neq 0$$

Démonstration du Théorème 3.1
Regardons $P(X,\gamma+Y)$ comme un polynôme en variable X. En appliquant la formule de Taylor à l'origine 0, on obtient

$$P(X,\gamma+Y)=\sum_{j=0}^{d}\hat{H}_j(\gamma+Y)X^j,$$

où

$$\hat{H}_j(\gamma+Y)=\sum_{k=0}^{d}\hat{H}_{j,k}(\gamma)Y^k.$$

Pour tout $0<y\leq B(\gamma)$, d'après la Proposition 3.1, on a

$$\text{sep}(P(X,\gamma+y))\geq f(d)^{-1}|D_Y(\gamma+y)|^{1/2}||P(X,\gamma+y)||^{1-d},$$

avec $f(d)=(d/\sqrt{3})d^{d/2}$.

En appliquant la Proposition 3.2, on montre que

$$\text{sep}(P(X,\gamma+y))\geq\frac{(\bar{A}(\gamma)\left|y\right|^{v(\gamma)})^{1/2}}{||P(X,\gamma+y)||^{d-1}f(d)}.$$

Déterminons une estimation de $||P(X,\gamma+y)||$. On a

$$||P(X,\gamma+y)||=\left(\sum_{j=0}^{d}\left|\hat{H}_j(\gamma+y)\hat{H}_j(\bar{\gamma}+y)\right|\right)^{1/2}$$

Sachant que $0<y\leq B(\gamma)$ et $B(\gamma)\leq 1$ par construction, donc

$$\sum_{j=0}^{d}\left|\hat{H}_j(\gamma+y)\hat{H}_j(\bar{\gamma}+y)\right|\leq\sum_{j=0}^{d}\sum_{k=0}^{d}\sum_{\ell=0}^{d}\left|\hat{H}_{j,k}(\gamma)\hat{H}_{j,\ell}(\bar{\gamma})\right|.$$

Finalement, on pose

$$H(\gamma)=\sum_{j=0}^{d}\sum_{k=0}^{d}\sum_{\ell=0}^{d}\left|\hat{H}_{j,k}(\gamma)\hat{H}_{j,\ell}(\bar{\gamma})\right|$$

donc $||P(X,\gamma+y)||\leq H(\gamma)^{1/2}$. On définit

$$A(\gamma)=\frac{\bar{A}(\gamma)^{1/2}}{H(\gamma)^{(1-d)/2}f(d)}.\tag{3.20}$$

Le polynôme $P(X,\gamma)$ n'étant pas identiquement nul, alors il existe un indice $k(\gamma)$ tel que pour tout $k<k(\gamma)$, $\hat{H}_{0,k(\gamma)}(\gamma)\neq 0$ et $\hat{H}_{0,k}(\gamma)=0$. Notons que $H(\gamma)\geq|\hat{H}_{0,k(\gamma)}(\gamma)|$.

En appliquant la Proposition 1.8, on établit que

$$\prod_{\gamma|S_Y(\gamma)=0}|H_{0,k(\gamma)}(\gamma)|^{\mu(\gamma)}\geq\frac{1}{E'}$$

où E'est un entier naturel de taille binaire $O(\tau d^2+d^3)$.

Notons aussi que, pour tout couple d'indice (j,k), tel que $0\leq j,k\leq d$, le degré du polynôme $H_{j,k}$ est borné par d et ses coefficients de taille binaire de l'ordre $O(\tau+d)$.
En appliquent la Proposition 1.8 b) à la suite de polynômes $(H_{k(\gamma),0})_{\{\gamma|S_Y(\gamma)=0\}}$; on montre que

$$\sum_{\gamma|S_Y(\gamma)=0}\mu(\gamma)\left|\log|H_{k(\gamma),0}(\gamma)|\right|\in O(d^2\tau+d^3)\tag{3.21}$$

Par ailleurs, pour toute racine γ de S_Y, il existe deux polynômes $\hat{H}_{j(\gamma),k(\gamma)}$ et $\hat{H}_{j(\gamma),\ell(\gamma)}$, tels que

$$\left|\hat{H}_{j(\gamma),k(\gamma)}(\gamma)\hat{H}_{j(\gamma),\ell(\gamma)}(\bar{\gamma})\right|=\max\{|\hat{H}_{j,k}(\gamma)\hat{H}_{j,\ell}(\gamma)|,0\leq j,k,\ell\leq d\}.$$

On sait que

$$\mathrm{H}(\gamma) \leq (d+1)^3 \left|\hat{\mathrm{H}}_{j(\gamma),k(\gamma)}(\gamma)\hat{\mathrm{H}}_{j(\gamma),\ell(\gamma)}(\bar{\gamma})\right|.$$

Donc,

$$\prod_{\gamma|\mathrm{S_Y}(\gamma)=0} \mathrm{H}(\gamma)^{\mu(\gamma)} \leq \prod_{\gamma|\mathrm{S_Y}(\gamma)=0} \left((d+1)^3 \left|\hat{\mathrm{H}}_{j(\gamma),k(\gamma)}(\gamma)\hat{\mathrm{H}}_{j(\gamma),\ell(\gamma)}(\bar{\gamma})\right|\right)^{\mu(\gamma)}.$$

Sachant que,

$$\prod_{\gamma|\mathrm{S_Y}(\gamma)=0} (d+1)^{3\mu(\gamma)} \in 2^{\tilde{\mathrm{O}}(d^2)}$$

et en appliquant la Proposition 1.8 b) aux suites de polynômes $(\hat{\mathrm{H}}_{j(\gamma),k(\gamma)})_{\{\gamma|\mathrm{S_Y}(\gamma)=0\}}$ et $(\hat{\mathrm{H}}_{j(\gamma),\ell(\gamma)})_{\{\gamma|\mathrm{S_Y}(\gamma)=0\}}$; on montre que

$$\sum_{\gamma|\mathrm{S_Y}(\gamma)=0} \mu(\gamma)\left|\log|\hat{\mathrm{H}}_{j(\gamma),k(\gamma)}(\gamma)|\right| \in \mathrm{O}(d^2\tau + d^3),$$

$$\sum_{\gamma|\mathrm{S_Y}(\gamma)=0} \mu(\gamma)\left|\log|\hat{\mathrm{H}}_{j(\gamma),\ell(\gamma)}(\bar{\gamma})|\right| \in \mathrm{O}(d^2\tau + d^3).$$

On en déduit que

$$\sum_{\gamma|\mathrm{S_Y}(\gamma)=0} \mu(\gamma)\left(\log(d+1)^3 + \log\left|\hat{\mathrm{H}}_{j(\gamma),k(\gamma)}(\gamma)\hat{\mathrm{H}}_{j(\gamma),\ell(\gamma)}(\bar{\gamma})\right|\right) \in \tilde{\mathrm{O}}(d^2\tau + d^3). \tag{3.22}$$

Ainsi, en utilisant les équations (3.21) et (3.22), on montre que

$$\sum_{\gamma|\mathrm{S_Y}(\gamma)=0} \mu(\gamma)\left|\log \mathrm{H}(\gamma)\right| \in \tilde{\mathrm{O}}(d^2\tau + d^3).$$

$$\begin{aligned}
\sum_{\gamma|\mathrm{S_Y}(\gamma)=0} \mu(\gamma)\left|\log \mathrm{A}(\gamma)\right| &= \sum_{\gamma|\mathrm{S_Y}(\gamma)=0} \mu(\gamma)\left|\log\bar{\mathrm{A}}(\gamma) - \left(\frac{(d-1)}{2}\log \mathrm{H}(\gamma) + \log f(d)\right)\right| \\
&\leq \sum_{\gamma|\mathrm{S_Y}(\gamma)=0} \mu(\gamma)\left(\left|\log\bar{\mathrm{A}}(\gamma)\right| + \frac{(d-1)}{2}\left|\log \mathrm{H}(\gamma)\right| + \left|\log f(d)\right|\right) \\
&\in \tilde{\mathrm{O}}(d^3\tau + d^4),
\end{aligned}$$

sachant que $\log f(d) \in \tilde{\mathrm{O}}(d)$.

On choisit $\mathrm{B}(\gamma)$ comme décrit dans le Théorème 3.1 (3.8).

□

Démonstration du Théorème 3.2

Regardons $\mathrm{P}(\alpha+\mathrm{X}, \gamma+\mathrm{Y})$ comme un polynôme en la variable X. En appliquant la formule de Taylor au point α, on obtient

$$\mathrm{P}(\alpha+\mathrm{X}, \gamma+\mathrm{Y}) = \sum_{k=0}^{d} \bar{\Delta}_k(\alpha, \gamma+\mathrm{Y})\mathrm{X}^k;$$

où

$$\bar{\Delta}_k(\alpha, \gamma+\mathrm{Y}) = \sum_{\ell=0}^{d} \bar{\Delta}_{k,\ell}(\alpha,\gamma)\mathrm{Y}^\ell.$$

Notons que $\bar{\Delta}_0(\alpha, \gamma+\mathrm{Y}) = \mathrm{P}(\alpha, \gamma+\mathrm{Y})$, $\bar{\Delta}_{0,i}(\alpha,\gamma) = \Delta_i(\alpha,\gamma)$ (voir la Définition 3.2).

Pour tout $0 < y \leq \mathrm{B}(\alpha,\gamma)$, on désignera par $x(\alpha, \gamma+y)$ la racine de $\mathrm{P}(\alpha+\mathrm{X}, \gamma+y)$ qui a la plus petite valeur absolue. D'après la Proposition 1.1, on a

$$x(\alpha,\gamma+y) \geq \frac{\left|\mathrm{P}(\alpha,\gamma+y)\right|}{\sum_{k=0}^{d}\left|\bar{\Delta}_k(\alpha,\gamma+y)\right|}.$$

En appliquant la Proposition 3.4, on montre que

$$x(\alpha,\gamma+y)\geq\frac{\bar{A}(\alpha,\gamma)\left|y\right|^{i}}{\sum_{k=0}^{d}\left|\bar{\Delta}_{k}(\alpha,\gamma+y)\right|}.$$

Sachant que par définition $0<y\leq B(\alpha,\gamma)$ et $B(\alpha,\gamma)\leq 1$, on montre que

$$\sum_{k=0}^{d}\left|\bar{\Delta}_{k}(\alpha,\gamma+y)\right|\leq\sum_{k=0}^{d}\sum_{\ell=0}^{d}\left|\bar{\Delta}_{k,\ell}(\alpha,\gamma)\right|.$$

Finalement, on pose

$$\Delta(\alpha,\gamma)=\sum_{k=0}^{d}\sum_{\ell=0}^{d}\left|\bar{\Delta}_{k,\ell}(\alpha,\gamma)\right|$$

et

$$A(\alpha,\gamma)=\Delta(\alpha,\gamma)^{-1}\times\bar{A}(\alpha,\gamma). \tag{3.23}$$

Notons que

$$\Delta_{\nu(\alpha,\gamma)}(\alpha,\gamma)\leq\Delta(\alpha,\gamma),$$

donc

$$\prod_{(\alpha,\gamma)\in Z}\Delta(\alpha,\gamma)^{\mu(\gamma)}\geq\frac{1}{E''}$$

avec $E''\in 2^{\tilde{O}(d^3\tau+d^4)}$ (voir l'équation (2.26)).

Pour tout indice k, tel que $0\leq k\leq d$, le degré du polynôme Δ_k est borné par d et la taille binaire de ses coefficients est de l'ordre de $O(\tau+d)$. En appliquant la Proposition 2.9 b) à la suite de polynômes $(\Delta_{\nu(\alpha,\gamma)})_{\{(\alpha,\gamma)\in Z\}}$; on obtient

$$\sum_{\gamma|S_Y(\gamma)=0}\mu(\gamma)\sum_{\alpha\in Z}\left|\log\left|\Delta_{\nu(\alpha,\gamma)}(\alpha,\gamma)\right|\right|\in\tilde{O}(d^3\tau+d^4). \tag{3.24}$$

Par ailleurs, pour tout $(\alpha,\gamma)\in Z$, il existe un polynôme $\bar{\Delta}_{(\alpha,\gamma)}$, tel que

$$\left|\bar{\Delta}_{(\alpha,\gamma)}\right|=\max\{|\bar{\Delta}_{k,\ell}(\alpha,\gamma)|,0\leq k,\ell\leq d\}.$$

Notons que

$$N(\alpha,\gamma)\leq(d+1)^2\left|\bar{\Delta}_{(\alpha,\gamma)}\right|.$$

En appliquant la Proposition 2.9 b) à la suite de polynômes $(\Delta_{(\alpha,\gamma)})_{\{(\alpha,\gamma)\in Z\}}$; on montre que

$$\sum_{\gamma|S_Y(\gamma)=0}\mu(\gamma)\sum_{\alpha\in Z_\gamma}\log(d+1)^2+\left|\log\left|\bar{\Delta}_{(\alpha,\gamma)}\right|\right|\in\tilde{O}(d^3\tau+d^4). \tag{3.25}$$

Donc, en utilisant les équations (3.24) et (3.25), on montre que

$$\sum_{\gamma|S_Y(\gamma)=0}\mu(\gamma)\sum_{\alpha\in Z_\gamma}\left|\log\bar{\Delta}(\alpha,\gamma)\right|\in\tilde{O}(d^3\tau+d^4).$$

$$\begin{aligned}\sum_{\gamma|S_Y(\gamma)=0}\mu(\gamma)\sum_{\alpha\in Z_\gamma}\left|\log A(\alpha,\gamma)\right| &= \sum_{\gamma|S_Y(\gamma)=0}\mu(\gamma)\sum_{\alpha\in Z_\gamma}\left|\log\bar{A}(\alpha,\gamma)-\log\bar{\Delta}(\alpha,\gamma)\right|\\ &\leq \sum_{\gamma|S_Y(\gamma)=0}\mu(\gamma)\sum_{\alpha\in Z_\gamma}\left(\left|\log\bar{A}(\alpha,\gamma)\right|+\left|\log\bar{\Delta}(\alpha,\gamma)\right|\right)\\ &\in \tilde{O}(d^3\tau+d^4).\end{aligned}$$

On choisit $B(\alpha,\gamma)$ comme décrit dans le Théorème 3.2 (3.15).

□

Deuxième partie

Topologie de surfaces analytiques réelles dans $\mathbb{R}^3$

Chapitre 4

Théorie des singularités et Méthodes Numériques

Introduction

Les tous premiers résultats sur la théorie des singularités de fonctions différentiables peuvent être essentiellement attribués à Whitney, Thom et Mather. Ils se sont intéressés, tout particulièrement, au problème de la classification des singularités des germes de fonctions définies de $\mathbb{K}^n$ à valeur dans $\mathbb{K}^p$, où $\mathbb{K}$ est un corps. En effet Whitney [52] donna une classification des applications stables définies du plan à valeur dans lui même. Plus précisément, il démontre que, tout germe stable est équivalent à un pli (*fold*) ou un cuspide (*cusp*). Quant aux travaux de Thom, ils portaient sur la théorie des catastrophes, alors que ceux de Mather [31, 30, 32] ont aboutis à la classification faite par Arnol'd [1] sur les singularités simples de fonctions. Depuis lors, ce dernier thème de recherche a été le plus investi par les chercheurs dans le domaine de la théorie des singularités. C'est dans ce contexte que, les classifications plus complètes furent établies par Rieger [45], Rieger and Ruas [46], Mond [36], Goryunov [18], Marar and Tari [28], Atique [2], pour certaines valeurs de (n, p) assez grandes.

Toutefois, la bibliographie sur les multigermes reste beaucoup moins exhaustive. La toute première référence fut l'œuvre de Mather [32]. Elle portait sur la classification des multigermes stables ; suivi de Goryunov [19] qui établit une liste de multigermes de $\mathbb{R}^2$ à valeur dans $\mathbb{R}^3$, sans les formes normales, incluant les singularités de codimension 1. Dans leurs travaux respectifs, Hobbs and Kirk [20] et Mond [36] donnèrent une classification des multigermes simples définis dans les mêmes espaces. Les formes normales pour les multigermes définies sur plan à valeur dans lui même sont étudiées par Ohmoto and Aicardi [41]. Dans la suite, Kolgushkin et Sadykov étudièrent les multigermes simples de courbes dans $\mathbb{R}^3$.

En général, la classification des multigermes à l'aide de techniques classiques sur la Théorie des Singularité s'avère très difficile. Cependant, le besoin croissant de disposer de nouvelles classifications pour des valeurs de (n, p) assez grandes, y compris pour les multigermes, se justifie par leurs applications dans des domaines connexes à la théorie de la singularité, tels que les invariants topologiques ou la généricité de certains objets géométriques : c'est ce dernier point qui fait l'objet de cette deuxième partie de la thèse. C'est dans ce sens que, de nouvelles techniques ont été développées. En effet, les opérations visant à obtenir des germes dans certaines dimensions à partir de germes avec moins de branches dans des dimensions inférieures se sont révélées être un outil très important.

Ce chapitre a été introduit pour contextualiser le thème abordé dans cette deuxième partie : topologie d'objets géométriques obtenus par projection canonique de courbes ou surfaces analytiques. En effet, la section 4.3 constitue un rappel des résultats établis dans le cas de la projection d'une courbe de l'espace $\mathbb{R}^3$ vers le plan. C'est ainsi que la section 4.1 s'appuie sur Wall [51], Mond and Nunõ-Ballesteros [35] pour aborder un rappel sur la Théorie des singularités. La section 4.2 revient sur quelques méthodes numériques utiles à la résolution des systèmes réguliers d'équa-

tions.

4.1 Classification des singularités

Le probléme soulevé dans cette deuxième partie est celui de la classification des fonctions de classe C^∞. Plus précisément, il s'agit des objets du type $(\mathrm{E}, \mathrm{F}, a, b, f)$ où E et F sont des espaces vectoriels de dimensions finies, a et b sont des points appartenant respectivement à E et F, et f est une fonction de classe C^∞ définie sur un voisinage du point a à valeurs dans F, telle que $f(a) = b$.

Définition 4.1 *Demazure [8, section 4.3]*
Deux objets de type $(\mathrm{E}_1, \mathrm{F}_1, a_1, b_1, f_1)$ *et* $(\mathrm{E}_2, \mathrm{F}_2, a_2, b_2, f_2)$ *sont dits équivalent s'il existe deux difféomorphismes locaux* u *et* v *tels que* $f_2 = v \circ f_1 \circ u$ *(ce qui signifie que le diagramme 4.1 commute).*

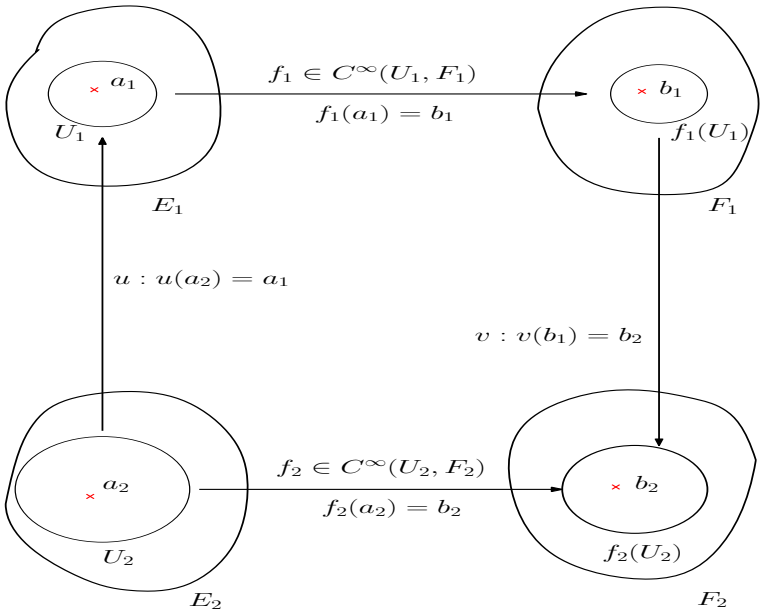


FIGURE 4.1 – **Diagramme commutatif de fonctions équivalentes**

Sous cette relation d'équivalence, le problème auquel nous nous intéressons ici est celui de la détermination, si possible, d'une liste de classes d'équivalences. Il s'agit tout particulièrement de germes de fonctions définis sur des $\mathbb{K}$-espaces vectoriels; où $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. En effet, l'ensemble quotient hérite d'une structure naturelle d'anneau appelé anneau des germes de fonctions au voisinage du point a. Il s'agit en réalité d'un anneau local dû au fait que l'évaluation en a induit un morphisme surjectif m définit sur l'anneau quotient à valeur dans $\mathbb{K}$. De plus, si une fonction f ne s'annule pas au point a, elle reste non nulle sur un voisinage de a. Ce qui signifie que le noyau de m est l'unique idéal maximal de l'anneau local. La notion de germe en mathématiques capture les propriétés locales d'un phénomène, par exemple la coïncidence infinitésimale entre fonctions. C'est une notion à l'origine analytique qui possède une structure algébrique naturelle, et qui apparaît naturellement en géométrie algébrique et en théorie des groupes de Lie.

Soit $\mathcal{O}_n^p$ l'espace vectoriel des monogermes à n variables et p composantes; i.e un élément de $\mathcal{O}_n^p$ est un germe de fonction $f : (\mathbb{K}^n, x_0) \to (\mathbb{K}^p, y_0)$, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Pour $p = 1$, $\mathcal{O}_n^1 = \mathcal{O}_n$ est l'anneau local des germes de fonctions en n variables et $\mathcal{M}_n$ désigne son idéal maximal.

Définition 4.2 *Sinha and Atique [49]*
Un multigerme est un germe d'une fonction analytique (cas complexe) ou lisse (cas réel) $f = \{f_1, f_2, ..., f_r\} : (\mathbb{K}^n, \mathrm{S}) \to (\mathbb{K}^p, 0)$ *avec* $\mathrm{S} = \{x_1, \ldots, x_r\} \subset \mathbb{K}^n$, $f_i : (\mathbb{K}^n, x_i) \to (\mathbb{K}^p, 0)$. *Les fonctions* f_i, $i = 1, \ldots, r$ *sont appelées les branches du multigerme* f.

On peut définir plusieurs types d'équivalences sur les germes de fonctions. Nous pouvons citer entre autre **la $\mathscr{R}$-équivalence, la $\mathscr{L}$-équivalence, la $\mathscr{A}$-équivalence, la $\mathscr{K}$-équivalence** etc. Ici, nous nous intéresserons particulièrement à la $\mathscr{A}$-équivalence, utile pour introduire la définiton de la stabilité d'un germe.. Notons que, dans la sous-section 4.11.5, Demazure [8] donne une définition claire de la stabilité d'une fonction C^∞. Dans le cas des germes, nous utilisons des définitions assez techniques, tirées essentiellement de Sinha and Atique [49].

Définition 4.3 *Sinha and Atique [49]*
Deux multigermes $f, g : (\mathbb{K}^n, S) \to (\mathbb{K}^p, 0)$ sont $\mathscr{A}$-équivalents ($f \sim_{\mathscr{A}} g$) s'il existe deux difféomorphismes $\phi : (\mathbb{K}^n, S) \to (\mathbb{K}^n, S)$ et $\psi : (\mathbb{K}^p, 0) \to (\mathbb{K}^p, 0)$ tels que $g = \psi \circ f \circ \phi^{-1}$.

Définition 4.4 *Sinha and Atique [49]*
Soit $f : (\mathbb{K}^n, S) \to (\mathbb{K}^p, 0)$ un multigerme. Un dépliage *de paramètre s est un germe $F : (\mathbb{K}^n \times \mathbb{K}^s, S \times \{0\}) \to (\mathbb{K}^p \times \mathbb{K}^s, 0)$ tel que $F(x, \lambda) = (f_{\lambda(x)}, \lambda)$ avec $f_0(x) = f(x)$ pour tout $x \in (\mathbb{K}^n, S)$.*

Définition 4.5 *Sinha and Atique [49]*
Soient F, G deux dépliages du multigerme f de paramètre s. F et G sont isomorphes s'il existe deux difféomorphismes $\Phi : (\mathbb{K}^n \times \mathbb{K}^s, S \times \{0\}) \to (\mathbb{K}^n \times \mathbb{K}^s, S \times \{0\})$ et $\Psi : (\mathbb{K}^p \times \mathbb{K}^s, 0) \to (\mathbb{K}^p \times \mathbb{K}^s, 0)$; où Φ, Ψ sont des dépliages de l'identité dans respectivement $(\mathbb{K}^n, S)$ et $(\mathbb{K}^p, 0)$ tels que $G = \Psi \circ F \circ \Phi^{-1}$.

Un dépliage F est trivial s'il est isomorphe au dépliage produit $f \times id$. On a $\Phi(x, \lambda) = (\phi_\lambda(x), x)$ avec $\phi_0(x) = id(x)$ et $\Psi(y, \lambda) = (\psi_\lambda(y), y)$ avec $\psi_0(y) = id(y)$. Si $G(x, \lambda) = (g_\lambda(x), x)$ alors d'après la définition il s'en suit que $g_\lambda = \psi_\lambda \circ f_\lambda \circ \phi_\lambda^{-1}$.

Définition 4.6 *Sinha and Atique [49]*
Un germe $f : (\mathbb{K}^n, S) \to (\mathbb{K}^p, 0)$ est dit stable si tout dépliage F de f est trivial.

Par conséquent, f_λ est $\mathscr{A}$-équivalent à f (en temps que fonction, ϕ_λ et ψ_λ ne préservent pas respectivement S et l'origine).

Soit θ_n le $\mathscr{O}_n$-module des germes de champs de vecteurs aux points de S sur $\mathbb{K}^n$ et θ_p le $\mathscr{O}_p$-module des germes de champs de vecteurs à l'origine 0 sur $\mathbb{K}^p$. Soit $\theta(f)$ le $\mathscr{O}$-module des germes $\xi : (\mathbb{K}^n, S) \to T\mathbb{K}^p$ tels que $\pi_p \circ \xi = f$; où $T\mathbb{K}^p$ est le fibré tangent de la variété $\mathbb{K}^p$ et $\pi_p : T\mathbb{K}^p \to \mathbb{K}^p$ désigne le faisceau tangent sur $\mathbb{K}^p$. Par conséquent, $\theta(f) \cong \mathscr{O}_n^p \bigoplus \mathscr{O}_n^p \ldots \mathscr{O}_n^p$ (r-fois). Étant donné un germe $f : (\mathbb{K}^n, S) \to \mathscr{K}^p, 0$, on définit l'application $f^* : \mathscr{O}_p \to \mathscr{O}_n$ telle que $f^*(h) = h \circ f$; ce qui confère à $\theta(f)$ une structure de $\mathscr{O}_p$-module via f^*.

Soient les applications $tf : \theta_n \to \theta(f)$ qui à $\xi \mapsto df \circ \xi$ et $wf : \theta_p \to \theta(f)$ qui à $\eta \mapsto \eta \circ f$. Le $\mathscr{A}_e$-espace tangent d'un germe f est défini par $T\mathscr{A}_e f = tf(\theta_n) + wf(\theta_p)$.

Définition 4.7 *Sinha and Atique [49]*
La $\mathscr{A}_e$-codimension d'un germe f est la dimension du $\mathbb{K}$-espace vectoriel

$$N\mathscr{A}_e(f) = \frac{\theta(f)}{T\mathscr{A}_e(f)}.$$

De la même manière, la $\mathscr{A}$-codimension de$f$ est définie comme étant la dimension du $\mathbb{K}$-espace vectoriel

$$N\mathscr{A}(f) = \frac{\mathscr{M}_n\theta(f)}{T\mathscr{A}f}.$$

Théorème 4.1 (Critère infinitésimal de Mather [31])
Un germe $f : (\mathbb{K}^n, S) \to (\mathbb{K}^p, 0)$ est stable si et seulement si $\mathscr{A}_e - cod(f) = 0$.

Par conséquent, si f est stable alors tout champ de vecteurs de $\theta(f)$ appartient à l'espace tangent de f.

Exemple 4.1 *Soit le bigerme* $f(x) = \{f_1, f_2\} = \{(0,x),(x^2,x^3)\}$. $\theta(f) \cong \mathscr{O}^2_{1,S} \cong \mathscr{O}^2_1 \bigoplus \mathscr{O}^2_1$. *Soient* $\xi^1, \xi^2 \in \mathscr{O}_1$ *et* $\eta = (\eta_1, \eta_2) \in \mathscr{O}_2$. *En écrivant les champs de vecteurs en colonnes, on note que l'espace tangent est composé de champs de vecteurs de type*

$$\begin{pmatrix} df_1(\xi^1) & df_2(\xi^2) \end{pmatrix} + \begin{pmatrix} \eta_1(0,x) & \eta_1(x^2,x^3) \\ \eta_2(0,x) & \eta_2(x^2,x^3) \end{pmatrix} = \begin{pmatrix} 0 & 2x\xi^2(x) \\ \xi^1(x) & 3x^2\xi^2(x) \end{pmatrix} + \begin{pmatrix} \eta_1(0,x) & \eta_1(x^2,x^3) \\ \eta_2(0,x) & \eta_2(x^2,x^3) \end{pmatrix}$$

Ainsi, à partir de ξ^1, η_1 *et* η_2, *on en déduit les champs de vecteurs suivants*

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}.$$

On peut voir qu'il manque un champ de vecteur constant. Ainsi, tous les termes en x *peuvent être obtenus à partir de* ξ^1 *en la position* $(2,1)$. *Si on pose* $\eta_i(X,Y) = X^m Y^n$ *avec* $m > 0$, *on obtient* x^k *pour* $k \neq 1,3$, *à partir des positions* $(1,2)$ *et* $(2,2)$. *Pour* $\xi^2(x) = x^2$ *fixé, on obtient* x^3 *en la position* $(2,1)$ *dû au fait qu'on obtient* x^4 *à partir de la position* $2,2$, *et pour* $\xi^2 = 1$, *on obtient le terme* x *en la position* $(1,2)$ *puisqu'on obtient* x^2 *en la position* $(2,2)$. *De façon similaire, on obtient le terme* x^3 *en la position* $(2,2)$. *En ayant tous les termes en position* $(1,2)$ *pour un* $\eta_1(X,Y) = Y^r$ *fixé, on peut aussi obtenir tous les termes en la position* $(1,1)$. *Par conséquent, il manque, outre le champ de vecteurs constants, le terme* x *en la position* $(2,2)$ *; ce qui signifie que la codimension vaut 2.*

De façon générale, il est difficile de calculer la codimension d'un germe à cause de la structure de module de l'espace tangent. Cependant, il existe des formules et des méthodes alternatives beaucoup plus simples; dont l'une d'elles consiste à utiliser le fait qu'un germe est déterminé de manière finie. Ce qui veut dire que les termes d'ordres supérieurs peuvent être négligés.

Théorème 4.2 *Mather [30]*
Un germe $f : (\mathbb{K}^n, S) \to (\mathbb{K}^p, 0)$ *est fini (i.e il peut être déterminé de façon finie) si et seulement si* $\mathscr{A}_e - cod(f) < \infty$.

Définition 4.8 *Sinha and Atique [49]*
Soit $f = \{f_1, f_2, \ldots, f_r\} : (\mathbb{K}^n, S) \to (\mathbb{K}^p, 0)$ *un multigerme avec* $S = \{x_1, \ldots, x_r\}$.

- *La multiplicité de* f *est donnée par*

$$m_0(f) = \dim_{\mathbb{K}} \frac{\mathscr{O}_{n,S}}{f^*(\mathscr{M}_p)} = \sum_{i=1}^{r} \dim_{\mathbb{K}} \frac{\mathscr{O}_{n,x_i}}{f_i^*(\mathscr{M}_p)}.$$

- *Le multigerme* f *est de corang* k *si et seulement si pour tout* $i = 1, \ldots, r$, f_i *est de corang inférieur ou égale* k.
- f *est dit multigerme simple s'il existe un nombre fini de* $\mathscr{A}$*-classe (i.e sous l'action des germes de difféomorphismes dans les espaces de départ et d'arrivée) telles que, pour tout dépliage* $F : (\mathbb{K}^n \times \mathbb{K}^d, S \times \{0\}) \to (\mathbb{K}^n \times \mathbb{K}^d, 0)$ *avec* $F(x,\lambda) = (f_\lambda(x), \lambda)$ *et* $f_0 = f$, *il existe un voisinage* U *suffisamment petit de* $S \times \{0\}$ *tel que pour tout* $(y_1,\lambda) \ldots (y_r,\lambda) \in U$ *avec* $F(y_1,\lambda) = \ldots = F(y_r,\lambda)$, *le multigerme* $f_\lambda : (\mathbb{K}^n, \{y_1, \ldots, y_r\}) \to (\mathbb{K}^p, f_\lambda(y_i))$ *appartient à l'une de ces classes.*

Définition 4.9 *Sinha and Atique [49]*

— *Un germe de champ de vecteurs* $\eta \in \theta_p$ *est dit relevable (*liftable*) sur* f *s'il existe* $\xi \in \theta_n$ *tel que* $df \circ \xi = \eta \circ f$ *(i.e* $tf(\xi) = wf(\eta)$*). L'ensemble des germes de champs de vecteurs relevables sur* f *est noté* $Lift(f)$. *De plus,* $Lift(f)$ *est un* $\mathscr{O}_p$*-module.*

— *Soit* $\tau(f) = ev_0(Lift(f))$ *l'évaluation des éléments de* $Lift(f)$ *à l'origine.*

Soit F un espace vectoriel de dimension finie. Une famille finie de sous-espaces vectoriels $E_1,\ldots,E_r$ de F admet une intersection presque régulière d'ordre k (par rapport à F) si

$$\text{codim}(E_1\cap\ldots\cap E_r)=\text{codim}(E_1)+\ldots\text{codim}(E_r)-k.$$

En particulier, lorsque $k=0$ l'intersection est dite régulière et lorsque $k=1$, elle est dite *presque* régulière.

Théorème 4.3 *Mather [32]*
Un multigerme $f=\{f_1,\ldots,f_r\}:(\mathbb{K}^n,S)\to(\mathbb{K}^p,0)$ est dit stable si et seulement si chacune de ses branches f_i est stable et que les sous-espaces vectoriels $\tau(f_1),\ldots,\tau(f_r)$ ont une intersection régulière.

Théorème 4.4 *T. Cooper and Atique [50]*
Si $f=\{f_1,\ldots,f_r\}$ est un multigerme de $\mathscr{A}_e$-codimension 1 alors chacune de ses branche f_i est stable et $\tau(f_1),\ldots,\tau(f_r)$ ont une intersection presque régulière :

$$\text{codim}(\tau(f_1)\cap\ldots\cap\tau(f_r))=\sum_{i=1}^{r}\text{codim}\tau(f_i)-1$$

Exemple 4.2 *Sinha and Atique [49]*
Si f est un bigerme de $\mathbb{K}^2\to\mathbb{K}^3$ tel que chaque branche est une immersion, alors f est soit $\mathscr{A}_e$-équivalent à :

$$\begin{cases}(x,y)\mapsto(x,y,0)\\(x,y)\mapsto(x,0,y)\end{cases}$$

qui est stable puisque $\tau(f_1)=\{(X,Y,Z)/Z=0\}$ et $\tau(f_2)=\{(X,Y,Z)/Y=0\}$; où

$$\begin{cases}(x,y)\mapsto\quad(x,y,0)\\(x,y)\mapsto(x,y,\phi(x,y))\end{cases}$$

où ϕ est appelée fonction de séparation. Concernant la $\mathscr{A}$ équivalence, D. Mond démontre dans Mond [36] que les bigermes d'immersions sont classifés par la $\mathscr{K}$-classe de la fonction de séparation. Donc $\phi(x,y)=x^2\pm y^{k+1}$ (A_k); $\phi(x,y)=x^2y\pm y^{k-1}$ (D_k); $\phi(x,y)=x^3+y^4$ (E_6); $\phi(x,y)=x^3\pm xy^3$ (E_7); $\phi(x,y)=x^3+y^5$ (E_8). Aussi, $\mathscr{A}_e-cod(f)=\mathscr{K}_e-cod(\phi)$. Notons que, pour toutes ces fonctions de séparation ci-dessus, $\tau(f_1)=\tau(f_2)=\{(X,Y,Z)/Z=0\}$. Ce qui signifie que $\tau(f_1)$ et $\tau(f_2)$ ont une intersection presque régulière.

4.2 Quelques méthodes numériques

La plupart des définitions et résultats énoncés dans cette sous-section sont extraits de Moore et al. [39]. Étant donné une équation du type

$$f(x)=0 \tag{4.1}$$

et F une extension d'intervalle de f, où f est une fonction réelle de classe C^∞; on définit la procédure itérative suivante

$$X_{k+1}=F(X_k)\cap X_k,\ \text{ pour } k=0,1,2,\ldots \tag{4.2}$$

Si X_0 est tel que $F(X_0)\subseteq X_0$, alors la formule (4.2) génère un ensemble d'intervalles imbriqués et qui convergent vers un intervalle $X*$ tel que, pour tout $k=0,1,2,\ldots$, $X*=F(X*)$ et $X*\subseteq X_k$. Sur un ordinateur, il est toujours possible d'interrompre la procédure itérative dès que $X_{k+1}=X_k$; en utilisant l'arithmétique des intervalles (IA) [1] avec un nombre spécifique de digits (précision sur le nombre de chiffres) fournissant ainsi le plus petit intervalle pouvant contenir $X*$.

Les méthodes de Newton par intervalle et de Krawczyk ont des propriétés similaires. En effet, elles peuvent être implémentées de façon itérative sur un ordinateur et elles sont aussi utilisées pour garantir l'existence et l'unicité d'une solution d'un système régulier d'équations non linéaires sur un domaine (il s'agit d'intervalle, rectangle ou boite selon la dimension dans laquelle on travaille).

1. Interval Arithmetic, voir [27].

4.2.1 Arithmétique des intervalles

Les méthodes de calculs numériques rappelées dans cette section sont particulièrement utilisées, ici, sur des domaines fermés. On rappelle donc qu'un intervalle fermé est défini par

$$[a,b] := \{x \in \mathbb{R}, a \leq x \leq b\}.$$

Dans ce chapitre, on ne considèrera que des intervalles fermés. Pour tout intervalle X, $\underline{X}$ et $\overline{X}$ désigneront respectivement sa borne inférieure et supérieure ; i.e

$$X = [\underline{X}, \overline{X}].$$

Deux intervalles X et Y sont égaux si et seulement si

$$\underline{X} = \underline{Y} \text{ et } \overline{X} = \overline{Y}.$$

Un intervalle X est dit dégénéré lorsque $\underline{X} = \overline{X}$. L'intersection et l'union de deux intervalles X et Y sont respectivement définies par

$$X \cap Y = \{s : s \in X \text{ et } s \in Y\} = [\max(\underline{X}, \underline{Y}), \min(\overline{X}, \overline{Y})]$$

$$X \cup U = \{s : s \in X \text{ ou } s \in Y\}.$$

La coque de deux intervalles X et Y est donnée par

$$X \underline{\cup} Y = [\min(\underline{X}, \underline{Y}), \max(\overline{X}, \overline{Y})].$$

On a

$$X \cup Y \subset X \underline{\cup} Y$$

Définition 4.10
Soit $X = [\underline{X}, \overline{X}]$ *un intervalle de* $\mathbb{R}$.

- *La* ***largeur*** *de* X*, notée* $l(X)$*, est égale à*

$$l(X) = \overline{X} - \underline{X}.$$

- *Le* ***centre*** *de* X*, noté* $c(X)$*, vaut*

$$c(X) = \frac{1}{2}(\underline{X} + \overline{X}).$$

- *La* ***valeur absolue*** *de* X*, notée* $|X|$ *est égale au maximum de la valeur absolue de ses bornes :*

$$|X| = \max(|\underline{X}|, |\overline{X}|)$$

La droite réelle $\mathbb{R}$, munie de la relation d'ordre ($<$), est un ensemble ordonné. L'ensemble des intervalles de $\mathbb{R}$ peut aussi être muni d'une relation d'ordre (noté $<$) définie comme suit : soient X et Y deux intervalles dans $\mathbb{R}$

$$X < Y \Longleftrightarrow \overline{X} < \underline{Y}.$$

Opérations arihtmétiques sur les intervalles
Des opérations élémentaires sur $\mathbb{R}$ telles que l'addition, la soustraction, la multiplication et la division s'étendent aussi aux intervalles. Par exemple la somme de deux intervalles donne un sous-ensemble de $\mathbb{R}$ constitué de toutes les sommes possibles entre deux réels des intervalles.

$$\begin{aligned} X + Y &= \{s = x + y : x \in X \text{ et } y \in Y\} \\ &\subseteq [\underline{X} + \underline{Y}, \overline{X} + \overline{Y}] \end{aligned}$$

$$\begin{aligned} \mathrm{X}-\mathrm{Y} &= \{s = x - y : x \in \mathrm{X} \text{ et } y \in \mathrm{Y}\} \\ &\subseteq [\underline{\mathrm{X}} - \overline{\mathrm{Y}}, \overline{\mathrm{X}} - \underline{\mathrm{Y}}] \end{aligned}$$

$$\begin{aligned} \mathrm{X}\cdot\mathrm{Y} &= \{s = x \cdot y : x \in \mathrm{X} \text{ et } y \in \mathrm{Y}\} \\ &\subseteq [\min \mathrm{S}, \max \mathrm{S}],\ \mathrm{S} = \{\underline{\mathrm{X}}\cdot\underline{\mathrm{Y}}, \underline{\mathrm{X}}\cdot\overline{\mathrm{Y}}, \overline{\mathrm{X}}\cdot\underline{\mathrm{Y}}, \overline{\mathrm{X}}\cdot\overline{\mathrm{Y}}\} \end{aligned}$$

$$\begin{aligned} \mathrm{X}/\mathrm{Y} &= \{s = x/y : x \in \mathrm{X}, y \in \mathrm{Y} \text{ et } y \neq 0\} \\ &= \mathrm{X}\cdot\mathrm{Y}',\ \mathrm{Y}' = 1/\mathrm{Y} = [1/\overline{\mathrm{Y}}, 1/\underline{\mathrm{Y}}]. \end{aligned}$$

Tout intervalle $\mathrm{X} = [\underline{\mathrm{X}}, \overline{\mathrm{X}}]$ peut s'écrire sous la forme

$$\begin{aligned} \mathrm{X} &= c(\mathrm{X}) + [-\frac{1}{2}l(\mathrm{X}), \frac{1}{2}l(\mathrm{X})] \\ &= c(\mathrm{X}) + \frac{1}{2}c(\mathrm{X})[-1, 1]. \end{aligned}$$

Vecteurs et Matrices d'intervalles
Un vecteur d'intervalles X de dimension n est la donnée d'un n-uplets d'intervalles $\mathrm{X} = (\mathrm{X}_1, \ldots, \mathrm{X}_n)$. La plupart des propriétés étudiées sur les intervalles restent valables pour les vecteurs d'intervalles.

Définition 4.11
Soient X *et* Y *deux vecteurs d'intervalles de dimension n.*

- *Un vecteur de réels* $x = (x_1, \ldots, x_n) \in \mathrm{X}$ *si et seulement si pour tout* $i = 1, \ldots, n$ *on a* $x_i \in \mathrm{X}_i$.
- *La largeur de* X*, notée* $l(\mathrm{X})$*, est donnée par*

$$l(\mathrm{X}) = \max_{i=1,\ldots,n} (l(\mathrm{X}_i))$$

- *Le centre de* X *est donné par*

$$c(x) = (c(\mathrm{X}_1), \ldots, c(\mathrm{X}_n)).$$

- *La norme de* X *est donnée par*

$$\| \mathrm{X} \| = \max_{i=1,\ldots,n} | \mathrm{X}_i | .$$

- *L'intersection et l'union de* X *et* Y *sont respectivement données par :*

$$\mathrm{X} \cap \mathrm{Y} = (\mathrm{X}_1 \cap \mathrm{Y}_1, \ldots, \mathrm{X}_n \cap \mathrm{Y}_n)$$

$$\mathrm{X} \cup \mathrm{Y} = (\mathrm{X}_1 \cup \mathrm{Y}_1, \ldots, \mathrm{X}_n \cup \mathrm{Y}_n)$$

$$\mathrm{X} \cap \mathrm{Y} = \emptyset \Leftrightarrow \exists i \in [\![1 \ldots n]\!],\ \mathrm{X}_i \cap \mathrm{Y}_i = \emptyset$$

$$\mathrm{X} \subseteq \mathrm{Y} \Leftrightarrow \mathrm{X}_i \subseteq \mathrm{Y}_i\ \forall i \in [\![1 \ldots n]\!].$$

Définition 4.12
Un matrice d'intervalles de taille $n \times m$ *est constituée de* m *vecteurs d'intervalles de dimension* n.

Ensemble image d'une fonction

Définition 4.13 *Soient $f = f(x_1,\ldots,x_n)$ une fonction en plusieurs variables à valeur dans réel. L'ensemble image de f sur un vecteur d'intervalles $\mathrm{X} = (\mathrm{X}_1,\ldots,\mathrm{X}_n)$ est caractérisé par*

$$f(\mathrm{X}) = f(\mathrm{X}_1,\ldots,\mathrm{X}_n) = \{f(x_1,\ldots,x_n) : x_1 \in \mathrm{X}_1,\ldots,x_n \in \mathrm{X}_n\};$$

où X_i pour $i = 1,\ldots,n$ sont des intervalles spécifiques.

Dans cette sous-section, il s'agit de déterminer l'ensemble image par d'un vecteur d'intervalle $\mathrm{Y} \subseteq \mathrm{X}$. Dans le cas d'une fonction monotone il est facile de calculer $f(\mathrm{Y})$. En effet, si f est croissante (respectivement décroissante) sur Y alors

$$f(\mathrm{Y}) = [f(\underline{\mathrm{Y}}), f(\overline{\mathrm{Y}})] \text{ (resp. } f(\mathrm{Y}) = [f(\overline{\mathrm{Y}}), f(\underline{\mathrm{Y}})]).$$

En général il est difficile de déterminer avec exactitude l'ensemble image d'une fonction sur un sous-ensemble Y de X (voir Gaganov [14]). Toutefois, il est toujours possible de calculer un intervalle $\mathrm{W} \subset \mathbb{R}$ tel que $f(\mathrm{Y}) \subseteq \mathrm{W}$. L'ensemble W est appelé une extension d'intervalle de f.

Définition 4.14 (fonction à une variable)
F *est appelée une extension d'intervalle de f si, sur tout intervalle dégénéré $[x,x]$,* F *et f sont égales :*

$$\mathrm{F}([x,x]) = f(x).$$

Définition 4.15 (fonction à plusieurs variables)
Si f est une fonction réelle de plusieurs variables, alors une extension d'intervalle F *de f est une fonction d'intervalle de n variables $\mathrm{X}_1,\ldots,\mathrm{X}_n$ telle que pour tout argument $x_1,\ldots,x_n$,*

$$\mathrm{F}(x_1,\ldots,x_n) = f(x_1,\ldots,x_n).$$

Le concept défini ci-dessous est étroitement à la continuité. Elle permet d'examiner la procédure par laquelle $f(\mathrm{X})$ peut être approximée aussi près que l'on veut par une union finie d'intervalles.

Définition 4.16 (Extension d'intervalle Lipschitzienne)
Soient X_0 un intervalle ou vecteur d'intervalles et F *une extension d'intervalle sur X_0.* F *est dite Lipschitzienne dans X_0 s'il existe une constante* L *telle que, pour tout $\mathrm{X} \subseteq \mathrm{X}_0$,*

$$l(\mathrm{F}(\mathrm{X})) \leq \mathrm{L} \times l(\mathrm{X})$$

NB : Dans la suite de ce chapitre, nous manipulerons exclusivement des extensions d'intervalles Lipschitziennes.

4.2.2 Méthode de Newton

Nous commençons par rappeler la méthode de Newton dans le cas des fonctions en une variable. Soit f une fonction de classe C^∞ dans $\mathbb{R}$. D'après le Théorème de la valeur moyenne,
$\forall x,\ y \in \mathbb{R},\ \exists s \in [x,y]$ tel que :

$$f(x) = f(y) + f'(s)(x-y) \tag{4.3}$$

Soit $[a,b]$ un intervalle dans lequel on cherche une solution de l'équation

$$f(x) = 0.$$

Pour tout $y \in [a,b]$, une solution x de cette équqtion vérifie

$$f(y) + f'(s)(x-y) = 0;$$

en particulier pour $y = c([a,b]) = \frac{b-a}{2}$.
Donc

$$x = y - \frac{f(y)}{f'(s)}. \tag{4.4}$$

Soit F′(X) une extension d'intervalle de $f'(x)$ et considérons l'algorithme suivant

$$X^{(k+1)} = X^{(k)} \cap N(X^{(k)}), \quad \text{pour } k = 0,1,2,\ldots \tag{4.5}$$

avec

$$N(X) = c(X) - \frac{f(c(X))}{F'(X)} \tag{4.6}$$

D'après l'équation (4.4), l'intervalle N(X) contient la solution x si $y = c(X)$ et si x est contenu dans l'intervalle X, alors s dans l'équation (4.3) appartient aussi à X. Par conséquent, si $x \in X^{(0)}$ alors pour tout indice k, $x \in X^{(k)}$.

Proposition 4.1 *Moore et al. [39, Thm 8.1]*
Si un intervalle $X^{(0)}$ *contient une solution* x_0 *de l'équation* $f(x) = 0$, *alors* x_0 *appartient aussi* $X^{(k)}$ *pour tout* $k = 0,1,2,\ldots$. *De plus, si* $0 \notin F'(X^{(0)})$, *alors les intervalles* $X^{(k)}$ *constituent une suite imbriquée qui converge vers* x_0.

La méthode de Newton par intervalle s' interprète géométriquement de manière presque similaire à la méthode de Newton classique. Excepté qu'ici le nouvel intervalle $X^{(k+1)}$ est délimité par l'intersection des deux droites tangentes dont les pentes correspondent aux extrémités de l'intervalle $X^{(k)}$ avec l'axe des abscisses (voir Figure 4.2).

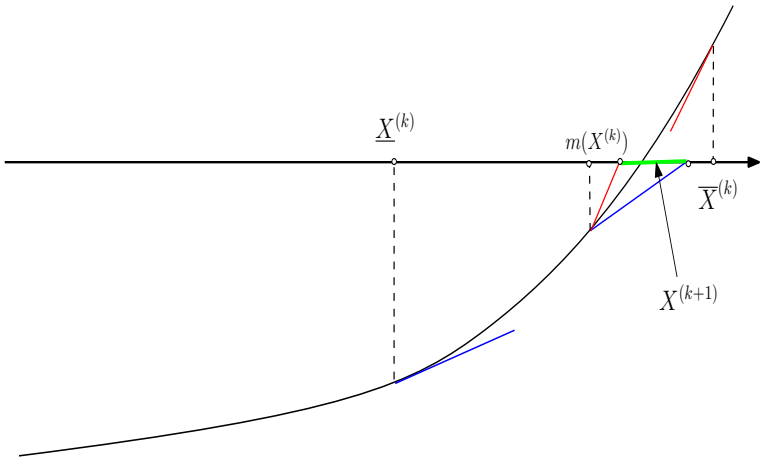


FIGURE 4.2 – **Interprétation géométrique de la méthode de Newton par intervalle (univarié)**

Remarque 4.1 (Proposition4.1)
Si $0 \in F'(X)$, *on procède généralement à une subdivision de l'intervalle comme suit : Rappelons tout d'abord la division de deux intervalles*

$$[a,b]/[c,d] = [a,b]\,(1/[c,d])$$

avec

$$1/[c,d] = \{1/y : y \in [c,d]\}.$$

— *Si* $c = 0 < d$, *alors* $1/[c,d] = [1/d, +\infty[$.
— *Si* $c < 0 < d$, *alors* $1/[c,d] =]-\infty, 1/c] \cup [1/d, +\infty[$.
— *Si* $c < d = 0$, *alors* $1/[c,d] =]-\infty, 1/c]$.

4.2.3 Méthode de Krawczyk

La méthode de Krawczyk peut être vue comme une généralisation directe de la méthode de Newton par intervalle. Elles sont aussi utlisées en pratique pour garantir l'existence et l'unicité d'une solution dans un domaine. Toutefois, elles ont chacune des avantages particuliers. Soit le système d'équations non linéaires

$$f(x) = 0 \Leftrightarrow \begin{cases} f_1(x_1,\ldots,x_n) = 0 \\ \vdots \\ f_n(x_1,\ldots,x_n) = 0 \end{cases}; \tag{4.7}$$

où les f_i sont des fonctions C^∞ sur un ouvert de $\mathbb{R}^n$ et à valeurs réelles. Soient F et F′ des extensions d'intervalles de f et f', et X_0 une boite de $\mathbb{R}^n$; un vecteur d'intervalles de dimension n. Le théorème ci-dessous donne un test d'existence d'une solution au système 4.7.

Définition 4.17 (Opérateur de Krawczyk) *Moore et al. [39]*
Soient M *une matrice réelle non singulière approximant l'inverse de la matrice jacobienne réelle de* $F'(c(X))$ *dont les éléments sont donnés par* $F'(c(X))_{ij} = \partial f_i(c(X))/\partial x_j$. *L'opérateur de Krawczyk* K *appliqué à* X *est défini par*

$$K(X) = y - Mf(y) + \left(I - MF'(X)\right)(X - y),$$

où y *est un vecteur appartenant à* X. *Donc* K(X) *est une boite de* $\mathbb{R}^n$ *ou l'ensemble vide.*

Théorème 4.5 *Moore et al. [39, Thm 8.2]*[2]
Si $K(X) \subseteq X$, *alors l'équation (4.7) admet une solution* x_0 *appartenant à* K(X).

En particulier, si le vecteur d'intervalles $X = (X_1,\ldots,X_n)$ est un n-cube (i.e $l(X_i) = l(X)$ pour tout $i \in [\![1,n]\!]$) et $y = c(X)$ alors K(X) est strictement contenu dans l'intérieur de X dès que

$$\| K(X) - c(X) \| < \frac{l(X)}{2}. \tag{4.8}$$

Il apparait ainsi que, la condition (4.8) est suffisante pour garantir l'existence d'une solution de l'équation (4.7) dans X. De plus, la même condition (4.8) est suffisante pour garantir la convergence de la méthode de Krawczyk par intervalle.

Théorème 4.6 *Moore et al. [39, Thm 8.3]*[3]
Soient X *un* n*-cube de* $\mathbb{R}^n$, $y = c(X)$ *et* M *une matrice réelle non singulière. Supposons que la condition (4.8) est satisfaite et posons* $X^{(0)} = X$, $M^{(0)} = M$. *Soit* $x^{(0)}$ *un vecteur dans* $X^{(0)}$, *alors le système (4.7) admet une unique solution dans* X, *et l'algorithme ci-dessous converge vers la solution :*

$$X^{(k+1)} = X^{(k)} \cap K(X^{(k)}) \quad (k = 1,2,\ldots) \tag{4.9}$$

avec

$$K(X^{(k)}) = y^{(k)} - M^{(k)} f(y^{(k)}) + \left(I - M^{(k)} F'(X^{(k)})\right) Z^{(k)}$$

et

$$y^{(k)} = c(X^{(k)}),\ Z^{(k)} = X^{(k)} - c(M^{(k)})$$

où $M^{(k)}$ *est choisi comme étant*

$$M^{(k)} = \begin{cases} M \text{ est une approximation de } \left[c\left(F'(X^{(k)})\right)\right]^{-1}, \\ si\ \| I - MF'(X^{(k)}) \| \leq \| I - M^{(k-1)} F'(X^{(k-1)}) \| \\ M^{(k-1)}\ sinon \end{cases}$$

2. Voir aussi Krawczyk [26], Moore [37]
3. Voir aussi dans Moore [37, 38]

4.3 Projection d'une courbe lisse de $\mathbb{R}^3$ dans $\mathbb{R}^2$

Dans cette section, nous traitons du problème qui consiste à calculer une représentation topologiquement correcte de la projection d'une courbe de $\mathbb{R}^3$ dans $\mathbb{R}^2$. Ici, on se place dans le cas où une telle courbe dans l'espace est définie soit comme étant l'intersection de deux surfaces, soit le contour apparent d'une surface dans $\mathbb{R}^3$. En général, sa projection dans le plan n'est pas une courbe lisse ; i.e elle peut comporter des points singuliers : **un noeud** ou bien **cuspide**. Dans de récents travaux de Imbach et al. [22], les auteurs proposent un algorithme qui prend en entrée une courbe implicite dans l'espace et un domaine compact de résolution. Cet algorithme engendre une structure de données qui est composée d'une approximation de la courbe spatiale et une représentation certifiée de la topologie de sa projection dans un compact du plan. Une de leur principales contributions consiste à caractériser un ensemble de singularités comme étant des solutions régulières d'un système d'équations.

Dans le chapitre qui suit, nous proposons une généralisation en dimension supérieure du problème énoncé ci-dessus, en s'appuyant sur des techniques similaires. Il s'agit donc ici, de rappeler les résultats principaux établis dans Imbach et al. [21] ainsi que les nouvelles techniques développées dans cet article.

Soient

$$F, G : \mathbb{R}^3 \to \mathbb{R}$$

deux fonctions C^∞ et $\mathscr{M}$ la courbe contenu dans $\mathbb{R}^3$ définie par :

$$\mathscr{M} := \{(x, y, z) \in \mathbb{R}^3 \mid F(x, y, z) = G(x, y, z) = 0\}.$$

Soient $\mathbf{B}$ un compact de $\mathbb{R}^2$, $X_0 = \mathbf{B} \times \mathbb{R}$ et $\pi : \mathbb{R}^3 \to \mathbb{R}^2$ la projection dans le plan (x, y) qui à tout point $(x, y, z) \mapsto (x, y)$. Soit $\mathscr{C} := \pi_{|\mathbf{B}\times\mathbb{R}}(\mathscr{M})$.

Définition 4.18 *Arnol'd [1]*
Un point $P \in \mathscr{C}$ *est une singularité de type* $A_k^{\pm}$ *s'il existe un voisinage* $U \subset \mathbb{R}^2$ *de* P *dans lequel* $\mathscr{C}$ *est implicitement définie par l'équation* $x^2 \pm y^{k+1} = 0$.
En particulier :

- *Un* ***noeud*** *est une intersection de deux branches réelles de* $\mathscr{C}$. *Il est de type* A_1^-.
- *Un* ***cuspide*** *est une singularité de type* A_{2k} [4]. *Un cuspide ordinaire est une singularité de type* A_2.
- *Un point* ***régulier*** *est une singularité de type* A_0.

Compte tenu du fait que les méthodes numériques de résolution de systèmes d'équations n'aboutissent que sous certaines conditions de régularité, les résultats rappelés ici sont établis sous les hypothèses ci-dessous :

(H_1) $\mathscr{C}$ est lisse au dessus de $\mathbf{B}$; i.e $\pi^{-1}(\mathscr{C})$ ne contient pas de singularités dans $\pi^{-1}(\mathbf{B})$.

(H_2) Pour tout $(\alpha, \beta) \in \mathbf{B}$ fixé, le système $F(\alpha, \beta, z) = G(\alpha, \beta, z) = 0$ admet au plus deux racines comptées avec multiplicité.

(H_3) L'ensemble des points $(\alpha, \beta) \in \mathbf{B}$, tels que le système $F(\alpha, \beta, z) = G(\alpha, \beta, z) = 0$ admet deux racines distinctes comptées avec multiplicité, est discret.

(H_4) La restriction de la projection π sur $\mathscr{M} \cap (\mathbf{B} \times \mathbb{R})$ est une application propre ; i.e l'image inverse de tout compact est un compact.

(H_5) Les singularités de $\mathscr{C}$ sont des noeuds ou des cuspides ordinaires.

La proposition suivante décrit les types de singularités sur $\mathscr{C}$.

Proposition 4.2 *Imbach et al. [21, Lemma 2, Corollary 1]*
Sous les hypothèses ((H_1*))-((*H_4*)), soit* $P \in \mathscr{C}$.

4. Compte tenu de l'équivalence entre les singularités de types A_{2k}^+ et A_{2k}^-, on notera simplement A_{2k}

(a_1) *Si* P *admet deux antécédents via la projection* π, *alors est un point singulier de* $\mathscr{C}$ *du type* A^-_{2k+1} *avec* $k \geq 0$.

(a_2) *Si* P *est une valeur critique de la projection* π, *alors* P *est un cuspide* $\mathscr{C}$ *du type* $A_{2(k+1)}$ *avec* $k \geq 0$.

Les systèmes ci-dessous constituent une représentation naïve des singularités de la courbe $\mathscr{C}$ dans le plan (x, y).

Soit $(x, y, z_1, z_2) \in \mathbf{B} \times \mathbb{R}^2$ tel que :

$$\begin{cases} F(x, y, z_1) = 0 \\ G(x, y, z_1) = 0 \\ F(x, y, z_2) = 0 \\ G(x, y, z_2) = 0 \\ z_1 \neq z_2 \end{cases} \tag{S-noeud}$$

Soit $(x, y, z) \in \mathbf{B} \times \mathbb{R}$ tel que :

$$\begin{cases} F(x, y, z) = 0 \\ G(x, y, z) = 0 \\ \partial_z F(x, y, z) = 0 \\ \partial_z G(x, y, z) = 0 \end{cases} \tag{S-cusp}$$

Toutefois, le système (S-noeud) reste numériquement instable lorsque $z_1 = z_2$ (le système n'est plus équidimensionnel), rendant ainsi le système (S-cusp) surdéterminé. La technique développée dans Imbach et al. [21] consiste à construire un nouveau système, appelé **ball-system**, dont les solutions régulières sont une caractérisation des singularités de $\mathscr{C}$.

Définition 4.19 *Imbach et al. [21]*
Soit $A(x, y, z)$ *une fonction analytique réelle,* $c = \frac{|z_1 - z_2|}{2}$ *et* $r_2 = r^2$ *avec* $r = \mid z_1 - c \mid = \mid z_2 - c \mid$. *Les fonctions* S.A *et* D.A *sont définies par :*

$$S.A(x, y, c, r_2) = \begin{cases} \frac{1}{2}(A(x, y, c + \sqrt{r}) + A(x, y, c - \sqrt{r})) & if\ r > 0 \\ A(x, y, c) & if\ r = 0 \\ \frac{1}{2}(A(x, y, c + i\sqrt{-r}) + A(x, y, c - i\sqrt{-r})) & if\ r < 0 \end{cases}$$

et

$$D.A(x, y, c, r_2) = \begin{cases} \frac{1}{2\sqrt{r}}(A(x, y, c + \sqrt{r}) - A(x, y, c - \sqrt{r})) & if\ r > 0 \\ \partial_z A(x, y, c) & if\ r = 0 \\ \frac{1}{2\sqrt{-r}}(A(x, y, c + i\sqrt{-r}) - A(x, y, c - i\sqrt{-r})) & if\ r < 0 \end{cases}$$

On désignera par Σ l'ensemble des singulartés de $\mathscr{C}$ dans $\mathbf{B}$.

Les figures 4.3 et 4.4 illustrent le cas particulier de la projection du contour apparent du tore dans le plan avec l'utilisation du ball-système. On constate que les singularités qui en résultent dans le plan sont des cusps et des noeuds.

Proposition 4.3 *Imbach et al. [21]*

(b_1) *Si* A *est une fonction analytique réelle, alors les fonctions* S.A *et* D.A *le sont aussi.*

(b_2) *Si* $\mathscr{S}$ *l'ensemble des solutions dans* $\mathbf{B} \times \mathbb{R} \times \mathbb{R}^+$ *du ball-system suivant :*

$$\begin{cases} S.F(x, y, c, r_2) = 0 \\ S.G(x, y, c, r_2) = 0 \\ D.F(x, y, c, r_2) = 0 \\ D.G(x, y, c, r_2) = 0 \end{cases} \tag{ball-system}$$

alors $\pi_{xy}(\mathscr{S}) = \Sigma$, *où* π_{xy} *la projection de* $\mathbb{R}^4$ *dans le plan.*

(b_3) *Sous les hypothèses* (H_1)-(H_4), *dans* $\mathbf{B} \times \mathbb{R} \times \mathbb{R}^+$ *les solutions du ball-system sont régulieres si et seulement si la condition* (H_5) *est satisfaite.*

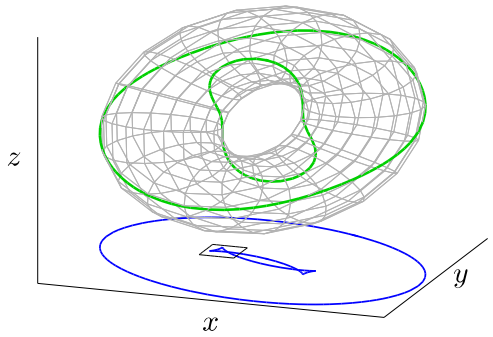


FIGURE 4.3 – Projection du contour apparent du Tore dans le plan : l'ensemble des points z critiques du Tore.

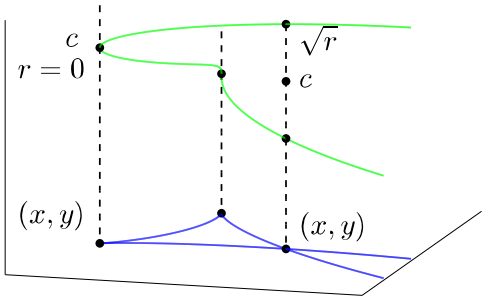


FIGURE 4.4 – Changement de variables rayon et centre aboutissant au ball-system.

Chapitre 5

Projection de surfaces analytiques lisses de $\mathbb{R}^4$ dans $\mathbb{R}^3$

Introduction

Le problème étudié dans ce chapitre s'inspire des résultats obtenus par Imbach et al. [21] (voir aussi la section 4.3 du chapitre 4).
Soit $\mathscr{M}$ une surface analytique définie comme étant l'intersection de deux hypersurfaces contenues dans $\mathbb{R}^4$, et Ω l'image de $\mathscr{M}$ par la projection canonique dans $\mathbb{R}^3$. L'objectif est de calculer un complexe simplicial isotope à Ω. En général, la surface Ω n'est pas lisse : c'est-à-dire qu'elle comporte des singularités. Nous proposons dans la section 5.3, un algorithme permettant de calculer le graphe des singularités de Ω. Cet algorithme est effectif sous certaines conditions de généricité. La caractérisation des différents types de singularités, sous forme de solutions régulières de systèmes, est effectuée dans la section 5.2. La section 5.1 introduit les définitions et notations utilisées dans ce chapitre.

5.1 Définitions et notations

Soient F et G deux fonctions analytiques réelles de $\mathbb{R}^4 \to \mathbb{R}$ qui définissent une la surface analytique réelle $\mathscr{M}$ par : $\mathscr{M} := \{(x,y,z,t) \in \mathbb{R}^4,\ \mathrm{F}(x,y,z,t) = \mathrm{G}(x,y,z,t) = 0\} \subset \mathbb{R}^4$. En d'autres termes $\mathscr{M}$ est l'intersection de deux hypersurfaces $\mathscr{M}_1$ et $\mathscr{M}_2$ définies respectivement par les équations $\mathrm{F}(x,y,z,t) = 0$ et $\mathrm{G}(x,y,z,t) = 0$, dans $\mathbb{R}^4$. Étant donné un point $q \in \mathscr{M}$, le plan tangent $\mathscr{P}$ à $\mathscr{M}$ au point q est donné par l'ensemble des vecteurs orthogonaux à ∇F et ∇G.
On considère l'application

$$\begin{aligned} \mathfrak{p} : \mathscr{M} &\to \mathbb{R}^3 \\ (x,y,z,t) &\mapsto (x,y,z) \end{aligned}$$

et on définit $\Omega = \mathfrak{p}(\mathscr{M})$. $\mathfrak{p}$. On dira qu'un plan dans $\mathbb{R}^4$ est *vertical* s'il est parallèle l'axe t; ce qui signifie qu'il contient la direction $(0,0,0,1)$. Par conséquent, le pan tangent $\mathscr{P}$ à $\mathscr{M}$ au point q est *vertical* si et seulement si $\partial_t \mathrm{F}(q) = \partial_t \mathrm{G}(q) = 0$.

5.1.1 Définitions

Définition 5.1
Soient $\mathscr{F} = (\mathrm{F}_i)_{\{1 \le i \le n\}}$ une famille finie de fonctions analytiques réelles définies sur $\mathbb{R}^4$ dans $\mathbb{R}$, $q \in \mathscr{M}$ et $\mathrm{P} \in \Omega$.

— *Pour tout* $\mathrm{F} \in \mathscr{F}$, *la* ***multiplicité*** *de* $q \in \mathbb{R}^4$ *par rapport à la variable* t *est l'entier naturel* $\mathrm{mult}_q^t(\mathrm{F}) := \max\{k \in \mathbb{N}, \frac{\partial^i \mathrm{F}}{\partial t^i}(q) = 0,\ \forall i < k\}$. *Dans ce chapitre, nous nous intéressons uniquement à la multiplicité par rapport à la variable de projection* t. *Par conséquent, nous allons simplement noter* $\mathrm{mult}_q(\mathrm{F})$ *en lieu et place de* $\mathrm{mult}_q^t(\mathrm{F})$.

— *La multiplicité de q en tant que racine de la famille $\mathscr{F}$ est l'entier naturel*

$$\text{mult}_q(\mathscr{F}) = \min\{\text{mult}_q(\text{F}_i), 1 \leq i \leq n\}.$$

— *La multiplicité du point $\text{P} \in \Omega$ est l'entier naturel*

$$\text{mult}_{(\text{P})} = \sum_{q \in \mathfrak{p}^{-1}(\text{P})} \text{mult}_q(\text{F},\text{G});$$

où F,G sont les fonctions analytiques réelles définissant la surface $\mathscr{M}$ et $\mathfrak{p}$ la projection de $\mathscr{M} \to \mathbb{R}^3$.

Définition 5.2
Soient E, F *deux variétés différentiables, $f : \text{E} \to \text{F}$ une application différentiable et $q \in \text{E}$.*
*Le **corang** de f au point q est l'entier*

$$\text{corank}\,(df)_q = \min(\dim \text{E}, \dim \text{F}) - \text{rank}\,(df)_q$$

Notion de Transversalité

Définition 5.3 *Demazure [8, def 2.5.4]*
Soit E *une variété différentiable de dimension finie, $\mathscr{V}$ et $\mathscr{V}'$ deux sous-variétés de* E. *$\mathscr{V}$ et $\mathscr{V}'$ sont **transverses** (l'une à l'autre) si, pour tout $a \in \mathscr{V} \cap \mathscr{V}'$, les sous-espaces $\text{T}_a\mathscr{V}$ et $\text{T}_a\mathscr{V}'$ satisfont l'une des conditions suivantes (qui sont équivalentes) :*

— $\text{T}_a\mathscr{V} + \text{T}_a\mathscr{V}' = \text{E}$;

— $\text{codim}(\text{T}_a\mathscr{V} \cap \text{T}_a\mathscr{V}') = \text{codim}(\text{T}_a\mathscr{V}) + \text{codim}(\text{T}_a\mathscr{V}')$;

— $\dim(\text{T}_a\mathscr{V} \cap \text{T}_a\mathscr{V}') = \dim(\text{T}_a\mathscr{V}) + \dim(\text{T}_a\mathscr{V}') - \dim(\text{E})$.

On note $\mathscr{V} \pitchfork \mathscr{V}'$.

Remarque 5.1
*Si $\dim(\text{T}_a\mathscr{V}) + \dim(\text{T}_a\mathscr{V}') < \dim(\text{E})$ alors $\text{T}_a\mathscr{V}$ n'est pas **transverse** à $\text{T}_a\mathscr{V}'$. Si $\dim(\text{T}_a\mathscr{V}) + \dim(\text{T}_a\mathscr{V}') = \dim(\text{E})$ alors $\text{T}_a\mathscr{V}$ est **transverse** à $\text{T}_a\mathscr{V}'$ si et seulement les deux sous-espaces sont complémentaires.*

La notion de transversalité s étend de façon naturelle aux fonctions de classe C^∞.

Définition 5.4 *Demazure [8, def 3.7.1]*
Soient E, F *deux espace vectoriels de dimensions finie, $\mathscr{V}$ et $\mathscr{W}$ des sous-variétés respectifs de* E *et* F.
Soit $f : \mathscr{V} \to \text{F}$ une fonction de classe C^∞.

- *f est **transverse** à $\mathscr{W}$ au point $q \in \mathscr{V}$*
  — *si $f(q)$ n'appartient pas à $\mathscr{W}$ ou bien,*
  — *$f(q)$ appartient $\mathscr{W}$ et l'image de $\text{T}_q\mathscr{V}$, par l'application linéaire tangente $df(q)$, est transverse à $\text{T}_{f(q)}\mathscr{W}$.*
- *f est **transverse** à $\mathscr{W}$ si elle l'est en tout point q appartenant à $\mathscr{V}$.*

Par abus de notation, $f \pitchfork \mathscr{W}$ se lira f est transverse à $\mathscr{W}$.

Définition 5.5 *Demazure [8, section 3.8.3]*
Soit r un entier naturel, E *et* F *deux espaces vectoriels de dimensions finies. Soit $\mathscr{V}$ une sous-variété de* E *et $f : \mathscr{V} \to \text{F}$ une fonction de classe C^∞. On appelle le **r-jet** de f la fonction*

$$\begin{aligned} j^r f : \mathscr{V} &\to \text{J}^r(\mathscr{V}, \text{F}) \\ q &\mapsto (q, f(q), f'(q), \ldots, f^{(r)}(q)) \end{aligned}$$

*$\text{J}^r(\mathscr{V}, \text{F})$ est appelé l'espace des **jets d'ordre r** des fonctions définies de* E *vers* F.
Soit Σ^1 la sous-variété des jets de corang 1 de $\text{J}^1(\mathscr{M}, \mathbb{R}^3)$ et notons par $\Sigma^1(\mathfrak{p}) = (j^1\mathfrak{p})^{-1}(\Sigma^1)$ la sous-variété de $\mathscr{M}$ ainsi définie.

Définition 5.6 *Golubistky and Guillemin [16, def 4.5]*
*Un point $q \in \mathscr{M}$ est appelé un **cross-cap** s'il appartient à $\Sigma^1(\mathfrak{p})$ et que la fonction $j^1\mathfrak{p}$ est transverse à Σ^1 en ce point.*

D'après Golubistky and Guillemin [16, Théorème II.5.4], Σ^1 est une sous-variété de codimension 2. En un point cross-cap, $j^1\mathfrak{p}$ est transverse à Σ^1 et d'aprés Demazure [8, Corollaire 3.7.3] $\Sigma^1(\mathfrak{p})$ est une sous-variété de $\mathscr{M}$ de dimension 2 ; i.e les cross-caps apparaissent comme des points isolés.

Lemme 5.1
La projection $\mathfrak{p}$ admet une singularité de type cross-cap si et seulement si la direction de projection est contenue dans le plan tangent et si $(a(z,t), b(z,t), z, t)$ est une paramétrisation locale de $\mathscr{M}$, alors on a $a_{zt}b_{tt} - a_{tt}b_{zt} \neq 0$.

Démonstration
Soit $q \in \mathscr{M}$ une singularité de type cross-cap de la projection $\mathfrak{p} : \mathscr{M} \mapsto \mathbb{R}^3$.

Tout d'abord, la condition $q \in \Sigma^1(\mathfrak{p})$ est équivalente à dire que $d\mathfrak{p}(q)$est de corang 1. Sachant que le rank$(\mathfrak{p}) = 2 - $corank$(\mathfrak{p}) = 1$, alors la condition précédente est aussi équivalente à dire que $d\mathfrak{p}(q)$ est rang 1. En d'autres termes, la projection du plan dimension 2 tangent à $\mathscr{M}$ au point q est une ligne ; ce qui signifie que la direction de projection est contenue dans le plan tangent. Donc, la condition $q \in \Sigma^1(\mathfrak{p})$ dans la Définition 5.6 est équivalente à la première condition du Lemme 5.1 : la direction de projection est contenue (colinéaire) dans le plan tangent.

A présent, nous admettons que la surface $\mathscr{M}$ peut être localement paramétrisée dans un voisinage de q par $(z,t) \mapsto (a(z,t), b(z,t), z, t)$;
i.e

$$\mathfrak{p}(z,t) = (a(z,t), b(z,t), z).$$

L'espace $J^1(\mathscr{M}, \mathbb{R}^3)$ est donc localement égale à $U \times \mathbb{R}^3 \times L(\mathbb{R}^2, \mathbb{R}^3)$; où U est un sous-ensemble de $\mathbb{R}^2$ et L désigne l'espace des applications linéaires. Le 1-jet d'une application $(f_1(z,t), f_2(z,t), f_3(z,t)) : \mathscr{M} \mapsto \mathbb{R}^3$ est donné par

$$\left((z,t), (f_1(z,t), f_2(z,t), f_3(z,t)), \begin{pmatrix} f_{1z} & f_{1t} \\ f_{2z} & f_{2t} \\ f_{3z} & f_{3t} \end{pmatrix}\right).$$

Σ^1 est le sous-ensemble de $J^1(\mathscr{M}, \mathbb{R}^3)$ pour lequel, la matrice $\begin{pmatrix} f_{1z} & f_{1t} \\ f_{2z} & f_{2t} \\ f_{3z} & f_{3t} \end{pmatrix}$ est de corang 1 ; i.e de rang 1. Supposons, sans perte de généralité, que $(f_{3z}, f_{3t}) \neq (0,0)$, Σ^1 est définie de façon implicite par deux équations

$$\begin{vmatrix} f_{1z} & f_{1t} \\ f_{3z} & f_{3t} \end{vmatrix} = 0 \text{ et } \begin{vmatrix} f_{2z} & f_{2t} \\ f_{3z} & f_{3t} \end{vmatrix} = 0$$

Alors, on a d'une part $\Sigma^1 = \Phi^{-1}(0)$ avec

$$\begin{aligned} \Phi : J^1(\mathscr{M}, \mathbb{R}^3) &\to \mathbb{R}^2 \\ (f_1, f_2, f_3) &\longmapsto \big((f_{1z}f_{3t} - f_{1t}f_{3z}), (f_{2z}f_{3t} - f_{2t}f_{3z})\big) \end{aligned}$$

D'après Golubistky and Guillemin [16, Lemma 4.3], $j^1\mathfrak{p}$ est transverse à Σ^1 au point q si et seulement si $\Phi \cdot j^1\mathfrak{p}$ est une submersion en ce point q. D'autre part, on a aussi

$$\Phi \cdot j^1\mathfrak{p} = \Phi\left((z,t), (a(z,t), a(z,t), z), \begin{pmatrix} a_z & a_t \\ b_z & b_t \\ 1 & 0 \end{pmatrix}\right) = -(a_t, b_t).$$

Cette application est une submersion si et seulement si son jacobien $\begin{pmatrix} a_{zt} & a_{tt} \\ b_{zt} & b_{tt} \end{pmatrix}$ est de rang plein, ce qui équivaut à dire que $a_{zt}b_{tt} - a_{tt}b_{zt} \neq 0$. Cette contrainte correspond exactement à la deuxième condition du Lemme 5.1.

□

Remarque 5.2 *Lorsque le plan tangent contient la direction de projection, la surface $\mathscr{M}$ peut toujours être localement paramétrisée en fonction de l'un des couples de variables suivants :* (x,t), (y,t) *ou*(z,t).

Notation 5.1 *Rappelons que Ω désigne l'ensemble image de la surface analytique réelle $\mathscr{M}$ par l'application* $\mathfrak{p}$. *For tout $j \in \mathbb{N}$ tel que $1 \leq j \leq 3$, posons :*

- $\sharp\mathfrak{p}^{-1}(\mathrm{P})$ *: nombre de préimages de* P, *comptées sans la multiplicité, par l'application* $\mathfrak{p}$ *;*
- $\Omega_i^j = \{\mathrm{P} \in \Omega \mid \sharp\mathfrak{p}^{-1}(\mathrm{P}) = i \text{ et } \mathrm{mult}_{(\mathrm{P})} = j\}$
- *Lorsque $i = j$ on notera simplement* $\Omega_j = \{\mathrm{P} \in \Omega \mid \mathrm{mult}_{(\mathrm{P})} = \sharp\mathfrak{p}^{-1}(\mathrm{P}) = j\}$;
- $\nabla f :=$ *gradient de f, $f \in C^\infty(\mathbb{R}^n, \mathbb{R})$;*
- *Pour* $\mathrm{P} \in \Omega_j$, $(q_\ell)_{1\leq\ell\leq j}$) *désigneront les préimages de* P *par l'application* $\mathfrak{p}$;
- $\mathscr{P}_\ell$ *: plan tangent à $\mathscr{M}$ au point q_ℓ ;*
- Π_ℓ *: l'image de $\mathscr{P}_\ell$ par l'application linéaire tangente au point q_ℓ;*
- $\mathscr{B}_0$ *: un produit d'intervalles fermés et bornés dans $\mathbb{R}^3$; on parlera tout simplement d'une boîte dans $\mathbb{R}^3$.*
- Σ_i *l'ensemble des solutions du système indicé par i.*
- *Pour tout intervalle* $\mathrm{I} \subset \mathbb{R}$, $l(\mathrm{I})$ *(respectivement* $u(\mathrm{I})$*) désignera la borne inférieure (respectivement supérieure) de* I.

Définition 5.7 *[Généricité]Demazure [8, section 4.11.3]*
Les fonctions C^∞, $f : \mathbb{R}^n \to \mathbb{R}$, dites ***génériques*** *forment un ouvert dense dans l'espace des fonctions $C^\infty(\mathbb{R}^n, \mathbb{R})$. Elles sont caractérisées par les propriétés suivantes :*

(a) les points critiques de f sont des points de ***Morses*** *;*

(b) les valeurs de f en ses points critiques sont deux à deux distinctes.

Définition 5.8

— **Point régulier de $\mathfrak{p}$.**
Un point $q \in \mathscr{M}$ est appelé point regular point de $\mathfrak{p}$ *si la matrice jacobienne associée à $\mathfrak{p}$ est de rang maximal au point q. Ce qui signifie, ici, que* $\mathrm{rank}(d\mathfrak{p})_q = 2$. *Cette définition équivaut à dire que le plan tangent à $\mathscr{M}$ au point q n'est pas vertical.*

— **Point critique de $\mathfrak{p}$.**
Un point $q \in \mathscr{M}$ est appelé un un point critique de $\mathfrak{p}$ *s'il est non régulier. Ce qui équivaut à dire que le plan tangent à $\mathscr{M}$ au point q est vertical* $\partial_t \mathrm{F}(q) = \partial_t \mathrm{G}(q) = 0$.

— **Point régulier de Ω.**
Un point $\mathrm{P} \in \Omega$ *est dit régulier si Ω est localement une sous-variété de dimension 2 dans $\mathbb{R}^3$. Tout point non régulier de Ω est appelé un* point singulier de Ω.

— **Solution régulière d'un système.**
Une solution d'un système de dimension 0 est dite régulière si le jacobien ne s'annule pas en ce point.

Définition 5.9

— **Point double.**
$P \in \Omega$ *est dit* point double *s'il admet exactement deux préimages régulières* q_1 *et* q_2 *dans* $\mathscr{M}$ *tels que* $\Pi_1 \cap \Pi_2$ *soit une droite. D'après la classification faite dans [20, Table 1],* P *est l'image par l'application* $\mathfrak{p}$ *d'une singularité de type* A_0^2.

— **Point triple.**
$P \in \Omega$ *est dit* point triple *s'il admet exactement trois préimages régulières* q_1, q_2 *et* q_2 *appartenant à* $\mathscr{M}$ *telles que* $\cap_{\{1\leq i\leq 3\}}\Pi_i$ *soit égale à un point. D'après la classification faite dans [20, Table 1],* P *est l'image par l'application* $\mathfrak{p}$ *d'une singularité de* A_0^3.

— **Cross-cap.**
$P \in \Omega$ *est un* cross-cap *sa préimage de est point critique* q *de* $\mathscr{M}$ *dont la singularité est de type cross-cap (voir la Définition 5.6) pour* $\mathfrak{p}$. *D'après la classification faite dans [20, Table 1],* P *est l'image par l'application* $\mathfrak{p}$ *d'une singularité de type* S_0.

Définition 5.10 *Imbach et al. [22]*
Soit $\mathscr{X}$ *un sous-ensemble de* $\mathbb{R}^n$. *Une suite de boites* $(X_i)_{i=1}^m$ *est appelée une* δ*-approximation de* $\mathscr{X}$ *si* $\mathscr{X} \subseteq \cup_{i=1}^m X_i$, *et pour tout* $i \in [\![1, m]\!]$, $l(X_i) \leq \delta$ *et* $\mathscr{X} \cap X_i \neq \emptyset$.

Proposition 5.1 *Golubistky and Guillemin [16, Lemma 4.3]*
Soient $\mathscr{E}$, $\mathscr{F}$ *des variétés différentiables,* $\mathscr{W}$ *une sous-variété de* $\mathscr{F}$ *et* $f : \mathscr{E} \to \mathscr{F}$ *une fonction différentiable. Si, pour tout* $q \in \mathscr{E}$ *tel que* $f(q) \in W$, *il existe un voisinage ouvert* $\mathscr{V} \subset \mathscr{F}$ *de* $f(q)$ *et une submersion* $\Phi : \mathscr{V} \to \mathbb{R}^k$ ($k = \operatorname{codim} \mathscr{W}$) , *tel que* $\mathscr{W} \cap \mathscr{U} = \Phi^{-1}(0)$, *alors* $f \pitchfork \mathscr{W}$ *au point* q *si et seulement si* $\Phi \circ f$ *est submersion au point* q.

Proposition 5.2 *Demazure [8, Corollary 3.7.3]*
Soient E, F *des espaces vectoriels,* $\mathscr{V}$ *et* $\mathscr{W}$ *des sous-variétés respectives de* E *et* F. *Soit* $f : \mathscr{V} \to F$ *une fonction de classe* C^∞, $n = \dim(\mathscr{V})$ *et* $m = \operatorname{codim}(\mathscr{W})$. *Si* f *est transverse à* $\mathscr{W}$ *alors* $f^{-1}(W)$ *est une sous-variété de dimension* $n - m$.

Proposition 5.3 *Demazure [8, Theorem 3.9.4]*
Soient E, F *deux espaces vectoriels de dimensions finies et* U *un ouvert de* E. *Si* W *une sous-variété de* $J^r(U;F)$, *où* r *est un entier naturel, alors l'ensemble des fonctions* $f \in C^\infty(U,F)$ *telles que* $j^r f$ *est transverse à* W *est est un sous-ensemble résiduel dense de* $C^\infty(U,F)$. *En d'autres termes, pour toute fonction générique* f *appartenant à* $C^\infty(U,F)$, *la fonction* $j^r f$ *est transverse à* W.

Proposition 5.4 *Demazure [8, Theorem 3.9.7]*
Soient E, F *deux espaces vectoriels de dimensions finies et* U *un ouvert de* E. *Soit* W *une sous-variété de* $J^r_{(n)}(U,F)$; *où* $r \geq 0$ *et* $n \geq 1$ *sont deux entiers naturels. L'ensemble des fonctions* $f \in C^\infty(U,F)$ *telles que* $j^r_{(n)} f$ *est transverse à* W *est un sous-ensemble résiduel dense de* $C^\infty(U,F)$.

5.2 Étude des singularités de $\Omega = \mathfrak{p}(\mathscr{M})$

Dans cette section, nous traitons trois questions fondamentales à la conception de l'algorithme qui calcule le graphe des singularités de Ω : il s'agit de l'identification des différents types de singularités qui apparaissent sur la surface, de la modélisation des singularités et de l'analyse sur la régularité de ces modèles dans un contexte générique. Nous apportons des réponses à ces questions à travers deux résultats principaux. Le Théorème 5.1 liste les types de singularités sur Ω. La sous-section 5.2.2 donne une caractérisation des singularités sous forme de systèmes d'équations. Le Théorème 5.2 établit la régularité des systèmes sous les propriétés de généricités décrites dans la sous-section 5.2.1.

5.2.1 Propriétés génériques de Ω

Le théorème suivant résume les propriétés de généricité d'une surface incluse dans $\mathbb{R}^4$ et projetée dans $\mathbb{R}^3$.

Théorème 5.1

(a) La surface générique $\mathscr{M}$ définie par $F = G = 0$ *est une sous-variété de dimension* 2 *dans* $\mathbb{R}^4$.

(b) Les singularités de la projection dans $\mathbb{R}^3$ *d'une surface générique incluse dans* $\mathbb{R}^4$ *sont : une courbe lisse de points double (une sous-variété de dimension 1) et un ensemble discret de points triples et de cross-caps.*

Démonstration
Le théoréme ci-dessus découle directement de l'application des Propositions 5.2 et 5.4 de Transversalité dans le cas des jets multiples. Nous commençons fixer quelques notations [1]. Soient $\Delta_{(n)}(U)$ le sous-ensemble de $U^n = U \times U \times \ldots \times U$ constitué des points $(a_1, \ldots, a_n)$ dont les coordonnées sont deux à deux distinctes dans U. On définit $J^r_{(n)}(U,F)$ comme étant l'espace des n-multijets d'ordre r de fonctions définies sur U vàleurs dans F.

(a) On considère le jet

$$\begin{aligned} j &: \mathbb{R}^4 \to J^0(\mathbb{R}^4, \mathbb{R}^2) \equiv \mathbb{R}^6 \\ & q \mapsto \big(q, F(q), G(q)\big) \end{aligned}$$

et on pose $W \subset J^0(\mathbb{R}^4, \mathbb{R}^2)$ tel que $F(q) = G(q) = 0$. W est une sous-variété $J^0(\mathbb{R}^4, \mathbb{R}^2)$ de co-dimension 2. D'après la Proposition 5.2, $\mathscr{M} = j^{-1}(W)$ est une sous-variété de dimension 2.

(b) On considére le 2-multijet défini par :

$$\begin{aligned} j^0_{(2)}(F,G) : \Delta_{(2)}(\mathbb{R}^4) &\to J^0_{(2)}(\mathbb{R}^4, \mathbb{R}^2) \\ (q_1, q_2) &\mapsto ((x_1, y_1, z_1, t_1), F(q_1), G(q_1), (x_2, y_2, z_2, t_2), F(q_2), G(q_2)); \end{aligned}$$

avec $q_i = (x_i, y_i, z_i, t_i)$ dans $\mathbb{R}^4$.
Soit W la sous-ensemble de $J^0_{(2)}(\mathbb{R}^4, \mathbb{R}^2)$ dont les points satisfont les contraintes suivantes

$$x_1 = x_2, y_1 = y_2, z_1 = z_2, F(q_1) = G(q_1) = F(q_2) = G(q_2) = 0.$$

W est une sous-variété de $J^0_{(2)}(\mathbb{R}^4, \mathbb{R}^2)$ de co-dimension 7. D'après la Proposition 5.4 l'ensemble des fonctions appartenant à $C^\infty(\mathbb{R}^4, \mathbb{R}^2)$ telles que $j^0_{(2)}(F,G)$ est transverse à W est un sous-ensemble résiduel dense de $C^\infty(\mathbb{R}^4, \mathbb{R}^2)$. La Proposition 5.2 implique que l'ensemble $J^0_{(2)}(\mathbb{R}^4, \mathbb{R}^2)$ des points dans Ω ayant deux préimages dans $\mathscr{M}$ est une sous-variété de dimension 1.
La démonstration pour le cas des points triples et cross-caps s'appuie, comme précédemment, sur les Propositons 5.4 et 5.2. Il suffit de considérer respectivement les éléments suivants :

$$\begin{aligned} j^0_{(3)}(F,G) : \Delta_{(3)}(\mathbb{R}^4) &\to J^0_{(3)}(\mathbb{R}^4, \mathbb{R}^2) \\ (q_1, q_2, q_3) &\mapsto \big(q_1, F(q_1), G(q_1), q_2, F(q_2), G(q_2), q_3, F(q_3), G(q_3)\big) \\ W \subset J^0_{(3)}(\mathbb{R}^4, \mathbb{R}^2) &\text{ tel que } x_1 = x_2 = x_3, y_1 = y_2 = y_3, z_1 = z_2 = z_3, F(q_i) = G(q_i) = 0, 1 \le i \le 3 \end{aligned}$$

et

$$\begin{aligned} j^1(F,G) : \mathbb{R}^4 &\to J^1(\mathbb{R}^4, \mathbb{R}^2) \\ q &\mapsto (q, F(q), G(q), \nabla F(q), \nabla G(q)) \\ W' \subset J^1(\mathbb{R}^4, \mathbb{R}^2) &\text{ tel que } F(q) = G(q) = \partial_t F(q) = \partial_t G(q) = 0. \end{aligned}$$

1. pour plus détails voir Demazure [8, §3.9.6]

□

Remarque 5.3
Les cas de figures listés ci-dessous n'apparaissent jamais pour une surface $\mathscr{M}$ en position générique :

- *Un point de Ω admet plus de trois préimages par la projection $\mathfrak{p}$;*
- *Un point de Ω admet comme préimages un point régulier de $\mathscr{M}$ et un cross-cap.*

On s'en aperçoit par un procédé similaire à (a) et (b) du Théorème 5.1. En effet, supposons que q_1, q_2, q_3, q_4 sont quatre points de $\mathscr{M}$ tels que $\mathfrak{p}(q_1) = \mathfrak{p}(q_2) = \mathfrak{p}(q_3) = \mathfrak{p}(q_4)$.
Soit

$$\begin{aligned} j_{(4)}(\mathrm{F},\mathrm{G}) : \Delta_{(4)}(\mathbb{R}^4) &\to \mathrm{J}^0_{(4)}(\mathbb{R}^4,\mathbb{R}^2) \\ (q_1,q_2,q_3,q_4) &\mapsto \big(q_1,\mathrm{F}(q_1),\mathrm{G}(q_1),\ldots,q_4,\mathrm{F}(q_4),\mathrm{G}(q_4)\big) \end{aligned}$$

et $\mathrm{W} \subset \mathrm{J}^0_{(4)}(\mathbb{R}^4,\mathbb{R}^2)$ satisfaisant les dix sept (17) contraintes ci-dessous

$$\begin{cases} x_i = x_j \text{ avec } i \neq j \in [\![1,4]\!] \\ y_i = y_j \text{ avec } i \neq j \in [\![1,4]\!] \\ z_i = z_j \text{ avec } i \neq j \in [\![1,4]\!] \\ \mathrm{F}(q_i) = \mathrm{G}(q_i) = 0 \ \forall i \in [\![1,4]\!] \end{cases} \tag{5.1}$$

D'après les Propositions 5.4 et 5.2, $j^{-1}_{(4)}(\mathrm{W})$ est de dimension -1. Ce qui signifie que cette situation n'est pas un cas générique. La deuxième remarque se justifie de la même manière.

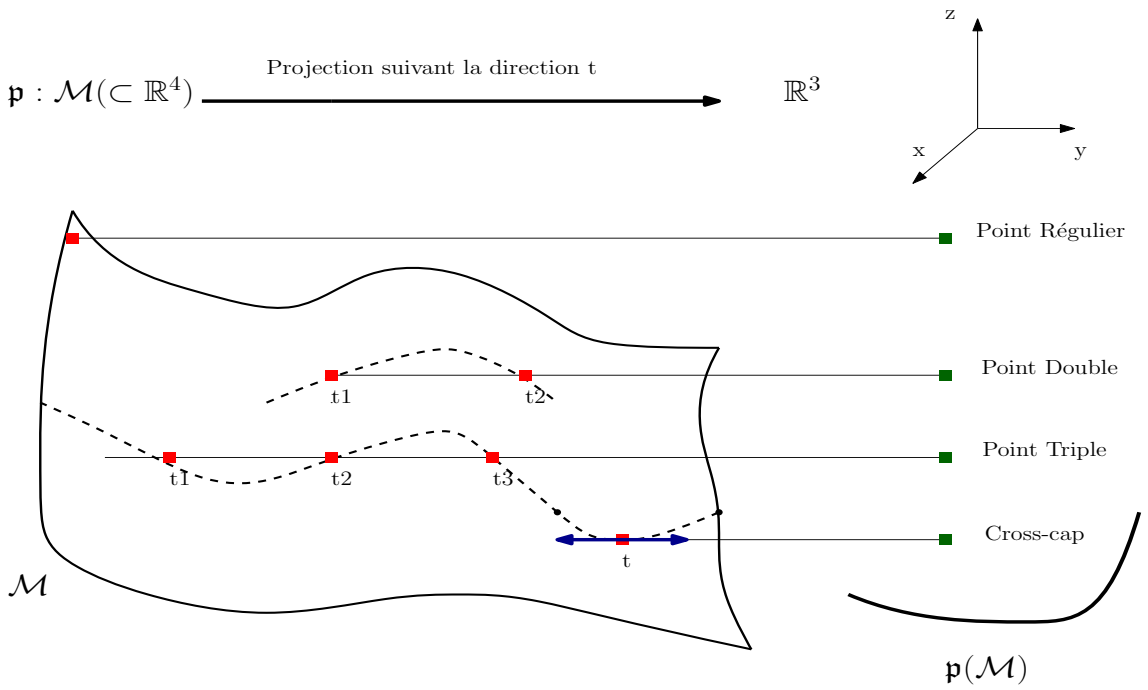
5.2.2 Caractérisation des singularités et régularité

Sous les propriétés de généricité énoncées dans section 5.2.1, la surface Ω est une union disjointe de points réguliers, de points triples et de cross-caps. Ces points sont caractérisés par les systèmes ci-dessous. La figure 5.2.2 illustre la géométrie des systèmes caractéristisant les singularités.

$$\begin{cases} \mathrm{F}(x,y,z,t_1) = 0, \\ \mathrm{G}(x,y,z,t_1) = 0, \\ \mathrm{F}(x,y,z,t_2) = 0, \\ \mathrm{G}(x,y,z,t_2) = 0, \\ t_1 \neq t_2. \end{cases} \tag{S-double}$$

$$\begin{cases} \mathrm{F}(x,y,z,t_1) = 0, \\ \mathrm{G}(x,y,z,t_1) = 0, \\ \mathrm{F}(x,y,z,t_2) = 0, \\ \mathrm{G}(x,y,z,t_2) = 0, \\ \mathrm{F}(x,y,z,t_3) = 0, \\ \mathrm{G}(x,y,z,t_3) = 0, \\ t_i \neq t_j \text{ avec } i \neq j. \end{cases} \tag{S-triple}$$

$$\begin{cases} \mathrm{F}(x,y,z,t) = 0, \\ \mathrm{G}(x,y,z,t) = 0, \\ \partial_t \mathrm{F}(x,y,z,t) = 0, \\ \partial_t \mathrm{G}(x,y,z,t) = 0. \end{cases} \tag{S-cross}$$



Types de singularités sur $\Omega = \mathfrak{p}(\mathcal{M})$ et leurs préimages

Remarque 5.4 *Les solutions du système (S-double) apparaissent par permutation des coordonnées t_1 et t_2. Par le même principe, une solution du système (S-triple) résulte trois paire de solutions du système (S-triple).*

Dans cette sous-section nous allons étudier la régularité des systèmes d'équations précédents. Plus précisément, nous établissons le résultat suivant.

Théorème 5.2
Sous les propriétés de généricité énoncées dans le Théorème 5.1, $\mathrm{P} = (x, y, z) \in \Omega$ *est un :*

(a) Point double si et seulement s'il admet deux préimages régulières (x, y, z, t_1) et (x, y, z, t_2), et la matrice jacobienne associée au système S-double soit de rang maximal au point (x, y, z, t_1, t_2).

(b) Point triple si et seulement s'il admet trois préimages régulières $q_i = (x, y, z, t_i)$ pour $i = 1, 2, 3$, tels que (x, y, z, t_1, t_2, t_3) est une solution régulière du système (S-triple).

(c) Cross-cap si et seulement si sa préimage est un point critique et solution régulière du système (S-cross).

Lemme 5.2
Soit P *un point de* Ω *et qui n'est pas une valeur critique de la projection* $\mathfrak{p}$. P *est un point régulier de* Ω *s'il admet exactement une seule préimage.*

Démonstration
Soient U un ouvert de $\mathbb{R}^3$ et $\mathfrak{p}^{\mathrm{U}}$ la restriction de $\mathfrak{p}$ sur $\mathfrak{p}^{-1}(\mathrm{U})$. Par hypothèse, P n'est pas une valeur critique de $\mathfrak{p}$, ce qui signifie qu'on peut trouver un voisinage $\mathrm{U} \subset \mathbb{R}^3$ de P qui ne contient aucune valeur critique de $\mathfrak{p}$, tel que $\mathfrak{p}^{\mathrm{U}\cap\Omega}$ est une immersion. Par ailleurs, P admet une seule préimage. Ce qui reste vrai reste vrai dans un voisinage certain $\mathrm{V} \subset \mathbb{R}^3$ de P. Ce qui implique la restriction $\mathfrak{p}^{\mathrm{V}\cap\Omega}$ est une application bijective. En résumé $\mathfrak{p}^{\mathrm{U}\cap\mathrm{V}\cap\Omega}$ est une immersion bijective dont un difféomorphisme. En conclusion $\mathfrak{p}^{\mathrm{U}\cap\mathrm{V}\cap\Omega}$ est un plongement et P est point régulier de Ω. □

Démonstration Théorème 5.2(a)
Soient P un point de Ω et q_1, q_2 ses préimages dans $\mathcal{M}$ par la projection $\mathfrak{p}$. Désignons par $\mathcal{P}_1$, $\mathcal{P}_2$ les plans tangent à $\mathcal{M}$ respectivement aux points q_1, q_2, et par Π_1, Π_2 les projections respectives de

$\mathscr{P}_1$, $\mathscr{P}_2$. On sait que $\mathscr{P}_1$, $\mathscr{P}_2$ ne sont pas verticaux car les préimages q_1, q_2 sont des points réguliers de $\mathfrak{p}$.

La matrice Jacobienne $\mathscr{J}_1$ associée à au système (S-double) est donnée par

$$\mathscr{J}_1 = \begin{pmatrix} \partial_x F_1 & \partial_y F_1 & \partial_z F_1 & \partial_{t_1} F_1 & 0 \\ \partial_x G_1 & \partial_y G_1 & \partial_z G_1 & \partial_{t_1} G_1 & 0 \\ \partial_x F_2 & \partial_y F_2 & \partial_z F_2 & 0 & \partial_{t_2} F_2 \\ \partial_x G_2 & \partial_y G_2 & \partial_z G_2 & 0 & \partial_{t_2} G_2 \end{pmatrix};$$

où les fonctions $F_i = F(x, y, z, t_i)$ et $G_i = G(x, y, z, t_i)$ dépendent de la variable t_i et ne dépendent pas de la variable t_j lorsque $i \neq j$.

— Tout d'abord, montrons que si $\Pi_1 \cap \Pi_2$ est une droite alors est de rang maximal au point (x, y, z, t_1, t_2).

La démontration se fait par contraposée. Supposons qu'il existe deux vecteurs non nuls $u = (u_x, u_y, u_z, u_1, u_2)$ et $v = (v_x, v_y, v_z, v_1, v_2)$ dans le noyau $Ker(\mathscr{J}_1)$. On a alors

$$\begin{cases} \nabla F(q_1) \cdot (u_x, u_y, u_z, u_1) = 0 \\ \nabla G(q_1) \cdot (u_x, u_y, u_z, u_1) = 0 \end{cases} \quad et \quad \begin{cases} \nabla F(q_2) \cdot (v_x, v_y, v_z, u_2) = 0 \\ \nabla G(q_2) \cdot (v_x, v_y, v_z, u_2) = 0 \end{cases}$$

où ∇f désigne le gradient de la fonction f. Par définition le plan tangent $\mathscr{P}_i$ à $\mathscr{M}$ au point q_i est constitué par l'ensemble des vecteurs simultanément orthogonaux à $\nabla F(q_i)$ et $\nabla G(q_i)$, donc

$$(u_x, u_y, u_z, u_1) \in \mathscr{P}_1 \qquad et \qquad (u_x, u_y, u_z, u_2) \in \mathscr{P}_2$$

Ce qui signifie que $(u_x, u_y, u_z) \in \Pi_1 \cap \Pi_2$. On montre de la même manière que si $v \in Ker(\mathscr{J}_1)$ alors $(v_x, v_y, v_z) \in \Pi_1 \cap \Pi_2$. Puisque $\Pi_1 \cap \Pi_2$ est une droite par hypothèse, alors il existe $\lambda \in \mathbb{R}$ tel que $\lambda(u_x, u_y, u_z) = (v_x, v_y, v_z)$.

Si $\lambda = 0$ alors $(v_x, v_y, v_z) = (0, 0, 0)$, donc le vecteur $(0, 0, 0, v_1)$ est dans le plan $\mathscr{P}_1$; ce qui est impossible car q_1 est un point régulier de $\mathfrak{p}$ donc $\mathscr{P}_1$ n'est pas vertical.

Si $\lambda \neq 0$, sachant que $\mathscr{P}_1$ n'est pas vertical, alors au moins une des dérivées partielles $\partial_t F$ et $\partial_t G$ ne s'annule pas au point q_1. Nous supposons, sans perte de géneéralité, que $\partial_t F(q_1) = \partial_{t_1} F_1 \neq 0$. Donc $u, v \in Ker(\mathscr{J}_1)$ implique que

$$\begin{cases} u_x \partial_x F_1 + u_y \partial_y F_1 + u_z \partial_z F_1 + u_1 \partial_{t_1} F_1 = 0 \\ v_x \partial_x F_1 + v_y \partial_y F_1 + v_z \partial_z F_1 + v_1 \partial_{t_1} F_1 = 0 \end{cases}$$

En multipliant la première par λ, en remplaçant (v_x, v_y, v_z) par $\lambda(u_x, u_y, u_z)$ et en prenant la différence, on obtient

$$\begin{aligned} & (\lambda u_1 - v_1)\partial_{t_1} F_1 = 0 \\ \Rightarrow \qquad & \lambda u_1 - v_1 = 0 \\ \Rightarrow \qquad & v_1 = \lambda u_1 \end{aligned}$$

On démontre aussi par la même méthode qu'au point q_2, où le plan tangent $\mathscr{P}_2$ n'est pas vertical, $v_2 = \lambda u_2$. Ce qui signifie que les vecteurs u et v sont colinéaires. Donc $\dim(Ker(\mathscr{J}_1)) = 1$ et $\mathscr{J}_1$ est de rang maximal.

— Inversement, supposons que la matrice Jacobienne est de rang maximal. Si $\Pi_1 \cap \Pi_2$ n'est pas une droite alors $\Pi := \Pi_1 = \Pi_2$ est un plan. Il existe alors deux vecteurs linéaires indépendants (u_x, u_y, u_z) et (v_x, v_y, v_z) dans Π

Soit $u = (u_x, u_y, u_z, u_1, u_2)$ le vecteur tel que (u_x, u_y, u_z, u_i) est la préimage de (u_x, u_y, u_z) dans $\mathscr{P}_i$. Par définition des plans tangents, on a

$$\begin{cases} \nabla \mathrm{F}(q_1)\cdot(u_x,u_y,u_z,u_1)=0 \\ \nabla \mathrm{G}(q_1)\cdot(u_x,u_y,u_z,u_1)=0 \\ \nabla \mathrm{F}(q_2)\cdot(v_x,v_y,v_z,u_2)=0 \\ \nabla \mathrm{G}(q_2)\cdot(v_x,v_y,v_z,u_2)=0 \end{cases}$$

donc, u appartient à $Ker(\mathscr{J}_1)$. De la même manière, soit $v=(v_x,v_y,v_z,v_1,v_2)$ le vecteur tel que (v_x,v_y,v_z,v_i) est la préimage de (v_x,v_y,v_z) dans $\mathscr{P}_i$, on a montre aussi que v appartient à $Ker(\mathscr{J}_1)$. Puisque les vecteurs (u_x,u_y,u_z) et (v_x,v_y,v_z) sont linéairement indépendant alors les vecteurs u et v sont aussi linéairement indépendants. Par conséquent, $\dim(Ker(\mathscr{J}_1))\geq 2$ et donc $\mathscr{J}_1$ n'est pas de rang maximal. Ainsi, $\Pi_1\cap\Pi_2$ est nécessairement une droite.

□

Démonstration Théorème 5.2(b)
Soient P un point de Ω et q_1,q_2,q_3 ses préimages régulières dans $\mathscr{M}$ par la projection $\mathfrak{p}$. Soit $\mathscr{P}_i$ le plan tangent à $\mathscr{M}$ au point q_i. Notons que $\mathscr{P}_i$ n'est pas vertical car q_i est un point régulier de $\mathfrak{p}$. La matrice Jacobienne $\mathscr{J}_2$ associée au système (S-triple) est donnée par

$$\mathscr{J}_2=\begin{pmatrix} \partial_x \mathrm{F}_1 & \partial_y \mathrm{F}_1 & \partial_z \mathrm{F}_1 & \partial_{t_1}\mathrm{F}_1 & 0 & 0 \\ \partial_x \mathrm{G}_1 & \partial_y \mathrm{G}_1 & \partial_z \mathrm{G}_1 & \partial_{t_1}\mathrm{G}_1 & 0 & 0 \\ \partial_x \mathrm{F}_2 & \partial_y \mathrm{F}_2 & \partial_z \mathrm{F}_2 & 0 & \partial_{t_2}\mathrm{F}_2 & 0 \\ \partial_x \mathrm{G}_2 & \partial_y \mathrm{G}_2 & \partial_z \mathrm{G}_2 & 0 & \partial_{t_2}\mathrm{G}_2 & 0 \\ \partial_x \mathrm{F}_3 & \partial_y \mathrm{F}_3 & \partial_z \mathrm{F}_3 & 0 & 0 & \partial_{t_3}\mathrm{F}_3 \\ \partial_x \mathrm{G}_3 & \partial_y \mathrm{G}_3 & \partial_z \mathrm{G}_3 & 0 & 0 & \partial_{t_3}\mathrm{G}_3 \end{pmatrix}$$

Si $\mathscr{J}_2$ est non inversible alors il existe un vector non nul $v=(v_x,v_y,v_z,v_1,v_2,v_3)\in Ker(\mathscr{J}_2)$. En d'autres termes,

$$\nabla \mathrm{F}(q_i)\cdot(v_x,v_y,v_z,v_i)=\nabla \mathrm{G}(q_i)\cdot(v_x,v_y,v_z,v_i)=0$$

ce qui signifie que

$$(v_x,v_y,v_z,v_i)\in\mathscr{P}_i.$$

Par conséquent, on a d'une part

$$(v_x,v_y,v_z)\in\cap_{i=1}^3\Pi_i$$

et d'autre part, $\mathscr{P}_i$ n'étant pas vertical alors (v_x,v_y,v_z) est non nul. Ce qui signifie que $\cap_{i=1}^3\Pi_i$ est un point.

Inversement, si $\cap_{i=1}^3\Pi_i$ n'est pas un alors il existe un vecteur non nul $(v_x,v_y,v_z)\in\cap_{i=1}^3\Pi_i$. Soit $(v_x,v_y,v_z,v_i)\in\mathscr{P}_i$ la préimage de (v_x,v_y,v_z), on a

$$\nabla \mathrm{F}(q_i)\cdot(v_x,v_y,v_z,v_i)=\nabla \mathrm{G}(q_i)\cdot(v_x,v_y,v_z,v_i)=0;$$

c'est-à-dire que

$$\det\big(\mathscr{J}_2(v_x,v_y,v_z,v_1,v_2,v_3)\big)=0$$

donc $\mathscr{J}_2$ n'est pas inversible. Ce qui est impossible. □

Le Lemme ci-dessous est un résultat clés dans la dans démonstration du Théorème 5.2(c).

Lemme 5.3 *Demazure [8, Lemma 4.2.1]*
Soient $\mathrm{I}\subset\mathbb{R}$ *un intervalle contenant* 0, $\mathrm{U}\subset\mathbb{R}^p$ *un ouvert, et* $f(x,y)=f(x,y_1,\ldots,y_\mathrm{P})$ *une fonction* C^∞ *sur* $\mathrm{I}\times\mathrm{U}$. *Alors il existe une unique fonction* $g(x,y)$ *de classe* C^∞ *sur* $\mathrm{I}\times\mathrm{U}$ *telle que* $f(x,y)-f(0,y)=x\cdot g(x,y)$. *De plus,*

$$g(0,y)=\frac{\partial f}{\partial x}(0,y).$$

Démonstration Théorème 5.2(c)
Tout d'abord, notons qu'une solution q du (S-cross) est un point appartenant à $\mathscr{M}$ tel que $\partial_t \mathrm{F}(q) = \partial_t \mathrm{G}(q) = 0$. Donc le plan tangent $\mathscr{P}$ à $\mathscr{M}$ au point q est vertical ; d'où la première la condition d'un cross-cap (voir Lemme 5.1) est vérifiée.

Supposons, sans perte de généralité, que la surface $\mathscr{M}$ est paramétrisée par rapport aux variables z et t. En effet, $\nabla \mathrm{F}(q)$ et $\nabla \mathrm{G}(q)$ sont indépendants donc il existe un mineur de taille 2×2 de determinant non nul. Si l'on suppose que $\det \begin{pmatrix} \partial_x \mathrm{F}(q) & \partial_y \mathrm{F}(q) \\ \partial_x \mathrm{G}(q) & \partial_y \mathrm{G}(q) \end{pmatrix} \neq 0$ alors, d'après le Théorème des Fonctions Implicites, $\mathscr{M}$ est localement l'image d'une fonction qui $(z,t) \mapsto (a(z,t), b(z,t), z, t)$, où a et b sont deux fonctions différentiables. En d'autre termes, $\mathscr{M}$ est le lieu des zéros des fonctions

$$\begin{cases} \tilde{\mathrm{F}}(x,y,z,t) &= -x + a(z,t) \\ \tilde{\mathrm{G}}(x,y,z,t) &= -y + b(z,t) \end{cases}$$

La matrice Jacobienne associée au système (S-cross), en utilisant les fonctions $\tilde{\mathrm{F}}$ et $\tilde{\mathrm{G}}$, est alors donnée par

$$\tilde{\mathscr{J}}_3 = \begin{pmatrix} -1 & 0 & \partial_z(a) & \partial_t(a) \\ 0 & -1 & \partial_z(b) & \partial_t(b) \\ 0 & 0 & \partial_{zt}(a) & \partial_{tt}(a) \\ 0 & 0 & \partial_{zt}(b) & \partial_{tt}(b) \end{pmatrix}$$

et son déterminant vaut $\det(\tilde{\mathscr{J}}_3) = \partial_{zt}(a)\partial_{tt}(b) - \partial_{tt}(a)\partial_{zt}(b)$, ce qui est précisément la quantité requise dans la seconde condition pour un cross-cap dans Lemme 5.1. En somme, nous venons de montrer que P est un cross-cap si et seulement si

$$\det(\tilde{\mathscr{J}}_3) \neq 0.$$

Il reste alors à montrer que $\det(\tilde{\mathscr{J}}_3) \neq 0$ si et seulement si $\det(\mathscr{J}_3) \neq 0$ où $\mathscr{J}_3$ est la matrice Jacobienne associée au système (S-cross) :

$$\mathscr{J}_3 = \begin{pmatrix} \partial_x \mathrm{F} & \partial_y \mathrm{F} & \partial_z \mathrm{F} & 0 \\ \partial_x \mathrm{G} & \partial_y \mathrm{G} & \partial_z \mathrm{G} & 0 \\ \partial_{xt} \mathrm{F} & \partial_{yt} \mathrm{F} & \partial_{zt} \mathrm{F} & \partial_{tt} \mathrm{F} \\ \partial_{xt} \mathrm{G} & \partial_{yt} \mathrm{G} & \partial_{zt} \mathrm{G} & \partial_{tt} \mathrm{G} \end{pmatrix}$$

On applique le Lemme 5.3 deux fois successivement. Tout d'abord à la fonction $\mathrm{F}(a+\mathrm{X}, b+\mathrm{Y}, z, t)$ par rapport à la variable X :

$$\mathrm{F}(a+\mathrm{X}, b+\mathrm{Y}, z, t) - \mathrm{F}(a, b+\mathrm{Y}, z, t) = \mathrm{X} g_1(\mathrm{X}, b+\mathrm{Y}, z, t) \tag{5.2}$$

avec

$$g_1(0, b+\mathrm{Y}, z, t) = \partial_x \mathrm{F}(a, b+\mathrm{Y}, z, t). \tag{5.3}$$

Ensuite, à la fonction $\mathrm{F}(a, b+\mathrm{Y}, z, t)$ par rapport à la variable Y :

$$\mathrm{F}(a, b+\mathrm{Y}, z, t) - \mathrm{F}(a, b, z, t) = \mathrm{Y} g_2(\mathrm{Y}, z, t)$$

avec

$$g_2(0, z, t) = \partial_y \mathrm{F}(a, b, z, t). \tag{5.4}$$

Par définition de la paramétrisation $(z,t) \mapsto (a(z,t), b(z,t), z, t)$, pour tout point sur la surface $\mathscr{M}$ suffisamment proche de q, $\mathrm{F}(a(z,t), b(z,t), z, t) = 0$, donc l'égalité (5.2) devient

$$\mathrm{F}(a+\mathrm{X}, b+\mathrm{Y}, z, t) = \mathrm{X} g_1(\mathrm{X}, b+\mathrm{Y}, z, t) + \mathrm{Y} g_2(\mathrm{Y}, z, t) \tag{5.5}$$

Considérons le changement de variable suivant :

$$\mathrm{X} = x - a(z,t)$$

$$\mathrm{Y} = y - b(z,t)$$

Par substitution X et Y dans les équations (5.5), (5.3) et (5.4), on obtient

$$\mathrm{F}(x,y,z,t) = -\tilde{\mathrm{F}}(x,y,z,t)g_1(x+a,y,z,t) - \tilde{\mathrm{G}}(x,y,z,t)g_2(b+y,z,t) \tag{5.6}$$

$$g_1(0,y,z,t) = \partial_x \mathrm{F}(a,y,z,t)$$

$$g_2(0,z,t) = \partial_y \mathrm{F}(a,b,z,t)$$

De façon similaire, en appliquant le Lemme 5.3 à la fonction $\mathrm{G}(a+\mathrm{X}, b+\mathrm{Y}, z, t)$, on démontre qu'il existe deux fonctions h_1 et h_2 telles que

$$\mathrm{G}(x,y,z,t) = -\tilde{\mathrm{F}}(x,y,z,t)h_1(x+a,y,z,t) - \tilde{\mathrm{G}}(x,y,z,t)h_2(b+y,z,t) \tag{5.7}$$

avec

$$h_1(0,y,z,t) = \partial_x \mathrm{G}(a,y,z,t)$$

$$h_2(0,z,t) = \partial_y \mathrm{G}(a,b,z,t)$$

Les relations (5.6) et (5.7) peuvent être réécrites comme suit

$$\begin{pmatrix} \mathrm{F} \\ \mathrm{G} \end{pmatrix} = \underbrace{-\begin{pmatrix} g_1 & g_2 \\ h_1 & h_2 \end{pmatrix}}_{\mathscr{A}} \begin{pmatrix} \tilde{\mathrm{F}} \\ \tilde{\mathrm{G}} \end{pmatrix} = \mathscr{A} \begin{pmatrix} \tilde{\mathrm{F}} \\ \tilde{\mathrm{G}} \end{pmatrix}$$

Notons que, au point q, $\mathscr{A}(q) = -\begin{pmatrix} \partial_x \mathrm{F}(q) & \partial_y \mathrm{F}(q) \\ \partial_x \mathrm{G}(q) & \partial_y \mathrm{G}(q) \end{pmatrix}$ et par hypothèse $\det \mathscr{A}(q) \neq 0$. La dérivé par rapport à t donne

$$\begin{pmatrix} \partial_t \mathrm{F} \\ \partial_t \mathrm{G} \end{pmatrix} = \partial_t \mathscr{A} \begin{pmatrix} \tilde{\mathrm{F}} \\ \tilde{\mathrm{G}} \end{pmatrix} + \mathscr{A} \begin{pmatrix} \partial_t \tilde{\mathrm{F}} \\ \partial_t \tilde{\mathrm{G}} \end{pmatrix}$$

Le système des cross-caps peut-être réécrit comme suit

$$\underbrace{\begin{pmatrix} \mathrm{F} \\ \mathrm{G} \\ \partial_t \mathrm{F} \\ \partial_t \mathrm{G} \end{pmatrix}}_{\mathscr{F}} = \underbrace{\begin{pmatrix} \mathscr{A} & 0 \\ \partial_t \mathscr{A} & \mathscr{A} \end{pmatrix}}_{\mathscr{N}} \underbrace{\begin{pmatrix} \tilde{\mathrm{F}} \\ \tilde{\mathrm{G}} \\ \partial_t \tilde{\mathrm{F}} \\ \partial_t \tilde{\mathrm{G}} \end{pmatrix}}_{\tilde{\mathscr{F}}} \tag{5.8}$$

Les déterminants valent $\mathscr{J}_3 = \det(Jac(\mathscr{F})) = \begin{pmatrix} \nabla \mathrm{F} \\ \nabla \mathrm{G} \\ \nabla(\partial_t \mathrm{F}) \\ \nabla(\partial_t \mathrm{G}) \end{pmatrix}$ et $\tilde{\mathscr{J}}_3 = \det(Jac(\tilde{\mathscr{F}}))$. La dérivé de (5.8) par rapport à toute variable vaut $\partial\mathscr{F} = \partial(\mathscr{N} \times \tilde{\mathscr{F}}) = \partial\mathscr{N} \times \tilde{\mathscr{F}} + \mathscr{N} \times \partial\tilde{\mathscr{F}}$, et sachant qu'en tout point q, $\tilde{\mathscr{F}}(q) = 0$, ce qui implique que $\partial\mathscr{F}(q) = \mathscr{N}(q) \times \partial\tilde{\mathscr{F}}(q)$. Au point q, nous avons l'égalité $\mathscr{J}_3(q) = \mathscr{N}(q) \times \tilde{\mathscr{J}}_3(q)$, et puisque $\det \mathscr{N}(q) = \det \mathscr{A}(q)^2 \neq 0$ nous en concluons que

$$\det \mathscr{J}_3(q) \neq 0 \Leftrightarrow \det \tilde{\mathscr{J}}_3(q) \neq 0 \tag{5.9}$$

□

5.2.3 Ball-system

Tout comme dans le cas de la projection d'une courbe dans l'espace (voir la section 4.3 du chapitre 4), le système (S-double) devient numériquement instable lorsque t_1 est suffisamment proche de t_2. En effet, on observe une chute de la dimension du système partout où $t_1 = t_2$. En s'inspirant de la technique du **ball-system** développée dans Imbach et al. [21], nous construisons un nouveau système (S-ball) dont les solutions régulières sont la courbe des points doubles et les cross-caps. Soit A une fonction analytique réelle dans $\mathbb{R}^4$, on définit les opérateurs S. et D. comme suit :

$$\mathrm{S.A}(x,y,z,c,r) = \begin{cases} \frac{1}{2}(\mathrm{A}(x,y,z,c+\sqrt{r}) + \mathrm{A}(x,y,z,c-\sqrt{r})) & si\ r>0 \\ \mathrm{A}(x,y,z,c) & si\ r=0 \\ \frac{1}{2}(\mathrm{A}(x,y,z,c+i\sqrt{-r}) + \mathrm{A}(x,y,z,c-i\sqrt{-r})) & si\ r<0 \end{cases}$$

et

$$\mathrm{D.A}(x,y,z,c,r) = \begin{cases} \frac{1}{2\sqrt{r}}(\mathrm{A}(x,y,z,c+\sqrt{r}) - \mathrm{A}(x,y,z,c-\sqrt{r})) & si\ r>0 \\ \partial_t \mathrm{A}(x,y,z,c) & si\ r=0 \\ \frac{1}{2i\sqrt{-r}}(\mathrm{A}(x,y,z,c+i\sqrt{-r}) - \mathrm{A}(x,y,z,c-i\sqrt{-r})) & si\ r<0 \end{cases}$$

On définit le *ball system* comme suit :

$$\begin{cases} \mathrm{S.F}(x,y,z,c,r) &= 0 \\ \mathrm{S.G}(x,y,z,c,r) &= 0 \\ \mathrm{D.F}(x,y,z,c,r) &= 0 \\ \mathrm{D.G}(x,y,z,c,r) &= 0 \end{cases} \qquad \text{(S-ball)}$$

Nous pouvons distinguer deux cas de figures : $r>0$ et $r=0$

$$(\mathrm{S}-ball)_{r>0} \begin{cases} \frac{1}{2}(\mathrm{F}(x,y,z,c+\sqrt{r}) + \mathrm{F}(x,y,z,c-\sqrt{r})) = 0 \\ \frac{1}{2}(\mathrm{G}(x,y,z,c+\sqrt{r}) + \mathrm{G}(x,y,z,c-\sqrt{r})) = 0 \\ \frac{1}{2\sqrt{r}}(\mathrm{F}(x,y,z,c+\sqrt{r}) - \mathrm{F}(x,y,z,c-\sqrt{r})) = 0 \\ \frac{1}{2\sqrt{r}}(\mathrm{G}(x,y,z,c+\sqrt{r}) - \mathrm{G}(x,y,z,c-\sqrt{r})) = 0 \end{cases}$$

$$(\mathrm{S}-ball)_{r=0} \begin{cases} \mathrm{F}(x,y,z,c) = 0 \\ \mathrm{G}(x,y,z,c) = 0 \\ \partial_c \mathrm{F}(x,y,z,c) = 0 \\ \partial_c \mathrm{G}(x,y,z,c) = 0 \end{cases}$$

Lemme 5.4
L'ensemble image par la projection dans le $\mathbb{R}^3$ des solutions du ball system lorsque $r \geq 0$ est égale à la projection dans $\mathbb{R}^3$ des solutions des systèmes (S-double) et (S-cross).

Démonstration
Soit (x,y,z,c,r) une solution du ball system. Si $r=0$, alors le ball system est égale au système (S-cross). Si $r>0$, en faisant convenablement le changement de variables $t_1 = c-\sqrt{r}$, $t_2 = c+\sqrt{r}$ dans le ball system, on retrouve le système (S-double) (on multiplie les deux dernières équations du ball system par $\sqrt{r}$ et on les additionne ou soustrait aux deux premières équations). □

Théorème 5.3
Les solutions régulières du ball system pour $r \geq 0$ sont équivalentes (à transformations près) aux solutions régulières des systèmes (S-double) et (S-cross). En d'autres termes, $\mathrm{P} = (x,y,z) \in \Omega$ *est un*

- *(c_1) Point Double si et seulement si il admet deux préimages régulières (x,y,z,t_1) et (x,y,z,t_2) avec $t_1 \neq t_2$ telles que $(x,y,z,(t_1+t_2)/2,(t_1-t_2)^2)$ soit une solution régulière du système (S-ball).*
- *(c_2) Cross-cap si et seulement si sa préimage est un point critique (x,y,z,t) telle que $(x,y,z,t,0)$ soit une solution régulière du système (S-ball).*

Notons tout d'abord que, les fonctions S.F, S.G, D.F et D.G sont analytiques. Le Lemme 5.3 est une variante du Imbach et al. [21, Lemma 6] adaptée aux fonctions définies sur $\mathbb{R}^4$ à valeurs dans $\mathbb{R}$.

Lemme 5.5
Si A *est une fonction analytique réelle, alors les fonctions* S.A *et* D.A *le sont aussi. De plus, les dérivées de* S.A *par rapport à* x, y, z, c, r *sont respectivement* $\mathrm{S.A}_x, \mathrm{S.A}_y, \mathrm{S.A}_z, \mathrm{S.A}_t, \frac{1}{2}\mathrm{D.A}_t$. *Les dérivées de* D.A *par rapport à* x, y, z, c, r *sont respectivement* $\mathrm{D.A}_x, \mathrm{D.A}_y, \mathrm{D.A}_z, \mathrm{D.A}_t$ *et* $\frac{1}{2r}(\mathrm{S.A} - \mathrm{D.A})$ *si* $r > 0$ *et* $\frac{1}{6}\mathrm{A}_{tt}$ *si* $r = 0$.

Démonstration Théorème 5.3
Pour $r = 0$, le système (S-ball) est équivalent au système (S-cross). Dans ce cas de figure, le Lemme se ramène au Théorème 5.2(c).

Pour $r > 0$, d'après le Lemme 5.5, la Jacobienne du système (S-ball) est donnée par

$$\mathscr{J}_{(c,r>0)} = \begin{pmatrix} \mathrm{S.}\partial_x\mathrm{F} & \mathrm{S.}\partial_y\mathrm{F} & \mathrm{S.}\partial_z\mathrm{F} & \mathrm{S.}\partial_t\mathrm{F} & \frac{\mathrm{D.}\partial_t\mathrm{F}}{2} \\ \mathrm{S.}\partial_x\mathrm{G} & \mathrm{S.}\partial_y\mathrm{G} & \mathrm{S.}\partial_z\mathrm{G} & \mathrm{S.}\partial_t\mathrm{G} & \frac{\mathrm{D.}\partial_t\mathrm{G}}{2} \\ \mathrm{D.}\partial_x\mathrm{F} & \mathrm{D.}\partial_y\mathrm{F} & \mathrm{D.}\partial_z\mathrm{F} & \mathrm{D.}\partial_t\mathrm{F} & \frac{\mathrm{S.}\partial_t\mathrm{F}-\mathrm{D.F}}{2r} \\ \mathrm{D.}\partial_x\mathrm{G} & \mathrm{D.}\partial_y\mathrm{G} & \mathrm{D.}\partial_z\mathrm{G} & \mathrm{D.}\partial_t\mathrm{G} & \frac{\mathrm{S.}\partial_t\mathrm{G}-\mathrm{D.G}}{2r} \end{pmatrix}$$

Soit $q = (x, y, z, c, r)$ une solution du ball système (S-ball) pour $r > 0$, $\mathscr{J}_{(c,r>0)}$ peut être simplifié compte tenu du fait que $\mathrm{D.F}(q) = \mathrm{D.G}(q) = 0$. Soient $q_1 = (x, y, z, c + \sqrt{r})$ et $q_2 = (x, y, z, c - \sqrt{r})$ deux points sur $\mathscr{M}$ tels que le point $(x, y, z, c + \sqrt{r}, c - \sqrt{r})$ soit une solution du système (S-double) (voir Lemme 5.4). En appliquant successivement les combinaisons linéaires aux lignes et colonnes de la matrice $\mathscr{J}_{(c,r>0)}$:

- $\ell_3 \longleftarrow \sqrt{r} \times \ell_3$
- $\ell_4 \longleftarrow \sqrt{r} \times \ell_4$
- $c_5 \longleftarrow (2\sqrt{r})c_5$
- $\ell_1 \longleftarrow \ell_1 + \ell_3$
- $\ell_3 \longleftarrow \ell_1 - \ell_3$
- $\ell_2 \longleftarrow \ell_2 + \ell_4$
- $\ell_4 \longleftarrow \ell_2 - \ell_4$

on a :

$$\det \mathscr{J}_{(c,r>0)} = 0 \Longleftrightarrow \det \begin{pmatrix} \partial_x\mathrm{F}(q_1) & \partial_y\mathrm{F}(q_1) & \partial_z\mathrm{F}(q_1) & \partial_t\mathrm{F}(q_1) & \partial_t\mathrm{F}(q_1) \\ \partial_x\mathrm{G}(q_1) & \partial_y\mathrm{G}(q_1) & \partial_z\mathrm{G}(q_1) & \partial_t\mathrm{G}(q_1) & \partial_t\mathrm{G}(q_1) \\ \partial_x\mathrm{F}(q_2) & \partial_y\mathrm{F}(q_2) & \partial_z\mathrm{F}(q_2) & \partial_t\mathrm{F}(q_2) & -\partial_t\mathrm{F}(q_2) \\ \partial_x\mathrm{G}(q_2) & \partial_y\mathrm{G}(q_2) & \partial_z\mathrm{G}(q_2) & \partial_t\mathrm{G}(q_2) & -\partial_t\mathrm{G}(q_2) \end{pmatrix} = 0$$

En faisant les transformations suivante $c_4 \longleftarrow \frac{1}{2}(c_4 + c_5)$ et $c_5 \longleftarrow \frac{1}{2}(c_4 - c_5)$, on a

$$\det \mathscr{J}_{(c,r>0)} = 0 \Longleftrightarrow \det \begin{pmatrix} \partial_x\mathrm{F}(q_1) & \partial_y\mathrm{F}(q_1) & \partial_z\mathrm{F}(q_1) & \partial_t\mathrm{F}(q_1) & 0 \\ \partial_x\mathrm{G}(q_1) & \partial_y\mathrm{G}(q_1) & \partial_z\mathrm{G}(q_1) & \partial_t\mathrm{G}(q_1) & 0 \\ \partial_x\mathrm{F}(q_2) & \partial_y\mathrm{F}(q_2) & \partial_z\mathrm{F}(q_2) & 0 & \partial_t\mathrm{F}(q_2) \\ \partial_x\mathrm{G}(q_2) & \partial_y\mathrm{G}(q_2) & \partial_z\mathrm{G}(q_2) & 0 & \partial_t\mathrm{G}(q_2) \end{pmatrix} = 0$$

On peut voir que la matrice de droite est exactement la Jacobienne associée au système d'équations (S-double). Ce qui veut dire que, pour $r > 0$, le Lemme se ramène au Lemme **??**. □

Soit $\mathscr{F} : \mathbb{R}^5 \longrightarrow \mathbb{R}^4$ une fonction différentiable dont les composantes sont données par les équations du système (S-ball). Soit $\mathscr{C}$ la courbe lisse définie par $\mathscr{C} := \{(x, y, z, c, r) \in \mathbb{R}^4 \times \mathbb{R}^+ \mid \mathscr{F}(x, y, z, c, r) = 0\}$; i.e $\mathscr{C}$ est l'ensemble des solutions de (S-ball).

5.3 Algorithme

Cette section est dédiée à l'élaboration d'un algorithme qui décrit une représentation correcte de la topologie du graphe des singularités de Ω (si elle existe[2]) ; i.e Ω_{sing}.

L'algorithme prend en entrée une surface lisse $\mathscr{M}$. Elle est définie de façon implicite comme étant l'ensemble des solutions réelles communes dans $\mathbb{R}^4$ des équations $F(x,y,z,t) = G(x,y,z,t) = 0$. Sous certaines hypothèses, aussi appelées hypothèses de généricité, l'algorithme renvoie un structure linéaires par morceaux qui est isotope à la partie singulière de $\Omega = \mathfrak{p}(\mathscr{M})$; où $\mathfrak{p} : \mathscr{M} \to \mathbb{R}^3$ qui à tout $(x,y,z,t) \mapsto (x,y,z)$. Il est basé sur deux principaux sous-programmes, considérés ici comme des boites noires. Le premier, appelé `IsolatingBoxes`[3] (voir (algorithm2)), est un algorithme qui prend en entrée un système d'équations zéro dimensionnel régulier, une boite initiale (domaine fermé dans lequel on cherche à résoudre le système) et un paramètre (un entier naturel strictement positif), et renvoie un ensemble de boites d'isolation deux à deux disjointes, telles que chaque boite contient exactement une solution du système. Le sous-programme 2 utilise la méthode de subdivision et le paramètre indique la largeur minimale des boites de sortie. Cette dernière dépend de la proximité de la solution à isoler par rapport au bord de la boite initiale. Dans la sous-section, on fait appel à `IsolateSols` pour isoler les solutions des systèmes (S-triple), (S-cross), du système des points x-critiques et les points au bord de la courbe $\mathscr{C}$ avec la boite initiale.

Le deuxième sous-programme, appelé ici `δ-Approx` (voir algorithme4), permet de faire du suivi courbe couramment appelé *tracking curve*. Il prend en entrée un ensemble discret **E** de points dans un espace prédéfini et renvoie un ensemble dont chaque élement est une suite de boites adjacentes qui englobent la composante connexe qui relie des points distinctes de **E**. Les éléments de **E**, souvent appelés *tracking points* (qui signifie en anglais points de suivi), sont constitués des points du bord d'une boite d'isolation donnée. Cet algorithme est utilisé dans la sous-section 5.3.3 pour déterminer une représentation correcte des composantes connexes de la courbe lisse $\mathscr{C}$ dans $\mathbb{R}^5$ ainsi que sa projection dans $\mathbb{R}^3$.

ALGORITHME GÉNÉRAL

— `Entrée:`

- `Une surface lisse` $\mathscr{M} := \{(x,y,z,t) \in \mathscr{B}_0 \times \mathbb{R}, F(x,y,z,t) = G(x,y,z,t) = 0\}$; où $\mathscr{B}_0 = \mathbf{I}_x \times \mathbf{I}_y \times \mathbf{I}_z$ `est une boite fermée de` $\mathbb{R}^3$ et
- `un nombre réel positif` δ

— `Sortie: Graphe des singularités représentant` Ω_{sing}.

1. $B^{sol}_{cross} \leftarrow$`IsolatingBoxes(S-cross,` $\mathscr{B}_{cross}$`,`δ`)`, $B^{sol}_{x-crit} \leftarrow$`IsolatingBoxes(S-xcrit,`$\mathscr{B}_{ball}$`,`$\delta$`)` avec $\mathscr{B}_{cross} := \mathscr{B}_0 \times [-T,T]$ et $\mathscr{B}_{ball} := \mathscr{B}_0 \times [-T,T] \times [0,T^2]$: Isoler les cross-caps et les points x-critiques de $\mathscr{C}$. Raffiner la taille des boites jusqu'à ce que leur projections dans $\mathbb{R}^3$ soient deux à deux disjointes.
   # voir les détails dans les sous-sections 5.3.1 et 5.3.1.
2. $\mathscr{W}_{cross} \leftarrow$`PreWitnessBoxes(S-cross,`$B^{sol}_{cross}$`,`$\delta$`,1, S-ball,`$\mathscr{B}_{ball}$`)`, $\mathscr{W}_{x-crit}$`:=PreWitnessBoxes(S-xcrit,`B^{sol}_{x-crit}`,`δ`,2,S-ball,`$\mathscr{B}_{ball}$`)` : Calculer une boite *pre-witness* pour chaque solution de (S-cross) et (S-xcrit). Une boite *pre-witness* d'un cross-cap (resp. d'un point x-critique) a un seul et unique point au bord (resp. deux points au bord).
   # voir les détails dans la sous-section 5.3.2.
3. $B^{sol}_{y-crit} \leftarrow$`IsolatingBoxes(S-ycrit,`$\mathscr{B}_{ball}$`,`$\delta$`)` `et` $B^{sol}_{z-crit} \leftarrow$`IsolatingBoxes(S-zcrit,`$\mathscr{B}_{ball}$`,`$\delta$`)`. Raffiner la taille des boites jusqu'à ce qu'elles soient deux à deux disjointes des élements de $\mathscr{W}_{cross}$.
   # voir les détails dans la sous-section 5.3.1.

2. Ω peut être entièrement lisse, donc sans partie singulière
3. voir aussi l'algorithme `IsolateSols` dans [29] qui réalise les mêmes calculs

4. `Calculer les boites de suivi qui correspondent aux` *tracking points*. `Elles sont obtenues par un relèvement dans` $\mathbb{R}^5$ `des boites` *pre-witness* `des cross-caps et des points` x`-critiques.`
   # voir les détails dans la sous-section 5.3.3.
5. $\mathscr{P} \leftarrow \delta$-`Approx(`S-ball$,\mathscr{B}_{ball}$,$(\mathbf{C}_0$, S-ball$)$,$\mathbf{L},\delta$`)` : Calculer un ensemble discret $\mathscr{P} := \{(\mathscr{P}_i, c_i, r_i)_i\}$ dont un élément est une suite de parallélotopes qui englobe les composantes connexes de $\mathscr{C} \cap \mathscr{B}_{ball}$.
   # voir les détails dans la sous-section 5.3.3.
6. `Première étape combinatoire` : Déduire le graphe combinatoire $\mathrm{Gr}(\mathscr{C}) := \{(\mathrm{V},\mathrm{E})\}$ de la courbe $\mathscr{C}$ à partir de la δ-approximation.
7. $\mathrm{B}_t^{sol} \leftarrow$`IsolatingBoxes(`S-triple$,\mathscr{B}_0 \times \mathscr{D}$,$\frac{r_{min}}{2}$`)` : Calculer des boites d'isolation pour les points triples avec $r_{min} := \min\{r_i, (\mathscr{P}_i, c_i, r_i) \in \mathscr{P}\}$ et $\mathscr{D} := \{(t_1, t_2, t_3) \in \mathbb{R}^3$ tels que $t_1 \in [-\mathrm{T},\mathrm{T}]$, $t_2 \in [t_1 + r_{min}, \mathrm{T}]$ et $t_3 \in [t_2 + r_{min}, \mathrm{T}]\}$.
   # voir les détails dans la sous-section 5.3.1.
8. $\mathscr{W}_{triple} \leftarrow$`PreWitnessBoxes(`S-triple$,\mathrm{B}_t^{sol}$,$\delta$,6,S-ball$,\mathscr{B}_{ball}$`)` : Calculer des boites *pre-witness* pour les points triples.
   # voir les détails dans la sous-section 5.3.2.
9. `Raffiner les boites de` $\mathscr{W}_{triple}$ `jusqu'à ce qu'elles soient deux à deux disjointes des boites de` $\mathscr{W}_{cross} \cup \mathscr{W}_{x-crit}$.
   # voir les détails dans la sous-section 5.3.2.
10. `Processus d'identification aboutissant à la détermination du graphe des singularités de` $\Omega = \mathfrak{p}(\mathscr{M})$ `dans` $\mathbb{R}^3$: Il s'agit, d'une part, d'identifier parmi les intersections de boites dans $\mathbb{R}^3$ celles qui proviennent de la projection de composantes connexes distinctes et de les substituer par une intersection unique de branches. D'autre part, celles qui proviennent d'une même composante connexe sont remplacées par des branches. On obtient au final un graphe isotope à partie singulière de Ω.

5.3.1 Résoudre les systèmes zéro dimensionnels

Il s'agit ici d'isoler les solutions d'un système zéro dimensionnel régulier dans un domaine fermé borné. C'est-à-dire calculer, pour chaque solution régulière du système, une boite qui contient ce point telle que : chacune d'elle contienne exactement une seule et unique solution du système et qu'il n'existe pas de solution sur le bord d'une boite. D'ailleurs, le sous-programme `IsolatingBoxes` n'est effectif que si la dernière condition est satisfaite.

Algorithm 2 `IsolatingBoxes(`$\mathrm{S}ys,\mathrm{B},\delta$`)`

Input: Une boite fermé borné $\mathrm{B} \subset \mathbb{R}^n$, un système zéro dimensionnel ($\mathrm{S}ys$) dont toutes les solutions sont régulières dans B et qui n'admet aucune solution sur le bord $\partial\mathrm{B}$ de B, l'opérateur de Krawczyk K_S, et un nombre réel positif δ.

Output: Un ensemble B^{sol} constitué de boites qui vérifient :

- Les boites de B^{sol} sont deux à deux disjointes,
- **Si** $\mathrm{X} \in \mathrm{B}$ est une solution de ($\mathrm{S}ys$) **alors** $\exists \mathrm{B}_i \in \mathrm{B}^{sol}$ telle que $x \in \mathrm{B}_i$,
- **Si** $\mathrm{B}_i \in \mathrm{B}^{sol}$ **alors** $\mathrm{B}_i \subset i(\mathrm{B})$ et $\mathrm{K}_\mathrm{S}(\mathrm{B}_i) \subset i(\mathrm{B}_i)$

Isoler les cross-caps et les points triples

Il existe plusieurs algorithmes qui combinent les méthodes de subdivision et de Newton par intervalle pour calculer un ensemble discret de boites d'isolation pour les solutions d'un système régulier(voir dans Neumaier [40, section 5.6] et Imbach et al. [22]). Dans la première étape de l'algorithme général, le sous-programme `IsolatingBoxes` permet de calculer des boites d'isolations

pour les cross-caps. Il prend en entrée un boite fermé borné inclus dans $\mathbb{R}^4$, le système (S-cross) et un nombre réel positif δ. Si la boite initiale n'admet aucun cross-cap sur son bord, `Isolating-Boxes` renvoie en sortie un nombre fini de boites $\mathrm{B}_{cros}^{sol} := \{(\mathrm{B}_i, \mathrm{S}ys)_{i=1}^{m}\}$ deux à deux disjointes, telles que chaque boite contient une seule et unique solution de (S-cross) : de telles boites sont appelées des boites d'isolation pour les solutions du système donné en entrée.

Par ailleurs, le traitement du cas des points triples nécessite au préalable de déterminer le domaine de résolution système (S-triple). En effet, étant donné trois points $q_i = (x, y, z, t_i)$ avec $i = 1, 2, 3$ appartenant à $\mathscr{M}$ tels que $\mathfrak{p}(q_1) = \mathfrak{p}(q_2) = \mathfrak{p}(q_3)$, le point (x, y, z, t_1, t_2, t_3) est une solution régulier de (S-triple) si $t_1 \neq t_2 \neq t_3$. Dès lors, le requête revient à déterminer ce qui sera une boite initiale $\mathscr{B}_{triple}$ à donner en entrée dans laquelle la condition précédente est vérifiée. En utilisant le suivi de courbe réalisé dans l'algorithme général, on peut déduire une borne minimale sur la distance entre les t_i. Soit r_{min} le plus petit rayon des boites englobantes générées par le sous-programme δ-`Approx` sur $\mathscr{C}$. Le domaine de résolution s'écrit alors $\mathscr{B}_{triple} := \mathscr{B}_0 \times \mathscr{D}$, où $\mathscr{B}_0 \subset \mathbb{R}^3$ est un fermé borné (domaine de projection) et $\mathscr{D} := \{(t_1, t_2, t_3) \in \mathbb{R}^3$ tels que $t_1 \in [-\mathrm{T}, \mathrm{T}], t_2 \in [t_1 + r_{min}, \mathrm{T}]$ et $t_3 \in [t_2 + r_{min}, \mathrm{T}]\}$. Et nous garantissons dans la sous-section5.3.4 que, notre algorithme fini par localiser tous les points triples et les isole tous.

Isoler les points x-critiques et les points au bord de $\mathscr{C} \cap \mathscr{B}_{ball}$

Le calcul des suites de parallélotopes qui englobent les composantes connexes de $\mathscr{C}$ se fait à partir d'un point suivi (*tracking point*). Plus précisément, ce type point est donné par un ensemble de coordonnées qui décrivent une boite (*tracking box*). Les *tracking points* de l'algorithme général sont constitués des points x-critiques, des points au bord de$\mathscr{C} \cap \mathscr{B}_{ball}$ et des points sur la courbe $\mathscr{C}$ obtenus par un relèvement dans $\mathbb{R}^5$ des points au bord des boites *pre-witness* des cross-caps et des points triples. Il s'agit donc, dans cette étape, de calculer ces points pour réaliser le suivi de courbe sur les composantes connexes de $\mathscr{C}$. On suppose dans cet algorithme que le cross-cap n'est pas x-critique. Par définition, $\mathscr{C}$ regroupe l'ensemble des solutions réelles du système d'équations $\{(x, y, z, c, r) \in \mathbb{R}^5 \mid \mathscr{F}(x, y, z, c, r) = 0\}$. Soit $\mathscr{B}_0 = (\mathbf{I}_x, \mathbf{I}_y, \mathbf{I}_z)$ une boite dans $\mathbb{R}^3$, $\mathscr{B}_{ball} = \mathscr{B}_0 \times \mathbf{I}_{(c,r)}$, avec $\mathbf{I}_{(c,r)} = [-\mathrm{T}, \mathrm{T}] \times [0, \mathrm{T}^2]$, et désignons par $\mathscr{F}_x$ la fonction déterminant de la matrice carrée suivante :

$$\begin{pmatrix} \partial_y \mathscr{F} & \partial_z \mathscr{F} & \partial_c \mathscr{F} & \partial_r \mathscr{F} \end{pmatrix}.$$

Ainsi, les points critiques de la courbe $\mathscr{C}$ deviennent les solutions réelles du système d'équations ci-dessous

$$\begin{cases} \mathscr{F}(x, y, z, c, r) = 0 \\ \mathscr{F}_x(x, y, z, c, r) = 0 \end{cases} \tag{S-xcrit}$$

Les systèmes qui encodent les points y-critiques et les points z-critiques sont définis de la même manière :

$$\begin{cases} \mathscr{F}(x, y, z, c, r) = 0 \\ \mathscr{F}_y(x, y, z, c, r) = 0 \end{cases} \tag{S-ycrit}$$

et

$$\begin{cases} \mathscr{F}(x, y, z, c, r) = 0 \\ \mathscr{F}_z(x, y, z, c, r) = 0 \end{cases} \tag{S-zcrit}$$

Dans la suite, nous admettons les conditions hypothèses suivantes :

- (A_1) Le système (S-xcrit) admet un nombre fini de solutions régulières dans $\mathscr{B}_{ball}$ et aucune solution sur son bord $\partial\mathscr{B}_{ball}$.
- (A_2) Le système d'équations $\mathscr{F}(\mathbf{x}, y, z, c, r) = 0$ admet un nombre fini de solutions régulières ; où $\mathbf{x} = l(\mathbf{I}_x)$ ou $\mathbf{x} = u(\mathbf{I}_x)$.
- (A_3) Le système d'équations $\mathscr{F}(x, \mathbf{y}, z, c, r) = 0$ admet un nombre fini de solutions régulières ; où lorsque $\mathbf{y} = l(\mathbf{I}_y)$ ou $\mathbf{y} = u(\mathbf{I}_y)$.

(A_4) Le système d'équations $\mathscr{F}(x,y,\mathbf{z},c,r)=0$ admet un nombre fini de solutions régulières; où $\mathbf{z}=l(\mathbf{I}_z)$ ou $\mathbf{z}=u(\mathbf{I}_z)$.

(A_5) Au dessus d'un point du bord $\partial\mathscr{B}_0$, (S-ball) admet une seule solution et aucune solution sur ses coins.

Lemme 5.6 *Imbach et al. [22, Proposition 7]*
Les composantes connexes de $\mathscr{C}\cap\mathscr{B}_{ball}$ sont des sous-variétés lisses qui peuvent avoir des bord. De plus, si les hypothèses ci-dessus sont vérifiées, alors toute composante connexe $\mathscr{C}^k$ de $\mathscr{C}\cap\mathscr{B}_{ball}$ satisfait au moins une des propriétés suivantes :

(a) $\mathscr{C}^k$ est délimité par deux points de $\mathscr{C}$,

(b) $\mathscr{C}^k$ admet au moins deux points x-critiques.

Corollaire 5.1
On définit les systèmes d'équations suivant :

- $(S-xcrit) : \mathscr{F}(x,y,z,c,r)=\tilde{\mathscr{F}}(x,y,z,c,r)=0$, *pour* $(x,y,z,c,r)\in\mathscr{B}_{ball}$.
- $(S-xcrit_{\underline{x}}) : \mathscr{F}(l(\boldsymbol{I}_x),y,z,c,r)=0$, *avec* $y\in\boldsymbol{I}_y,\ z\in\boldsymbol{I}_z$ *et* $(c,r)\in\mathbb{R}^2$.
- $(S-xcrit_{\overline{x}}) : \mathscr{F}(u(\boldsymbol{I}_x),y,z,c,r)=0$, *avec* $y\in\boldsymbol{I}_y,\ z\in\boldsymbol{I}_z$ *et* $(c,r)\in\mathbb{R}^2$.
- $(S-xcrit_{\underline{y}}) : \mathscr{F}(x,l(\boldsymbol{I}_y),z,c,r)=0$, *avec* $x\in\boldsymbol{I}_x,\ z\in\boldsymbol{I}_z$ *et* $(c,r)\in\mathbb{R}^2$.
- $(S-xcrit_{\overline{y})} : \mathscr{F}(x,u(\boldsymbol{I}_y),z,c,r)=0$, *avec* $x\in\boldsymbol{I}_x,\ z\in\boldsymbol{I}_z$ *et* $(c,r)\in\mathbb{R}^2$.
- $(S-xcrit_{\underline{z}}) : \mathscr{F}(x,y,l(\boldsymbol{I}_z),c,r)=0$, *avec* $x\in\boldsymbol{I}_x,\ y\in\boldsymbol{I}_y$ *et* $(c,r)\in\mathbb{R}^2$.
- $(S-xcrit_{\overline{z}}) : \mathscr{F}(x,y,u(\boldsymbol{I}_z),c,r)=0$, *avec* $x\in\boldsymbol{I}_x,\ y\in\boldsymbol{I}_y$ *et* $(c,r)\in\mathbb{R}^2$.

D'après la condition (A_2), les systèmes $(S-xcrit_{\underline{x}}),\ldots,(S-xcrit_{\overline{z}})$ *admet un nombre fini de solutions, qui sont les points au bord de $\mathscr{C}\cap\mathscr{B}_{ball}$. La condition ($A_1$) implique que le système* $(S-xcrit)$ *admet un nombre fini de solutions, qui sont les points x-critiques de $\mathscr{C}\cap\mathscr{B}_{ball}$. Les conditions ($A_1$)...($A_4$) garantissent que les systèmes* $(S-xcrit),(S-xcrit_{\underline{x}}),\ldots,(S-xcrit_{\overline{z}})$ *admettent un nombre fini de solutions dans $\mathscr{B}_0\times\boldsymbol{I}_{(c,r)}$.*

Le calcul de boites d'isolation pour les solutions de ces systèmes se fait aussi à l'aide de l'algorithme2 : En effet, `IsolatingBoxes(`$\mathbf{B}\times\mathbf{I}_{(c,r)}$, S-xcrit,0 `)` renvoie l'ensemble B^{sol}_{x-crit} de boites d'isolation de taille au plus $\delta>0$. Cet algorithme s'arrêtera dès que tous les points x-critiques sont isolés. Car compte tenu du fait que le système admet un nombre fini de solutions et aucune sur le bord de la boite donnée en entrée, la subdivision est interrompue aussitôt que le dernière point est isolé. Les instructions `IsolatingBoxes(`$\mathbf{I}_y\times\mathbf{I}_z\times\mathbf{I}_{(c,r)}$, $S-xcrit_{\underline{x}}$, 0) et `IsolatingBoxes(`$\mathbf{I}_y\times\mathbf{I}_z\times\mathbf{I}_{(c,r)}$, $S-xcrit_{\overline{x}}$, 0) renvoient respectivement les ensembles $B^{sol}_{\underline{x}}$ et $B^{sol}_{\overline{x}}$ pour les systèmes $(S-xcrit_{\underline{x}})$ et $(S-xcrit_{\overline{x}})$. D'après les conditions (A_2) et (A_5), $(S-xcrit_{\underline{x}})$, $(S-xcrit_{\overline{x}})$ admettent un nombre fini de solutions régulières sur $(\mathbf{I}_y\times\mathbf{I}_z\times\mathbb{R}^2)$ et aucune sur son bord $\partial(\mathbf{I}_y\times\mathbf{I}_z)\times\mathbb{R}^2$. Le même procédé est utilisé pour calculer les ensembles $B^{sol}_{\underline{y}},\ldots,B^{sol}_{\overline{z}}$ pour les systèmes $(S-xcrit_{\underline{y}}),\ldots,(S-xcrit_{\overline{z}})$; par le biais de l'algorithme2. De plus, les conditions (A_3),(A_4) et (A_5) garantissent que le programme s'achève dès que toutes les solutions de chaque système sont englobées dans des boites d'isolation.

5.3.2 Calcul des boites *witness*

La représentation topologique local d'un point singulier dépend du type de singularité. Tout d'abord, nous allons définir les notions de boites *pre-witness* et *witness*. Étant donné un point singulier $P\in\mathbb{R}^3$, une boite d'isolation $\mathbf{B}\subseteq\mathbb{R}^3$ de P est dite *pre-witness* si le nombre de points sur son bord $\partial\mathbf{B}$ est égale au nombre de branches connectées à P. Ce qui signifie que, une boite *pre-witness* d'un cross-cap (respectivement un point x-critique et point triple) admet un point (respectivement deux points et six points) sur son bord. On construit de telles boites en faisant appel à l'algorithme `PreWitnessBoxes` (voir algorithme3). Il prend en entrée un système d'équations

zéro dimensionnel régulier (Sys), un nombre fini de boites d'isolation, un nombre réel non nul δ et le nombre N de points sur le bord requis par le type de point singulier isolé par l'ensemble des boites données en entrée. En sortie, l'algorithme `PreWitnessBoxes` renvoie le même nombre de boites d'isolation qui comptent chacune N point sur son bord. Toutefois, le graphe obtenu en connectant les points sur le bord d'une boite *pre-witness* à son centre peut ne pas être localement isotope à la courbe. Puisque, une telle boite peut bien contenir une boucle (un lacet) qui ne croise pas son bord; i.e aucune de ses faces. Ainsi, une boite d'isolation $\mathbf{B} \subset \mathbb{R}^3$ sera dite *witness*[4] si elle vérifie les conditions suivantes :

- la topologie locale est isotope au graphe obtenu en connectant les points sur bord au centre de la boite;
- si $\mathrm{B}' \in \mathrm{B}_t^{sol} \cup \mathrm{B}_{cros}^{sol}$, alors B' ne contient pas de point x-critique.

Étant donné une boite *pre-witness* $\mathscr{W}_i$,, on désigne par $\mathrm{C}_i := \pi_{ball}^{-1}(\mathscr{W}_i)$ la boite $\mathrm{I}_x \times \mathrm{I}_y \times \mathrm{I}_z \times \mathrm{I}_c \times \mathrm{I}_r$, avec $\mathrm{I}_x = [x_\ell, x_u], \ldots, \mathrm{I}_r = [r_\ell, r_u]$, obtenue par relèvement de la boite $\mathscr{W}_i$ dans $\mathscr{B}_{ball}$ par la projection $\mathfrak{p}$. On note par $(\mathrm{S}-ball)_{x_\ell}$ le système d'équations zéro dimensionnel obtenu en substituant x par x_ℓ dans le système d'équations (S-ball), et $\mathrm{C}_i^{x_\ell}$ comme étant la face $x_\ell \times \mathrm{I}_y \times \mathrm{I}_z \times \mathrm{I}_c \times \mathrm{I}_r$ de $\mathscr{B}_{ball}$. On définit de la même manière par analogie les systèmes $(\mathrm{S}-ball)_{x_u}, (\mathrm{S}-ball)_{y_\ell} \ldots, (\mathrm{S}-ball)_{r_u}$ et les cylindre $\mathrm{C}_i^{x_u}, \mathrm{C}_i^{y_\ell} \ldots, \mathrm{C}_i^{r_\ell}, \mathrm{C}_i^{r_u}$. Soit $\pi_{ball} : \mathscr{B}_{ball} \to \mathscr{B}_0$ qui à (x, y, z, c, r) associe (x, y, z).

Algorithm 3 `PreWitnessBoxes`$(\mathrm{S}ys, \mathrm{B}^{sol}, \delta, \mathrm{N}, \mathrm{S}-ball, \mathscr{B}_{ball})$

Input:

- Un système zéro dimensionnel régulier $\mathrm{S}ys$ et un ensemble fini B^{sol} de boites d'isolation;
- un nombre réel positif δ;
- le nombre N de points requis sur le bord des boites *pre-witness*;
- le système (S-ball) et un domaine fermé borné $\mathscr{B}_{ball} := \mathscr{B}_0 \times [-\mathrm{T}, \mathrm{T}] \times [0, \mathrm{T}^2] \subset \mathbb{R}^5$ représentant la courbe lisse $\mathscr{C}$.

Output: Un ensemble $\mathscr{W}^{sol}$ de boites d'isolation inclus dans $\mathbb{R}^3$ ayant chacune N sur son bord.

```
W^sol ← ∅
for i ∈ ⟦1, ♯(B^sol)⟧ do
    ε ← δ
    N_∂W_i ← 0
    while N_∂W_i ≠ N " N_∂W est le nombre de points sur le bord de W " do
        L_i ← [x_ℓ, x_u, y_ℓ, y_u, z_ℓ, z_u, c_ℓ, c_u, r_ℓ, r_u]
        for a ∈ L_i do
            B_a^sol ← IsolatingBoxes((S − ball)_a, C_i^a, δ′)
            N_∂W_i ← N_∂W_i + ♯B_a^sol
        ε ← ε/2
        B_i ← IsolatingBoxes(Sys, π_ball^{-1}(W_i), ε)
        W_i ← π_ball(B_i)
        mise à jour de la liste L_i
    Ajouter W_i dans la liste W^sol
```

5.3.3 Calcul des composantes connexes

Comme indiqué dans l'algorithme général, la boite dans laquelle on cherche à résoudre le système (S-triple) est déterminé à l'aide des coordonnées des parallélotopes du suivi de courbe. Rappelons que ces dernières sont obtenues en faisant appel à l'algorithme δ-`approx` sur chaque

4. Cette notion fut introduite pour la première fois par Imbach et al. [22]

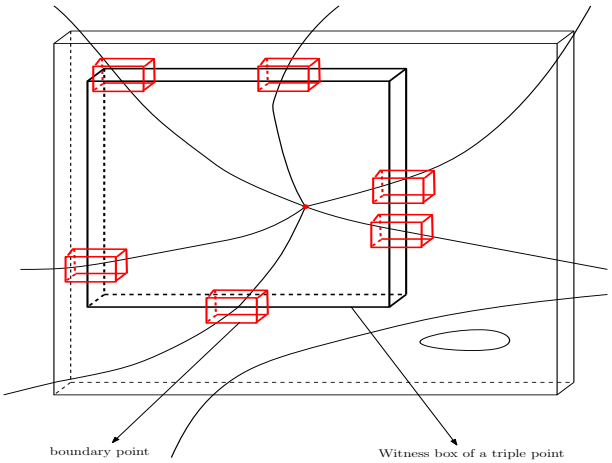


FIGURE 5.1 – **Boite *witness* d'un point triple avec les boites isolant les points sur son bord**

tracking point. Ainsi, il s'agit dans cette sous-section de donner les détails sur le calcul des *tracking points* mais aussi des suites parallÍotopes en dimension 4 qui représenteront les composantes connexes de la courbe lisse $\mathscr{C}$ dans un domaine fermé borné précis.

Calcul des *tracking points* de $\mathscr{C}$

La courbe $\mathscr{C}$ définit l'ensemble des solutions régulières réelles du système (S-ball) dans la boite $\mathscr{B}_{ball} := \mathscr{B}_0 \times \mathbf{I}_{(c,r)} \subset \mathbb{R}^5$. On rappelle que $\mathrm{B}^{sol}_{x-crit}$ désigne l'ensemble des boites d'isolation pour les points x-critiques de $\mathscr{C} \cap \mathscr{B}_{ball}$. Soit B^{sol}_{bord} l'ensemble des boites d'isolations des points de $\mathscr{C}$ sur $\partial\mathscr{B}_{ball}$; i.e chaque boite contient un seul et unique point de $\mathscr{C} \cap \partial\mathrm{B}_{ball}$. L'ensemble $\mathbf{L} = \mathrm{B}^{sol}_{x-crit} \cup \mathrm{B}^{sol}_{bord}$ impose naturellement une décomposition de $\mathscr{C} \cap \mathrm{B}_{ball}$ en un nombre fini de morceaux de courbes lisses. Chaque morceau de courbe est délimité par deux éléments de $\mathbf{L}$. Par abus de langage, nous appellerons les éléments de $\mathbf{L}$ des *tracking points*. Ce sont des points à partir desquels l'algorithme `δ-Approx` calcul une suite de parallélotopes. À cette liste de *tracking points*, on ajoute les pre-images par la projection π_{ball} des boites *witness* des cross-caps.

Topologie de la courbe singulière dans $\mathscr{B}_0$

La courbe singulière obtenue dans $\mathscr{B}_0$ découle de la projection de la courbe lisse $\mathscr{C} \cap \mathrm{B}_{ball}$. Le calcul d'une représentation correcte de $\mathscr{C} \cap \mathrm{B}_{ball}$ se fera à l'aide de l'instruction `δ-Approx(`$(\mathrm{S}-ball)_{r>0}, \mathscr{B}_{ball}$`,`$\mathrm{L}, \delta$`)` (voir algorithme4), qui permet de faire un suivi de courbe. En d'autres termes, en s'appuyant sur la décomposition de $\mathscr{C} \cap \mathrm{B}_{ball}$ en des composantes connexes, comme décrit dans la sous-section précédente, il s'agira de générer une suite adjacente de parallélotopes qui englobe chaque morceau de courbe. Puisque, chaque composante connexe est délimitée par deux éléments de $\mathbf{L}$ (i.e les *tracking points)*, l'algorithme part d'un *tracking point* A et s'arrête dès qu'il atteint un autre *tracking point* B, donnant ainsi une représentation de ma composante $\mathscr{L}_{\mathrm{A}\to\mathrm{B}}$. Dans l'étape suivante, la même instruction est exécutée mais avec l'ensemble $\mathbf{L}-\mathrm{A}$. Si le dernier parallélotopes du suivi de courbe croise le point B alors il s'agit de la même composante connexe et elle est retirée de la base de données de la sortie de l'algorithme. Sinon, l'algorithme continue jusqu'à lépuisement total de l'ensemble $\mathbf{L}$. Finalement, on obtient la structure finie $\mathscr{P} := (\mathscr{P}_i)$; où chaque $\mathscr{P}_i = \cup_j \mathrm{C}_j$ est une union finie de parallélotopes C_j.
La projection $\pi_{ball}(\mathscr{P})$ de B_{ball} dans $\mathscr{B}_0$ représente aussi une suivi de courbe de $\pi_{ball}(\mathscr{C} \cap \mathrm{B}_{ball})$ qui, à tout point $(x, y, z, c, r) \mapsto (x, y, z)$. Notons que, deux ou trois parallÍotopes appartenant tous à des suites adjacentes différentes peuvent s'intersecter en projection. En effet, ce phénomène se produit lorsque deux ou trois points distincts de $\mathscr{C}$ ont la même image par π_{ball}. Ce qui signifie que $\pi(\mathscr{C})$ peut avoir des auto-intersections. Si m parallélotopes s'intersectent en projection, alors le graphe dans $\mathscr{B}_0$ est localement déterminé par un croisement de $2m$ arêtes.

Algorithm 4 δ−`Approx` ($(Sys), \mathbf{C}, (\mathbf{C}_0, Sys_0), \mathbf{L}, \delta$)

Input:

- Un système d'équations (Sys) et un domaine fermé borné $\mathbf{C}$ définissant une courbe lisse $\mathscr{C}$ inclus dans $\mathbf{C}$;
- Un ensemble fini de *tracking points* $\mathbf{L}$ appartenant à la courbe $\mathscr{C}$. et un paramètre réel $\delta > 0$ indiquant la taille maximale des parallélotopes.

Output: Un ensemble fini de suites adjacentes de parallélotopes $\mathscr{P} := (\mathscr{P}_i)_i$ tel que pour tout i $\mathscr{P}_i$ est une δ-approximation d'une seule et unique composante connexe de $\mathscr{C} \cap \mathbf{C}$.

5.3.4 Certificat sur l'isolation des points triples

Compte tenu du fait que le domaine de résolution du système (S-triple) $\mathscr{B}_{triple}$ dépend des coordonnées des suites de parallélotopes de $\mathscr{P}$, Il devient donc impératif de garantir l'effectivité de l'algorithme général sur ces points. Il s'agit donc d'établir un certificat qui prouve que l'algorithme fini par calculer tous les points triples du système (S-triple). En d'autres termes, il reste à démontrer qu'une boite *pre-witness* d'un cross-cap ne peut contenir un point triple. L'idée principale de ce certificat consiste à démontrer que, s'il existe un point dans une boite *pre-witness* pour un cross-cap, alors il existe au moins un lacet [5] (une boucle) à l'intérieur de cette boite. Cela vient du fait qu'une telle boite admet un seul et unique point de la courbe $\mathscr{C}$ sur son bord. Or, tout lacet admet au moins une direction critique. en effet, il peut être strictement contenu dans un des plans; i.e $(x, y), (y, z)$ ou (x, z). Ce qui signifie que, tout comme les points x-critiques, il suffit d'isoler les points y-critiques et z-critiques de $\mathscr{C}$ (i.e calculer $\mathrm{B}^{sol}_{y-crit}$ et $\mathrm{B}^{sol}_{z-crit}$), tout en s'assurant que les boites dans $\mathscr{W}cross$ ne croisent aucune de $\mathrm{B}^{sol}_{y-crit} \cup \mathrm{B}^{sol}_{z-crit}$. A défaut, il suffira de réduire de moitié la taille des boites *pre-witness* des solutions du système (S-cross), jusqu'à ce que la condition précédente soit vérifiée. En définitive, on obtient le résultat suivant :

Lemme 5.7
Au sortir de l'étape 3 *dans l'algorithme général, une boite* pre-witness *d'un point cross-cap ne peut contenir un lacet.*

Ce résultat devient évident du fait que, une fois cette étape exécutée, toute boite *pre-witness* d'un point cross est en réalité *witness*. En effet, dès l'instant qu'elle ne chevauche aucune boite *pre-witness* d'un point x-critique ou y-critique ou z-critique, la topologie locale est obtenue en connectant le point au centre à son point au bord.

Corollaire 5.2
Soit ***B*** *un boite* pre-witness *d'un point cross-cap. Si* ***B*** *ne contient ni un point x-critique ou y-critique ou z-critique, alors* ***B*** *ne contient pas de point triple.*

En somme, nous avons établi que sous les hypothèses de généricité citées dans la section 5.2, une surface analytique lisse $\mathscr{M} := \{(x, y, z, t) \in \mathbb{R}^4,\ \mathrm{F}(x, y, z, t) = \mathrm{G}(x, y, z, t) = 0\}$ projetée dans $\mathbb{R}^3$ ne peut contenir que trois types de singularités : une courbe lisse de points doubles, un ensemble discret de points triples et de cross-caps (Théorème 5.1). Une analyse méthodique sur la régularité des systèmes qui caractérisent ces singularités permet d'écrire un algorithme (voir section 5.3) qui calcule le graphe de singularité de la surface obtenue dans $\mathbb{R}^3$.

Dès lors, il devient naturel de s'interroger sur la possibilité de généraliser ce résultat pour des objets définis dans des espaces de dimensions supérieurs à 4. Une généralisation du ball-system serait-il nécessaire pour analyser la stabilité du système qui encode les points doubles lorsque ces derniers sont assez proche l'un de l'autre?

5. Un lacet est un chemin continu, non réduit à un point, et dont les extremités sont confondues.

Conclusion

L'objectif de cette thèse était, d'une part, d'établir une variante de l'algorithme de calcul de la topologie d'une courbe algébrique proposé par Mehlhorn et al. [33], qui soit effectif et efficace en terme de complexité binaire. D'autre part, de proposer une généralisation des résultats de Imbach et al. [21] sur la projection d'une courbe de l'espace vers le plan.

C'est dans cette perspective, que nous avons élaboré un premier algorithme de calcul de la topologie d'une courbe algébrique avec une complexité en $(d^5\tau + d^6)$ opérations binaires. Il est effectif et ne requiert pas, au préalable, de placer la courbe en position générique comme instruit dans l'algorithme décrit par Mehlhorn et al. [33]. Ce résultat est rendu possible par une application intelligente de la DCA (Décomposition Cylindrique Algébrique) et des informations collectées à partir des boîtes adjacentes. Par ailleurs, nous avons établi deux résultats quantitatifs (voir le chapitre 3) en rapport avec le choix de la taille d'une boite adjacente; puisque une telle boîte nous informe du nombre de branches qui arrivent à gauche et à droite d'un point spécial. Cependant, ces résultats, introduit dans un algorithme, ont l'inconvénient d'augmenter significativement la complexité. En effet, leur exécution coûte nettement plus que $\tilde{O}(d^5\tau + d^6)$ opérations binaires.

Notre troisième contribution s'inscrit dans l'objectif d'avoir, dans un projet futur, un algorithme qui calcul la triangulation d'une surface dans $\mathbb{R}^3$, obtenue par la projection d'une autre surface analytique réelle, définie comme intersection de deux hypersurfaces dans $\mathbb{R}^4$. L'algorithme décrit dans le chapitre 5 calcule le graphe des singularités de l'image, par la projection canonique de la surface, dans $\mathbb{R}^3$. Sous des hypothèses de généricité préétablies, nous donnons une caractérisation des singularités observées, comme étant les solutions régulières de systèmes d'équations. En faisant appel à des techniques numériques, nous proposons un algorithme qui calcule le graphe des singularités. Dès lors, la perspective immédiate est de s'appuyer sur ce graphe pour reconstruire la topologie globale de la surface.

Bibliographie

[1] V. I. Arnol'd. Critical points of smooth functions and their normal forms. *Russian Math. Surveys 30*, 1975. (or in Singularity Theory, LMS Lecture Note Series 53, Cambridge UP (1981)). 73, 83

[2] R. Wik Atique. On the classification of multi-germs of maps from $\mathbb{C}^2$ to $\mathbb{C}^3$ under $\mathscr{A}$-equivalence. *Research Notes in Maths Series, Chapman and Hall / CRC*, pages 119–133, 2000. in J.W.Bruce and F.Tari(eds.) Real and Complex Singularities. 73

[3] S. Basu and T. Zell. On projections of semi-algebraic sets defined by few quadratic inequalities. *Discrete Comput. Geom.*, 39(1-3) :100–122, 2008. ISSN 0179-5376. 14

[4] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2006 (second edition). ISBN 3-540-00973-6. Revised version of the second edition online at http://perso.univ-rennes1.fr/marie-francoise.roy/. 4, 5, 6, 7, 8, 11, 13, 19, 20, 24, 46, 64

[5] R. Becker, M. Sagraloff, V. Sharma, and C. Yap. A Near-Optimal Subdivision Algorithm for Complex Root Isolation based on the Pellet Test and Newton Iteration. *ArXiv e-prints*, September 2015. 15, 17

[6] J. Cheng, S. Lazard, L. Penaranda, M. Pouget, F. Rouillier, and E. Tsigaridas. On the topology of planar algebraic curves. *Mathematics in Computer Science*, 1(14) :113–137, 2011. 19

[7] M. Coste and M.-F. Roy. Thom's lemma, the coding of real algebraic numbers and the topology of semi-algebraic sets. *Journal of Symbolic Computation*, 5(1/2) :121–129, 1988. 19

[8] M. Demazure. *Bifurcations and catastrophes : geometry of solutions to nonlinear problems*. Universitext. Springer, Berlin, New York, 2000. ISBN 3-540-52118-6. École polytechnique. 74, 75, 88, 89, 90, 91, 92, 96

[9] Daouda Niang Diatta, Fabrice Rouillier, and Marie-Françoise Roy. On the computation of the topology of plane curves. In *39th International Symposium on Symbolic and Algebraic Computation*, pages 130–137, Kobe, Japan, July 2014. ACM Press, ISSAC. 19

[10] Daouda Niang Diatta, Seny Diatta, Fabrice Rouillier, Marie-Francoise Roy, and Michael Sagraloff. Bounds for polynomials on algebraic numbers and application to curve topology. *arXiv*, 2018. URL https://arxiv.org/pdf/1807.10622.pdf. vii

[11] Dimitrios I. Diochnos, Ioannis Z. Emiris, and Elias P. Tsigaridas. On the asymptotic and practical complexity of solving bivariate systems over the reals. *Journal of Symbolic Computational*, 7(44) :818–835, 2009. 19

[12] A. Eingenwillig. *Real root Isolation for Exact and Approximate Polynomials Using Descartes' Rule of Signs*. PhD thesis, Universität des Saarlandes, 2008. 8

[13] Paula Escorcielo and Daniel Perrucci. On the davenport-mahler bound. *J. Complexity*, 41 :72–81, 2017. doi : 10.1016/j.jco.2016.12.001. URL https://doi.org/10.1016/j.jco.2016.12.001. 8

[14] A. A. Gaganov. Computation complexity of the range of a polynomial in several variables. *Cybernetics*, 21(4) :418–421, 1985/07/01 1985. isbn : 1573-8337. 80

[15] J. Von Zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge University Press, New York, 1999. ISBN 0-521-64176-4. 14

[16] M. Golubistky and V. Guillemin. *Stable Mapping and Their Singularities*. Springer-Verlag New York, 1973. ISBN 13 : 978-0-387-90073-5. 89, 91

[17] L. Gonzalez-Vega and M. El Kahoui. An improved upper complexity bound for the topology computation of a real algebraic curve. *Journal of Complexity*, 12 :527–544, 1996. 19

[18] V. Goryunov. Singularities of projections of complete intersections. *J. Soviet Math*, 27 :2785–2811, 1984. 73

[19] Victor V. Goryunov. *Local invariants of mappings of surfaces into three-space*, pages 223–255. Birkhäuser Boston, Boston, MA, 1997. ISBN 978-1-4612-4122-5. doi : 10.1007/978-1-4612-4122-5_11. URL http://dx.doi.org/10.1007/978-1-4612-4122-5_11. viii, 73

[20] C. A. Hobbs and N. P. Kirk. On the classification and bifurcation of multigerms of maps from surfaces to 3-space. *Math. Scand.*, 89(1) :57–96, 2001. ISSN 0025-5521. doi : 10.7146/math.scand.a-14331. URL http://dx.doi.org/10.7146/math.scand.a-14331. 73, 91

[21] Rémi Imbach, Guillaume Moroz, and Marc Pouget. Numeric and certified isolation of the singularities of the projection of a smooth space curve. In *Proceedings of the 6th International Conferences on Mathematical Aspects of Computer and Information Sciences*, MACIS'15, 2015. to appear. vii, 83, 84, 87, 99, 100, 109

[22] Rémi Imbach, Guillaume Moroz, and Marc Pouget. Reliable location with respect to the projection of a smooth space curve. In *Proceedings of the 6th International Conferences on Mathematical Aspects of Computer and Information Sciences*, MACIS'18, 2018. to appear. 83, 91, 102, 104, 105

[23] Michael Kerber and Michael Sagraloff. Root refinement for real polynomials using quadratic interval refinement. *Journal of Computational and Applied Mathematics*, 280 :377 – 395, 2015. ISSN 0377-0427. doi : http://dx.doi.org/10.1016/j.cam.2014.11.031. URL http://www.sciencedirect.com/science/article/pii/S037704271400510X. 14, 16

[24] Alexander Kobel and Michael Sagraloff. On the complexity of computing with planar algebraic curves. *Journal of Complexity*, 31(2) :206 – 236, 2015. ISSN 0885-064X. doi : http://dx.doi.org/10.1016/j.jco.2014.08.002. URL http://www.sciencedirect.com/science/article/pii/S0885064X1400082X. 13, 20

[25] Alexander Kobel, Fabrice Rouillier, and Michael Sagraloff. Computing real roots of real polynomials ... and now for real! In *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '16, pages 303–310, New York, NY, USA, 2016. ACM. ISBN 978-1-4503-4380-0. doi : 10.1145/2930889.2930937. URL http://doi.acm.org/10.1145/2930889.2930937. 16, 17

[26] Rudolf Krawczyk. Newton-algorithmen zur bestimmungvon nullstellenmit fehler- schranken. *Interner Bericht des Inst. für Informatik 68/6, Universität Karlsruhe*, 4 :187–201, 1969. 82

[27] Ulrich W. Kulisch and Willard L. Miranker. *Computer Arithmetic in Theory and Practice*. Academic Press, New York, 1981. 77

[28] W. L. Marar and F. Tari. On the geometry of simple germs of co-rank 1 maps from $\mathbb{R}^3$ to $\mathbb{R}^3$. *Math. Proc. Cambridge Philos. Soc*, 119(3) :469–481, 1996. 73

[29] B. Martin, A. Goldsztejn, L. Granvilliers, and C. Jermann. Certified parallelotope continuation for one-manifolds. *SIAM J. Numerical Analysis*, 51(6) :3373–3401, 2013. 101

[30] J. N. Mather. Stability of $\mathbb{C}^\infty$ mappings : Iii. finitely determined mapgerms. *Inst. Hautes Etudes Sci. Publ. Math*, (35) :279–308, 1968. 73, 76

[31] J. N. Mather. Stability of $\mathbb{C}^\infty$ mappings : Ii. infinitesimal stability implies stability. *Ann. of Math*, 89(2) :254–291, 1969. 73, 75

[32] J. N. Mather. Stability of $\mathbb{C}^\infty$ mappings : Iv classification of stable maps by $\mathbb{R}$-algebras. *Inst. Hautes Etudes Sci. Publ. Math*, (37) :223–248, 1969. viii, 73, 77

[33] Kurt Mehlhorn, Michael Sagraloff, and Pengming Wang. From approximate factorization to root isolation. In *Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation*, ISSAC '13, pages 283–290, New York, NY, USA, 2013. ACM. ISBN 978-1-4503-2059-7. doi : 10.1145/2465506.2465523. URL http://doi.acm.org/10.1145/2465506.2465523. ii, vii, viii, 3, 14, 15, 17, 19, 109

[34] Kurt Mehlhorn, Michael Sagraloff, and Pengming Wang. From approximate factorization to root isolation with application to cylindrical algebraic decomposition. *Journal of Symbolic Computation*, 66 :34 – 69, 2015. ISSN 0747-7171. doi : http://dx.doi.org/10.1016/j.jsc.2014.02.001. URL http://www.sciencedirect.com/science/article/pii/S0747717114000200. 15, 17

[35] D. Mond and J. J. Nunõ-Ballesteros. Singularities of mappings. Available at. URL http://homepages.warwick.ac.uk/~masbm/LectureNotes/book.pdf. 73

[36] David Mond. On the classification of germs of maps from $\mathbb{R}^2$ to $\mathbb{R}^3$. *Proceedings of the London Mathematical Society*, s3-50(2) :333–369, 1985. ISSN 1460-244X. doi : 10.1112/plms/s3-50.2.333. URL http://dx.doi.org/10.1112/plms/s3-50.2.333. 73, 77

[37] Ramon E. Moore. A test for existence of solutions to nonlinear systems. *SIAM J. Numer. Anal.*, (4) :611–615, 1977. 82

[38] Ramon E. Moore. A computational test for convergence of iterative methods for nonlinear systems. *SIAM J. Numer. Anal.*, 15(6) :1194–1196, 1978. 82

[39] Ramon E. Moore, R. Baker Keaffort, and Michael J. Cloud. *Introduction to Interval Analysis*. Society for Industrial and Applied Mathematics (SIAM), 2009. ISBN 968-0-898716-69-6. 77, 81, 82

[40] A. Neumaier. *Interval methods for systems of equations*. Cambridge University Press, 1990. ISBN 052133196. URL http://www.loc.gov/catdir/toc/cam041/89070812.html. 102

[41] T. Ohmoto and F. Aicardi. First order local invariants of apparent contours. *Topology*, (1) : 27–45, 2006. 73

[42] Victor Y. Pan. Univariate polynomials : Nearly optimal algorithms for numerical factorization and root-finding. *J. Symb. Comput.*, 5(33) :701–733, 2002. viii, 14

[43] Victor Y. Pan and Elias P. Tsigaridas. On the boolean complexity of real root refinement. In *ISSAC*, pages 299–306, 2013. 15, 17

[44] P. Pedersen. *Counting real zeroes of polynomials*. PhD thesis, Courant Institute, New York University, 1991. 15, 17

[45] J. H. Rieger. Families of maps from the plane to the plane. *J. London Math. Soc*, 36(2) :351–369, 1986. 73

[46] J. H. Rieger and M. A. S. Ruas. Classification of a-simple germs from $\mathbb{K}^n$ to $\mathbb{K}^2$. *Composition Math*, 79(1) :99–108, 1991. 73

[47] Michael Sagraloff and Kurt Mehlhorn. Computing real roots of real polynomials. *Journal of Symbolic Computation*, 73 :46 – 86, 2016. ISSN 0747-7171. doi : http://dx.doi.org/10.1016/j.jsc.2015.03.004. URL http://www.sciencedirect.com/science/article/pii/S0747717115000292. 16, 17

[48] Michael Sagraloff and Kurt Mehlhorn. Computing real roots of real polynomials. *Journal of Symbolic Computation*, 73 :46 – 86, 2016. ISSN 0747-7171. doi : http://dx.doi.org/10.1016/j.jsc.2015.03.004. URL http://www.sciencedirect.com/science/article/pii/S0747717115000292. 15, 17

[49] R. O. Sinha and R. W. Atique. Classification of multigerms (from a modern viewpoint). Lecture Note, 2016. URL www.worksing.icmc.usp.br/main_site/2016/minicourse3_notes.pdf. 74, 75, 76, 77

[50] D. Mond T. Cooper and R. Wik Atique. Vanishing topology of codimension 1 multi-germs over $\mathbb{R}$ and $\mathbb{C}$. *Compositio Math*, 131(2) :121–160, 2002. 77

[51] C. T. C. Wall. Finite determinacy of smooth map-germs. 13 :481–539, 1981. 73

[52] H. Whitney. On singularities of mappings of euclidean spaces. i. map- pings of the plane into the plane. *Ann. of Math*, 62(2) :374–410, 1955. 73