Calcul effectif de la topologie de courbes et surfaces algébriques réelles

Daouda Diatta

UNIVERSITE DE LIMOGES

ECOLE DOCTORALE Science - Technologie - Santé
Faculté des Sciences et Techniques

Thèse N° - - -

Préparée aux laboratoires :
XLIM-DMI et **INRIA Projet GALAAD**

Thèse

pour obtenir le grade de

DOCTEUR DE L'UNIVERSITE DE LIMOGES
Spécialité : Mathématiques et ses applications

présentée et soutenue publiquement par

Daouda Niang Diatta

le 28 Septembre 2009

CALCUL EFFECTIF DE LA TOPOLOGIE DE COURBES ET SURFACES ALGÉBRIQUES RÉELLES

Thèse dirigée par :
Moulay Barkatou, Bernard Mourrain
Olivier Ruatta

Jury

Président	
Marie-Françoise Roy	Professeur Université Rennes 1.
Rapporteurs	
Marie-Françoise Roy	Professeur Université Rennes 1.
M'Hammed El Kahoui	Professeur Université Cadi Ayad.
Eric Schost	Professeur Université Western Ontario.
Examinateurs	
Moulay Barkatou	Professeur Université de Limoges.
Bernard Mourrain	Directeur de recherche INRIA.
Olivier Ruatta	Maître de conférences Université de Limoges.

Calcul de topologie de courbes et surfaces algebriques réelles

Résumé : ce travail de thèse relève du registre de ***l'algorithmique de courbes et surfaces algébriques réelles***. Dans le domaine de la **représentation de formes** nous avons développé trois algorithmes. Le premier est un algorithme symbolique-numérique certifié, fortement basé sur les propriétés des sous-résultants, et permettant le calcul de la topologie d'une courbe algébrique plane avec la meilleure complexité connue. Le deuxième algorithme traite le problème du calcul de la topologie d'une courbe algébrique spatiale définie comme intersection de deux surfaces algébriques implicites. Pour construire cet algorithme, nous avons introduit la notion de courbe spatiale en position pseudo-générique par rapport à un plan. Cette approche conduit à un algorithme symbolique-numérique certifié disposant de la meilleure complexité connue pour traiter ce problème. Le troisième est un algorithme de maillage de surfaces implicites. C'est le premier algorithme certifié et implémenté qui résoud le problème du maillage isotopique de surfaces implicites singulières. Soulignons que ce travail rentre aussi dans le cadre des **applications mathématiques** puisqu'on peut, à partir d'une triangulation, calculer de nombreux invariants topologiques. Enfin dans un travail sur les arrangements pouvant se placer dans le cadre des **problèmes de configurations spatiales**, nous évoquons un algorithme permettant le calcul d'un tel arrangement.

Effective Topology of Real Algebraic Curves and Surfaces

Abstract : In this thesis, we got interested into ***the Effective Computation of the Topology of Real Algebraic Curves and Surfaces***. One can distinguish three main new algorithms in the field of **shape representation**. Our first algorithm is a certified symbolic-numerical based on sub-resultants properties and computes the topology of a plane algebraic curve with the best known complexity. The second algorithms computes the topology of a space curve defined as the intersection of two implicit algebraic surfaces. For the designing of this algorithm, we introduce the notion of space curve in pseudo-generic position with respect to a given plane. This approach leads to a certified symbolic-numerical algorithm with the best known complexity. The third algorithms is a new and complete one for computing the isotopic meshing of an implicit algebraic surface. It involves only subresultant computations and entirely relies on rational manipulation, which makes it direct to implement. Finally, we also design an algorithm for computing the cells in an arrangement of quadrics which may be classify on the area of **configuration spaces computation**.

Remerciements

Tout d'abord, je tiens à remercier vivement mes directeurs de thèse Moulay Barkatou, Bernard Mourrain et Olivier Ruatta pour le soutien et la confiance qu'ils m'ont accordés durant ce travail de thèse.
Je tiens également à exprimer ma profonde gratitude à Marie-Françoise Roy qui a acceptée d'être rapporteur, et dont les nombreuses suggestions m'ont aidées à clarifier et à mieux présenter les idées développées dans cette thèse.
Je souhaite remercier très chaleureusement Eric Schost et M'Hammed El Kahoui , également rapporteurs, pour l'intérêt qu'ils ont porté à mon travail.
Mes remerciements s'adressent également à Marie-Eve Modolo pour son aide inestimable pendant la rédaction de cette thèse.

Je profite de l'occasion pour remercier tous les membres du Projet Galaad. Ces remerciements s'adressent en particulier à Jean-Pascal Pavone Julien Wintz, Jean-Pierre Técourt, Lionel Alberti, Laurent Busé, Jerome Brachat, Elias Tsigaridas, Angelos Mantzaflaris.
Je remercie également tous les membres du DMI, avec une mention spéciale aux doctorants du bâtiment de Maths, Elsa, Christophe, Sandrine, Delphine, Carole, Amel, Ainhoa, Benjamin, Julien, Aurore, ZhenZhong.
Je remercie également mes amis **Bamba Sy**, Karimou Bâ, Benoit Rossignol, Jean-Pascal Pavone pour leur soutien dans les moments d'intense travail comme dans les moments de détente.
Je remercie ma mère, mes frères et soeurs, ma belle-famille pour leur soutien.

Je souhaite enfin exprimer ma gratitude à ma chérie, **Sarah Mekdjian**, pour sa tendresse et la confiance qu'elle m'a toujours portée. Merci de m'aimer quelque soit la lune. Cette thèse t'est entièrement dédiée.

Table des matières

Chapitre 1

Introduction

Au cours des dernières décennies, la géométrie algorithmique est devenue un thème de recherche très productif, avec des applications dans des domaines tels que le graphisme, la robotique et la conception assistée par ordinateur. Initialement la géométrie algorithmique traitait principalement des problèmes d'ensemble de points, de polygones et de polyèdres et utilisait des techniques de combinatoire pour les résoudre. La nécessité d'accélérer les progrès dans la visualisation des informations a mis en contact la géométrie algorithmique avec d'autres branches des mathématiques (topologie, géométrie algébrique, géométrie différentielle...) et a fait énormément évoluer ses outils et ses champs d'applications. Ainsi, en modélisation, on distingue le problème de l'approximation d'un objet à celui de l'étude de sa structure i.e. sa topologie. Le calcul effectif de la topologie d'objets mathématiques est un sujet assez récent de recherche en géométrie algorithmique. Dans l'article [8], plusieurs spécialistes avaient ciblé différents domaines dans lesquels le développement du calcul effectif de topologie aurait un rôle crucial à jouer :

- **La simulation physique**

  Dans plusieurs domaines tels que la modélisation de la combustion de systèmes, l'aérodynamique, la mécanique des structures, la dynamique moléculaire..., on utilise beaucoup la représentation d'objets géométriques par des maillages pour la simulation de phénomènes physiques. Toutefois, ces applications sont de plus en plus complexes et la convergence locale des algorithmes numériques n'assure absolument plus en pratique leur bon fonctionnement. On voit alors apparaître l'intérêt de chercher à combiner des techniques d'analyse numérique avec des considérations topologiques.

- **Les configurations spatiales**

  En robotique, biologie moléculaire, chimie..., on considère des modèles avec un certain nombre de degrés de liberté. On est alors confronté à la détermination des configurations possibles d'un tel système. Ce peut être les positions d'un robot ou d'une

molécule dont on connaît quelques propriétés ou encore certaines distances entre certains atomes. La modélisation des contraintes géométriques et physiques que doivent satisfaire de tels systèmes débouche sur des systèmes d'équations polynomiales. L'étude de la structure topologique des solutions de ces systèmes permet de comprendre, de décrire et de classifier les différentes configurations possibles.

– **L'acquisition de formes**

  L'acquisition automatique de la forme d'un objet physique est une technique très utile en imagerie médicale. Les formes qui vont être manipulées par un ordinateur sont obtenues à partir d'un objet réel par scanner. Il faut ensuite en recréer une approximation fiable à partir des mesures réalisées. Une partie de ce processus concerne le développement d'algorithmes permettant de transformer une série de mesures en une forme de représentation topologiquement valide. Les techniques utilisant la triangulation de Delaunay 3D sont alors souvent combinées à des considérations différentielles et topologiques.

– **La représentation de formes**

  De nombreux modes de représentation de formes ont été développés, notamment les représentations paramétrées, implicites, avec des ensembles de points, des maillages. Il est important de développer des outils permettant de passer d'un mode de représentation à un autre. Les échanges d'informations à travers le monde via le web, se développent beaucoup. Malgré les progrès technologiques, le flot d'informations est trop grand, et il devient de plus en plus nécessaire de typer et compresser les données. On voit donc se développer le web sémantique et un ensemble d'outils dont il a besoin pour fonctionner. Il est essentiel d'adjoindre à un objet un ensemble de champs qui permettent de le classifier et de le cibler plus facilement lors d'une recherche. En ce sens le calcul de topologie apparaît comme un outil essentiel du web sémantique.

– **L'application mathématique**

  Le développement d'algorithmes autour du calcul de topologie est intéressant en lui-même. Cela a permis de résoudre, en utilisant la puissance de calcul de l'ordinateur, certains problèmes, comme le théorème des quatre couleurs et le problème du calcul du nombre de types topologiques de courbes implicites de degrés huit. De nombreux travaux actuels portent sur le calcul d'invariants topologiques. Ces travaux permettent de rendre effectives certaines classifications et même de les améliorer.

Ce travail de thèse se situe dans le champ de ***l'algorithmique de courbes et surfaces algébriques***. Nous avons développé trois algorithmes.
Le premier est un algorithme symbolique-numérique certifié, fortement basé sur les propriétés des sous-résultants, et permettant le calcul de la topologie d'une courbe algébrique plane. Cet algorithme d'une complexité binaire de $\tilde{O}_B(d^{10}\tau)$ (d étant le degré du polynôme définissant la courbe étudiée, et τ la taille binaire de ses coefficients) est une amélioration de l'algorithme décrit dans [32] dont la complexité binaire est de $\tilde{O}_B(d^{16}\tau)$.

Le deuxième algorithme résoud le problème du calcul de la topologie d'une courbe algébrique spatiale définie comme intersection de deux surfaces algébriques implicites. Pour construire cet algorithme, nous avons introduit la notion de courbe spatiale en position pseudo-générique par rapport à un plan, notion qui nous a permis de garantir l'existence de paramétrisations rationnelles par morceaux de la courbe par rapport à sa projection sur ce plan. L'obtention de ces paramétrisations a permis de ramener de façon claire le problème au cas du calcul de la topologie d'une courbe algébrique plane. Cette approche conduit à un algorithme symbolique-numérique certifié dont la complexité binaire est de $\tilde{O}_B(d^{21}\tau)$.
Le troisième est un algorithme de triangulation de surfaces implicites. Sa complexité binaire est dominée par la phase de calcul de la "silhouette" de la surface et est de $\tilde{O}_B(d^{21}\tau)$. C'est le premier algorithme certifié et entièrement implémenté qui traite le problème de la triangulation isotopique de surfaces implicites singulières. Soulignons que ce travail s'inscrit aussi dans le champ des **applications mathématiques** puisqu'on peut, à partir d'une triangulation, calculer de nombreux invariants topologiques.
Enfin dans un travail sur les arrangements pouvant se placer dans le cadre des **problèmes de configurations spatiales**, nous évoquons un algorithme permettant le calcul d'un tel arrangement.

Structure de la thèse. Cette thèse se compose de trois parties :

- Prérequis algébriques
- Partie I. Topologie de courbes. Chapitre 3 et 4.
- Partie II. Topologie de surfaces. Chapitre 5 et 6

Le Chapitre 2 aborde différents outils et méthodes algébriques qui sont nécessaires dans les algorithmes que nous présenterons dans la suite. La première section de ce chapitre est une discussion sur les outils essentiels permettant la gestion des nombres algébriques. Dans cette section, nous rappelons les algorithmes fondamentaux permettant de compter, de comparer et d'isoler les racines réelles d'un polynôme univarié à coefficients dans $\mathbb{Q}$ ou dans un anneau $\mathbb{Q}[\alpha]$, α étant un nombre algébrique. La deuxième section présente la résolution de systèmes algébriques réels de dimension 0. Nous y rappelons les algorithmes fondamentaux qui sont à la base des solveurs de systèmes d'équations polynomiales comportant un nombre fini de solutions complexes. La troisième section est un rappel sur la théorie des sous-résultants. Nous y étudions les propriétés fondamentales des sous-résultants aidant à appréhender les problèmes sous-jacents au calcul de la topologie des courbes et surfaces algébriques réelles. La dernière section est un bref rappel sur la décomposition cylindrique algébrique, particulièrement axée sur l'algorithme de Collins et ses applications en calcul de topologie de variétés semi-algébriques réelles.

Le Chapitre 3 traite du problème du calcul de la topologie d'une courbe algébrique plane. Nous y présentons un algorithme symbolique-numérique certifié, fortement basé sur les pro-

priétés des sous-résultants. L'algorithme calcule la topologie d'une courbe algébrique plane de degré d, avec une complexité binaire de $\tilde{O}_B(d^{10}\tau)$, et s'inspire des techniques décrites dans [32]. L'apport majeur de ce travail consiste en l'introduction d'un algorithme modulaire, utilisant les propriétés des polynômes sous-résultants pour certifier la généricité de la position d'une courbe algébrique plane. Comparé à l'algorithme de test de généricité (par calcul d'encodage de Thom) décrit dans [32], ce nouvel algorithme permet de réaliser un gain d'un facteur d^6 sur la complexité binaire globale de l'algorithme. Dans la section 3.2, nous menons une analyse détaillée de la géométrie d'une courbe algébrique plane. La section 3.3 regroupe les différentes phases de l'algorithme calculant la topologie d'une courbe algébrique implicite plane. Nous y effectuons une étude comparative de notre algorithme de test et de mise en position générique avec celui décrit dans [32]. La section 3.4 porte sur l'étude de la complexité binaire de l'algorithme de calcul de topologie. Pour finir nous évoquerons l'implémentation de l'algorithme avec MATHEMAGIX et les expérimentations réalisées.

Dans le Chapitre 4 nous présentons un algorithme symbolique-numérique certifié calculant la topologie d'une courbe intersection de deux surfaces implicites. L'approche que nous developpons est basée sur une analyse des propriétés des sous-résultants. Contrairement aux algorithmes décrits dans [31] et [5], il n'utilise qu'une projection de la courbe d'intersection, et permet de calculer sa topologie dans le cas où elle est non réduite. Nous introduisons la notion de courbe en position pseudo-générique par rapport à un plan, ce qui nous permettra de garantir l'existence de paramétrisations rationnelles par morceaux de la courbe par rapport à sa projection sur ce plan. La topologie de la courbe projetée est calculée avec l'algorithme décrit dans le Chapitre 3, puis relevée morceau par morceau dans l'espace en utilisant les paramétrisations. L'utilisation de ces paramétrisations rend le relévement rapide, et évite les problèmes numériques souvent rencontrés dans ce type de calcul. L'une des difficultés majeures des algorithmes basés sur la méthode "projection puis relèvement" est la distinction entre les singularités de la courbe plane introduites par la projection, et les singularités provenant de la projection de vraies singularités de la courbe spatiale. Nous proposons un algorithme certifié permettant de distinguer ces deux types de singularités de la courbe projetée. Ce travail a été présenté et publié lors de la conférence internationale sur le calcul symbolique et algébrique *ISSAC 2008*([17]).

Dans le Chapitre 5, nous proposons un algorithme certifié calculant la triangulation d'une surface algébrique implicite. Notre approche consiste à calculer d'abord la topologie d'une "silhouette" de la surface $\mathcal{S}$. La "silhouette" calculée partitionne l'espace en des cylindres connexes à l'intérieur desquels le nombre de nappes est constant. Ensuite des sections de la surface $\mathcal{S}$, permettant le maillage des nappes à l'intérieur de chaque cylindre, sont calculées. Concernant la phase de connection des différentes nappes, nous proposons un nouvel algorithme ne nécessitant pas le calcul de la topologie de sections de la surface en les points x-critiques de sa "silhouette". La connection est entièrement guidée par la topologie de

la "silhouette" calculée au départ. Une implémentation de l'algorithme a été effectuée avec MATHEMAGIX. Il est essentiel de remarquer qu'il s'agit du premier code disponible, complet et certifié calculant la topologie d'une surface algébrique implicite singulière. La complexité binaire de l'algorithme est dominée par la phase de calcul d'une "silhouette" de la surface, et est de $\tilde{O}_B(d^{21}\tau)$, où d est le degré du polynôme définissant la surface, et τ la taille binaire de ses coefficients. Ce travail a été soumis à la *Special Issue du Journal of Symbolic Computation 2009*.

Enfin dans le dernier chapitre nous évoquons un travail encours sur le calcul d'un arrangement de quadriques. Le calcul d'un tel arrangement sous-tend certains problèmes de géométrie algorithmique. Nous expliquons comment les techniques développées dans les chapitres précédents permettent d'aborder ce problème.

Chapitre 2

Prérequis algébriques

La première section de ce chapitre est une discussion sur les outils essentiels permettant la gestion des nombres algébriques. Nous faisons références aux algorithmes fondamentaux permettant de compter, de comparer et d'isoler les racines réelles d'un polynôme univarié à coefficients dans $\mathbb{Q}$ ou dans un anneau $\mathbb{Q}[\alpha]$, α étant un nombre algébrique. La deuxième section présente la résolution de systèmes algébriques réels zéro-dimensionnel. Nous évoquons les algorithmes fondamentaux qui sont à la base des solveurs de systèmes d'équations polynomiales comportant un nombre fini de solutions complexes. La troisième section est un rappel sur la théorie des sous-résultants. Nous y étudions les propriétés fondamentales des sous-résultants aidant à appréhender les problèmes sous-jacents au calcul de la topologie des courbes et surfaces algébriques réelles. La dernière section est un bref rappel sur la décomposition cylindrique algébrique, particulièrement axé sur l'algorithme de Collins et ses applications en calcul de topologie de variétés semi-algébriques réelles.

2.1 Gestion des nombres algébriques réels

Les objets que nous étudierons dans les chapitres suivants sont des courbes et des surfaces définies à l'aide d'équations polynomiales à coefficients rationnels. Nous allons principalement nous intéresser à leurs propriétés topologiques. Nous aurons donc besoin, au cours de l'exécution de nos algorithmes, de répondre à certains prédicats notamment : "la coordonnée selon l'axe des x de ce point est-elle plus grande que celle de cet autre point ?", "combien y a-t-il de points réels sur l'intersection d'une courbe avec une droite ?". La réponse à ces questions est naturellement liée au problème de la manipulation de nombres réels. En effet, durant l'exécution des algorithmes de calcul de topologie, apparaissent des polynômes univariés,

à coefficients entiers, rationnels ou algébriques, concentrant l'information topologique que nous cherchons à décrire. Pour extraire de manière certifiée cette information, il est nécessaire de pouvoir compter, isoler et comparer sans ambiguité les racines réelles de ces polynômes. Nous discutons les techniques usuelles permettant de traiter ces questions.

2.1.1 Dénombrement et isolation des racines réelles de $P \in \mathbb{Q}[X]$

Intéressons nous d'abord au problème du dénombrement et de l'isolation des racines réelles d'un polynôme univarié à coefficients rationnels. Etant donné un polynôme $P \in \mathbb{Q}[X]$, cela signifie construire une séquence d'intervalles de $\mathbb{R}$ deux à deux disjoints contenant chacun une et une seule racine de P. Il existe plusieurs techniques permettant de répondre à ces questions. Nous exposerons les trois principales méthodes dites de Sturm, de Descartes et de Thom. Nous nous sommes inspirés de [6] et [7] pour rédiger cette sous-section, les démonstrations des résultats exposés ici peuvent y être consultées.

La méthode de Sturm

Cette méthode est basée sur les propriétés des suites de Sturm associées au polynôme $P \in \mathbb{Q}[X]$ sur un intervalle $[a,b]$ de $\mathbb{R}$ et sur la notion de variation d'une séquence de nombre réels.

Définition 2.1.1 *Soient $P \in \mathbb{Q}[X]$, $(f_i)_{i\in[\![0,s]\!]}$ une séquence d'éléments de $\mathbb{Q}[X]$ et $[a,b]$ un intervalle de $\mathbb{R}$. On dit que $(f_i)_{i\in[\![0,s]\!]}$ est une séquence de Sturm associée à P sur $[a,b]$ si les conditions suivantes sont remplies :*

- $f_0 = P$;
- f_s *ne s'annule pas sur* $[a,b]$;
- *pour tout* $i \in [\![0,s]\!]$, *pour tout* $\alpha \in [a,b]$ *tel que* $f_i(\alpha) = 0$ *on a* $f_{i-1}(\alpha) f_{i+1}(\alpha) < 0$;
- *pour tout* $\alpha \in [a,b]$ *tel que* $f_0(\alpha) = 0$, *il existe* $\varepsilon > 0$ *tel que* $f_0(\alpha+\varepsilon) f_1(\alpha+\varepsilon) > 0$ *et* $f_0(\alpha-\varepsilon) f_1(\alpha-\varepsilon) < 0$.

Définition 2.1.2 *Soit $A := (a_0,\ldots,a_n)$ une séquence de nombres réels. On appelle variation (ou nombre de changements de signes) de A, noté $V(A)$ ou $V(a_0,\ldots,a_n)$, le nombre de paires $(i,i+k)$ $(k \geqslant 1)$ tels que $a_i a_{i+k} < 0$ et $a_{i+r} = 0$ pour $0 < r < k$.*

Exemple 2.1.3 Pour $A = (-9,0,2,0,0,7,0,-1,4)$, on a $V(A) = 3$.

Soient $P \in \mathbb{Q}[X]$ et $(f_i)_{i\in[\![0,s]\!]}$ une séquence de Sturm associée à P sur l'intervalle $[a,b]$. Soit $w : \mathbb{R} \longrightarrow \mathbb{N}$ l'application définie par $w(x) = V(f_0(x),\ldots,f_s(x))$. La proposition suivante explique l'intérêt porté aux suites de Sturm dans la résolution du problème du dénombrement et d'isolation des racines réelles d'un polynôme univarié.

Proposition 2.1.4 *Le nombre de racines réelles de P sur $]a,b]$ est égal à $(w(a)-w(b))$.*

Pour tout élément $Q \in \mathbb{Q}[X]$, nous noterons $\mathrm{lc}(Q)$ le coefficient de tête de Q. La proposition précédente s'étend sur l'intervalle $\mathbb{R}$.

Corollaire 2.1.5 *Soient $P \in \mathbb{Q}[X]$, $(f_i)_{i\in[\![0,s]\!]}$ une séquence de Sturm associée à P sur $\mathbb{R}$, $w(+\infty)$ la variation de $(\mathrm{lc}(f_0),\ldots,\mathrm{lc}(f_s))$ et $w(-\infty)$ celle de $(\mathrm{lc}(f_0(-X)),\ldots,\mathrm{lc}(f_s(-X)))$. Alors le nombre de racines réelles de P est égal à $(w(-\infty)-w(+\infty))$.*

La question qui se pose ensuite est celle du calcul effectif d'une suite de Sturm associée à P. La proposition suivante présente une manière algorithmique de construire une telle suite.

Proposition 2.1.6 *Soient $[a,b]$ un intervalle de $\mathbb{R}$ et $P \in \mathbb{Q}[X]$ un polynôme sans facteur carré. Soient $f_0 = P$, $f_1 = P'$ et pour $i \geqslant 2$ $f_{i-2} = f_{i-1}g_i - f_i$ avec $\deg(f_i) < \deg(f_{i-1})$ (f_i est l'opposé du reste de la division euclidienne de f_{i-2} par f_{i-1}). Soit s le plus petit entier naturel tel que f_s n'admette aucune racine réelle dans $[a,b]$. Alors la séquence $(f_i)_{i\in[\![0,s]\!]}$ est une séquence de Sturm associée à P sur $[a,b]$.*

Remarque 2.1.7 L'algorithme d'Euclide appliqué à $f_0 = P$ et $f_1 = P'$ termine en retournant $f_t := \mathrm{pgcd}(P,P')$. Comme nous avons supposé que P est sans facteur carré, alors f_t est une constante et n'admet donc pas de racine réelle. En pratique on choisit $s = t$.

Le théorème suivant, connu sous le nom de théorème de Sturm, est à la base de l'algorithme de séparation des racines réelles d'un polynôme univarié par la méthode de Sturm.

Théorème 2.1.8 *Soient $[a,b]$ un intervalle de $\mathbb{R}$ et $P \in \mathbb{Q}[X]$ un polynôme sans facteur carré. Soient $f_0 = P$, $f_1 = P'$ et pour $i \geqslant 2$ $f_{i-2} = f_{i-1}g_i - f_i$ avec $\deg(f_i) < \deg(f_{i-1})$ (f_i est l'opposé du reste de la division euclidienne de f_{i-2} par f_{i-1}). Soit s le plus petit entier naturel tel que f_s n'admette aucune racine réelle dans $[a,b]$. Alors le nombre de racines réelles de P sur $]a,b]$ est égal à $(w(a)-w(b))$ avec $w(a) = V(f_0(a),\ldots,f_s(a))$ et $w(b) = V(f_0(b),\ldots,f_s(b))$.*

Notation 2.1.9 *Soit $\tilde{O}_B$ la complexité binaire en ignorant les facteurs logarithmiques. Pour $a \in \mathbb{Z}^*$, nous désignons par $\mathcal{L}(a) := \lceil \log_2 |a| \rceil$ la taille binaire de l'entier a. Soit P un polynôme à coeffients entiers $(a_0,\ldots,a_n)$ (en une ou plusieurs variables), nous désignons par :*

$$\mathcal{L}(P) := \max(\mathcal{L}(a_0),\ldots,\mathcal{L}(a_n))$$

$$M := \sum_{i=0}^{n} |\frac{a_i}{a_n}|$$

Nous supposons que $\deg(P) = O(\mathcal{L}(P))$.

Proposition 2.1.10 *[43, 44, 55, 19] Soient* $P \in \mathbb{Z}[X]$, $n := \deg(P)$, $\tau := \mathcal{L}(P)$, $(f_i)_{i\in[\![0,s]\!]}$ *une séquence de Sturm associée à* P *sur* $\mathbb{R}$, $a \in \mathbb{Z}$ *et* $\sigma := \mathcal{L}(a)$. *Le calcul de* $V(f_0(a),\ldots,f_s(a))$ *s'effectue avec une complexité binaire de* $\tilde{O}_B(n^2\tau + n^2\sigma)$.

Corollaire 2.1.11 *[43, 44, 55, 19] Soient* $P \in \mathbb{Z}[X]$, $n := \deg(P)$, $\tau := \mathcal{L}(P)$ *et* $\sigma := \mathcal{L}(M)$. *La complexité binaire de l'algorithme de dénombrement des racines de* P *par la méthode de Sturm est de* $\tilde{O}_B(n^2\tau + n^2\sigma)$.

A présent voici l'algorithme de séparation des racines réelles d'un polynôme univarié à coeffients dans $\mathbb{R}$ par la méthode de Sturm. Précisons que séparer les racines réelles d'un polynôme consiste à fournir une séquence d'intervalles de $\mathbb{R}$ deux à deux disjoints contenant chacun une et une seule racine du polynôme.

Algorithme 2.1.1 : `Isolation des racines par la méthode de Sturm`

Entrées : $P = \sum_{i=0}^{n} a_i X^i$ sans facteur carré et $M = \sum_{i=0}^{n} |\frac{a_i}{a_n}|$

Sorties : Liste d'intervalles, chacun contenant exactement une racine de P

a) Construire une séquence de Sturm $(f_i)_{i\in[\![0,s]\!]}$ associée à P.
Pour $x \in \mathbb{R}$, soit $w(x) = V(f_0(x),\ldots,f_s(x))$.

b) Soit $x_0 = -M$, $x_1 = M$ et $w = w_1 = w(x_0) - w(x_1)$.
Si $w = 0$ alors P n'admet pas de racine réelle.
Si $w = 1$ alors P a exactement une racine dans $]x_0, x_1]$.
Si $w > 1$, soit $x_2 = \frac{1}{2}(x_0 + x_1)$. Calculer $w_2 = w(x_0) - w(x_2)$ et
$w_3 = w(x_2) - w(x_1)$ et retourner en b) avec $w = w_2$ puis $w = w_3$.

L'algorithme se termine lorsque les valeurs de tous les w_i calculés valent 0 ou 1.

La proposition suivante rappelle la complexité binaire d'un tel processus.

Proposition 2.1.12 *[19] Soient* $P \in \mathbb{Z}[X]$, $n := \deg(P)$ *et* $\tau := \mathcal{L}(P)$. *L'algorithme d'isolation des racines réelles de* P *par la méthode de Sturm a une complexité binaire de* $\tilde{O}_B(n^4\tau^2)$.

Démonstration En effet, l'algorithme d'isolation par la méthode Sturm réalise $O(n\tau)$ appels de l'algorithme de dénombrement. Les $O(n\tau)$ appels correspondent au nombre de subdivisions nécessaires pour isoler toutes les racines réelles de P. Les tailles binaires des entiers manipulés au cours de ce processus sont bornées bornes par $O(n^2 + n\tau)$. Ainsi par le Corol-

laire 2.1.11, la complexité binaire est de $O(n\tau) * \tilde{O}_B(n^2\tau + n^2(O(n^2 + n\tau))) = \tilde{O}_B(n^3\tau^2 + n^5\tau + n^4\tau^2)$. Comme $n = O(\tau)$, alors la complexité binaire est $\tilde{O}_B(n^4\tau^2)$. □

La méthode de Descartes

Cette méthode est basée sur le lemme de Descartes :

Lemme 2.1.13 *Soient $P = \sum_{i=0}^{n} a_i X^i$ un polynôme à coefficients réels et $A = (a_0, \ldots, a_n)$. Le nombre $N_+(P)$ de racines strictement positives de P comptées avec multiplicité est majoré par $V(A)$. De plus $N_+(P)$ est congru à $V(A)$ modulo 2.*

Pour l'isolation de racines, cette règle est souvent combinée à la manipulation de polynômes univariés écrits dans la base de Bernstein [49], [48].

Définition 2.1.14 *Un polynôme univarié P de degré n peut être représenté dans la base de Bernstein par :*

$$P(X) = \sum_{i=0}^{n} b_i B_i^n(X),$$

où $B_i^n(X) = \binom{n}{i} X^i (1-X)^{n-i}$. La suite $b = [b_i]_{i=0,\ldots,n}$ est appelée ensemble des coefficients de contrôle sur $[0,1]$. Les polynômes B_d^i forment la base de Bernstein sur $[0,1]$. De manière similaire, on dira qu'une séquence b représente le polynôme P sur l'intervalle $[a,b]$ si :

$$P(X) = \sum_{i=0}^{n} b_i \binom{n}{i} \frac{1}{(b-a)^n} (X-a)^n (b-X)^{n-i},$$

et les polynômes $\binom{d}{i} \frac{1}{(b-a)^n} (X-a)^n (b-X)^{n-i}$ forment la base de Bernstein sur $[a,b]$.

Si on connait un polynôme dans la base de Bernstein associée à un intervalle $[a,c]$, pour avoir les représentations de ce polynôme dans les bases associées à $[a,b]$ et $[b,c]$, on utilise l'algorithme de de Casteljau.

Dans la base de Bernstein, la règle de Descartes s'énonce comme suit :

Théorème 2.1.15 *Soit $V(b)$ le nombre de changements de signe dans la liste des coefficients de contrôle $b = [b_i], i = 1 \ldots d$, sur $[0,1]$ d'un polynôme univarié P, on a :*

1. *le nombre de racines de P sur $]0,1[$ est borné par $V(b)$;*
2. *le nombre de racines de P sur $]0,1[$ est congru à $V(b)$ modulo 2.*

On peut alors isoler, avec une précision ε fixée, les racines d'un polynôme $P = ([b],[a,c])$ ($[b]$ désigne les coordonnées de P dans la base de Bernstein sur l'intervalle $[a,c]$).

Algorithme 2.1.2 : `Isolation de racines par méthode de Descartes`

Entrées : Une précision ε et un polynôme représenté dans la base de Bernstein sur un intervalle $[a,c]$: $P = ([b],[a,c])$

Sorties : Une liste de sous-intervalles de $[a,c]$ contenant exactement une racine simple de P ou une racine à ε près, c'est-à-dire un point dans un intervalle de longueur inférieure à ε.

a) Calcul du nombre de changements de signe $V(b)$.

b) Si $V(b) > 1$ et $|c-a| > \varepsilon$, subdiviser la représentation en deux sous-représentations b^- et b^+ correspondant à la subdivision de l'intervalle en deux (algorithme de Casteljau) et appliquer récursivement l'algorithme à chacune des deux représentations.

c) Si $V(b) > 1$ et $|c-a| < \varepsilon$, renvoyer $(a+c)/2$ avec multiplicité $V(b)$.

d) Si $V(b) = 0$ supprimer l'intervalle $[a,c]$

e) Si $V(b) = 1$ l'intervalle contient exactement une racine qui peut être isolée à ε prés.

Proposition 2.1.16 *[27] Soient $P \in \mathbb{Z}[X]$, $n := \deg(P)$ et $\tau := \mathcal{L}(P)$. L'algorithme d'isolation des racines réelles de P par la méthode de Descartes a une complexité binaire de $\tilde{O}_B(n^4\tau^2)$.*

Encodage de Thom des racines réelles de $P \in \mathbb{Q}[X]$

Outre les méthodes de Descartes et de Sturm, l'encodage de Thom constitue une méthode permettant de dénombrer les racines réelles d'un polynôme. Le calcul d'encodage de Thom nécessite de disposer d'un algorithme de détermination de conditions de signe réalisées par une famille de polynômes en un ensemble fini de points. De tels algorithmes sont détaillés dans [6]. Nous rappelons ici ce qu'est l'encodage de Thom des racines réelles d'un polynôme univarié, et comment il est possible de l'utiliser pour compter les racines réelles d'un polynôme.

La caractérisation des racines réelles d'un polynôme par encodage de Thom est une méthode basée sur le lemme de Thom [6]. L'idée fondamentale de cette méthode est que les racines réelles de P se distinguent les unes des autres en comparant les signes pris par les dérivées successives de P. En d'autres termes, chaque racine réelle α de P possède sa signature qui est une succession de signes pris par l'évaluation des dérivées successives de P en α.

Soit $P \in \mathbb{Q}[X]$ un polynôme de degré n et $\mathrm{Der}(P)$ l'ensemble défini par :

$$\mathrm{Der}(P) := \{P^{(i)} \mid i = 0,\ldots,n\}$$

où $P^{(i)}$ désigne la dérivée d'ordre i du polynôme P.

Définition 2.1.17 *Une **condition de signe** σ sur l'ensemble* $\mathrm{Der}(P)$ *est un élément de*

$$\{0,1,-1\}^{\mathrm{Der}(P)} \text{ avec } \begin{cases} \sigma(x)=0 & \iff x=0 \\ \sigma(x)=1 & \iff x>0 \\ \sigma(x)=-1 & \iff x<0 \end{cases}$$

Définition 2.1.18 *Soit P un polynôme univarié à coefficients réels et σ une condition de signe sur l'ensemble* $\mathrm{Der}(P)$. *On appelle **réalisation d'une condition de signe** σ l'ensemble* $\mathcal{R}(\sigma) := \left\{ x \in \mathbb{R} \mid \bigwedge_{Q\in \mathrm{Der}(P)} \mathrm{signe}(Q(x)) = \sigma(Q) \right\}$. *On dira que la condition de signe est **réalisable** si $\mathcal{R}(\sigma)$ est non vide.*

A présent voici le lemme de Thom.

Lemme 2.1.19 *Soient P un polynôme univarié à coefficients réels et σ une condition de signe sur l'ensemble* $\mathrm{Der}(P)$. *Alors $\mathcal{R}(\sigma)$ est soit vide, soit réduit à un point, soit un intervalle ouvert.*

La proposition suivante est une conséquence du lemme de Thom.

Proposition 2.1.20 *Soient $P \in \mathbb{Q}[X]$ un polynôme de degré n, x et x' deux réels donnés. Soient σ et σ' les conditions de signe sur* $\mathrm{Der}(P)$ *réalisées en x et x'.*

1. *Si $\sigma = \sigma'$ avec $\sigma(P) = \sigma'(P) = 0$ alors $x = x'$.*
2. *Si $\sigma \neq \sigma'$ alors nous pouvons comparer x et x' de la manière suivante. Soit k le plus petit entier tel que $\sigma(P^{(n-k)}) \neq \sigma'(P^{(n-k)})$. Alors :*
   - $\sigma(P^{(n-k+1)}) = \sigma'(P^{(n-k+1)}) \neq 0$,
   - *si* $\sigma(P^{(n-k+1)}) = \sigma'(P^{(n-k+1)}) = 1$, *alors* $x > x' \iff \sigma(P^{(n-k)}) > \sigma'(P^{(n-k)})$,
   - *si* $\sigma(P^{(n-k+1)}) = \sigma'(P^{(n-k+1)}) = -1$, *alors* $x > x' \iff \sigma(P^{(n-k)}) < \sigma'(P^{(n-k)})$.

Définition 2.1.21 *Soient $P \in \mathbb{Q}[X]$ et $\sigma \in \{0,1,-1\}^{\mathrm{Der}(P)}$ une condition de signe sur l'ensemble* $\mathrm{Der}(P)$. *La condition de signe σ est **un encodage de Thom** de $x \in \mathbb{R}$ si $\sigma(P) = 0$ et si σ est la liste des signes réalisés par les éléments de* $\mathrm{Der}(P)$ *en x. Si tel est le cas, nous dirons que x est spécifié par σ.*

Etant donné un encodage de Thom σ, nous noterons $x(\sigma)$ la racine réelle de P dans $\mathbb{R}$ spécifiée par σ. L'intérêt du calcul des encodages de Thom d'une racine réelle de P réside dans le fait qu'il permet de la distinguer des autres racines réelles de P. La liste ordonnée des encodages de Thom de P est la liste $(\sigma_1, \ldots, \sigma_r)$ des encodages de Thom des racines

$x(\sigma_1) < \ldots < x(\sigma_r)$. Cette liste peut être obtenue grâce à un algorithme de détermination du signe d'un polynôme univarié. Ci-dessous, nous rappelons la complexité de l'algorithme de calcul de l'encodage de Thom d'un polynôme univarié. Pour plus de détails, consulter [6].

Proposition 2.1.22 *[6]Soient $P \in \mathbb{Z}[X]$, $n = \deg(P)$ et $\tau = \mathcal{L}(P)$. La complexité binaire de l'algorithme calculant l'encodage de Thom des racines de P est de $\tilde{O}_B(n^4\tau^2)$.*

Remarque 2.1.23 Pour l'isolation des racines, l'algorithme disposant de la meilleure complexité est celui de Schanhage-Pan [54]. Son algorithme calcule une approximation des racines avec une précison ε en $\tilde{O}_B(d^3\tau + d\varepsilon)$ avec $\varepsilon \in \tilde{O}(d\tau)$ qui est la borne de séparation pour un polynôme de degré d et des coefficients de taille τ. C'est l'algorithme que nous considérerons, dans la suite, lorsqu'on doit éffectuer une isolation.

Outre dénombrer ou isoler les racines réelles d'un polynôme, il arrive souvent qu'on ait besoin d'effectuer des comparaisons de nombres algébriques ou de déterminer le signe de l'évaluation d'un autre polynôme en un nombre algébrique donné. Il existe plusieurs méthodes permettant de répondre à ces questions, amplement décrites dans [6]. Dans la sous-section suivante nous exposons une méthode basée sur les suites de Sturm généralisées.

2.1.2 Suite de Sturm et comparaison de nombres algébriques réels

Nous tâcherons de répondre aux deux questions suivantes :

1. Soient $P, Q \in \mathbb{Q}[X]$ et α une racine réelle de P. Quel est le signe de $Q(\alpha)$?
2. Soient $P, Q \in \mathbb{Q}[X]$, $(\alpha, \beta) \in \mathbb{R}^2$ tel que $P(\alpha) = 0$ et $Q(\beta) = 0$. A-t-on $\alpha > \beta$, $\alpha < \beta$ ou $\alpha = \beta$?

Définition 2.1.24 *Soient $P, Q \in \mathbb{Q}[X]$. Une séquence de polynômes $(S_i)_{i \in [\![0,r]\!]}$ est une séquence de Sturm associée à P et Q si et seulement si :*

- *$S_0 = P$, $S_1 = Q$,*
- *pour tout $i \in [\![1, r]\!]$, S_r divise S_i,*
- *pour tout $j \in [\![1, r]\!]$, notant $\sigma_j := \frac{S_j}{S_r}$ on a :*
  si c est un réel tel que $\sigma_j(c) = 0$ avec $0 < j < r$ alors $\sigma_{j-1}(c)\sigma_{j+1}(c) < 0$;
  si c est un réel tel que $\sigma_0(c) = 0$ alors $\sigma_0\sigma_1$ est du signe de $X - c$ au voisinage de c.

Soient $P, Q \in \mathbb{Q}[X]$ et $(S_i)_{i \in [\![0,r]\!]}$ une séquence de Sturm associée à P et $P'Q$.
Soit $W : \mathbb{R} \longrightarrow \mathbb{N}$ l'application définie par $W(x) = V(S_0(x), \ldots, S_r(x))$. On a alors le théorème de Sturm généralisé :

Théorème 2.1.25 *Soient $P,Q \in \mathbb{Q}[X]$, $(S_i(X))_{i\in[\![0,r]\!]}$ une séquence de Sturm associée à P et $P'Q$ et $]a,b[$ un intervalle tel que $P(a)P(b) \neq 0$. Soit $Z_{Q>0}(P)$ (resp. $Z_{Q<0}(P)$) le nombre de racines $\alpha \in]a,b[$ de P telles que $Q(\alpha) > 0$ (resp. $Q(\alpha) < 0$). On a :*

$$Z_{Q>0}(P) - Z_{Q<0}(P) = W(a) - W(b)$$

Remarque 2.1.26 Dans le théorème précédent, si P ou Q sont sans facteur carré, le calcul de la suite de Sturm associée à P et Q est suffisant.

Le théorème de Sturm généralisé nous permet de répondre aux deux questions posées préalablement. En effet, soit α un nombre algébrique, racine d'un polynôme $P \in \mathbb{Q}[X]$, on cherche à évaluer pour un polynôme $Q \in \mathbb{Q}[X]$ donné, le signe de $Q(\alpha)$. Supposons que l'on ait isolé α dans un intervalle $]a,b[$ avec les techniques précédentes. Soit $(S_i)_{i\in[\![0,r]\!]}$ une séquence de Sturm associée à P et $P'Q$. Comme α est l'unique racine de P dans $]a,b[$, alors par le théorème de Sturm généralisé, $W(a) - W(b)$ vaut 1 si $Q(\alpha) > 0$, -1 si $Q(\alpha) < 0$ et 0 si $Q(\alpha) = 0$.
Concernant la deuxième question, considérons deux nombres algébriques α et β racines de $P \in \mathbb{Q}[X]$ et $Q \in \mathbb{Q}[X]$ respectivement. Supposons que l'on ait isolé α et β dans deux intervalles $]a,b[$ et $]c,d[$ avec les techniques précédentes. On cherche à comparer α et β. Pour simplifier la présentation, supposons que α et β sont des racines simples de P et Q. Si $b < c$ (resp. $d < a$), on a $\alpha < \beta$ (resp. $\beta < \alpha$). Supposons maintenant que $a < c < b < d$ (les autres cas se traitent de manière similaire). Tout d'abord, on calcule le signe s de $P(a)P(c)$. Si $s < 0$ alors on a $\alpha \in]a,c[$ et $\alpha < \beta$. Si $s = 0$, on a $\alpha = c$ (puisque $\alpha \neq a$), ce qui implique que $\alpha < \beta$. Si, $s > 0$, P n'a pas de racine dans l'intervalle $[a,c]$. Soit $(S_i)_{i\in[\![0,r]\!]}$ une séquence de Sturm associée à P et $P'Q$ et $v = W(c) - W(b)$. Supposons que $Q(c) > 0$ et $Q(b) < 0$. Alors si $v = 1$, on déduit du théorème de Sturm généralisé que : $Q(\alpha) > 0$ et $\alpha < \beta$. Si $v = -1$ et $Q(\alpha) < 0$ alors $\alpha > \beta$. Si $v = 0$, alors $Q(\alpha) = 0$ et $\alpha = \beta$. Le cas $Q(c) < 0$, $Q(b) > 0$ se traite de manière analogue. Enfin, si $Q(c)$ et $Q(b)$ ont même signe, on a $\alpha < \beta$.

La question que nous allons considérer à présent est fondamentale dans l'élaboration d'algorithmes certifiés de calcul de topologie de courbes et de surfaces algébriques réelles.

2.1.3 Dénombrement et isolation des racines réelles de $P \in \mathbb{Q}[\alpha][X]$

Soit α un nombre algébrique racine d'un polynôme $Q \in \mathbb{Q}[X]$. Supposons que l'on ait isolé α dans un intervalle $]a,b[$ avec les techniques précédentes. Soit $P \in \mathbb{Q}[\alpha][X]$ un polynôme à coefficients dans l'anneau $\mathbb{Q}[\alpha]$. On suppose que P est sans facteur carré. Dans ce qui suit, nous décrivons une méthode permettant de dénombrer puis d'isoler sans ambiguité les racines réelles de P, sachant que α est l'unique racine sur $]a,b[$ d'un polynôme $Q \in \mathbb{Q}[X]$.

Soit $(f_i)_{i\in[\![0,s]\!]} \in (\mathbb{Q}[\alpha][X])^{s+1}$ une séquence de Sturm associée à P sur $\mathbb{R}$. Soit $w(+\infty)$ la variation de $(\mathrm{lc}(f_0),\ldots,\mathrm{lc}(f_s))$ et $w(-\infty)$ celle de $(\mathrm{lc}(f_0(-X)),\ldots,\mathrm{lc}(f_s(-X)))$ où $\mathrm{lc}(f_i)$ désigne le coefficient de tête du polynôme f_i. Alors par le Corollaire 2.1.5, le nombre de racines réelles de P est égal à $(w(-\infty)-w(+\infty))$. Cependant comme pour tout $i\in[\![0,s]\!]$, $f_i\in\mathbb{Q}[\alpha][X]$, alors $\mathrm{lc}(f_i)\in\mathbb{Q}[\alpha]$. La détermination de son signe n'est donc pas immédiate. Elle passe par un calcul de séquence de Sturm généralisée tel que décrit dans la sous-section précédente.

Algorithme 2.1.3 : `Dénombrement des racines réelles de` $P\in\mathbb{Q}[\alpha][X]$

Entrées : $P\in\mathbb{Q}[\alpha][X]$, $Q\in\mathbb{Q}[X]$ tel que $Q(\alpha)=0$ et $]a,b[$ intervalle d'isolation
Sorties : Nombre de racines réelles de P

a) Construire la séquence $(\mathrm{lc}(f_i(X)))_{i\in[\![0,s]\!]}$ associée à P
b) Evaluer les signes de $(\mathrm{lc}(f_0(X)),\ldots,\mathrm{lc}(f_s(X)))$
c) Evaluer les signes de $(\mathrm{lc}(f_0(-X)),\ldots,\mathrm{lc}(f_s(-X)))$
d) Evaluer $w(+\infty)$ la variation de la séquence $(\mathrm{lc}(f_0(X)),\ldots,\mathrm{lc}(f_s(X)))$
e) Evaluer $w(-\infty)$ la variation de la séquence $(\mathrm{lc}(f_0(-X)),\ldots,\mathrm{lc}(f_s(-X)))$
f) Retourner $(w(-\infty)-w(+\infty))$

Proposition 2.1.27 *Soient* $n:=\deg(P)$, $m:=\deg(Q)$, $\tau_P:=\mathcal{L}(P)$ *et* $\tau_Q:=\mathcal{L}(Q)$. *La complexité binaire de l'algorithme de dénombrement des racines réelles de* $P\in\mathbb{Q}[\alpha][X]$ *avec* $Q(\alpha)=0$, *est de* $\tilde{O}_B(mn^3\times max(n\tau_P,\tau_Q))$.

Démonstration En effet, d'après le Théorème 2.3.10, l'étape a) a un coût binaire de $\tilde{O}_B(n^4\tau_P)$ et retourne une liste $(f_i)_{i\in[\![0,n]\!]}$ de polynômes de degrés bornés par n^2 et dont les coefficients sont de taille $O(n\tau_P)$. Toujours par le Theorème 2.3.10, comme $\deg(\mathrm{lc}(f_i))=O(n^2)$ et $\mathcal{L}(\mathrm{lc}(f_i))=O(n\tau_P)$ alors l'évalution du signe de $\mathrm{lc}(f_i)$ a un coût binaire de $\tilde{O}_B(m(n^2)\times max(n\tau_P,\tau_Q))=\tilde{O}_B(mn^2\times max(n\tau_P,\tau_Q))$. Cette opération devant être répétée pour tous les $\mathrm{lc}(f_i)$, on arrive à une complexité binaire de $\tilde{O}_B(mn^3\times max(n\tau_P,\tau_Q))$. □

Quant à l'isolation des racines, elle s'opère avec une variante de l'algorithme d'isolation par la méthode de Sturm et nécessite $O(n\tau_P)$ appels de l'algorithme précédent. Conduisant ainsi à la complexité binaire rappelée ci-dessous.

Corollaire 2.1.28 *Soient* $n:=\deg(P)$, $m:=\deg(Q)$, $\tau_P:=\mathcal{L}(P)$ *et* $\tau_Q:=\mathcal{L}(Q)$. *La complexité binaire de l'algorithme d'isolation des racines réelles de* $P\in\mathbb{Q}[\alpha][X]$ *avec* $Q(\alpha)=0$, *est de* $\tilde{O}_B(mn^4\times max(n^2\tau_P,\tau_Q))$.

2.2 Résolution de systèmes zéro-dimensionnels

Dans les algorithmes que nous décrivons dans cette thèse, il arrive souvent que l'on ait besoin de résoudre efficacement des systèmes polynomiaux ayant un nombre fini de solutions complexes. Différentes approches existent pour résoudre de tels systèmes :

- les méthodes analytiques qui consistent à suivre les racines durant un processus itératif, comme Newton, Weierstrass [57], Aberth [9] ;
- les méthodes par homotopie [60] ;
- les methodes numériques de subdivision [47] ;
- les méthodes matricielles [26] ;
- Les méthodes algébriques basées sur des systèmes de réécriture [52, 51, 56, 28].

Nous nous sommes inspirés de [25] pour rédiger cette section. Nous rappelons ici deux algorithmes algébriques qui transforment la résolution d'un sytème zéro-dimensionnel en des problèmes d'algèbre linéaire.

Soient $f_1,\ldots,f_n \in \mathbb{R}[X_1,\ldots,X_m]$ tels que le système $\{f_1=0,\ldots,f_n=0\}$ soit de dimension 0. Considérons l'idéal engendré par les polynômes $f_1,\ldots,f_n$, $I := \langle f_1,\ldots,f_n\rangle$, et $\mathcal{A} := \mathbb{R}[X_1,\ldots,X_m]/I$ l'algèbre quotient associée à I. Pour tout $a \in \mathcal{A}$ soit M_a l'opérateur de multiplication par a dans $\mathcal{A}$ et ${}^tM_a$ l'endomorphisme transposé de M_a.

La résolution des systèmes polynomiaux par des méthodes matricielles est basée sur le résultat suivant :

Théorème 2.2.1 *Soit $(\zeta_1,\ldots,\zeta_D)$ l'ensemble des solutions complexes de notre système. Nous avons :*

- *pour tout $a \in \mathcal{A}$, les valeurs propres de M_a (et ${}^tM_a$) sont $a(\zeta_1),\ldots,a(\zeta_D)$.*
- *pour tout $a \in \mathcal{A}$, les formes linéaires évaluations $1_{\zeta_1},\ldots,1_{\zeta_D}$ sont des vecteurs propres ${}^tM_a$ associés respectivement aux valeurs propres $a(\zeta_1),\ldots,a(\zeta_D)$. De plus, à un scalaire près, ce sont les seuls vecteurs propres communs à tous les endomorphismes ${}^tM_a$, $a \in \mathcal{A}$.*

Ce théorème permet de réduire la résolution d'un système zéro-dimensionnel à un problème d'algèbre linéaire. Les algorithmes de résolution basés sur ce théorème ont besoin de construire les matrices de multiplication dans $\mathcal{A}$ et font appel à des calculs de formes normales [51], ou de formes normales généralisées [46], [52]. Les différentes étapes du processus de résolution sont résumées dans l'algorithme suivant :

Algorithme 2.2.1 : `Résolution de systèmes 0-dimensionnels`

Entrées : $I = \langle f_1, \ldots, f_n \rangle$

Sorties : $\{\zeta_1, \ldots, \zeta_D\}$ liste des solutions du système $\{f_1 = 0, \ldots, f_n = 0\}$

a) Calcul d'une base de $\mathcal{A}$.

b) En déduire les matrices de multiplication par $X_1, \ldots, X_m$ dans cette base.

c) Calculer simultanément les vecteurs propres de ${}^tM_{X_1}, \ldots, {}^tM_{X_m}$ ainsi que les valeurs propres correspondantes.

Une autre technique de résolution de système zéro-dimensionnel utilisant des calculs de matrices de multiplication est la Représentation Univariée Rationnelle (R.U.R). La R.U.R est la description des solutions d'un système multivarié et zéro-dimensionnel $\{f_1 = 0, \ldots, f_n = 0\}$ à l'aide des zéros d'un polynôme en une variable et d'une application rationnelle. Cette approche se prête bien aux calculs exacts sur des nombres algébriques, mais la méthode des vecteurs propres décrites précedemment est plus avantageuse en terme de coût. Nous résumons ci-dessous les différentes étapes de l'algorithme de calcul de la R.U.R des solutions d'un système zéro-dimensionnel. Les détails concernant cet algorithme peuvent être consultés dans [56, 25].

Algorithme 2.2.2 : `Calcul D'une Représentation Univariée Rationnelle`

Entrées : $f_1, \ldots, f_n \in \mathbb{R}[X_1, \ldots, X_m]$ et $I = \langle f_1, \ldots, f_n \rangle$

Sorties : Une liste de polynômes univariés $(d_0, d_1, \ldots, d_m)$ tel que :
$\zeta_1 = \frac{d_1(\alpha)}{d_0'(\alpha)}, \ldots, \zeta_m = \frac{d_m(\alpha)}{d_0'(\alpha)}$, avec α racine de d_0.

a) Calcul d'une base de $\mathcal{A}$.

b) En déduire les matrices de multiplication par $X_1, \ldots, X_m$ dans cette base.

c) Calculer le determinant $\Delta(u_0, \ldots., u_m) := \det(u_0 \mathrm{Id} + u_1 M_{X_1} + \ldots + u_m M_{X_m})$ et sa partie sans facteur carré $d(u_0, \ldots, u_m)$.

d) Choisir un $(t_1, \ldots, t_m) \in \mathbb{R}^m$ générique et calculer les premiers coefficients de $d(u_0, t_1 + u_1, \ldots, t_m + u_m)$, considéré comme polynôme en $u_1, \ldots, u_m$:

$$d(u_0, t_1 + u_1, \ldots, t_m + u_m) = d_0(u_0) + u_1 d_1(u_0) + \ldots + u_m d_m(u_0) + \ldots$$

La condition de généricité requise pour $(t_1, \ldots, t_m) \in \mathbb{R}^m$ est que ce m-uplet *sépare* les solutions du système, c'est-à-dire pour tout $\zeta_k = (\zeta_{k,1}, \ldots, \zeta_{k,m})$ et $\zeta_j = (\zeta_{j,1}, \ldots, \zeta_{j,m})$, $\zeta_k \neq \zeta_j \Longrightarrow \sum_{i=1}^m t_i.\zeta_{k,i} \neq \sum_{i=1}^m t_i \zeta_{j,i}$.

2.3 Sous-résultants

La théorie des sous-résultants est un outil essentiel pour l'étude de la topologie des courbes et des surfaces algébriques. Elle permet de répondre de manière précise à plusieurs questions d'ordre géométrique. Par exemple, considérons deux courbes algébriques planes d'équations respectives $f(X,Y)=0$ et $g(X,Y)=0$ et α un nombre algébrique donné. Nous nous intéressons aux propriétés géométriques de leurs points d'intersections d'abscisse α. Pour trouver ces points, nous devons calculer le plus grand diviseur commun, noté pgcd, des polynômes $f(\alpha,Y)$ et $g(\alpha,Y)$. Au lieu de calculer ce pgcd avec l'algorithme d'Euclide, nous utiliserons la théorie des polynômes sous-résultants. Les raisons de ce choix résident principalement dans les propriétés importantes de ces polynômes. En effet :

1. Ils se définissent comme des expressions algébriques en les coefficients de $f(X,Y)$ et $g(X,Y)$.
2. Leurs coefficients de tête nous indiquent le degré du pgcd de $f(\alpha,Y)$ et de $g(\alpha,Y)$.
3. La séquence des polynômes sous-résultants contient tous les polynômes qui apparaissent au cours de l'algorithme d'Euclide mais avec des tailles de coefficients plus petites.
4. Les polynômes sous-résultants ont un comportement intéressant par rapport aux homomorphismes : en effet, si φ est un homomorphisme d'anneaux qui préserve le degré de f et g, alors la suite des polynômes sous-résultants associée aux polynômes $\varphi(f)$ et $\varphi(g)$ est l'image par φ de la suite des polynômes sous-résultants associée à f et g.

Cette dernière propriété est particulièrement utile quand on travaille sur des objets géométriques. Nous nous sommes inspirés de [7] et [6] pour rédiger cette section.

2.3.1 Définition et principales propriétés des sous-résultants

Soit $\mathbb{A}$ un anneau commutatif unitaire et intègre. Soient $P=\sum_{i=0}^{p} a_i X^i$, $Q=\sum_{i=0}^{q} b_i X^i$ deux polynômes à coefficients dans $\mathbb{A}$, de degré respectif p et q. Pour tout $r \geqslant 0$, notons $\mathbb{A}[X]_r$ l'ensemble des éléments de $\mathbb{A}[X]$ de degré inférieur ou égal à r. Soit $\Psi : \mathbb{A}[X]_{q-1} \times \mathbb{A}[X]_{p-1} \to \mathbb{A}[X]_{q+p-1}$ l'application $\mathbb{A}$-linéaire définie par $\Psi(U,V)=P\,U+Q\,V$ et $M(P,Q)$ la matrice, à $(p+q)$ lignes et $(p+q)$ colonnes, associée à Ψ dans les bases monomiales de $\mathbb{A}[X]_{q-1} \times \mathbb{A}[X]_{p-1}$ et de $\mathbb{A}[X]_{q+p-1}$:

$$M(P,Q)=\begin{pmatrix} a_0 & & & b_0 & & \\ \vdots & \ddots & & \vdots & \ddots & \\ a_p & & a_0 & b_q & & b_0 \\ & \ddots & \vdots & & \ddots & \vdots \\ & & a_p & & & b_q \end{pmatrix}$$

La matrice $M(P,Q)$ s'appelle matrice de Sylvester associée à P et Q.

Définition 2.3.1 *On appelle résultant de P et Q, noté* $\mathrm{Res}(P,Q)$*, le déterminant de la matrice de Sylvester associée à P et Q :*

$$\mathrm{Res}(P,Q) = \det(M(P,Q))$$

L'intérêt majeur du résultant associé à P et Q, tient au fait qu'il donne une conditon nécessaire et suffisante pour que P et Q aient un facteur commun dans $\mathbb{A}[X]$.

Théorème 2.3.2 *Soient* $P,Q \in \mathbb{A}[X]$*, alors* $\mathrm{Res}(P,Q) = 0$ *si et seulement si P et Q ont un facteur commun dans* $\mathbb{A}[X]$.

Le résultant nous indique seulement que P et Q ont un facteur commun. L'outil qui permet d'en savoir plus sur ce facteur commun est la suite des sous-résultants associée à P et Q.
Soient $k \in [\![0, \inf(p,q)]\!]$, $\Psi_k : \mathbb{A}[X]_{q-k-1} \times \mathbb{A}[X]_{p-k-1} \to \mathbb{A}[X]_{q+p-k-1}$ l'application $\mathbb{A}$-linéaire définie par $\Psi_k(U,V) = P\,U + Q\,V$ et $M_k(P,Q)$ la matrice, à $(p+q-2k)$ lignes et $(p+q-k)$ colonnes, associée à l'application Ψ_k dans les bases canoniques de $\mathbb{A}[X]_{q-k-1} \times \mathbb{A}[X]_{p-k-1}$ et de $\mathbb{A}[X]_{q+p-k-1}$.
Soit $\mathrm{sr}_{k,i}(P,Q) \in \mathbb{A}$ le déterminant de la sous matrice $(p+q-2k) \times (p+q-2k)$ de $M_k(P,Q)$ formée à partir :

- des $(p+q-2k-1)$ dernières colonnes de $M_k(P,Q)$,
- de la i^{eme} colonne de $M_k(P,Q)$,
- de toutes les lignes de $M_k(P,Q)$.

Définition 2.3.3 *On appelle* k^{eme} *sous-résultant associé aux polynômes P et Q, l'élément de* $\mathbb{A}[X]_k$ *défini par :*

$$\mathrm{Sr}_k(P,Q) = \sum_{i=0}^{k} \mathrm{sr}_{k,i}(P,Q) X^i$$

Pour tout $(k,i) \in [\![0, \inf(p,q)]\!] \times [\![0,k]\!]$, $\mathrm{sr}_{k,i}(P,Q) \in \mathbb{A}$ *se nomme le* $(k,i)^{\text{eme}}$ *coefficient sous-résultant associé à P et Q. En particulier, pour* $i = k$, $\mathrm{sr}_{k,k}(P,Q)$ *s'appelle* k^{eme} *coefficient sous-résultant principal.*

Remarque 2.3.4

1. Pour $k = 0$, $M_0(P,Q)$ correspond à la matrice de Sylvester, par conséquent $\mathrm{Sr}_0(P,Q) = \mathrm{sr}_{0,0}(P,Q) = \det(M_0(P,Q)) = \mathrm{Res}(P,Q)$.
2. Si $q < p$, nous avons $\mathrm{Sr}_q(P,Q) = (b_q)^{p-q-1} Q(X)$ et $\mathrm{sr}_{q,q}(P,Q) = (b_q)^{p-q}$.
3. Pour $i \in [\![k, p+q-k-1]\!]$, on a $\mathrm{sr}_{k,i}(P,Q) = 0$ car c'est le déterminant d'une matrice ayant deux colonnes identiques. Donc on peut écrire $\mathrm{Sr}_k(P,Q) = \sum_{i=0}^{p+q-k-1} \mathrm{sr}_{k,i}(P,Q) X^i$.

Lemme 2.3.5 *Pour tout* $k \in [\![0, \inf(p,q)]\!]$, $\mathrm{Sr}_k(P,Q) \in \mathrm{Im}\,\Psi_k$.

Démonstration Soit $M_k(P,Q) = (c_{i,j})_{(i,j)\in[\![1,p+q-2k]\!]\times[\![0,p+q-k-1]\!]}$. Developpant $\mathrm{sr}_{k,j}(P,Q)$ par rapport à sa première colonne, on obtient :

$$\mathrm{sr}_{k,j}(P,Q) = \sum_{i=1}^{p+q-2k} (-1)^{1+i} c_{i,j} m_{i,k}$$

où $m_{i,k}$ est le déterminant de la matrice formée par les $(p+q-2k-1)$ dernières colonnes de $M_k(P,Q)$ et de toutes ses lignes à l'exception de la i^{eme}. Par le troisième point de la remarque précédente on a :

$$\begin{array}{rcl} \mathrm{Sr}_k(P,Q) & = & \sum_{j=0}^{p+q-k-1} \mathrm{sr}_{k,j}(P,Q) X^j = \sum_{j=0}^{p+q-k-1} \sum_{i=1}^{p+q-2k} (-1)^{i+1} c_{i,j} m_{i,k} X^j \\ & = & \sum_{i=1}^{p+q-2k} (-1)^{i+1} m_{i,k} \sum_{j=0}^{p+q-k-1} c_{i,j} X^j \\ & = & \sum_{i=1}^{p+q-2k} (-1)^{i+1} m_{i,k} A_i \qquad \text{où} \qquad A_i = \sum_{j=0}^{p+q-k-1} c_{i,j} X^j \end{array}$$

Pour tout $i \in [\![1, p+q-2k]\!]$, $A_i \in \mathrm{Im}\,\Psi_k$. En effet, pour tout $i \in [\![1, q-k]\!]$ $A_i = X^{i-1}P$ et pour tout $i \in [\![q-k+1, p+q-2k]\!]$ $A_i = X^{i-1-q+k}Q$. Comme $\mathrm{Im}\,\Psi_k$ est stable par combinaisons linéaires, il vient que $\mathrm{Sr}_k(P,Q) \in \mathrm{Im}\,\Psi_k$. □

La proposition suivante justifie le nom de sous-pgcd souvent donné aux polynômes sous-résultants.

Proposition 2.3.6 *Soient* $P, Q \in \mathbb{A}[X]$, $D = \mathrm{pgcd}(P,Q)$, p, q *et* d *leur degré respectif et* $k \in [\![0,d]\!]$. *On a :*

1. $k < d \iff \Psi_k$ *non injective* $\iff \mathrm{Sr}_k(P,Q) = 0 \iff \mathrm{sr}_{k,k}(P,Q) = 0$.
2. *Si* $k = d$, *alors* $\mathrm{sr}_{k,k}(P,Q) \neq 0$ *et* $\mathrm{Sr}_k(P,Q) = \mathrm{pgcd}(P,Q)$.

Démonstration

1. $k < d \Longrightarrow \Psi_k$ injective : soient $P_1, Q_1 \in \mathbb{A}[X]$ tels que $P = P_1 D$, $Q = Q_1 D$. Comme $d > k \geqslant 0$ alors $\deg(P_1) = p - d < p - k$ et $\deg(Q_1) < q - k$. Donc $(Q_1, P_1) \in \ker \Psi_k$ d'où Ψ_k est non injective.

   Ψ_k injective $\Longrightarrow \mathrm{Sr}_k(P,Q) = 0$: Comme Ψ_k est non injective alors les colonnes de $M_k(P,Q)$ sont linéairement dépendantes d'où $\mathrm{Sr}_k(P,Q) = 0$.

   $\mathrm{Sr}_k(P,Q) = 0 \Longrightarrow \mathrm{sr}_{k,k}(P,Q) = 0$: Comme $\mathrm{Sr}_k(P,Q) = \sum_{i=0}^{k} \mathrm{sr}_{k,i}(P,Q) X^i$ alors $\mathrm{Sr}_k(P,Q) = 0 \Longrightarrow \mathrm{sr}_{k,k}(P,Q) = 0$.

   $\mathrm{sr}_{k,k}(P,Q) = 0 \Longrightarrow k < d$: résulte de 2.
2. Par le théorème de Bézout il existe $U, V \in \mathbb{A}[X]$ tel que $\deg(U) \leqslant q - d - 1$, $\deg(V) \leqslant p - d - 1$ et $D = PU + QV$. Donc $D \in \mathrm{Im}\,\Psi_d$. Par ailleurs tout élément de $\mathrm{Im}\,\Psi_d$ est un

multiple de D car l'ensemble des polynômes $PU+QV$ est un idéal principal dont D est un générateur. Par le lemme précédent, $\mathrm{Sr}_d(P,Q) \in \mathrm{Im}\,\Psi_d$, donc $\mathrm{Sr}_d(P,Q)$ est un multiple de D. Comme par hypothèse $\deg(\mathrm{Sr}_d(P,Q)) \leqslant d$ alors $\mathrm{Sr}_d(P,Q) = \lambda D$ avec $\lambda \in \mathbb{A}$. Puisque $\mathrm{sr}_{d,d}(P,Q) \neq 0$, λ est non nul. Ainsi $\mathrm{Sr}_d(P,Q)$ est le pgcd de P et Q.

□

De cette proposition découle le théorème fondamental des polynômes sous-résultants.

Théorème 2.3.7 *Soient $P,Q \in \mathbb{A}[X]$ de degrés respectifs p et q et $k \in [\![0, \inf(p,q)]\!]$. Alors* $\mathrm{pgcd}(P,Q) = \mathrm{Sr}_k(P,Q)$ *si et seulement si :*

$$\mathrm{sr}_{0,0}(P,Q) = \ldots = \mathrm{sr}_{k-1,k-1}(P,Q) = 0 \text{ et } \mathrm{sr}_{k,k}(P,Q) \neq 0.$$

Soit $\mathbb{A}'$ un anneau commutatif unitaire et intègre et $\varphi : \mathbb{A} \longrightarrow \mathbb{A}'$ un homomorphisme d'anneaux. Notons encore φ l'homomorphisme de $\mathbb{A}[X] \longrightarrow \mathbb{A}'[X]$ qui à $f = \sum_{i=0}^{n} f_i X^i$ associe $\varphi(f) = \sum_{i=0}^{n} \varphi(f_i) X^i$. Alors nous avons le théorème suivant appelé propriété de spécialisation des sous-résultants :

Théorème 2.3.8 *Si $a_p \notin \ker\varphi$ et $b_q \notin \ker\varphi$ alors pour tout $k \in [\![0, \inf(p,q)]\!]$ on a :*

$$\mathrm{Sr}_k(\varphi(P), \varphi(Q)) = \varphi(\mathrm{Sr}_k(P,Q))$$

.

Remarque 2.3.9 Le nom de ce théorème vient de son application principale : soient $\mathbb{A} = \mathbb{R}[Y]$, $\alpha \in \mathbb{R}$ et φ l'homomorphisme de $\mathbb{A}$ dans $\mathbb{R}$ qui spécialise Y à α. Alors pour $P,Q \in \mathbb{A}[X]$, $\mathrm{Sr}_k(P(\alpha,X), Q(\alpha,Y)) = \mathrm{Sr}_k(P(X,Y), Q(X,Y))(\alpha)$.

2.3.2 Algorithme de calcul des sous-résultants

Soit $\mathbb{A}$ un anneau commutatif unitaire et intègre. Soient $P = \sum_{i=0}^{p} a_i X^i$, $Q = \sum_{i=0}^{q} b_i X^i$ deux polynômes à coefficients dans $\mathbb{A}$ de degrés respectifs p et q.
Soit S la séquence $(\mathrm{Sr}_k(P,Q))_{k \in [\![0,\inf(p,q)]\!]}$ des polynômes sous-résultants associés à P et Q. L'algorithme suivant, extrait de [21], calcule la séquence S des polynômes sous-résultants non nuls. Dans cet algorithme, "`prem`" désigne le pseudo-reste, $\cup$ permet de concaténer deux listes.

Algorithme 2.3.1 : `Calcul des polynômes sous-résultants`

Entrées : $P, Q \in \mathbb{A}[X]$ avec $\deg(P) \geqslant \deg(Q) \geqslant 1$

Sorties : Séquence S des polynômes sous-résultants associés à P et Q

1. $S := []$, $s := \mathrm{lc}(Q)^{\deg(P)-\deg(Q)}$, $A := Q$, $B := \mathtt{prem}(P, -Q)$
   boucle
2. $d := \deg(A)$, $e := \deg(B)$,
3. Si $B = 0$ alors Retourner S,
4. Si $B \neq 0$ alors
   $S := [B] \cup S$,
   $\delta = d - e$,
   Si $\delta > 1$ alors $C := \frac{\mathrm{lc}(B)^{\delta-1}B}{s^{\delta-1}}$, $S := [C] \cup S$
   Si $\delta \leqslant 1$ alors $C := B$,
5. Si $e = 0$ alors Retourner S,
6. Si $e > 0$ alors $B := \frac{\mathtt{prem}(A,-B)}{s^{\delta}\,\mathrm{lc}(A)}$, $A := C$, $s := \mathrm{lc}(A)$
   Fin boucle

Soient $P, Q \in \mathbb{Z}[Y_1, \ldots, Y_k][X]$, $\deg_X(P) = p \geqslant q = \deg_X(Q)$, $d_i := \max(\deg_{Y_i}(P), \deg_{Y_i}(Q))$ et $d = \prod_{i=1}^{k} d_i$. On suppose que les coefficients entiers de P et Q sont de taille majorée par τ. Alors on a le théorème suivant :

Théorème 2.3.10 *[55, 20] Il existe un algorithme calculant la suite des coefficients sous-résultants principaux (respectivement des sous-résultants), par rapport à la variable X, associée à P et Q avec un coût binaire de $\tilde{O}_B(q(p+q)^{k+1}d\tau)$ (respectivement $\tilde{O}_B(q(p+q)^{k+2}d\tau)$). De plus pour tout $i \in [\![0, q]\!]$, la taille des coefficients de $\mathrm{Sr}_i(P, Q)$ est $O(p\tau)$.*

La section suivante est un rappel sur la décomposition cylindrique algébrique, plus particulièrement son intérêt pour le calcul de topologie de variétés semi-algébriques

2.4 Décomposition cylindrique algébrique

Les premiers algorithmes permettant de décider si une formule du premier ordre est vraie, se trouvent dans les travaux de Tarski et Seidenberg. La complexité de ceux-ci n'était pas élémentairement récursive. L'algorithme de décomposition cylindrique algébrique de Collins [14] a une bien meilleure complexité et est l'algorithme le plus connu pour décider si une formule du premier ordre est vraie. Dans cette section, nous rappelons la définition de la Décomposition Cylindrique Algébrique adaptée àune famille de polynômes ainsi que l'algo-

rithme de Collins. Puis nous montrerons comment cet algorithme est utilisé pour calculer la topologie de variétés algébriques réelles. La rédaction de cette sous-section fait réference à [6].

2.4.1 Ensembles et fonctions semi-algébriques

Définition 2.4.1 *Un ensemble semi algébrique de $\mathbb{R}^n$ est un sous-ensemble de $\mathbb{R}^n$ vérifiant une combinaison booléenne d'équations et d'inéquations polynomiales.*

Proposition 2.4.2 *Tout ensemble semi-algébrique de $\mathbb{R}^n$ est réunion finie de sous-ensembles de la forme :*

$$\{M \in \mathbb{R}^n \mid P(M) = 0 \text{ et } Q_1(M) > 0, \ldots, Q_l(M) > 0\}$$

avec $l \in \mathbb{N}$ et $P, Q_1, \ldots, Q_l \in \mathbb{R}[X_1, \ldots, X_n]$.

L'ensemble des ensembles semi-algébriques de $\mathbb{R}^n$ possède des propriétés de stabilité (par unions, intersections finies, passage au complémentaire, image réciproque par une application polynomiale, produit cartésien). Une autre propriété importante est la stabilité par projection.

Théorème 2.4.3 $(\textit{Version génométrique}-\textit{Tarski-Seidenberg})$
Soit $\mathcal{S}$ un ensemble semi-algébrique de $\mathbb{R}^n$ et π la projection qui à tout point $(x_1, \ldots, x_n)$ associe $(x_1, \ldots, x_{n-1})$. Alors $\pi(\mathcal{S})$ est un ensemble semi-algébrique de $\mathbb{R}^{n-1}$.

Les conséquences de ce résultat sont multiples, en voici quelques-unes.

Corollaire 2.4.4

- *Soit $\mathcal{S}$ un ensemble semi-algébrique de $\mathbb{R}^{n+k}$, son image par la projection qui à tout point $(x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+k})$ associe $(x_1, \ldots, x_n)$ est un ensemble semi-algébrique de $\mathbb{R}^n$.*
- *Soit $\mathcal{S}$ un ensemble semi-algébrique de $\mathbb{R}^n$ et F une application polynomiale de $\mathbb{R}^n$ dans $\mathbb{R}^m$. Alors $F(\mathcal{S})$ est un ensemble semi-algébrique de $\mathbb{R}^m$.*

Définition 2.4.5 *Formule du premier ordre.*

1. *Si $P \in \mathbb{R}[X_1, \ldots, X_n]$ alors $P = 0$ et $P > 0$ sont des formules.*
2. *Si Φ et Ψ sont des formules, alors Φ et Ψ, Φ ou Ψ, non Φ sont des formules.*
3. *Si Φ est une formule, X une variable réelle, alors $\exists X \Phi$ et $\forall X \Phi$ sont des formules.*

L'ensemble des formules ainsi obtenues s'appelle l'ensemble des formules du premier ordre à paramètres dans $\mathbb{R}$. L'ensemble des formules obtenues avec 1 et 2 s'appelle l'ensemble des formules sans quantificateur.

Un ensemble $\mathcal{S} \in \mathbb{R}^n$ est semi-algébrique si et seulement si il existe une formule sans quantificateur $\Phi(X_1,\ldots,X_n)$ telle que :

$$(x_1,\ldots,x_n) \in \mathcal{S} \Longleftrightarrow \Phi(X_1,\ldots,X_n).$$

Théorème 2.4.6 (*Version logique−Tarski-Seidenberg*)
Si Φ est une formule du premier ordre dont les variables libres sont $(x_1,\ldots,x_n)$, l'ensemble des $(x_1,\ldots,x_n) \in \mathbb{R}^n$ qui satisfont Φ est un sous ensemble semi-algébrique de $\mathbb{R}^n$.

Définition 2.4.7 *Soit $A \subset \mathbb{R}^m$ et $B \subset \mathbb{R}^n$ deux ensembles semi-algébriques. Une fonction $f : A \longrightarrow B$ est dite semi-algébrique si et seulement si son graphe :*

$$\Gamma_f = \{(M,N) \in A \times B \mid N = f(M)\}$$

est un ensemble semi-algébrique de $\mathbb{R}^m \times \mathbb{R}^n$.

Des propriétés importantes découlent du théorème de Tarski-Seidenberg :

Corollaire 2.4.8

- *L'image d'un ensemble semi-algébrique par une fonction semi-algébrique est un ensemble semi-algébrique. De même pour l'image réciproque.*
- *La composée de deux fonctions semi-algébriques est une fonction semi-algébrique.*

Définition 2.4.9 *Un ensemble semi-algébrique $\mathcal{S}$ est dit semi-algébriquement connexe quand pour tout M et N de $\mathcal{S}$, il existe une fonction semi-algébrique continue $\phi : [0,1] \longrightarrow \mathcal{S}$ telle que $\phi(0) = M$ et $\phi(N) = 1$.*

Proposition 2.4.10 *Le nombre de composantes semi-algébriquement connexes d'un ensemble semi-algébrique quelconque est fini.*

2.4.2 Décomposition cylindrique algébrique

Une **décomposition** d'un ensemble semi-algébrique S est une partition finie de S en sous-ensembles semi-algébriques. Une décomposition cylindrique algébrique de $\mathbb{R}^n$ est une suite $\mathcal{S}_1,\ldots,\mathcal{S}_n$ telle que pour tout $i \in [\![1,n]\!]$, $\mathcal{S}_i$ soit une décomposition de $\mathbb{R}^i$ en sous-ensembles semi-algébriques connexes appelés **cellules** et ayant les propriétés suivantes :

- toute cellule $S \in \mathcal{S}_1$ est soit un point soit un intervalle ouvert ;

– pour tout $i \in [\![1,n]\!]$ et toute cellule $S \in \mathcal{S}_i$, il existe un nombre fini de fonctions semi-algébriques continues $\xi_{S,1} < \ldots < \xi_{S,l_S} : \longrightarrow \mathbb{R}$ telles que le cylindre $S \times \mathbb{R}$ soit l'union disjointe des cellules de $\mathcal{S}_i$ qui sont :
  - soit le graphe $\Gamma_{S,j}$ d'une fonction $\xi_{S,j}$ pour $j \in \{1,\ldots,l_S\}$:
$$\Gamma_{S,j} = \{(x', x_{j+1}) \in S \times \mathbb{R} \mid \xi_{S,j}(x')\}$$
  - soit une **bande** $B_{S,j}$ du cylindre borné par les graphes des fonctions $\xi_{S,j}$ et $\xi_{S,j+1}$ pour $j \in \{0,\ldots,l_S\}$, où on prend par convention $\xi_{S,0} = -\infty$ et $\xi_{S,l_S+1} = +\infty$:
$$B_{S,j} = \{(x', x_{j+1}) \in S \times \mathbb{R} \mid \xi_{S,j}(x') < x_{j+1} < \xi_{S,j+1}(x')\}$$

Proposition 2.4.11 *Toute cellule d'une décomposition cylindrique algébrique est semi-algébriquement homéomorphe à un hypercube ouvert* $]0,1[^i$ (*par convention* $]0,1[^0$*est un point*).

Etant donnée une famille de polynômes $\mathcal{P}$ dans $\mathbb{R}[X_1,\ldots,X_n]$, un sous-ensemble S de $\mathbb{R}^n$ est dit $\mathcal{P}$-invariant si tout polynôme $P \in \mathcal{P}$ est de signe constant sur S. Nous allons montrer comment construire une décomposition cylindrique algébrique $\mathcal{S}_n$ de $\mathbb{R}^n$ adaptée à $\mathcal{P}$, c'est-à-dire pour laquelle chaque cellule $S \in \mathcal{S}_n$ est $\mathcal{P}$-invariante.
Soit S un ensemble semi-algébrique quelconque. Une décomposition cylindrique algébrique adaptée à S, est une décomposition cylindrique algébrique de $\mathbb{R}^n$ telle que S est union finie de cellule de cette décomposition. Il est clair que si $\mathcal{P}$ est une famille de polynômes telle que S soit la réalisation d'une formule sans quantificateur avec atomes dans $\mathcal{P}$, une décomposition cylindrique algébrique adaptée à $\mathcal{P}$ est une décomposition cylindrique algébrique adaptée à S.
Pour construire une décomposition cylindrique algébrique adaptée à $\mathcal{P}$, il est utile que pour tout $S \in \mathcal{S}_{n-1}$ nous puissions choisir la fonction $\xi_{S,j}$ de S dans $\mathbb{R}$ comme étant une fonction qui à $(x_1,\ldots,x_{n-1}) \in S$ associe une racine de $P \in \mathcal{P}$. Le théorème suivant explique quelles conditions doit vérifier une cellule $S \in \mathcal{S}_{n-1}$ pour pouvoir choisir chaque fonction $\xi_{S,j}$ de S dans $\mathbb{R}$ comme étant une fonction qui, à $(x_1,\ldots,x_{n-1}) \in S$, associe une racine de $P \in \mathcal{P}$.

Théorème 2.4.12 *Soit $P \in \mathbb{R}[X_1,\ldots,X_n]$ et S une composante semi-algébriquement connexe de $\mathbb{R}^{n-1}$ telle que :*
– $\forall x' \in S$, *le nombre de racines distinctes de $P(x', X_n)$ dans $\mathbb{C}$ est constant.*
– $\forall x' \in S$, *le degré de $P(x', X_n)$ est constant.*

Alors il existe l fonctions semi-algébriquement continues $\xi_1,\ldots,\xi_l : S \longrightarrow \mathbb{R}$ telles que $\forall x' \in S$, l'ensemble des racines réelles de $P(x', X_n)$ soit exactement $\{\xi_1(x'),\ldots,\xi_l(x')\}$. De plus, pour $i = 1,\ldots,l$, la multiplicité de $\xi_i(x')$ est constante pour tout $x' \in S$.

La proposition suivante permet de généraliser le théorème ci-dessus au cas de deux polynômes.

Proposition 2.4.13 *Soient $P,Q \in \mathbb{R}[X_1,\ldots,X_n]$ et S une composante semi-algébriquement connexe de $\mathbb{R}^{n-1}$ telle que :*

- *$\forall x' \in S$, les nombres de racines distinctes de $P(x',X_n)$ et de $Q(x',X_n)$ dans $\mathbb{C}$ restent constants.*
- *$\forall x' \in S$, les degrés de $P(x',X_n)$ et de $Q(x',X_n)$ restent constants.*
- *$\forall x' \in S$, le degré du pgcd de $P(x',X_n)$ et de $Q(x',X_n)$ reste constant.*

Alors il existe l fonctions semi-algébriquement continues $\xi_1,\ldots,\xi_l : S \longrightarrow \mathbb{R}$ telles que pour tout $x' \in S$, l'ensemble des racines réelles de $PQ(x',X_n)$ soit exactement $\{\xi_1(x'),\ldots,\xi_l(x')\}$. De plus, pour $i = 1,\ldots,l$, la multiplicité de $\xi_i(x')$ racine de $P(x',X_n)$ (resp $Q(x',X_n)$ est constante pour tout $x' \in S$.

2.4.3 L'algorithme de Collins

L'algorithme de décomposition cylindrique algébrique se divise en deux étapes : l'étape de projection et l'étape de remontée.

Etape de projection : Soit P un polynôme de $\mathbb{R}[X_1,\ldots,X_n]$ vu comme polynôme univarié en X_n à coefficients dans $\mathbb{R}[X_1,\ldots,X_{n-1}]$. On note $\mathrm{lc}(P)$ le coefficient dominant de P. On note $\mathrm{Tr}(P)$ le polynôme égal à $P - \mathrm{lc}(P)X_n^{\deg_{X_n}(P)}$. On définit un opérateur de projection $\mathrm{PROJ}(\mathcal{P})$ comme étant le plus petit ensemble de polynômes de $\mathbb{R}[X_1,\ldots,X_{n-1}]$ tel que :

- si $P \in \mathcal{P}$ et $\deg_{X_n}(P) = p \geqslant 2$, $\mathrm{PROJ}(\mathcal{P})$ contient tous les coefficients sous-résultants non constants $\mathrm{sr}_{j,j}(P,\partial_{X_n}P)$ pour $j \in [\![0,p]\!]$,
- si $(P,Q) \in \mathcal{P}^2$, $\mathrm{PROJ}(\mathcal{P})$ contient tous les coefficients sous-résultants non constants $\mathrm{sr}_{j,j}(P,Q)$ pour $j \in [\![0,\min(\deg_{X_n}(P),\deg_{X_n}(Q))]\!]$,
- si $P \in \mathcal{P}$, $\deg_{X_n}(P) \geqslant 1$ et $\mathrm{lc}(P)$ est non constant alors $\mathrm{PROJ}(\mathcal{P})$ contient $\mathrm{lc}(P)$ et $\mathrm{PROJ}(\mathcal{P}\backslash\{P\} \cup \{\mathrm{Tr}(P)\})$.
- si $P \in \mathcal{P}$, $\deg_{X_n}(P) = 0$ et P est non constant, alors $\mathrm{PROJ}(\mathcal{P})$ contient P.

Théorème 2.4.14 *Soit $\mathcal{P}$ une famille finie de polynômes dans $\mathbb{R}[X_1,\ldots,X_n]$ et soit S une composante semi-algébriquement connexe d'un sous-ensemble semi-algébrique de $\mathbb{R}^{n-1}$, qui est $\mathrm{PROJ}(\mathcal{P})$-invariant. Alors, il existe l fonctions continues $\xi_1 < \ldots < \xi_l : S \longrightarrow \mathbb{R}$ telles que $\forall x' \in S$, l'ensemble de points $\{\xi_1(x'),\ldots,\xi_l(x')\}$ soit exactement l'ensemble des racines réelles de tous les polynômes non nuls $P(x',X_n)$ avec $P \in \mathcal{P}$. Le graphe de chaque fonction ξ_i ainsi que chaque bande du cylindre $S \times \mathbb{R}$ bornée par ces graphes, sont des ensembles semi-algébriques, semi-algébriquement connexes et semi-algébriquement homéomorphes soit à S, soit à $S \times]0,1[$, et $\mathcal{P}$-invariants.*

Ainsi, étant donnée une décomposition cylindrique algébrique de $\mathbb{R}^{n-1}$ adaptée à PROJ($\mathcal{P}$), on définit récursivement des sous-ensembles finis de polynômes $\mathcal{P}_i$ tels que :

- $\mathcal{P}_n = \mathcal{P}$,
- Pour tout $i \in \{1,\ldots,n-1\}$ $\mathcal{P}_i = \text{PROJ}(\mathcal{P}_{i+1})$.

Etape de remontée : Il est clair que $\mathcal{P}_1$ est une famille de polynômes univariés. La construction d'une décomposition cylindrique algébrique $\mathcal{S}_1$ adaptée à $\mathcal{P}_1$ se fait en donnant un point représentatif dans chaque composante semi-algébriquement connexe de $\mathcal{S}_1$. Ceci revient à isoler, puis trier les racines réelles, $\{\alpha_{1,1},\ldots,\alpha_{1,s_1}\}$, des polynômes de $\mathcal{P}_1$ et donner un point dans chaque intervalle $]\alpha_{1,i},\alpha_{1,i+1}[$ pour $i \in [\![0, s_1+1]\!]$ (avec $\alpha_{1,0} = -\infty$ et $\alpha_{1,s_1+1} = +\infty$). Il nous faut maintenant montrer comment construire une décomposition cylindrique algébrique adaptée à $\mathcal{P}_2$ à partir de $\mathcal{S}_1$.
Tous les polynômes de $\mathcal{P}_2$ sont des polynômes en les variables X_1 et X_2. Lorsque l'on spécialise la variable X_1 aux nombres algébriques réels de $\mathcal{S}_1$ on obtient une famille de polynômes univariés en X_2 à coefficients dans $\mathbb{R}$. On peut donc réitérer le processus d'isolation et de tri de cette famille de polynômes. Ainsi on construit récursivement une décomposition cylindrique algébrique adaptée à $\mathcal{P}_{i+1}$ à partir d'une décomposition cylindrique algébrique adaptée à $\mathcal{P}_i$. Ceci constitue la phase de remontée de l'algorithme de décomposition cylindrique algébrique. L'algorithme de décomposition cylindrique algébrique Collins est la succession des deux routines décrites ci-dessus.

Remarque 2.4.15 La phase de remontée nécessite la manipulation symbolique de nombres algébriques réels. Ceci ne se fait pas de manière simple. Il est important de noter qu'au cours de l'étape de remontée, il est nécessaire de travailler au-dessus de tours d'extensions algébriques lorsque les racines d'un polynôme ne sont pas rationnelles. Ceci induit des méthodes et des calculs délicats à mettre en oeuvre.

On obtient le théorème suivant :

Théorème 2.4.16 *Pour toute famille finie $\mathcal{P}$ de polynômes dans $\mathbb{R}[X_1,\ldots,X_n]$, il existe une décomposition cylindrique algébrique de $\mathbb{R}^n$ adaptée à $\mathcal{P}$.*

L'algorithme de décomposition cylindrique algébrique de Collins est fortement pénalisé par sa complexité. D'un point de vue pratique, il subit cette complexité à deux niveaux :

- lors de la phase de projection, le nombre de polynômes ainsi que leur degré devient une étape bloquante de l'algorithme lorsque le nombre de variables est supérieur à trois.
- lors de la phase de remontée, la gestion des nombres algébriques réels est crutiale. Ainsi, il arrive très souvent que pour des problèmes de plus de trois variables la phase

de projection de passe pas. Même lorsque celle-ci passe, la phase de remontée est aussi bloquante du fait du nombre de points réels qui doivent être manipulés.

Le théorème suivant donne la complexité arithmétique de l'algorithme de Collins (voir [23]).

Théorème 2.4.17 *Soit $\mathcal{P}$ une famille finie de m polynômes de $\mathbb{R}[X_1,\ldots,X_n]$ et d le maximum des degrés totaux des polynômes de $\mathcal{P}$. La complexité arithmétique du calcul d'une décomposition cylindrique algébrique adaptée à $\mathcal{P}$ est $O(m^{2^n}d^{n2^n})$.*

2.4.4 Algorithme de Collins et calcul de topologie de variétés algébriques

L'algorithme de Collins permet de décomposer un ensemble semi-algébrique en des cellules homéomorphes à des hypercubes ouverts mais ne donne pas d'information sur les relations d'adjacence entre les cellules obtenues. De plus nous ne savons pas, en général, ce qu'il advient en passant d'une cellule à une autre. Ces informations sont nécessaires pour déterminer la topologie de l'ensemble semi-algébrique considéré. Pour remédier à ce problème, l'algorithme de décomposition cylindrique algébrique est combiné avec le lemme de Thom.

$$\text{Si } \varepsilon \in \{-1,0,1\} \text{ est signe, nous notons : } \bar{\varepsilon} = \begin{cases} \{0\} \text{ si } \varepsilon = 0 \\ \{0,1\} \text{ si } \varepsilon = 1 \\ \{0,-1\} \text{ si } \varepsilon = -1 \end{cases}$$

Proposition 2.4.18 *(Lemme de Thom) Soit $P_1,\ldots,P_s \in \mathbb{R}[X]$ une famille finie de polynômes non nuls, stable par dérivation (ie $\forall i \in [\![1,s]\!]$, si $P_i' \neq 0$ alors il existe $j \in [\![1,s]\!]$ tel que $P_i' = P_j$). Pour tout $\varepsilon = (\varepsilon_1,\ldots,\varepsilon_s) \in \{-1,0,1\}^s$, soit $A_\varepsilon \subset \mathbb{R}$ définie par :*

$$A_\varepsilon = \{x \in \mathbb{R}; \text{signe}(P_i(x)) = \varepsilon_i \text{ pour } i = 1,\ldots,s\}.$$

Alors,

- *soit A_ε est un ensemble vide,*
- *soit A_ε est réduit à un point,*
- *soit A_ε est un intervalle ouvert non vide.*

Soit l'ensemble $A_{\bar{\varepsilon}} := \{x \in \mathbb{R}; \text{sign}(P_i(x)) \in \bar{\varepsilon}_i \text{ pour } i = 1,\ldots,s\}$. Alors $A_{\bar{\varepsilon}}$ est soit vide, soit réduit à un point, soit un intervalle fermé différent d'un point.

Le lemme de Thom permet d'obtenir une description de chaque cellule de la décomposition cylindrique algébrique par une combinaison booléenne d'équations et d'inéquations polynomiales. Pour cela il suffit d'ajouter à la famille de polynôme de départ leurs dérivées successives non nulles.

Ce lemme admet une généralisation au cas d'une famille de polynômes multivariés.

Théorème 2.4.19 *Soit $(P_{i,j})_{(i,j)\in[\![1,n]\!]\times[\![1,s_i]\!]}$ une famille de polynômes à coefficients réels tel que :*

- *pour i fixé, $(P_{i,1},\dots,P_{i,s_i})$ est une famille de polynômes dans $\mathbb{R}[X_1,\dots,X_i]$ stable par dérivation, telle que pour tout $j\in[\![1,s_i]\!]$ $\mathrm{lc}_{X_i}(P_{i,j})\in\mathbb{R}^*$,*
- *pour $i<n$, la famille de polynômes $(P_{i,1},\dots,P_{i,s_i})$ contient la famille $\mathrm{PROJ}(P_{i+1,1},\dots,P_{i+1,s_{i+1}})$.*

Pour $0<k\leqslant n$, soit $\varepsilon=(\varepsilon_{i,j})_{(i,j)\in[\![1,k]\!]\times[\![1,s_i]\!]}$ une famille de signes dans $\{-1,0,1\}$ et :

$$C_\varepsilon=\{x\in\mathbb{R}^n;\mathrm{signe}(P_{i,j}(x))=\varepsilon_{i,j}\text{ pour }i=1,\dots,k\text{ et }j=1,\dots,s_i\},$$

$$C_{\overline{\varepsilon}}=\{x\in\mathbb{R}^n;\mathrm{signe}(P_{i,j}(x))=\overline{\varepsilon}_{i,j}\text{ pour }i=1,\dots,k\text{ et }j=1,\dots,s_i\}.$$

Alors les ensembles C_ε non vide sont les cellules de la décomposition cylindrique algébrique de $\mathbb{R}^n$, et l'adhérence d'une cellule non vide C_ε est $C_{\overline{\varepsilon}}$, qui est une union de cellules.

Le théorème précédent permet de déterminer les relations d'adjacences entre les cellules d'une décomposition cylindrique algébrique. Il fonctionne pour une famille de polynômes avec des propriétés spéciales. Néanmoins, toute famille finie de polynômes de $\mathbb{R}[X_1,\dots,X_n]$ peut être transformée en une famille satisfaisant ces propriétés à un changement de variable linéaire prés.

Proposition 2.4.20 *Soient $P_1,\dots,P_l\in\mathbb{R}[X_1,\dots,X_n]$. Il existe un automorphisme linéaire u de $\mathbb{R}^n$et une famille $(P_{i,j})$ satisfaisant les conditions du théorème précédent, telle que : $P_{n,j}(X_1,\dots,X_n)=P_j(u(X_1,\dots,X_n))$ pour $i=1,\dots,l$.*

Ainsi, combinant l'algorithme de Collins et le le lemme de Thom, il est possible de caractériser la topologie d'un ensemble semi-algébrique donné. Mais cette combinaison a un fort coût. En effet, l'utilisation du lemme de Thom nécessite que les familles de polynômes manipulées après chaque projection soient stables par dérivation. Donc, après chaque projection la famille de polynôme doit être stabilisée en ajoutant les dérivées successives des polynômes sous-résultants. On a le résultat suivant :

Théorème 2.4.21 *[23] Soit $\mathcal{P}$ une famille de m polynômes de $\mathbb{R}[X_1,\dots,X_n]$ et d le maximum des degrés totaux des polynômes de $\mathcal{P}$. La complexité arithmétique de l'algorithme combinant le lemme de Thom et le de calcul d'une décomposition cylindrique algébrique adaptée à $\mathcal{P}$ est $O(m^{2^n}d^{n2^{n+1}})$.*

La complexité de l'algorithme de décomposition cylindrique algébrique est très élevée. Dans la pratique, pour calculer la topologie d'ensemble semi-algébrique, l'algorithme de décomposition cylindrique algébrique s'avère donc difficilement utilisable. Cela justifie l'émergence

de nouvelles techniques, souvent inspirées de l'algorithme de décomposition cylindrique algébrique, pour calculer la topologie de variétés semi-algébriques en petite dimension.

Première partie

Topologie de courbes algébriques

Chapitre 3

Topologie d'une courbe algébrique plane

3.1 Introduction

Soit $f \in \mathbb{Q}[X,Y]$ un polynôme sans facteur carré et $\mathcal{C}(f)$ le lieu de ses zéros réels :

$$\mathcal{C}(f) := \{(\alpha,\beta) \in \mathbb{R}^2 | f(\alpha,\beta) = 0\}$$

Le problème auquel on s'intéresse dans ce chapitre est celui du calcul de la topologie de $\mathcal{C}(f)$, c'est-à-dire le calcul d'un complexe simplicial isotope à $\mathcal{C}(f)$.
Le calcul de la topologie d'une courbe algébrique plane admet plusieurs applications très importantes. En effet outre son intérêt évident pour la visualisation des courbes algébriques planes, il constitue une opération essentielle en géométrie algorithmique pour l'acquisition de formes. Il apparaît comme une primitive incontournable dans plusieurs algorithmes en CAGD (calcul d'intersection de surfaces algébriques, maillage de surfaces algébriques implicites, calcul de la courbe d'auto-intersection d'une surface paramétrée...). En plus de ces applications pratiques, le problème du calcul de la topologie de courbe est lié à plusieurs questions de mathématiques pures telles que l'énumération des types topologiques des courbes algébriques planes de degré d fixé (qui reste ouverte même pour les petits degrés $(d \geqslant 8)$).
Le premier algorithme permettant de traiter ce problème est celui de la décomposition cylindrique algébrique. Mais nous avons vu que sa complexité le rend difficilement utilisable pour résoudre efficacement ce problème. Cependant il a inspiré de nouvelles techniques pour le calcul de topologie de variétés algébriques en petites dimensions. Les algorithmes qui découlent de ces travaux peuvent être classés en deux catégories :

Les algorithmes de type balayage

Inspirés des méthodes de la Décomposition Cylindrique Algébrique [6], ils consistent à balayer le plan par une droite orthogonale à l'axe des abscisses afin de détecter les positions où la topologie de la courbe change. Ces algorithmes exigent que la courbe soit dans une position générique et procèdent par projection puis relèvement pour reconstruire la topologie de la courbe. La principale difficulté dans ces algorithmes est d'allier l'efficacité et la certification des calculs utilisant des nombres algébriques de degrés très élévés.
Dans [32] Gonzalez-Véga et El Kahoui proposent un algorithme certifié basé sur les propriétés des sous-résultants et l'encodage de Thom des racines réelles d'un polynôme univarié [6, 16]. Leur algorithme requière des conditions de généricité et ils utilisent l'encodage de Thom des racines du discriminant de $f(X,Y)$ par rapport à la variable Y pour certifier la généricité de la position de la courbe $\mathcal{C}(f)$. Cependant, si l'utilisation de l'encodage de Thom pour tester la généricité de la position de $\mathcal{C}(f)$ permet d'obtenir un algorithme certifé, sa complexité pénalise l'efficacité de leur algorithme. Ainsi la complexité binaire de l'algorithme décrit dans [32] est dominée par celle de la phase de test et de mise en position générique de $\mathcal{C}(f)$. Pour une courbe algébrique plane de degré d dont les coefficients sont de taille τ, elle est de $\tilde{O}_B(d^{16}\tau)$.
Dans [33], Gonzalez-Vega et Necula proposent un algorithme utilisant des calculs de suites de Sturm-Habicht pour déterminer les points en lesquels la topologie de la courbe change. Puis, afin d'éviter le coût du calcul de l'encodage de Thom, ils testent la généricité de la position de la courbe avec des méthodes numériques. Les auteurs décrivent leur algorithme comme étant semi-numérique, i.e. plusieurs étapes des calculs sont menées avec des nombres flottants, notamment le test de généricité de la position de la courbe. Cet algorithme est plus efficace que celui décrit dans [32] mais il n'est pas certifié. Ainsi dans certains cas où les courbes présentent des singularités pathologiques, il peut retourner des résultats faux.
Dans [19], Diochnos, Emiris et Tsigaridas proposent un algorithme utilisant les mêmes techniques que dans [33] mais en certifiant les phases de résolution en utilisant la représentation univariée rationnelle des points x-critiques de la courbe plane en position générique. Ils évaluent la complexité binaire de leur algorithme en $\tilde{O}_B(d^{12}\tau)$. Cependant dans cette évaluation, les auteurs n'ont pas pris en compte la complexité binaire de la phase de test et de mise en position générique de la courbe qui domine en général les autres phases.
Nous mentionnons aussi les travaux [31, 22] dans lesquels des techniques symboliques-numériques basées sur des calculs de séquences de Sturm-Habicht combinées à des méthodes d'isolations de racines réelles sont utilisées pour accélerer les calculs.

Les algorithmes de type subdivision

Ils consistent à découper le plan en petites boîtes puis à calculer la topologie de la courbe dans chaque boîte. S'il est assez facile de calculer numériquement la topologie dans les boîtes ne contenant que des points réguliers de $\mathcal{C}(f)$, le calcul de la topologie dans les boîtes contenant des points singuliers est un problème difficile car nécessite la connaissance de la structure des singularités de $\mathcal{C}(f)$. Certains de ces algorithmes présentent l'avantage d'être très rapides car purement numériques, par contre, ils ne garantissent pas toujours la topologie dans les boîtes contenant des singularités de la courbe. Des algorithmes symboliques-numériques ont été développés pour résoudre le problème de la certification de la topologie dans les boîtes singulières.
Dans [41], Hong propose une solution utilisant des séquences de Sturm pour calculer la topologie dans les boîtes contenant des singularités de la courbe. Pour un nombre algébrique α donné, il utilise la séquence de Sturm associée au polynôme $f(\alpha, Y)$ pour isoler ses racines dans des boîtes. Pour déterminer le nombre de branches passant en un point singulier, il calcule l'intersection de la courbe avec le bord de la boîte le contenant. Cette méthode nécessite des conditions de régularité sur la courbe et l'isolation des racines du polynôme $f(\alpha, Y)$ peut être très coûteuse dans certains cas.
Nous mentionnons aussi le travail [3]. Pour calculer la topologie de la courbe, les auteurs combinent des calculs de degré topologique au voisinage des singularités de la courbe, à des techniques d'enveloppement avec des polynômes représentés dans la base de Bernstein. Ils fournissent ainsi un algorithme donnant la topologie de courbes de degrés très élevés.
Citons les travaux [13] où une methode basée sur le calcul de représentation univariée rationnelle est utilisée pour déterminer la structure des singularités de la courbe.

Nous présentons dans ce chapitre un algorithme symbolique-numérique certifié fortement basé sur les propriétés des sous-résultants. L'algorithme que nous proposons calcule la topologie de $\mathcal{C}(f)$ avec une complexité binaire déterministe en $\tilde{\mathcal{O}}_B(d^{10}\tau)$. Nous nous sommes inspirée des techniques décrites dans [32]. L'apport majeur de ce travail consiste en l'introduction d'un algorithme modulaire utilisant les propriétés des polynômes sous-résultants pour certifier la généricité de la position d'une courbe algébrique plane. Comparé à l'algorithme de test de généricité décrit dans [32], cet algorithme de test de généricité permet de réaliser un gain d'un facteur d^6 sur la complexité binaire de la phase de test et de mise en position générique et en conséquence, sur la complexité globale de l'algorithme.

Dans la section 3.2, nous ferons une analyse détaillée de la géométrie d'une courbe algébrique plane. La section 3.3 regroupe les différentes phases de l'algorithme calculant la topologie d'une courbe algébrique implicite plane. Nous y effectuerons une étude comparative de notre algorithme de test et de mise en position générique avec celui décrit dans [32]. Dans la section 3.4, nous donnons une description complète de l'algorithme de calcul de la

topologie d'une courbe algébrique plane ainsi que l'étude de sa complexité binaire. Pour finir nous présenterons l'implémentation de l'algorithme sous MATHEMAGIX et les expérimentions réalisées.

3.2 Analyse de la géométrie d'une courbe algébrique plane

Dans cette section, nous introduisons les principaux concepts géométriques nécessaires pour comprendre les différentes approches du problème de calcul de la topologie d'une courbe algébrique plane. Les notions de points singuliers, de points réguliers et de points *x*-critiques, d'arcs d'une courbe algébrique plane sont abordées en insistant sur leur rôle dans l'analyse de la topologie d'une courbe algébrique.

Considérons un polynôme $f \in \mathbb{Q}[X,Y]$ sans facteur carré et $\mathcal{C}(f)$ le lieu de ses zéros réels : $\mathcal{C}(f) = \{(\alpha,\beta) \in \mathbb{R}^2 | f(\alpha,\beta) = 0\}$.

Nous souhaitons calculer la topologie de $\mathcal{C}(f)$, c'est-à-dire fournir une structure Λ, linéaire par morceaux, isotope à la courbe $\mathcal{C}(f)$.

Définition 3.2.1 *Une isotopie de* $\mathbb{R}^2$ *est une application* $\varphi : \mathbb{R}^2 \times [0,1] \longrightarrow \mathbb{R}^2$*, telle que* $\varphi(\cdot,0) = \mathrm{Id}_{\mathbb{R}^2}$ *et pour tout* $t \in]0,1]$, $\varphi(\cdot,t)$ *est un homéomorphisme.*

Définition 3.2.2 *Soient* $\Delta, \Lambda \subset \mathbb{R}^2$*, on dit que* Δ *est isotope à* Λ *s'il existe une isotopie* φ *de* $\mathbb{R}^2$ *telle que* $\varphi(\Delta,1) = \Lambda$.

Comme l'indique la théorie de Morse sur l'étude des ensembles semi-algébriques, le calcul de la topologie de $\mathcal{C}(f)$ passe par celui de la structure de ses points singuliers et des arcs lisses qui relient ces points. Afin de justifier cette affirmation, nous allons effectuer une analyse de la géométrie de $\mathcal{C}(f)$ en définissant une relation "$\sim$" sur l'ensemble de ses points. Nous prouverons que "$\sim$" est une relation d'équivalence permettant de décomposer $\mathcal{C}(f)$ en des arcs et points particuliers de $\mathcal{C}(f)$.

Définition 3.2.3 *Soit* $(\alpha,\beta) \in \mathcal{C}(f)$*. On dit que* (α,β) *est un point singulier de* $\mathcal{C}(f)$ *si et seulement si* $\partial_Y f(\alpha,\beta) = \partial_X f(\alpha,\beta) = 0$*. Les points non singuliers* $\mathcal{C}(f)$ *sont dits réguliers.*

Un point régulier (α,β) de la courbe $\mathcal{C}(f)$ admet une unique droite tangente. Si cette tangente n'est pas orthogonale à l'axe des abscisses, nous pouvons paramétriser $\mathcal{C}(f)$ au voisinage de (α,β) à l'aide du théorème des fonctions implicites que nous rappelons ici dans le contexte d'une courbe algébrique plane.

Théorème 3.2.4 *Soit $(\alpha,\beta) \in \mathcal{C}(f)$ tel que $\partial_Y f(\alpha,\beta) \neq 0$. Alors il existe un voisinage V de α, un voisinage W de β et une fonction de classe C^∞ $g : V \longrightarrow W$ tels que pour tout $x \in V$, $y = g(x)$ soit l'unique solution dans W de l'équation $f(x,y) = 0$. De plus on a :*

$$g'(x) = \frac{-\partial_X f(x,g(x))}{\partial_Y f(x,g(x))}$$

Géométriquement, le Théorème 3.2.4 indique que la courbe $\mathcal{C}(f)$ est décrite au voisinage de (α,β) par le graphe de la fonction $y = g(x)$.

Les points de la courbe $\mathcal{C}(f)$ où le théorème des fonctions implicites n'est pas applicable sont dits *x*-**critiques**.

Définition 3.2.5 *Soit $(\alpha,\beta) \in \mathcal{C}(f)$. On dit que (α,β) est un point x-critique de $\mathcal{C}(f)$ si et seulement si $\partial_Y f(\alpha,\beta) = 0$. On appelera valeur x-critique la valeur α lorsque (α,β) est un point x-critique et valeur régulière la valeur de α lorsque (α,β) est un point régulier.*

Les points *x*-critiques de $\mathcal{C}(f)$ sont constitués par ses points singuliers et ses points réguliers à tangente verticale.

Proposition 3.2.6 *Si la courbe $\mathcal{C}(f)$ n'admet pas de droite verticale comme composante, alors elle admet un nombre fini de points x-critiques.*

Démonstration En effet les points *x*-critiques de $\mathcal{C}(f)$ sont les solutions réelles du système $f(x,y) = \partial_Y f(x,y) = 0$. Comme $f \in \mathbb{Q}[X,Y]$ est sans facteur carré et n'admet pas, par hypothèse, de droite verticale comme composante, le théorème de Bézout donne le résultat. □

Supposons que $f(X,Y) = \sum_{i=0}^{n} f_i(X)Y^i$. Soit $P = \text{pgcd}(f_1,\ldots,f_n)$. Les droites orthogonales à l'axe des abscisses et composantes de $\mathcal{C}(f)$ sont les droites d'équation $x = \alpha$ avec α racine de P. Donc, pour forcer $\mathcal{C}(f)$ à ne contenir aucune droite orthogonale à l'axe des abscisses, il suffit d'exiger que P n'admette aucune racine réelle.

Intuitivement, si nous enlevons les points *x*-critiques de $\mathcal{C}(f)$, le reste de la courbe se décompose en plusieurs morceaux de courbes lisses ; nous les appellerons arcs de la courbe. Ces arcs peuvent être définis comme des classes d'équivalence d'une certaine relation sur les points de $\mathcal{C}(f)$. En effet :

Définition 3.2.7 *Soit $p = (\alpha_p,\beta_p)$ et $q = (\alpha_q,\beta_q)$ deux points de $\mathcal{C}(f)$. On dira que p est en relation avec q (et on note $p \sim q$) si et seulement si $p = q$ ou s'il existe une application continue $\varphi : [\alpha_p,\alpha_q] \longrightarrow \mathbb{R}$ (ou $\varphi : [\alpha_q,\alpha_p] \longrightarrow \mathbb{R}$) vérifiant :*

1. $\varphi(\alpha_p) = \beta_p$ *et* $\varphi(\alpha_q) = \beta_q$,
2. $\forall x \in [\alpha_p, \alpha_q], f(x, \varphi(x)) = 0$,
3. $\forall x \in [\alpha_p, \alpha_q], (x, \varphi_1(x))$ *n'est pas x-critique.*

De manière plus intuitive, $p \in \mathcal{C}(f)$ est en relation avec $q \in \mathcal{C}(f)$ si et seulement si $p = q$ ou s'il existe un morceau de courbe de $\mathcal{C}(f)$ reliant p à q sans passer par un point x-critique de $\mathcal{C}(f)$. La proposition suivante montre que la relation $\sim$ partitionne la courbe $\mathcal{C}(f)$:

Proposition 3.2.8

1. *La relation* $\sim$ *est une relation d'équivalence.*
2. *Tout point x-critique de* $\mathcal{C}(f)$ *constitue une classe d'équivalence singleton.*

Démonstration

1. La symétrie et la réfléxivité de $\sim$ sont évidentes. Pour la transitivité, si $p \sim q$ et $q \sim r$, il suffit de recoller les deux morceaux de courbes (celle reliant p à q et celle reliant q à r) pour avoir $p \sim r$. En effet le nouveau morceau de courbe obtenu ne peut pas contenir de point x-critique de $\mathcal{C}(f)$ car les morceaux qui le composent n'en contenaient pas.
2. Ce résultat est immédiat par définition de la relation $\sim$.

□

Définition 3.2.9 *Un arc de* $\mathcal{C}(f)$ *est une classe d'équivalence de la relation* $\sim$ *contenant un point non x-critique de* $\mathcal{C}(f)$.

Soit $\mathcal{A}$ l'ensemble des arcs de $\mathcal{C}(f)$, $\Pi_x : \mathbb{R}^2 \to \mathbb{R}$ l'application qui à $(x,y) \mapsto x$. Nous avons la proposition suivante :

Proposition 3.2.10 *Soit* $A \in \mathcal{A}$ *et* $A_x = \Pi_x(A)$. *Alors* A_x *est un intervalle ouvert de* $\mathbb{R}$ *et il existe une application continue* $\phi : A_x \longrightarrow \mathbb{R}$ *tel que* $A := \{(x, \phi(x)) \mid x \in A_x\}$.

Ainsi, la courbe $\mathcal{C}(f)$ est composée d'un nombre fini de points x-critiques et d'arcs correspondant à des graphes de fonctions continues sur des intervalles ouverts. Comment se comportent ces fonctions quand x tend vers un des bords de l'intervalle qui le contient ? Nous pouvons distinguer trois cas :

Soit $A \in \mathcal{A}$, $A_x =]a_-, a_+[$ et $\phi :]a_-, a_+[\longrightarrow \mathbb{R}$ l'application décrite dans la proposition précédente. Soit $p_- := (a_-, \lim_{x \to a_-} \phi(x)) \in (\mathbb{R} \cup \{\pm\infty\})^2$:

1. Si $a_- = -\infty$, on parle d'arc infini en $-\infty$.
2. Si $p_- = (\alpha, \pm\infty)$, on parle d'arc convergeant sur l'asymptote verticale d'équation $x = \alpha$ dans la direction $\pm\infty$ en restant à droite de celle-ci.
3. Si $p_- \in \mathbb{R}^2$, on parle d'arc incident à p_- par la droite.

Pour $p_+ := (a_+, \lim_{x \to a_+} \phi(x)) \in (\mathbb{R} \cup \{\pm\infty\})^2$:

1. Si $a_+ = +\infty$, on parle d'arc infini en $+\infty$.
2. Si $p_+ = (\alpha, \pm\infty)$, on parle d'arc convergeant sur l'asymptote verticale d'équation $x = \alpha$ dans la direction $\pm\infty$ en restant à gauche de celle-ci.
3. Si $p_+ \in \mathbb{R}^2$, on parle d'arc incident à p_+ par la gauche.

Nous avons la proposition suivante :

Proposition 3.2.11 *Si $p_+ \in \mathbb{R}^2$, alors p_+ est un point x-critique de $\mathcal{C}(f)$. Il en est de même pour p_-.*

Démonstration Soit (p_n) une suite de points de A convergeant vers p_+. Comme f est une fonction continue car polynômiale, alors $f(p_n)$ converge vers $f(p_+)$. Comme pour tout n $f(p_n) = 0$ alors $f(p_+) = 0$ d'où $p_+ \in \mathcal{C}(f)$. Si p_+ n'était pas un point x-critique de $\mathcal{C}(f)$ alors on aurait $p_+ \in A$ ce qui contredirait le fait que $\Pi_x(A) = A_x$ est un intervalle ouvert. □

Proposition 3.2.12 *$\mathcal{C}(f)$ admet un nombre fini d'arcs.*

Démonstration Pour tout arc A de $\mathcal{C}(f)$, $\Pi_x(A) = A_x$ est un intervalle ouvert dont les bords sont soit $\pm\infty$, soit des racines réelles du résultant de $f(X,Y)$ et $\partial_Y f(X,Y)$ par rapport à la variables Y. Donc il existe un nombre fini de choix possibles. De plus il est impossible que ce choix soit le même pour une infinité d'arcs. En effet, s'il existait un intervalle ouvert A_x sur lequel se projette une infinité d'arcs, alors il existerait $\alpha \in A_x$ tel que l'équation $f(\alpha, Y) = 0$ ait une infinité de racines. Ce qui est impossible. D'où le résultat. □

Les arcs de la courbe $\mathcal{C}(f)$ sont soit non bornés, soit ils relient deux points x-critiques. La définition d'arc incident peut être étendue à tout point de la courbe. Nous dirons qu'un arc A est incident à $p \in \mathcal{C}(f)$, de la gauche vers la droite, si $p \in A$. Pour tout point $p \in \mathcal{C}(f)$, nous pouvons ainsi définir le *nombre d'incidences* de p :

Définition 3.2.13 *Soit $p \in \mathcal{C}(f)$, le nombre d'incidences de p est la paire (g,d) où g désigne le nombre d'arcs incidents à p par la gauche et d le nombre d'arcs incidents à p par la droite. Le nombre total d'incidences de p est égal à $(g+d)$.*

Ainsi nous avons la proposition suivante :

Proposition 3.2.14 *Soit $p \in \mathbb{R}^2$ un point régulier de $\mathcal{C}(f)$. Alors le nombre total d'incidences de p est égal à 2.*

Reconstruire la topologie de la courbe $\mathcal{C}(f)$ revient à calculer les différentes classes d'équivalence de la relation $\sim$, c'est-à-dire les points x-critiques et les arcs de $\mathcal{C}(f)$, et de détérminer les connections existantes entre ces classes.

L'algorithme que nous proposons consiste à balayer le plan par une droite verticale afin de détecter les positions où la topologie de la courbe change. Afin de simplifier le calcul de la structure des points singuliers de $\mathcal{C}(f)$, la courbe doit être en position générique. En effet pour une courbe $\mathcal{C}(f)$ en position générique, le calcul de la topologie s'effectue plus facilement car la structure de ses points singuliers s'obtient rapidement.

3.3 Calcul certifié de la topologie de $\mathcal{C}(f)$

3.3.1 Description géométrique de l'algorithme

Lorsque la courbe $\mathcal{C}(f)$ est en position générique le calcul de ses points x-critiques est plus aisé car donné par des paramétrisations rationnelles avec des polynômes sous-résultants. L'utilisation de ces paramétrisations permet de calculer de manière certifiée la structure des fibres x-critiques de $\mathcal{C}(f)$ qui caractérisent sa topologie. En effet, pour une courbe en position générique, le calcul de l'ensemble de ses fibres x-critiques et celui d'une fibre regulière entre deux fibres x-critiques successives suffisent pour reconstruire tous ses arcs en utilisant l'algorithme de connection de Grandine [35]. Nous fournissons ici une description schématique de cet algorithme.

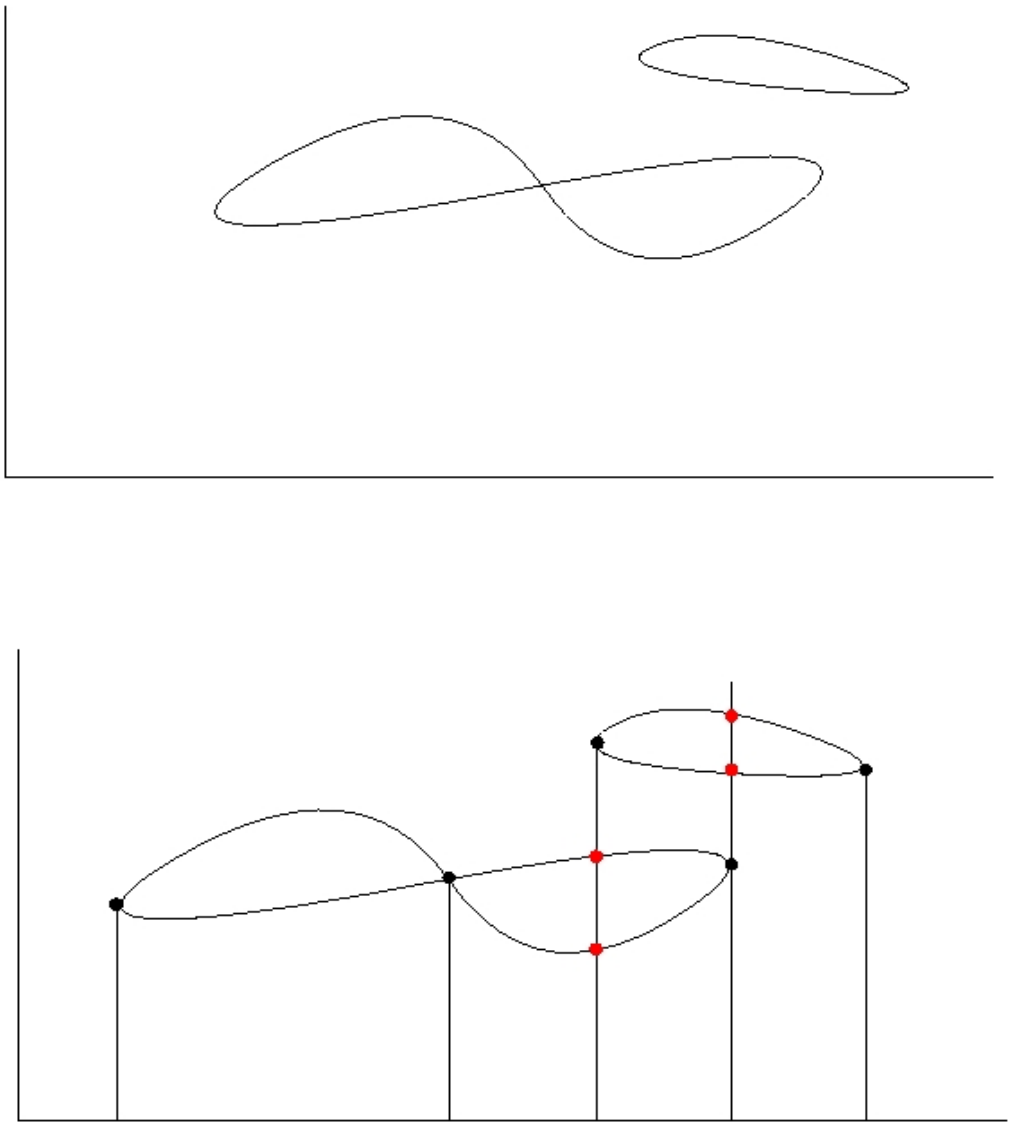

FIG. 3.1 – Calcul des fibres x-critiques

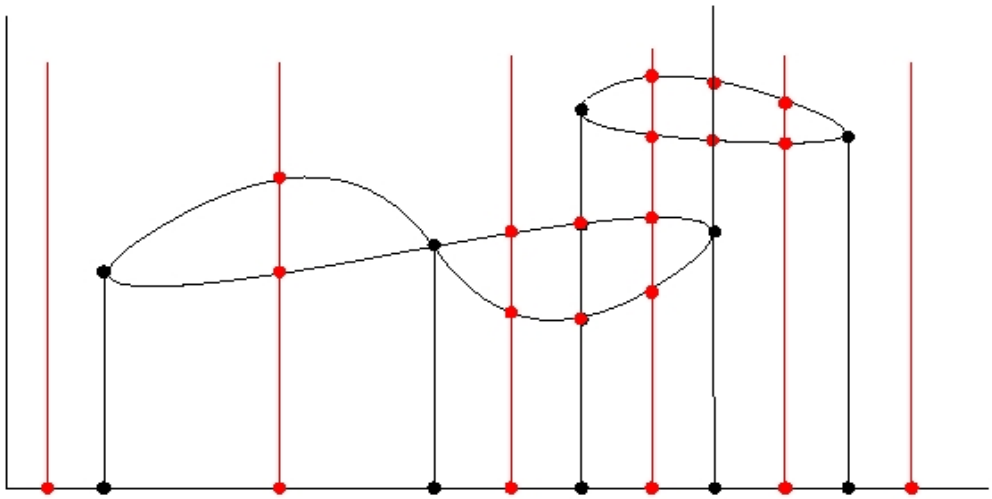

FIG. 3.2 – Calcul des fibres régulières

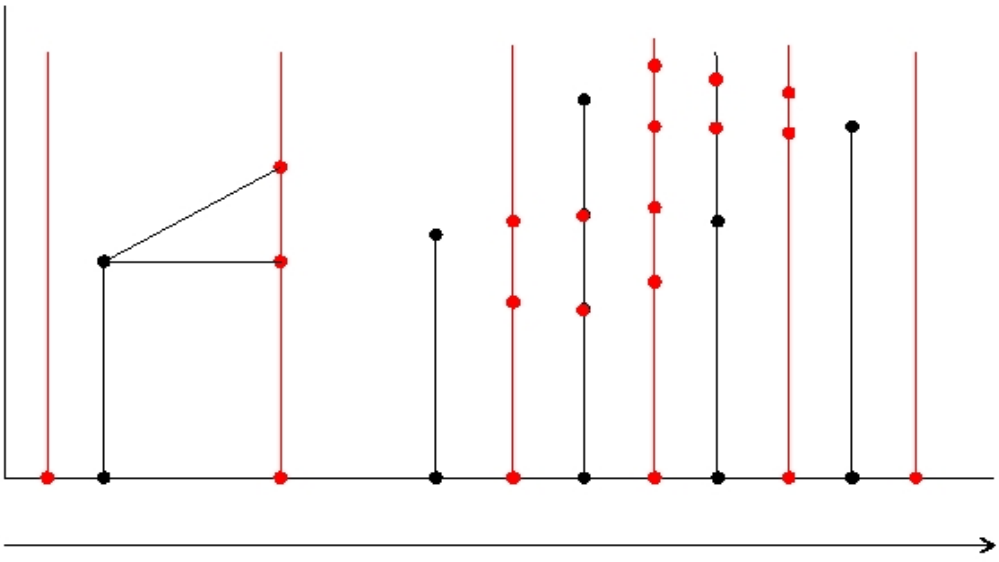

FIG. 3.3 – Connections

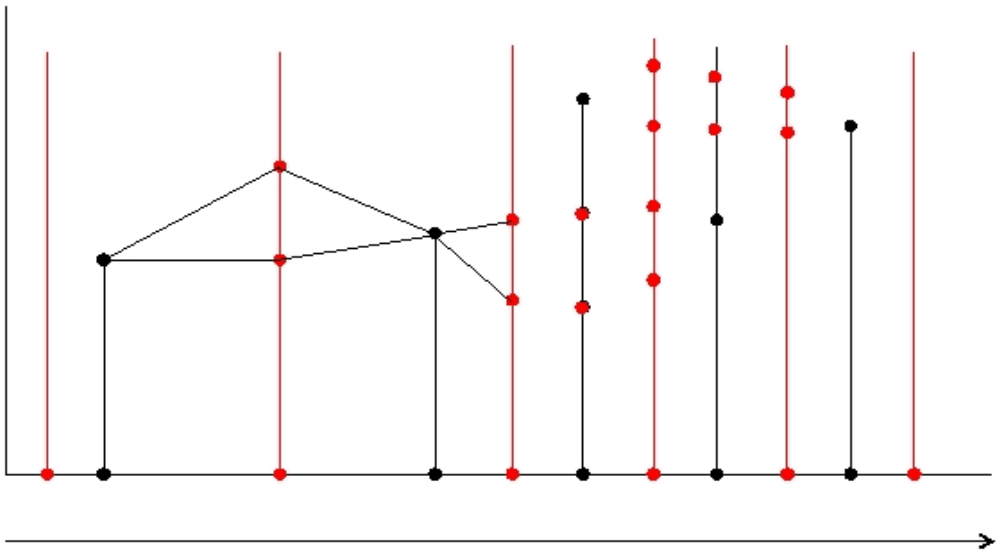

FIG. 3.4 – Connections

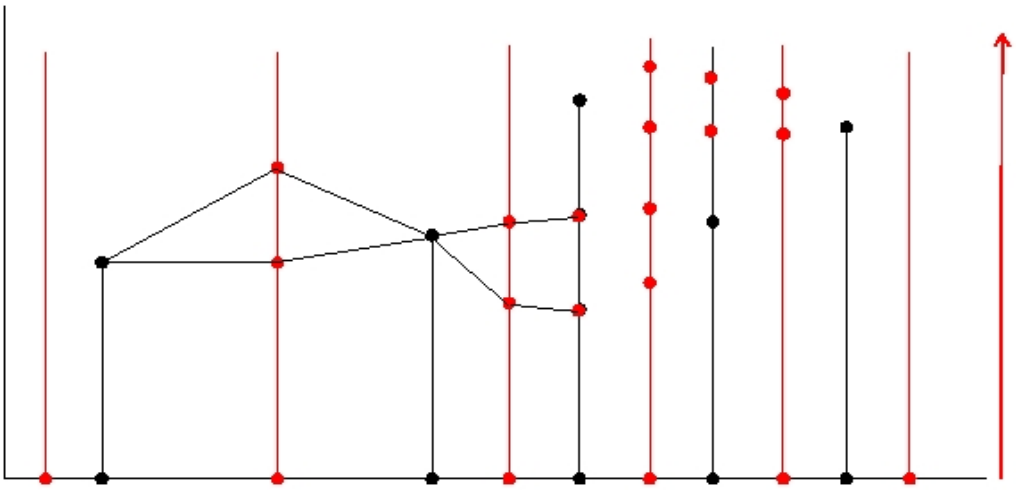

FIG. 3.5 – Connections

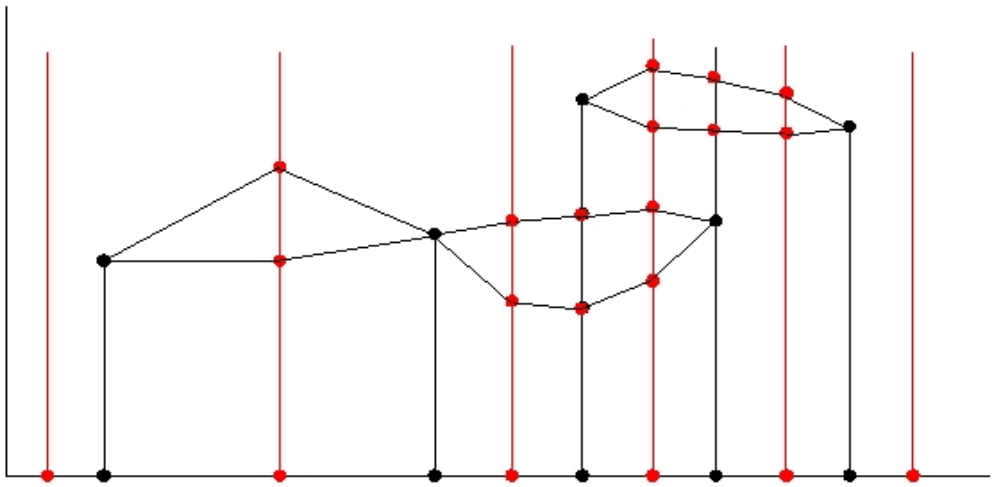

FIG. 3.6 – Connection

L'algorithme de connection que nous venons de décrire fonctionne lorsque la courbe est en position générique. Nous reviendrons sur cet algorithme dans la section 3.3.4

3.3.2 Notion de courbe en position générique

Définition 3.3.1 *Soit $\alpha \in \mathbb{R}$, on appelle fibre de la courbe $\mathcal{C}(f)$ en α, l'ensemble des points $(\alpha,\beta) \in \mathbb{R}^2$ avec β solution de l'équation $f(\alpha,Y) = 0$.*

On dira qu'une fibre de $\mathcal{C}(f)$ est x-critique si elle contient au moins un point x-critique de $\mathcal{C}(f)$. Sinon on dira qu'elle est régulière.

Les conditions de généricité requises pour le calcul de la topologie d'une courbe plane $\mathcal{C}(f)$ sont données ci dessous.

Définition 3.3.2 *Pour tout $\alpha \in \mathbb{C}$, soit $\mathcal{N}_x(\alpha) := \#\{\beta \in \mathbb{C}, f(\alpha,\beta) = \partial_Y f(\alpha,\beta) = 0\}$. On dit que $\mathcal{C}(f)$ est en position générique par rapport à l'axe des abscisses si :*

- $\forall \alpha \in \mathbb{C}, \mathcal{N}_x(\alpha) \leqslant 1$,
- *$\mathcal{C}(f)$ n'admet aucune direction asymptotique orthogonale à l'axe des abscisses.*

En position générique, la courbe $\mathcal{C}(f)$ n'admet pas d'asymptote orthogonale à l'axe des ab-

scisses et ses valeurs x-critiques sont différentes.
Nous allons à présent fournir une caractérisation algébrique de la notion de position générique.

Si $(\alpha,\beta) \in \mathbb{R}^2$ est un point x-critique de $\mathcal{C}(f)$, alors α est une racine du résultant de $f(X,Y)$ et $\partial_Y f(X,Y)$ par rapport à la variable Y. La proposition suivante fournit une représentation rationnelle de β en fonction de α en utilisant les propriétés des polynômes sous-résultants associés à $f(X,Y)$ et $\partial_Y f(X,Y)$.

Proposition 3.3.3 *Soient $i \in \mathbb{N}$ et $\mathrm{Sr}_i(X,Y) = \sum_{j\in[\![0,i]\!]} \mathrm{sr}_{i,j}(X)Y^j$ le i^{eme} sous-résultant associé à $f(X,Y)$ et $\partial_Y f(X,Y)$ considérés comme polynômes en Y à coefficients dans $\mathbb{Q}[X]$. Soit $(\alpha,\beta) \in \mathbb{R}^2$ un point x-critique de $\mathcal{C}(f)$. Si $\mathcal{C}(f)$ est en position générique alors il existe un unique $k \in \mathbb{N}$ tel que :*

$$\beta = \frac{-\mathrm{sr}_{k,k-1}(\alpha)}{k(\mathrm{sr}_{k,k}(\alpha))}$$

Démonstration Soit $k \in \mathbb{N}$ le degré du polynôme $\mathrm{pgcd}(f(\alpha,Y),\partial_Y f(\alpha,Y))$. D'aprés le théorème fondamental des sous-résultants il vient $\mathrm{sr}_{0,0}(\alpha) = \ldots = \mathrm{sr}_{k-1,k-1}(\alpha) = 0$, $\mathrm{sr}_{k,k}(\alpha) \neq 0$ et $\mathrm{pgcd}(f(\alpha,Y),\partial_Y f(\alpha,Y)) = \mathrm{Sr}_k(\alpha,Y) = \sum_{j\in[\![0,k]\!]} \mathrm{sr}_{k,j}(\alpha)Y^j$. Comme (α,β) est un point x-critique de $\mathcal{C}(f)$ alors β est une racine du $\mathrm{pgcd}(f(\alpha,Y),\partial_Y f(\alpha,Y))$. De plus, comme $\mathcal{C}(f)$ est en position générique, (α,β) est l'unique point x-critique d'abscisse α. Ainsi β est la seule racine du polynôme $\mathrm{pgcd}(f(\alpha,Y),\partial_Y f(\alpha,Y))$. Par conséquent, d'aprés les relations entre les coefficients d'un polynôme et ses racines, on a $\beta = \frac{-\mathrm{sr}_{k,k-1}(\alpha)}{k(\mathrm{sr}_{k,k}(\alpha))}$. □

Nous disposons d'une méthode permettant de vérifier qu'une courbe algébrique plane réelle n'admet aucune asymptote verticale. En effet, en notant $\mathrm{lc}_Y(f) \in \mathbb{Q}[X]$ le coefficient dominant du polynôme $f(X,Y)$ considéré comme polynôme en la variable Y, il vient que $\mathcal{C}(f)$ admet des asymptotes orthogonales à l'axe des abscisses si et seulement si le polynôme $\mathrm{lc}_Y(f)$ admet des racines réelles. Donc le test d'existence d'asymptotes verticales est équivalent au test d'existence de racines réelles d'un polynôme univarié à coefficients dans $\mathbb{Q}$. Ceci s'effectue aisément avec la méthode de Sturm présentée dans le Chapitre 2. Dans la pratique, sachant que la topologie de $\mathcal{C}(f)$ est invariante par changement linéaire de coordonnées, si $\mathcal{C}(f)$ admet des asymptotes verticales, nous effectuerons un changement de variable du type $X = X + \lambda Y$ avec $\lambda \in \mathbb{Q}^*$. En effet ce changement de variable rend le polynôme $\mathrm{lc}_Y(f)$ constant donc sans racines.

Rappelons que $f \in \mathbb{Q}[X,Y]$ est un polynôme sans facteur carré et que $\mathrm{lc}_Y(f) \in \mathbb{Q}[X]$ désigne son coefficient dominant considéré comme polynôme en la variable Y. Dans la suite de cette section, nous supposerons que $\mathrm{lc}_Y(f) \in \mathbb{Q}^*$.
Soit $d := \deg_Y(f)$ le degré de $f(X,Y)$ considéré comme polynôme en Y. Pour tout $i \in [\![0, d-1]\!]$, soit $\mathrm{Sr}_i(X,Y) = \sum_{j\in[\![0,i]\!]} \mathrm{sr}_{i,j}(X)Y^j$ le i^{eme} sous-résultant associé à $f(X,Y)$ et $\partial_Y f(X,Y)$

considérés comme polynômes en Y à coefficients dans $\mathbb{Q}[X]$. Rappelons que $\mathrm{Sr}_0(X,Y) = \mathrm{sr}_{0,0}(X)$ désigne le résultant des polynômes $f(X,Y)$ et $\partial_Y f(X,Y)$ par rapport à la variable Y. Soit $(\Gamma_i(X))_{i\in[\![1,d-1]\!]}$ la séquence d'éléments de $\mathbb{Q}[X]$ inductivement définie ci-dessous :

$$\Phi_0(X) = \frac{\mathrm{sr}_{0,0}(X)}{\mathrm{pgcd}(\mathrm{sr}_{0,0}(X), \mathrm{sr}'_{0,0}(X))};$$
$$\forall i \in [\![1,d-1]\!], \Phi_i(X) = \mathrm{pgcd}(\Phi_{i-1}(X), \mathrm{sr}_{i,i}(X)).$$
$$\forall i \in [\![1,d-1]\!], \Gamma_i(X) = \frac{\Phi_{i-1}(X)}{\Phi_i(X)}$$

Le lemme suivant nous permet de classer les valeurs x-critiques de $\mathcal{C}(f)$ selon leur multiplicité.

Lemme 3.3.4

1. $\Phi_0(X) = \prod_{i=1}^{d-1} \Gamma_i(X)$ *et* $\forall\, i, j \in \{1,\ldots,d-1\}$ *tel que* $i \neq j$*, on a*
$$\mathrm{pgcd}(\Gamma_i(X), \Gamma_j(X)) = 1$$
2. *Soient* $k \in [\![1,d-1]\!]$ *et* $\alpha \in \mathbb{C}$*. On a l'équivalence :*
$$\Gamma_k(\alpha) = 0 \Longleftrightarrow \mathrm{pgcd}(f(\alpha,Y), \partial_Y f(\alpha,Y)) = \mathrm{Sr}_k(\alpha,Y).$$
3. $\{(\alpha,\beta) \in \mathbb{C}^2 : f(\alpha,\beta) = \partial_Y f(\alpha,\beta) = 0\} = \bigcup_{k=1}^{d-1} \{(\alpha,\beta) \in \mathbb{C}^2 : \Gamma_k(\alpha) = \mathrm{Sr}_k(\alpha,\beta) = 0\}$.

Démonstration

1. Par définition, on a :
$$\forall i \in [\![1,d-1]\!],\ \Gamma_i(X) = \frac{\Phi_{i-1}(X)}{\Phi_i(X)}.$$
Ce qui entraîne :
$$\prod_{i=1}^{d-1} \Gamma_i(X) = \frac{\Phi_0(X)}{\Phi_{d-1}(X)}.$$
Comme $\Phi_{d-1}(X) = \mathrm{pgcd}(\Phi_{d-2}(X), \mathrm{sr}_{d-1,d-1}(X))$ et $\deg_Y(f) = d$, alors $\mathrm{sr}_{d-1,d-1}(X) = \mathrm{lc}_Y(f)$ par suite $\mathrm{sr}_{d-1,d-1}(X) \in \mathbb{Q}^*$. Ainsi $\Phi_{d-1}(X) = \mathrm{pgcd}(\Phi_{d-2}(X), \mathrm{sr}_{d-1,d-1}(X)) = 1$ et par suite $\Phi_0(X) = \prod_{i=1}^{d-1} \Gamma_i(X)$.
Comme $\Phi_0(X)$ est par définition la partie sans facteur carré du résultant $\mathrm{sr}_{0,0}(X)$ et que $\Phi_0(X) = \prod_{i=1}^{d-1} \Gamma_i(X)$, alors on a :
$$\forall i, j \in [\![1,d-1]\!]\, i \neq j \Longrightarrow \mathrm{pgcd}(\Gamma_i(X), \Gamma_j(X) = 1.$$

2. Soit $k \in [\![1, d-1]\!]$ et $\alpha \in \mathbb{C}$ tel que $\Gamma_k(\alpha) = 0$. Comme $\Gamma_k(X) = \frac{\Phi_{k-1}(X)}{\Phi_k(X)}$ et $\Phi_k(X) = \text{pgcd}(\Phi_{k-1}(X), \text{sr}_{k,k}(X))$ alors $\text{sr}_{k,k}(\alpha) \neq 0$ et $\Phi_{k-1}(\alpha) = 0$.
Comme $\Phi_{k-1}(X) = \text{pgcd}(\Phi_{k-2}(X), \text{sr}_{k-1,k-1}(X))$ alors $\Phi_{k-2}(\alpha) = 0$ et $\text{sr}_{k-1,k-1}(\alpha) = 0$.
Par une récurrence descendante on montre aisément que $\text{sr}_{k-2,k-2}(\alpha) = \ldots = \text{sr}_{0,0}(\alpha) = 0$.
En récapitulant, on a $\text{sr}_{0,0}(\alpha) = \ldots = \text{sr}_{k-1,k-1}(\alpha) = 0$ et $\text{sr}_{k,k}(\alpha) \neq 0$, donc par le théorème fondamental des sous-résultants, on a $\text{Sr}_k(\alpha, Y) = \text{pgcd}(f(\alpha, Y), \partial_Y f(\alpha, Y))$.
Réciproquement soit $k \in [\![1, d-1]\!]$ et $\alpha \in \mathbb{C}$ tel que $\text{pgcd}(f(\alpha, Y), \partial_y f(\alpha, Y)) = \text{Sr}_k(\alpha, Y)$.
Alors par le théorème fondamental des sous-résultants, on a $\text{sr}_{0,0}(\alpha) = \ldots = \text{sr}_{k-1,k-1}(\alpha) = 0$ et $\text{sr}_{k,k}(\alpha) \neq 0$. Comme $\Phi_0(X)$ est la partie sans facteur carré du résultant $\text{sr}_{0,0}(X)$ alors $\Phi_0(\alpha) = 0$. Par définition, pour tout $i \in [\![1, d-1]\!]$ $\Phi_i(X) = \text{pgcd}(\Phi_{i-1}(X), \text{sr}_{i,i}(X))$, donc $\text{sr}_{0,0}(\alpha) = \ldots = \text{sr}_{k-1,k-1}(\alpha) = 0$ implique par récurrence $\Phi_0(\alpha) = \ldots = \Phi_{k-1}(\alpha) = 0$.
Comme $\Phi_k(X) = \text{pgcd}(\Phi_{k-1}(X), \text{sr}_{k,k}(X))$, $\Phi_{k-1}(\alpha) = 0$ et $\text{sr}_{k,k}(\alpha) \neq 0$ alors $\Phi_k(\alpha) \neq 0$ d'où $\Gamma_k(\alpha) = \frac{\Phi_{k-1}(\alpha)}{\Phi_k(\alpha)} = 0$.
3. Si $(\alpha, \beta) \in \mathbb{C}^2$ est tel que $f(\alpha, \beta) = \partial_Y f(\alpha, \beta) = 0$, alors (α, β) est un point x-critique, donc $\Phi_0(\alpha) = 0$. Par conséquent, il existe $k \in [\![1, d]\!]$ tel que $\Gamma_k(\alpha) = 0$. Ainsi par la deuxième assertion du lemme, $\text{Sr}_k(\alpha, Y) = \text{pgcd}(f(\alpha, Y), \partial_Y f(\alpha, Y))$, d'où $\text{Sr}_k(\alpha, \beta) = 0$.
Réciproquement, soit $(\alpha, \beta) \in \mathbb{C}^2$ et $k \in [\![1, d-1]\!]$ tels que $\Gamma_k(\alpha) = 0$ et $\text{Sr}_k(\alpha, \beta) = 0$.
Comme $\Gamma_k(\alpha) = 0$ alors par ce qui précéde on a $\text{Sr}_k(\alpha, Y) = \text{pgcd}(f(\alpha, Y), \partial_Y f(\alpha, Y))$.
Comme $\text{Sr}_k(\alpha, \beta) = 0$, on a $f(\alpha, \beta) = \partial_Y f(\alpha, \beta) = 0$ d'où le résultat.

□

Proposition 3.3.5 *Soient $d := \deg_Y(f)$ et $\tau := \mathcal{L}(f)$. La séquence $(\Gamma_i(X))_{i \in [\![1, d-1]\!]}$ se calcule avec une complexité binaire de $\tilde{O}_B(d^6\tau)$, de plus pour tout $i \in [\![1, d-1]\!]$, $\mathcal{L}(\Gamma_i) = O(d(\tau + d))$.*
.

Démonstration En effet, par le Théorème 2.3.10, le calcul de la séquence $(\text{sr}_{i,i}(X))_{i \in [\![1, d-1]\!]}$ s'effectue avec un coût binaire de $\tilde{O}_B(d^4\tau)$, de plus, pour tout $i \in [\![1, d-1]\!]$ $\mathcal{L}(\text{sr}_{i,i}) = O(d\tau)$ et $\deg(\text{sr}_{i,i}) = O(d^2)$. $\Phi_0(X)$ étant par définition la partie sans facteur carré de $\text{sr}_{0,0}(X)$, alors $\deg(\Phi_0) = O(d^2)$ et $\mathcal{L}(\Phi_0) = O(d\tau)$. Par ailleurs comme $\Phi_0(X) = \prod_{i=1}^{d-1} \Gamma_i(X)$ alors $\sum_{i=1}^{d-1} \deg(\Gamma_i) = O(d^2)$ et, par la borne de Mignotte [45], $\mathcal{L}(\Gamma_i) = O(d(\tau + d))$. Pour calculer la séquence $(\Gamma_i(X))_{i \in [\![1, d-1]\!]}$, nous réalisons $O(d)$ calcul de pgcd de polynômes de degrés $O(d^2)$ (les polynômes $\Phi_i(X)$ et $\text{sr}_{i,i}(X)$) et dont les coefficients sont de tailles binaires $O(d\tau)$. Sachant que chaque calcul de pgcd a un coût binaire de $\tilde{O}_B(d^5\tau)$ d'après le Théorème 2.3.10, il vient que la complexité binaire de l'algorithme calculant la séquence $(\Gamma_i(X))_{i \in [\![1, d-1]\!]}$ est de $\tilde{O}_B(d^6\tau)$. □

La certification de la généricité de la position d'une courbe algébrique est une étape es-

sentielle dans le calcul de sa topologie. Dans [32], les auteurs décrivent un algorithme de test de généricité de la position de $\mathcal{C}(f)$, basé sur le calcul de l'encodage de Thom des racines réelles des polynômes $\Gamma_k(X)$. Nous rappelons ci-dessous la complexité binaire de cet algorithme. Ensuite nous proposons un algorithme modulaire de certification de généricité de la position de $\mathcal{C}(f)$ avec une complexité nettement plus faible. Sachant que la complexité de l'algorithme de calcul de $\mathcal{C}(f)$ décrit dans [32], est fixée par la phase de test et de mise en position générique, le nouvel algorithme que nous proposons, permet d'obtenir une amélioration de la complexité de l'algorithme global de calcul de la topologie de $\mathcal{C}(f)$.

Certificat de généricité de la position de $\mathcal{C}(f)$ par calcul d'encodage de Thom

Nous rappelons que pour $P \in \mathbb{Q}[X]$ de degré p, $\mathrm{Der}(P)$ désigne l'ensemble défini par :

$$\mathrm{Der}(P) := \{P^{(i)} \mid i = 0, \ldots, p\}$$

où $P^{(i)}$ désigne la dérivée d'ordre i du polynôme P. Rappelons qu'une condition de signes σ sur l'ensemble $\mathrm{Der}(P)$ est un élément de $\{0,1,-1\}^{\mathrm{Der}(P)}$ avec :

$$\begin{cases} \sigma(x) = 0 & \Longleftrightarrow \quad x = 0 \\ \sigma(x) = 1 & \Longleftrightarrow \quad x > 0 \\ \sigma(x) = -1 & \Longleftrightarrow \quad x < 0 \end{cases}$$

Définition 3.3.6 *Soient $P \in \mathbb{Q}[X]$ et $\sigma \in \{0,1,-1\}^{\mathrm{Der}(P)}$ une condition de signes sur l'ensemble* $\mathrm{Der}(P)$. *La condition de signes σ est **un encodage de Thom** de $x \in \mathbb{R}$ si $\sigma(P) = 0$ et σ est la liste des signes réalisés par les éléments de* $\mathrm{Der}(P)$ *en x. Nous dirons que x est spécifié par σ.*

La proposition suivante rappelle la complexité binaire de l'algorithme de test et de mise en position générique, par calcul d'encodage de Thom, décrit dans [32].

Proposition 3.3.7 *[32] Soient $f(X,Y) \in \mathbb{Z}[X,Y]$, $d := \deg(f)$ et $\tau := \mathcal{L}(f)$. La complexité binaire de l'algorithme de test et de mise en position générique de $\mathcal{C}(f)$ par encodage de Thom est de $\tilde{O}_B(d^{16}\tau)$.*

Cette phase de calcul est la plus coûteuse de l'algorithme décrite dans [32] et fixe donc la complexité globale de celui-ci. Dans la sous-section suivante, nous proposons un algorithme modulaire de test et de mise en position générique avec une complexité nettement plus faible permettant de réaliser un gain non négligeable sur la complexité globale de l'algorithme de calcul de la topologie de $\mathcal{C}(f)$.

Certificat de généricité de la position de $\mathcal{C}(f)$ par calcul modulaire

Contrairement à l'algorithme décrit dans [32] où le test de généricité consiste à calculer l'encodage de Thom de tous les points x-critiques de $\mathcal{C}(f)$ et ensuite de vérifier que chaque fibre x-critique contient un et un seul point x-critique, l'idée de base de l'algorithme que nous proposons consiste à traiter les fibres x-critiques par paquet selon la multiplicité du point x-critique qu'elles contiennent. En effet, nous avons le résultat suivant :

Théorème 3.3.8 *$\mathcal{C}(f)$ est en position générique si et seulement si pour tout $k \in [\![1, d-1]\!]$ et tout $i \in [\![0, k-1]\!]$, on a :*

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

Démonstration Supposons que $\mathcal{C}(f)$ soit en position générique. Soit $k \in [\![1, d-1]\!]$ et $\alpha \in \mathbb{C}$ tel que $\Gamma_k(\alpha) = 0$. Alors par l'assertion 2 du Lemme 3.3.4, $\mathrm{pgcd}(f(\alpha,Y), \partial_Y f(\alpha,Y)) = \mathrm{Sr}_k(\alpha,Y) = \sum_{i\in[\![0,k]\!]} \mathrm{sr}_{k,i}(\alpha)Y^i$. Comme $\mathcal{C}(f)$ est en position générique, par la Proposition 3.3.3 le polynôme $\mathrm{Sr}_k(\alpha,Y) = \mathrm{pgcd}(f(\alpha,Y), \partial_Y f(\alpha,Y))$ a une seule racine : $\beta(\alpha) = \frac{-\mathrm{sr}_{k,k-1}(\alpha)}{k(\mathrm{sr}_{k,k}(\alpha))}$. Ainsi $\mathrm{Sr}_k(\alpha,Y) = \mathrm{sr}_{k,k}(\alpha)(Y-\beta)^k$. Par la formule de Newton, $(Y-\beta)^k = \sum_{i\in[\![0,k]\!]} \binom{k}{i}(-\beta)^{k-i}Y^i$, donc $\mathrm{Sr}_k(\alpha,Y) = \mathrm{sr}_{k,k}(\alpha)\sum_{i=0}^{k}\binom{k}{i}(-\beta)^{k-i}Y^i$. Par définition, $\mathrm{Sr}_k(\alpha,Y) = \sum_{i\in[\![0,k]\!]} \mathrm{sr}_{k,i}(\alpha)Y^i$, donc en identifiant les deux expressions de $\mathrm{Sr}_k(\alpha,Y)$ on a pour tout $i \in [\![1,k]\!]$:

$$\mathrm{sr}_{k,i}(\alpha) = \binom{k}{i}\mathrm{sr}_{k,k}(\alpha)(-\beta(\alpha))^{k-i} \quad (1)$$

En substituant i par $(i+1)$ dans (1) on obtient pour tout $i \in [\![0,k-1]\!]$:

$$\mathrm{sr}_{k,i+1}(\alpha) = \binom{k}{i+1}\mathrm{sr}_{k,k}(\alpha)(-\beta(\alpha))^{k-i-1} \quad (2)$$

De (1) et (2) on deduit que pour tout $i \in [\![0,k-1]\!]$:

$$\binom{k}{i+1}\mathrm{sr}_{k,i}(\alpha) + \binom{k}{i}\beta(\alpha)\,\mathrm{sr}_{k,i+1}(\alpha) = 0$$

Sachant que $(i+1)\binom{k}{i+1} = (k-i)\binom{k}{i}$ et $\beta(\alpha) = \frac{-\mathrm{sr}_{k,k}(\alpha)}{k(\mathrm{sr}_{k,k-1}(\alpha))}$, alors pour tout $i \in [\![0,k-1]\!]$:

$$k(k-i)\,\mathrm{sr}_{k,i}(\alpha)\,\mathrm{sr}_{k,k}(\alpha) - (i+1)\,\mathrm{sr}_{k,k-1}(\alpha)\,\mathrm{sr}_{k,i+1}(\alpha) = 0$$

Réciproquement, supposons que pour tout $k \in [\![1,d-1]\!]$ et $i \in [\![0,k-1]\!]$ on ait :

$$k(k-i)\,\mathrm{sr}_{k,i}(X)\,\mathrm{sr}_{k,k}(X) - (i+1)\,\mathrm{sr}_{k,k-1}(X)\,\mathrm{sr}_{k,i+1}(X) = 0 \bmod \Gamma_k(X) \quad (3)$$

Soit α une valeur x-critique de $\mathcal{C}(f)$, alors α est une racine du résultant des polynômes $f(X,Y)$ et $\partial_Y f(X,Y)$ par rapport à la variable Y. Comme $\Phi_0(X) = \prod_{i=1}^{d-1}\Gamma_i(X)$ est la partie

sans facteur carré de ce résultant alors il existe un unique $j \in [\![1, d-1]\!]$ tel que $\Gamma_j(\alpha) = 0$. Considérons un tel j, de (3) nous déduisons que :

$$\forall i \in [\![0, j-1]\!], j(j-i)\,\mathrm{sr}_{j,i}(\alpha)\,\mathrm{sr}_{j,j}(\alpha) - (i+1)\,\mathrm{sr}_{j,j-1}(\alpha)\,\mathrm{sr}_{j,i+1}(\alpha) = 0 \quad (4)$$

En multipliant (4) par $\binom{j}{i}$ et en utilisant l'égalité $(i+1)\binom{j}{i+1} = (j-i)\binom{j}{i}$, on obtient :

$$\forall i \in [\![0, j-1]\!], j\binom{j}{i+1}\mathrm{sr}_{j,i}(\alpha)\,\mathrm{sr}_{j,j}(\alpha) - \binom{j}{i}\mathrm{sr}_{j,j-1}(\alpha)\,\mathrm{sr}_{j,i+1}(\alpha) = 0 \quad (5)$$

Par définition, $\Gamma_j(X) = \frac{\Phi_{j-1}(X)}{\Phi_j(X)}$, comme $\Gamma_j(\alpha) = 0$ et $\Phi_j(X) = \mathrm{pgcd}(\Phi_{j-1}(X), \mathrm{sr}_{j,j}(X))$ alors $\mathrm{sr}_{j,j}(\alpha) \neq 0$. On peut donc diviser l'égalité (5) par $j.\mathrm{sr}_{j,j}(\alpha)$, ainsi on obtient :

$$\forall i \in [\![0, j-1]\!], \binom{j}{i+1}\mathrm{sr}_{j,i}(\alpha) + \binom{j}{i}\beta(\alpha)\,\mathrm{sr}_{j,i+1}(\alpha) = 0 \,\text{avec}\, \beta(\alpha) = \frac{-\mathrm{sr}_{j,j-1}(\alpha)}{j.\mathrm{sr}_{j,j}(\alpha)}$$

De cette dernière égalité, on déduit par récurrence que pour tout t $i \in [\![0, j]\!]$:

$$\mathrm{sr}_{j,i}(\alpha) = \binom{j}{i}\mathrm{sr}_{j,j}(\alpha)(-\beta(\alpha))^{j-i}$$

d'où $\mathrm{Sr}_j(\alpha, Y) = \sum_{i\in[\![0,j]\!]}\mathrm{sr}_{j,i}(\alpha)Y^i = \sum_{i\in[\![0,j]\!]}\binom{j}{i}\mathrm{sr}_{j,j}(\alpha)(-\beta(\alpha))^{j-i}Y^i = \mathrm{sr}_{j,j}(\alpha)(Y-\beta(\alpha))^j$. Comme $\Gamma_j(\alpha) = 0$, alors par l'assertion 2 du Lemme 3.3.4, $\mathrm{Sr}_j(\alpha, Y) = \mathrm{pgcd}(f(\alpha, Y), \partial_Y f(\alpha, Y))$ d'où l'égalité $\mathrm{pgcd}(f(\alpha, Y), \partial_Y f(\alpha, Y)) = \mathrm{sr}_{j,j}(\alpha)(Y-\beta(\alpha))^j$. Le polynôme $\mathrm{pgcd}(f(\alpha, Y), \partial_Y f(\alpha, Y))$ admet donc une seule racine $\beta(\alpha)$. Ainsi $(\alpha, \beta(\alpha))$ est le seul point x-critique contenu dans la fibre x-critique de $\mathcal{C}(f)$ en α. Par conséquent $\mathcal{C}(f)$ est en position générique. □

L'algorithme suivant, basé sur le Théorème 3.3.8, permet de certifier la généricité de la position de $\mathcal{C}(f)$. Rappelons que $f \in \mathbb{Q}[X, Y]$ est sans facteur carré, que $\mathrm{lc}_Y(f) \in \mathbb{Q}^*$ et que $(\mathrm{Sr}_k(X, Y))_{k\in[\![0,d-1]\!]}$ désigne la séquence des polynômes sous-résultants associée à $f(X, Y)$ et $\partial_Y f(X, Y)$. De plus si $\deg_Y(f) = d$, alors $\forall \in k \in [\![0, d-1]\!]$, $\mathrm{Sr}_k(X, Y) = \sum_{i\in[\![0,k]\!]}\mathrm{sr}_{k,i}(X)Y^i$.

Algorithme 3.3.1 : `GenericTest`, teste la généricité de la position de $\mathcal{C}(f)$.

Entrées : $f(X,Y) \in \mathbb{Q}[X,Y]$ et $(\mathrm{Sr}_k(X,Y))_{k\in[\![0,d-1]\!]}$

Sorties : Un polynôme univarié

$\rightarrow$ Calcul de la séquence $(\Gamma_k(X))_{k\in[\![1,d-1]\!]}$:

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

Pour k allant de 1 à $d-1$ faire

$\Phi_k(X) = \mathrm{pgcd}(\Phi_{k-1}(X), \mathrm{sr}_{k,k}(X))$,

$\Gamma_k(X) = \frac{\Phi_{k-1}(X)}{\Phi_k(X)}$,

Fin faire.

$\rightarrow$ Test de généricité :

$S := 0$,

$k := 1$,

Tant que $k < d$ et $S = 0$, faire :

$i := 0$,

Tant que $S = 0$ et $i < k$, faire :

$S := (k(k-i)\,\mathrm{sr}_{k,i}(X)\,\mathrm{sr}_{k,k}(X) - (i+1)\,\mathrm{sr}_{k,k-1}(X)\,\mathrm{sr}_{k,i+1}(X)) \bmod \Gamma_k(X)$,

$i := i+1$,

Fin tant que,

$k := k+1$,

Fin tant que,

Retourner S,

L'algorithme retourne le polynôme S. La courbe $\mathcal{C}(f)$ est en position générique si et seulement si le polynôme S est nul.

Théorème 3.3.9 *Soient $f(X,Y) \in \mathbb{Z}[X,Y]$, $d = \deg(f)$ et $\tau = \mathcal{L}(f)$.* `GenericTest`*, teste la généricité de la position de $\mathcal{C}(f)$ avec une complexité binaire de $\tilde{O}_B(d^6\tau)$.*

Démonstration L'utilisation de l'algorithme `GenericTest` nécessite $O(d^2)$ appels de l'algorithme d'Euclide avec un polynôme de degré borné par $O(d^2)$ (polynôme $\Gamma_k(X)$) et un polynôme de degré borné par $O(d^2)$ (produit de deux polynômes coefficients sous-résultants de degrés bornés par $O(d^2)$) et dont les coefficients sont de tailles binaires bornées par $\tilde{O}_B(d(\tau+d))$. Le coût binaire du calcul des coefficients sous-résultants est de $\tilde{O}_B(d^5\tau)$ d'après le Théorème 2.3.10. Celui du calcul des polynômes $\Gamma_k(X)$ est de $\tilde{O}_B(d^6\tau)$ d'après la Propo-

sition 3.3.5. Sachant que la complexité arithmétique de l'algorithme d'Euclide rapide (voir [61]) pour deux polynômes univariés de degrés m et n est de $\tilde{O}(max(m,n))$, alors le coût binaire des réductions modulo les polynômes $\Gamma_k(X)$ est de $O(d^2) \times O(d^2) \times \tilde{O}_B(d(\tau+d)) = \tilde{O}_B(d^5(\tau+d))$. Ainsi la complexité binaire de l'algorithme `GenericTest` correspond au coût du calcul des polynômes $\Gamma_k(X)$ soit $\tilde{O}_B(d^6\tau)$. □

Dans le cas où la courbe $\mathcal{C}(f)$ n'est pas en position générique, on peut la mettre en position générique en effectuant un changement linéaire de variable du type $X := X + \lambda Y$ avec $\lambda \in \mathbb{Z}^*$. En effet, soit U une nouvelle variable et $g(U,X,Y)$ le polynôme défini par :

$$g(U,X,Y) := f(X+UY,Y)$$

Pour $\lambda \in \mathbb{Z}$, nous noterons $\mathcal{C}(f_\lambda)$ la courbe définie par le polynôme $f_\lambda(X,Y) = g(\lambda,X,Y) = 0$. Soit $\Delta(U,X)$ le discriminant de $g(U,X,Y)$ par rapport à la variable Y et $s(U)$ le plus petit sous-résultant principal non nul des polynômes $\Delta(U,X)$ et $\partial_X\Delta(U,X)$ par rapport à la variable X. Le résultat suivant provient de [6] :

Proposition 3.3.10 *Soit $\lambda \in \mathbb{Z}$ tel que $\deg_Y(f_\lambda) = \deg(f_\lambda)$ et $s(\lambda) \neq 0$. Alors la courbe $\mathcal{C}(f_\lambda)$ est en position générique.*

Comme le degré du polynôme $s(\lambda)$ est majoré par d^4, on a :

Corollaire 3.3.11 *Soit $f \in \mathbb{Z}[X,Y]$ et $d := \deg(f)$. Il y a au plus d^4 changements de variables du type $X := X + \lambda Y$, $\lambda \in \mathbb{Z}$ à réaliser pour être sûr d'atteindre une position générique de la courbe $\mathcal{C}(f_\lambda)$.*

Du Théorème 3.3.9 et du Corollaire 3.3.11 découle le théorème suivant :

Théorème 3.3.12 *Soit $f(X,Y) \in \mathbb{Z}[X,Y]$, $d := \deg(f)$ et $\tau := \mathcal{L}(f)$. La complexité binaire de l'algorithme de test et de mise en position générique de $\mathcal{C}(f)$ par calcul modulaire est de $\tilde{O}_B(d^{10}\tau)$.*

La prochaine étape dans l'algorithme de calcul de topologie de $\mathcal{C}(f)$ est la détermination de ses fibres x-critiques et régulières.

3.3.3 Calcul des fibres régulières et x-critiques de $\mathcal{C}(f)$

Le calcul des fibres régulières de $\mathcal{C}(f)$ ne pose pas de problème particulier. En effet, soit δ une valeur régulière de $\mathcal{C}(f)$ et $\mathrm{Reg}_\delta(f)$ la fibre de la courbe $\mathcal{C}(f)$ en δ. Alors par définition

on a :

$$\mathrm{Reg}_{\delta}(f) := \{(\delta,\kappa) \in \mathbb{R}^2 : f(\delta,\kappa) = 0\}.$$

Comme δ est une valeur régulière de $\mathcal{C}(f)$, alors le polynôme $f(\delta,Y)$ est sans facteur multiple. L'isolation de ses racines réelles se fait donc sans difficulté en utilisant les algorithmes classiques cités dans le chapitre précédent.

Par contre le calcul des fibres x-critiques de $\mathcal{C}(f)$ est plus délicat. En effet, soit α une valeur x-critique de $\mathcal{C}(f)$ et $\mathrm{Crit}_{\alpha}(f)$ la fibre de $\mathcal{C}(f)$ en α. Alors par définition on a :

$$\mathrm{Crit}_{\alpha}(f) := \{(\alpha,\mu) \in \mathbb{R}^2 : f(\alpha,\mu) = 0\}.$$

Ici deux difficultés se combinent. En effet, non seulement la valeur α est un nombre algébrique, mais le polynôme $f(\alpha,Y)$ peut avoir des facteurs multiples. Ces deux aspects rendent l'isolation des racines réelles du polynôme $f(\alpha,Y)$ assez délicate. Nous détaillons ci-dessous comment le calcul des fibres x-critiques de $\mathcal{C}(f)$ s'effectue, malgré cela, de manière certifiée.

Supposons que $\mathcal{C}(f)$ soit en position générique et soit (α,β) le point critique de $\mathcal{C}(f)$ d'abscisse α. Alors par le Lemme 3.3.4, il existe $k \in [\![1, d-1]\!]$ tel que $\Gamma_k(\alpha) = 0$ et $\beta = \frac{-\mathrm{sr}_{k,k-1}(\alpha)}{k(\mathrm{sr}_{k,k}(\alpha))}$ soit l'unique racine du polynôme $\mathrm{Sr}_k(\alpha,Y) = \mathrm{pgcd}(f(\alpha,Y),\partial_Y f(\alpha,Y))$. Alors $\mathrm{Crit}_{\alpha}(f) := \{\mathrm{Down}_{(\alpha,\beta)},(\alpha,\beta),\mathrm{Up}_{(\alpha,\beta)}\}$ où $\mathrm{Down}_{(\alpha,\beta)}$ désigne l'ensemble des points de la fibre x-critique situés en-dessous du point (α,β) et $\mathrm{Up}_{(\alpha,\beta)}$ celui de ceux situés au-dessus. Comme le polynôme $\mathrm{Sr}_k(\alpha,Y) = \mathrm{pgcd}(f(\alpha,Y),\partial_Y f(\alpha,Y))$ est de degré k alors β est une racine de $f(\alpha,Y)$ de mutiplicité $k+1$. Soit $F_k(\alpha,Y) = \frac{f(\alpha,Y)}{(Y-\beta)^{k+1}}$. La proposition suivante nous fournit $\mathrm{Down}_{(\alpha,\beta)}$ et $\mathrm{Up}_{(\alpha,\beta)}$.

Proposition 3.3.13 *$F_k(\alpha,Y+\beta)$ est un polynôme sans facteur carré qui ne s'annule pas en 0. De plus, si on désigne par E_+ (respectivement E_-) l'ensemble de ses racines positives (respectivement négatives), on a :*

1. $\mathrm{Down}_{(\alpha,\beta)} := \{(\alpha,\beta+\lambda) : \lambda \in E_-\}$,
2. $\mathrm{Up}_{(\alpha,\beta)} := \{(\alpha,\beta+\lambda) : \lambda \in E_+\}$.

Démonstration Puisque $\mathcal{C}(f)$ est en position générique, alors $\beta = \frac{-\mathrm{sr}_{k,k-1}(\alpha)}{k(\mathrm{sr}_{k,k}(\alpha))}$ est l'unique racine multiple de $f(\alpha,Y)$. Comme β est de multiplicité $k+1$, alors $(Y-\beta)^{k+1}$ divise $f(\alpha,Y)$ d'où $F_k(\alpha,Y)$ est sans facteur carré, $\deg_Y(F_k(\alpha,Y)) = (d-k-1)$ et $F_k(\alpha,\beta) \neq 0$. Par conséquent $F_k(\alpha,Y+\beta)$ est un polynôme sans facteur carré qui ne s'annule pas en 0.
Comme $\mathrm{Down}_{(\alpha,\beta)}$ désigne l'ensemble des points de la fibre x-critique situés en-dessous du point (α,β) et $\mathrm{Up}_{(\alpha,\beta)}$ celui de ceux situés au-dessus, alors il vient que :

$$\mathrm{Down}_{(\alpha,\beta)} := \{(\alpha,\beta+\lambda) : \lambda \in E_-\} \qquad \text{et} \qquad \mathrm{Up}_{(\alpha,\beta)} := \{(\alpha,\beta+\lambda) : \lambda \in E_+\}$$

□

Remarque 3.3.14 Pour tout $k \in [\![1, d-1]\!]$, $\text{pgcd}(\Gamma_k(X), \text{sr}_{k,k}(X)) = 1$. En effet, soit α une racine de $\Gamma_k(X)$, alors par le Lemme 3.3.4, $\text{pgcd}(f(\alpha,Y), \partial_Y f(\alpha,Y)) = \sum_{i=0}^{k} \text{sr}_{k,i}(\alpha)Y^i$ est de degré k, par conséquent $\text{sr}_{k,k}(\alpha) \neq 0$, on obtient bien $\text{pgcd}(\Gamma_k(X), \text{sr}_{k,k}(X)) = 1$. Donc pour tout α racine de $\Gamma_k(X)$, $\frac{1}{\text{sr}_{k,k}(\alpha)} \in \mathbb{Q}[\alpha]$ et par suite $\beta = \frac{-\text{sr}_{k,k-1}(\alpha)}{k(\text{sr}_{k,k}(\alpha))} \in \mathbb{Q}[\alpha]$.

Le polynôme $F_k(\alpha, Y+\beta) \in \mathbb{Q}[\alpha][Y]$ car $\beta \in \mathbb{Q}[\alpha]$, de plus $F_k(\alpha, Y+\beta)$ est sans facteur carré. Donc par l'algorihme décrit dans la section 2.1.3, nous pouvons isoler de manière certifié les racines de $F_k(\alpha, Y+\beta)$ et en déduire les ensembles $\text{Down}_{(\alpha,\beta)}$, $\text{Up}_{(\alpha,\beta)}$ et par suite, la fibre x-critique $\text{Crit}_\alpha(f) := \{(\alpha,\mu) \in \mathbb{R}^2 : f(\alpha,\mu) = 0\}$.

Proposition 3.3.15 *Soient $f \in \mathbb{Z}[X,Y]$, $d := \deg(f)$, $\tau := \mathcal{L}(f)$ et $\mathcal{C}(f)$ le lieu des zéros réels de f. Si $\mathcal{C}(f)$ est en position générique, alors le calcul de ses fibres x-critiques et de ses fibres régulières s'effectue avec une complexité binaire de $\tilde{O}_B(d^{10}\tau)$.*

Démonstration En effet, le calcul des fibres x-critiques de $\mathcal{C}(f)$ nécessite $O(d^2)$ appels de l'algorithme d'isolation décrit dans la section 2.1.3 avec $P = f(X,Y)$ et $Q = \Gamma_k(X)$. Sachant que pour tout k, $\deg(\Gamma_k) = O(d^2)$ et $\mathcal{L}(\Gamma_k) = O(d\tau)$, alors par la Proposition 2.1.28, la complexité binaire d'un tel calcul est de $O(d^2) \times \tilde{O}_B(d^2 d^4 \times max(d^2\tau, d\tau))$, soit $\tilde{O}_B(d^{10}\tau)$. Le calcul des fibres régulières correspond à $O(d^2)$ isolations de racines de polynômes univariés à coefficients rationnels et de degré d. Son coût binaire est de $\tilde{O}_B(d^5\tau)$ d'après la Proposition 3.4.2. □

Les fibres x-critiques et les fibres régulières étant calculées, il reste à les connecter pour reconstruire la topologie de $\mathcal{C}(f)$. Dans la section suivante nous décrivons l'algorithme de balayage de Grandine [35] qui permet de réaliser cette opération.

3.3.4 Algorithme de connection

Supposons que $\mathcal{C}(f)$ soit en position générique. Soit $(\alpha_i)_{i\in[\![1,n]\!]}$ la séquence strictement croissante des valeurs x-critiques de $\mathcal{C}(f)$ et $(\text{Crit}_{\alpha_i}(f))_{i\in[\![1,n]\!]}$ ses fibres x-critiques. Soit $(\delta_i)_{i\in[\![0,n]\!]}$ une séquence croissante de nombres réels vérifiant $\delta_0 < \alpha_1 < \delta_1 < \alpha_2 < \ldots < \alpha_{n-1} < \delta_{n-1} < \alpha_n < \delta_n$ et $(\text{Reg}_{\delta_i}(f))_{i\in[\![0,n]\!]}$ la liste des fibres régulières de $\mathcal{C}(f)$ en les valeurs δ_i.
Le but de l'algorithme de connection est de reconstruire la topologie de $\mathcal{C}(f)$ à partir de ses fibres x-critiques $(\text{Crit}_{\alpha_i}(f))_{i\in[\![1,n]\!]}$ et de ses fibres régulières $(\text{Reg}_{\delta_i}(f))_{i\in[\![0,n]\!]}$.

Rappelons que pour tout $i \in [\![1,n]\!]$, $\text{Crit}_{\alpha_i}(f) := \{\text{Down}_{(\alpha_i,\beta_i)}, (\alpha_i,\beta_i), \text{Up}_{(\alpha_i,\beta_i)}\}$ où β_i est l'ordonnée du point x-critique de $\mathcal{C}(f)$ d'abscisse α_i, $\text{Down}_{(\alpha_i,\beta_i)}$ désigne l'ensemble des points de la fibre x-critique situés en-dessous du point (α_i,β_i) et $\text{Up}_{(\alpha_i,\beta_i)}$ celui de ceux situés au-dessus. L'algorithme de connection suivant est du à Grandine [35]. Il consiste, pour tout $i \in [\![1,n]\!]$, à connecter la fibre x-critique $\text{Crit}_{\alpha_i}(f)$ aux fibres régulières $\text{Reg}_{\delta_{i-1}}(f)$ et $\text{Reg}_{\delta_i}(f)$.

Algorithme 3.3.2 : `Connection des fibres régulières aux fibres x-critiques`

Entrées : $(\text{Crit}_{\alpha_i}(f))_{i\in[\![1,n]\!]}$ et $(\text{Reg}_{\delta_i}(f))_{i\in[\![0,n]\!]}$
Sorties : Complexe simplicial isotope à $\mathcal{C}(f)$
$\mathcal{T} := \{\}$, Pour i allant de 1 à n faire :

- Pour j allant de 1 à $\#\text{Up}_{(\alpha_i,\beta_i)}$ faire
  $\mathcal{T} := \mathcal{T} \bigcup \{[\text{Reg}_{\delta_{i-1}}[j], \text{Up}_{(\alpha_i,\beta_i)}[j]], [\text{Reg}_{\delta_i}[j], \text{Up}_{(\alpha_i,\beta_i)}[j]]\}$,
- Pour j allant de 1 à $\#\text{Down}_{(\alpha_i,\beta_i)}$ faire
  $\mathcal{T} := \mathcal{T} \bigcup \{[\text{Reg}_{\delta_{i-1}}[\#\text{Reg}_{\delta_{i-1}} - j + 1], \text{Down}_{(\alpha_i,\beta_i)}[\#\text{Down}_{(\alpha_i,\beta_i)} - j + 1]], [\text{Reg}_{\delta_i}[\#\text{Reg}_{\delta_i} - j + 1], \text{Down}_{(\alpha_i,\beta_i)}[\#\text{Down}_{(\alpha_i,\beta_i)} - j + 1]]\}$,
- Pour j allant de $\#\text{Up}_{(\alpha_i,\beta_i)} + 1$ à $(\#\text{Reg}_{\delta_{i-1}} - \#\text{Down}_{(\alpha_i,\beta_i)})$ faire
  $\mathcal{T} := \bigcup \{[\text{Reg}_{\delta_{i-1}}[j], (\alpha_i,\beta_i)]\}$,
- Pour j allant de $\#\text{Up}_{(\alpha_i,\beta_i)} + 1$ à $(\#\text{Reg}_{\delta_i} - \#\text{Down}_{(\alpha_i,\beta_i)})$ faire
  $\mathcal{T} := \bigcup \{[\text{Reg}_{\delta_i}[j], (\alpha_i,\beta_i)]\}$,

Retourner $\mathcal{T}$ ensemble de segments.

Remarque 3.3.16 Soit c un point x-critique de $\mathcal{C}(f)$ et $\text{Crit} := \{\text{Up}, c, \text{Down}\}$ la fibre x-critique passant par c. Soit Reg une fibre régulière de $\mathcal{C}(f)$ connectée à Crit. Soit $p \in \text{Reg}$ et q le point de la fibre Crit connecté à p. Soit l'application $\varphi_c : \text{Reg} \longrightarrow \{-1, 0, 1\}$ définie par :

- $\varphi_c(p) = -1$ si $q \in \text{Up}$
- $\varphi_c(p) = 0$ si $q = c$
- $\varphi_c(p) = 1$ si $q \in \text{Down}$

L'application φ_c sera d'une très grande utilité dans la description de l'algorithme de maillage d'une surface algébrique implicite.

3.4 L'algorithme de calcul de la topologie de $\mathcal{C}(f)$

3.4.1 Description globale de l'algorithme `TopolCourbe2D`

Algorithme 3.4.1 : `TopolCourbe2D`

Entrées : $f \in \mathbb{Q}[X,Y]$ polynôme sans facteur carré de degré d

Sorties : Topologie de la courbe $\mathcal{C}(f)$

1. Prendre $\lambda := 0$ et poser $f_\lambda(X,Y) = f(X+\lambda Y, Y)$,
2. Calcul de la séquence des polynômes $(\Gamma_k(X))_{k\in[\![1,d-1]\!]}$.
3. Tester la généricité de la position de $\mathcal{C}(f_\lambda)$ avec l'algorithme `GenericTest`.
4. Calculer les fibres x-critiques de $\mathcal{C}(f_\lambda)$.
   - Calcul des points x-critiques : pour $k = 1,\dots,d-1$, soit $\alpha_1^{(k)}$,..., $\alpha_{s_k}^{(k)}$ les racines réelles de $\Gamma_k(X)$ et $\beta_i^{(k)} = -\frac{\mathrm{sr}_{k,k-1}(\alpha_i^{(k)})}{k\,\mathrm{sr}_{k,k}(\alpha_i^{(k)})}$.
     pCrit $:= \bigcup_{k=1}^{d-1}\bigcup_{i=1}^{s_k}\left\{(\alpha_i^{(k)},\beta_i^{(k)})\right\}$ est l'ensemble des points x-critique de $\mathcal{C}(f_\lambda)$.
   - Calcul des points réguliers des fibres x-critiques : pour $k = 1,\dots,d-1$, $j = 1,\dots,s_k$, soit $F_k(\alpha_j^{(k)},\beta_j^{(k)},Y) = \frac{f_\lambda(\alpha_j^{(k)},Y)}{(Y-\beta_j^{(k)})^{k+1}}$ et $\delta_{j,1}^{(k)}$, ..., $\delta_{j,n_k}^{(k)}$ les racines réelles de $F_k(\alpha_j^{(k)},\beta_j^{(k)},Y)$, alors :
     $B_j^{(k)} := \left\{(\alpha_j^{(k)},\delta_{j,1}^{(k)}),\dots,(\alpha_j^{(k)},\delta_{j,n_k}^{(k)})\right\}$ est l'ensemble des points réguliers de la fibre x-critique $x = \alpha_j^{(k)}$.
5. Calculer les fibres régulières de $\mathcal{C}(f_\lambda)$: Soit $\alpha_1 < \alpha_2 \dots < \alpha_{\#\mathrm{pCrit}}$ la liste strictement croissante des valeurs x-critiques de $\mathcal{C}(f_\lambda)$, $\alpha_0 = \alpha_1 - 1$ et $\alpha_{\#(\mathrm{pCrit})+1} = \alpha_{\#\mathrm{pCrit}} + 1$.
   Pour $i = 0,\dots,\#\mathrm{pCrit}$, soit $\rho_i = \frac{\alpha_i+\alpha_{i+1}}{2}$ et $\theta_1^{(i)}$, ..., $\theta_{m_i}^{(i)}$ les racines réelles du polynôme $f_\lambda(\rho_i,Y)$.
   $\mathrm{Reg}_i = \left\{(\rho_i,\theta_1^{(i)}),\dots(\rho_i,\theta_{m_i}^{(i)})\right\}$ est l'ensemble des points de la fibre régulière $x = \rho_i$.
6. Appliquer l'algorithme de connection aux fibres calculées.

3.4.2 Complexité de l'algorithme `TopolCourbe2D`.

Notations et résultats basiques

Nous rappelons que $\tilde{O}_B$ désigne la complexité binaire en ignorant les facteurs logarithmiques, $\mathcal{L}(a) := \lceil \log_2 |a| \rceil$ désigne la taille binaire d'un entier donné a et pour P polynôme à coeffients entiers $(a_0, \ldots, a_n)$ (en une ou plusieurs variables), $\mathcal{L}(P)$ désigne :

$$\mathcal{L}(P) := \max(\mathcal{L}(a_0), \ldots, \mathcal{L}(a_n))$$

L'algorithme de calcul de topologie que nous venons de décrire comporte essentiellement trois phases :

1. une phase d'élimination où on calcule la séquence des polynômes sous-résultants associés aux polynômes $f(X,Y)$ et $\partial_Y f(X,Y)$;
2. une phase où on teste si la courbe $\mathcal{C}(f)$, lieu des zéros réels du polynôme $f(X,Y)$, est en position générique ;
3. une phase d'isolation des racines réelles du résultant des polynômes $f(X,Y)$ et $\partial_Y f(X,Y)$.

Dans cette section nous rappelons les complexités binaires des algorithmes que nous utilisons dans ces phases de calcul.

Le résultat suivant provient du Théorème 2.3.10.

Proposition 3.4.1 *Soient $A, B \in \mathbb{Z}[X,Y]$ de degrés et de tailles binaires de coefficients respectivement majorés par d et τ. Il existe un algorithme calculant la séquence des sous-résultants $(\mathrm{Sr}_i(A,B))_{i\in[\![0,d]\!]}$, par rapport à la variable Y, associée à A et B avec une complexité de $\tilde{O}_B(d^5\tau)$. De plus pour tout $i \in [\![0,d]\!]$, $\mathcal{L}(\mathrm{Sr}_i(A,B)) = O(d\tau)$.*

Concernant l'isolation des racines, Pan décrit dans [54], un algorithme calculant une approximation des racines avec une précison ε en $\tilde{O}_B(d^3\tau + d\varepsilon)$ avec $\varepsilon \in \tilde{O}(d\tau)$ qui est la borne de séparation pour un polynôme de degré d et des coefficients de taille τ. Ainsi nous avons, pour l'isolation des racines, la proposition suivante :

Proposition 3.4.2 *Soient $A \in \mathbb{Z}[X]$, $d := \deg(A)$ et $\tau := \mathcal{L}(A)$. Il existe un algorithme d'isolation des racines réelles de A avec une complexité de $\tilde{O}_B(d^3\tau)$. De plus la taille des bornes des intervalles d'isolation est $\tilde{O}(d\tau)$.*

Etude de complexité de l'algorithme `TopolCourbe2D`.

Théorème 3.4.3 *Soient $f \in \mathbb{Z}[X,Y]$, $d := \deg(f)$, $\tau := \mathcal{L}(f)$ et $\mathcal{C}(f)$ le lieu des zéros réels de f. L'algorithme `TopolCourbe2D` calcule la topologie de la courbe $\mathcal{C}(f)$ avec une complexité binaire probabiliste en $\tilde{O}_B(d^{10}\tau)$ et déterministe en $\tilde{O}_B(d^{10}\tau)$.*

Démonstration La première étape de l'algorithme est le calcul de la séquence des sous-résultants $(\mathrm{Sr}_i(f,\partial_Y f))_{i\in[\![0,d]\!]}$ associée à $f(X,Y)$ et $\partial_Y f(X,Y)$ par rapport à la variable Y. D'aprés la Proposition 3.4.1, ce calcul s'effectue avec une complexité de $\tilde{O}_B(d^5\tau)$ et pour tout $i \in [\![0,d]\!]$, $\mathcal{L}(\mathrm{Sr}_i(f,\partial f)) = O(d\tau)$. La deuxième étape consiste à calculer la séquence $(\Gamma_i(X))_{i\in[\![1,d-1]\!]}$. D'après la Proposition 3.3.5, son coût binaire est de $\tilde{O}_B(d^6\tau)$. La troisième étape est la phase de test et de mise en position générique de $\mathcal{C}(f)$. D'aprés le Théorème 3.3.12 (respectivement Théorème 3.3.9), ce calcul s'effectue en une complexité binaire déterministe (respectivement probabiliste) en $\tilde{O}_B(d^{10}\tau)$ (repectivement $\tilde{O}_B(d^6\tau)$). Ensuite vient la phase de calcul des fibres x-critiques et des fibres régulières. Le calcul des valeurs x-critiques correspond à l'isolation des racines du résultant $\mathrm{Sr}_0(f,\partial_Y f)$ qui est un polynôme univarié de degré $\tilde{O}_B(d^2)$ avec $\mathcal{L}(\mathrm{Sr}_0(f,\partial f)) = O(d\tau)$. Par la Proposition 3.4.2, ce calcul s'effectue avec une complexité de $\tilde{O}_B((d^2)^3 d\tau) = \tilde{O}_B(d^7\tau)$. Les calculs des deuxièmes coordonnées des fibres x-critiques et des fibres régulières de $\mathcal{C}(f)$ s'effectue, d'après la Proposition 3.3.15, avec une complexité binaire de $\tilde{O}_B(d^{10}\tau)$. Ainsi le calcul de la topologie de $\mathcal{C}(f)$ s'effectue avec une complexité binaire deterministe en $\tilde{O}_B(d^5\tau + d^6\tau + d^{10}\tau + d^7\tau + d^{10}\tau) = \tilde{O}_B(d^{10}\tau)$ et probabiliste en $\tilde{O}_B(d^5\tau + d^6\tau + d^6\tau + d^7\tau + d^{10}\tau) = \tilde{O}_B(d^{10}\tau)$. □

3.5 Implémentation et expérimentation

L'algorithme que nous venons de décrire a été entièrement implémenté avec MATHEMAGIX. Dans cette section, nous fournissons quelques exemples de topologies calculées ainsi que les équations des courbes correspondantes.

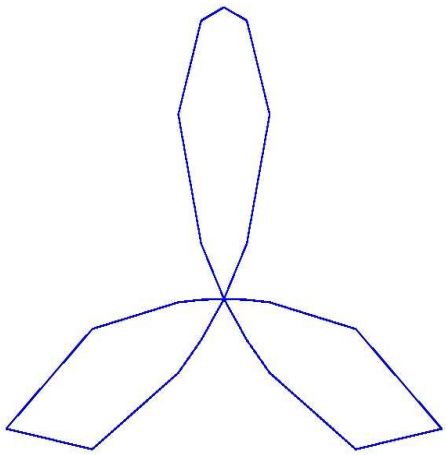

FIG. 3.7 – $x^4 + 2x^2y^2 + y^4 + 3x^2y - y^3$

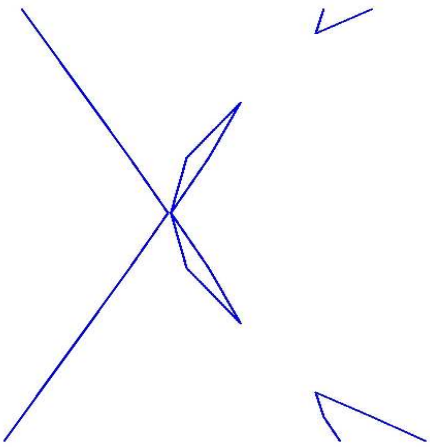

FIG. 3.8 – $y^4 - 6y^2x + x^2 - 4x^2y^2 + 24x^3$

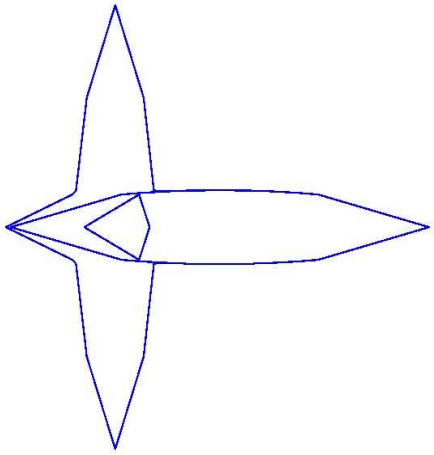

FIG. 3.9 – $-230390x^4 - 1558300x^3 + 37065600y^4 + 3590x^6 + 21700x^5 + 129600y^6 + 2604360x^2 - 74528640y^2 - 7277400x^2y^2 - 55969200y^2x + 1558800x^3y^2 + 27993600y^4x + 27975600x + 4672800y^4x^2 + 258940y^2x^4 + 37333439$

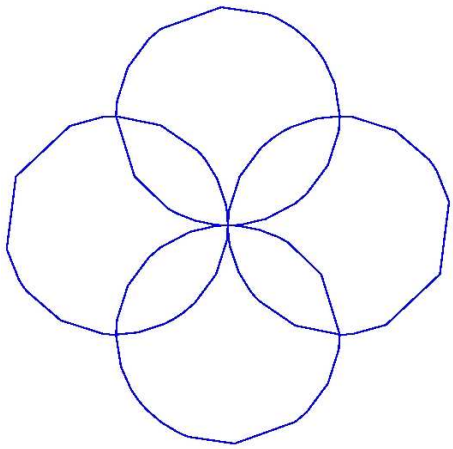

FIG. 3.10 – $x^8 + 4x^6y^2 + 6y^4x^4 + 4y^6x^2 + y^8 - 4x^6 - 12y^2x^4 - 12y^4x^2 - 4y^6 + 16x^2y^2$

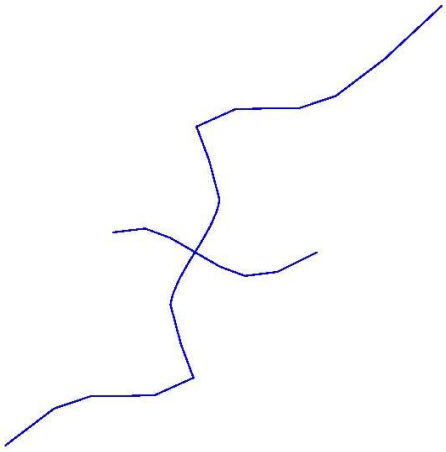

FIG. 3.11 – $x^6 + y^2x^4 - y^4x^2 - 2x^4 - y^6 + 2y^4 + x^2 - y^2 + xy$

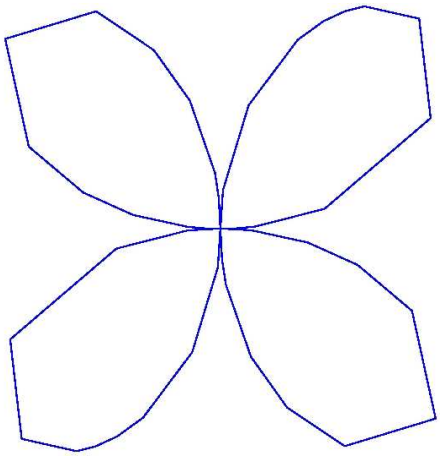

FIG. 3.12 – $x^6 + 3y^2x^4 + 3y^4x^2 + y^6 - 4x^2y^2$

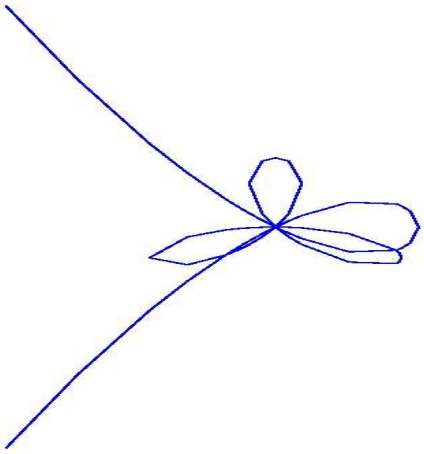

FIG. 3.13 – $-y^2x^4 - x^6 + x^7 + y^4x^2 + 2x^5y^2 + y^6 + x^3y^4 + 4x^2y^3 - 3x^4y + 3x^5y - y^5 - x^3y^3$

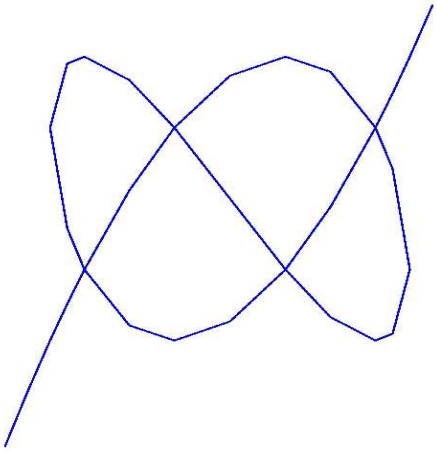

FIG. 3.14 – $16x^5 - 20x^3 + 5x - 4y^3 + 3y$

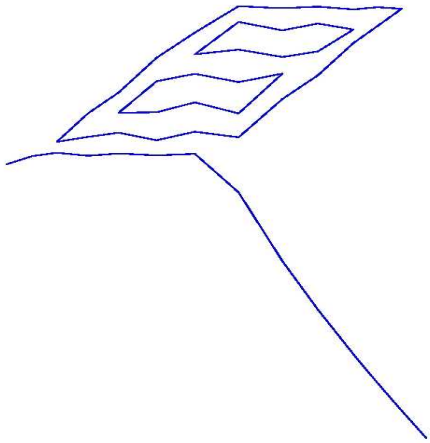

FIG. 3.15 – $-105y^2x^4 - 80y^3 + 140x^3y^3 - 140y^3x + 35y^4 - 105y^4x^2 + 48y^5 + 42xy^5 - 42x^2 + 35x^4 - 7x^6 + 32y + 84xy - 140x^3y + 42x^5y + 210x^2y^2 - 42y^2 - 7y^6 - 8y^7 + 7$

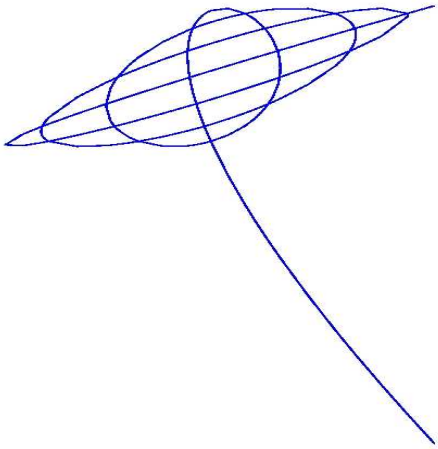

FIG. 3.16 – $-y^8 + x^7 - 7x^6y + 21x^5y^2 - 35x^4y^3 + 35x^3y^4 - 21x^2y^5 + 7xy^6 - y^7 + 8y^6 - 7x^5 + 35x^4y - 70x^3y^2 + 70x^2y^3 - 35xy^4 + 7y^5 - 20y^4 + 14x^3 - 42x^2y + 42xy^2 - 14y^3 + 16y^2 - 7x + 7y - 2$

Chapitre 4

Topologie d'une courbe intersection de deux surfaces implicites.

4.1 Introduction

Dans le chapitre précédent, nous nous sommes intéressés au calcul de la topologie d'une courbe algébrique plane. Ce calcul peut être interprété comme la détermination de la topologie d'une section d'une surface algébrique, c'est-à-dire, la topologie de l'intersection d'une surface avec un plan. A présent, nous abordons le problème, plus général, du calcul de la topologie de l'intersection de deux surfaces algébriques. On suppose que les deux surfaces n'ont pas de composante commune, c'est-à-dire que leur intersection est une réunion de courbes et de points isolés.
Le calcul de la topologie de l'intersection de deux surfaces algébriques implicites est une primitive essentielle dans plusieurs algorithmes utilisés en CAGD. En effet, il apparait indispensable dans les algorithmes de calcul de maillages isotopiques de surfaces algébriques singulières. Il existe plusieurs travaux dédiés à ce problème. Dans [5], Alcazar et Sendra étudient le cas particulier où la courbe d'intersection est réduite. Ils proposent un algorithme symbolique-numérique utilisant la théorie des sous-résultants et le calcul de pgcd d'approximations de polynômes. Leur approche donne de bons résultats pratiques, mais les topologies retournées ne sont pas certifiées du à l'utilisation de calcul de pgcd d'approximations de polynômes. Dans [53], Owen et Rockwood étudient aussi le cas où la courbe d'intersection est réduite. Ils proposent un algorithme numérique utilisant des techniques de subdivision. Mais la topologie aux voisinages des singularités de la courbe est non certifiée voire inconnue. Nous mentionnons aussi le travail dans [31], où les auteurs s'attaquent au problème dans le cas où l'intersection est une courbe réduite. Trés récemment, El Kahoui a proposé

dans [24] un algorithme symbolique-numérique certifié pour le calcul de la topologie de courbes définies comme intersection de *n* surfaces implicites. Son algorithme exige le calcul des générateurs du radical de l'idéal engendré par les polynômes définissant les surfaces considérées, faisant ainsi appel à des calculs de base de Gröbner, en plus des calculs des suites de sous-résultants.
Dans ce chapitre, nous présentons un algorithme, symbolique-numérique, certifié de calcul de topologie d'une courbe intersection de deux surfaces implicites. L'approche que nous développons est basée sur une analyse des propriétés des sous-résultants. Contrairement aux algorithmes décrits dans [31] et [5], elle n'utilise qu'une projection de la courbe d'intersection et permet de calculer sa topologie dans le cas où elle est non réduite.
Nous introduisons la notion de courbe en position pseudo-générique par rapport à un plan, ce qui nous permettra de garantir l'existence de paramétrisations rationnelles par morceaux de la courbe, par rapport à sa projection sur ce plan. La topologie de la courbe projetée est calculée avec l'algorithme décrit dans le Chapitre 3, puis relevée morceau par morceau dans l'espace, en utilisant les paramétrisations. L'utilisation de ces paramétrisations permet un relèvement rapide, et évite les problèmes numériques souvent rencontrés dans ce type de calcul.
L'une des difficultés majeures des algorithmes basés sur la méthode "projection puis relèvement" réside dans la distinction entre les singularités de la courbe plane, introduites par la projection, et les singularités provenant de la projection de vraies singularités de la courbe spatiale. Nous proposons un algorithme certifié permettant de distinguer ces deux types de singularités de la courbe projetée.

4.2 Analyse de la géométrie d'une courbe implicite

Soient $P_1, P_2 \in \mathbb{R}[X,Y,Z]$, $\mathcal{Z}(P_1,P_2) = \{(x,y,z) \in \mathbb{C}^3 \mid P_1(x,y,z) = P_2(x,y,z) = 0\}$ la variété algébrique définie par P_1 et P_2.

Définition 4.2.1 *On dit que la variété algébrique $\mathcal{Z}(P_1,P_2)$ est une courbe algébrique dans $\mathbb{C}^3$ si elle est de dimension 1.*

Supposons que la variété algébrique $\mathcal{C} := \mathcal{Z}(P_1,P_2)$ soit une courbe algébrique et nommons $\mathcal{C}_\mathbb{R}$ sa partie réelle :

$$\mathcal{C}_\mathbb{R} := \mathcal{Z}(P_1,P_2) \cap \mathbb{R}^3 = \{(x,y,z) \in \mathbb{R}^3 \mid P_1(x,y,z) = P_2(x,y,z) = 0\}.$$

Nous nous intéressons au problème du calcul de la topologie de la courbe algébrique réelle $\mathcal{C}_\mathbb{R}$, c'est-à-dire la détermination d'une structure Λ, linéaire par morceaux, isotope à $\mathcal{C}_\mathbb{R}$.

Définition 4.2.2 *Une isotopie de $\mathbb{R}^3$ est une application $\varphi : \mathbb{R}^3 \times [0,1] \longrightarrow \mathbb{R}^3$, telle que $\varphi(\cdot,0) = \mathrm{Id}_{\mathbb{R}^3}$ et pour tout $t \in]0,1]$, $\varphi(\cdot,t)$ est un homéomorphisme.*

Définition 4.2.3 *Soient $\Delta, \Lambda \subset \mathbb{R}^3$, on dit que Δ est isotope à Λ s'il existe une isotopie φ de $\mathbb{R}^3$ telle que $\varphi(\Delta, 1) = \Lambda$.*

Comme pour les courbes algébriques planes, le calcul de la topologie d'une courbe algébrique de $\mathbb{R}^3$ passe par celui de la structure de ses points singuliers et des arcs lisses qui relient ces points. Soit I l'ensemble des polynômes s'annulant sur la courbe algébrique :

$$I := \{G \in \mathbb{R}[X,Y,Z] \mid \forall (\alpha,\beta,\gamma) \in \mathcal{Z}(P_1,P_2), G(\alpha,\beta,\gamma) = 0\}$$

Il est clair que I est un idéal de l'anneau $\mathbb{R}[X,Y,Z]$. De plus par le théorème des zéros de Hilbert, I est le radical de l'idéal $\langle P_1,P_2\rangle$, engendré par P_1 et P_2. Nous notons $G_1,\ldots,G_m$ un système de générateurs de l'idéal I i.e. $I := \langle G_1,\ldots,G_m\rangle$. Les deux idéaux, $\langle G_1,\ldots,G_m\rangle$ et $\langle P_1,P_2\rangle$, décrivent algébriquement le même objet géométrique $\mathcal{C}$. Cependant pour l'analyse de la topologie de la courbe $\mathcal{C}_\mathbb{R}$, la description de $\mathcal{C}$ par $\langle G_1,\ldots,G_m\rangle$ est plus convenable, car la caractérisation des singularités géométriques de $\mathcal{C}_\mathbb{R}$ s'effectue aisément avec une chute de rang de la matrice jacobienne associée à $G_1,\ldots,G_m$. En effet l'idéal $\langle P_1,P_2\rangle$ n'étant pas radical, il arrive qu'il existe des composantes de $\mathcal{C}$ géométriquement lisses sur lesquelles on observe une chute du rang de la matrice jacobienne associée à P_1 et P_2.

Exemple 4.2.4 Soient $P_1 = X^2+Y^2-1, P_2 = X^2+Y^2+Y^2-1$ et $\mathcal{C}_\mathbb{R} = \{(x,y,z) \in \mathbb{R}^3 \mid P_1(x,y,z) = P_2(x,y,z) = 0\}$. La courbe $\mathcal{C}_\mathbb{R}$ est un cercle, donc géométriquement lisse. Cependant, le rang de la matrice jacobienne associée à P_1 et P_2, en tout point de $\mathcal{C}_\mathbb{R}$ est strictement inférieur à 2.

Définition 4.2.5 *Soit $M(X,Y,Z)$ la matrice jacobienne $m \times 3$ avec $(\partial_X G_i, \partial_Y G_i, \partial_Z G_i)$ comme i^{eme} ligne.*

1. *$(\alpha,\beta,\gamma) \in \mathcal{C}_\mathbb{R}$ est régulier si et seulement si le rang de la matrice $M(\alpha,\beta,\gamma)$ est égal à 2.*
2. *$(\alpha,\beta,\gamma) \in \mathcal{C}_\mathbb{R}$ singulier si le rang de la matrice $M(\alpha,\beta,\gamma)$ est strictement inférieur à 2.*

L'une des difficultés majeures du problème de la construction de la topologie de $\mathcal{C}_\mathbb{R}$ réside dans le calcul de la structure de ses points singuliers. A cette difficulté, s'ajoute celle de l'élaboration d'algorithme permettant de connecter convenablement les arcs lisses de $\mathcal{C}_\mathbb{R}$ à ses singularités. Dans ce chapitre, nous fournissons un algorithme résolvant le problème, sans passer par le calcul du radical de l'idéal $\langle P_1,P_2\rangle$. L'algorithme que nous développons dans ce chapitre peut être décomposé en trois phases :

1. calculer une projection de la courbe $\mathcal{C}_\mathbb{R}$ sur "un plan bien choisi",
2. calculer la topologie de la projection de $\mathcal{C}_\mathbb{R}$ obtenue en 1 en utlisant l'algorithme `TopolCourbe2D` décrit dans le chapitre précédent,
3. relever, de façon certifiée, la topologie de la courbe projetée obtenue en 2.

Par "plan de projection bien choisi", nous entendons un plan tel que la projection $\mathcal{C}_{\mathbb{R}}$ sur ce dernier, présente un certain nombre de propriétés de généricité simplifiant le calcul et le relèvement de sa topologie.

4.3 Calcul certifié de la topologie de $\mathcal{C}_{\mathbb{R}}$

4.3.1 Description géométrique de l'algorithme

Considérons une courbe algébrique spatiale (figure 4.1). La première étape de l'algorithme consiste à calculer une projection de notre courbe sur un plan donné (figure 4.2). Une fois la courbe projetée, nous calculons la topologie de sa projection en utilisant l'algorithme `TopolCourbe2D` décrit dans le chapitre précédent. Rappelons que ce dernier fonctionne en calculant les fibres x-critiques de la courbe plane, puis une fibre régulière entre deux fibres x-critiques consécutives (figure 4.3). Après ce calcul, vient la phase de relèvement. Cette phase commence par le relèvement des fibres précédemment calculées (figure 4.4). La dernière étape est celle de la connection des points dans l'espace (figure 4.5). Si la courbe est dans une "bonne position", ces connections peuvent être déduites de celles obtenues sur la courbe plane.

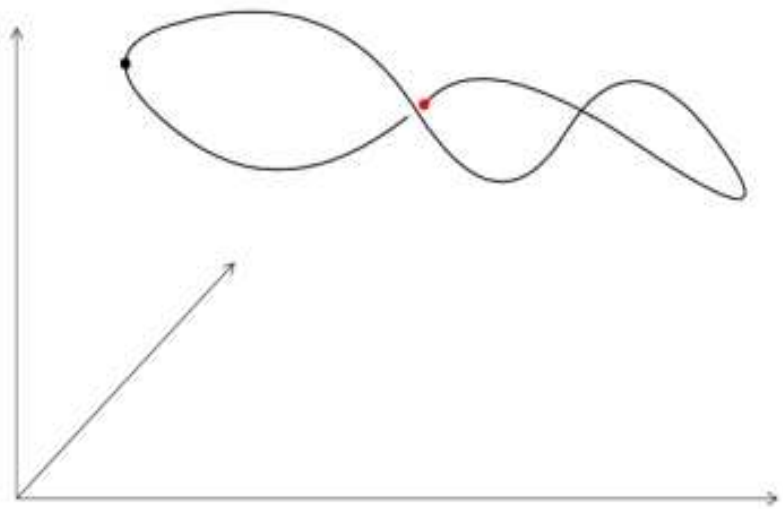

FIG. 4.1 – Courbe spatiale

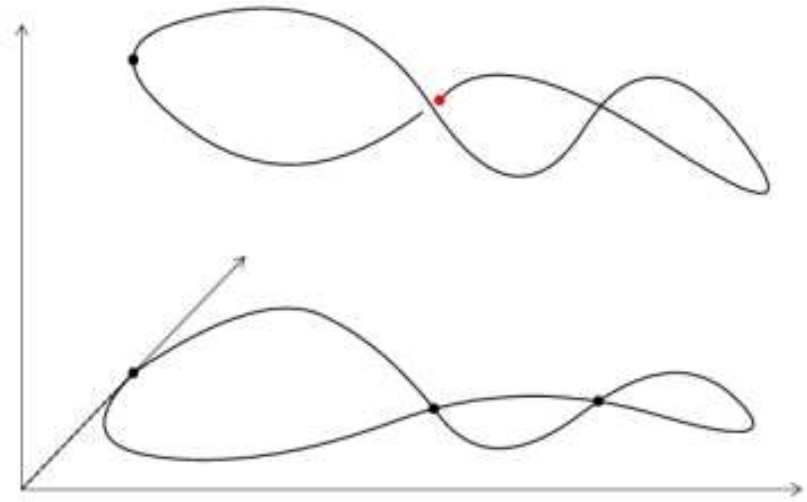

FIG. 4.2 – Phase de projection

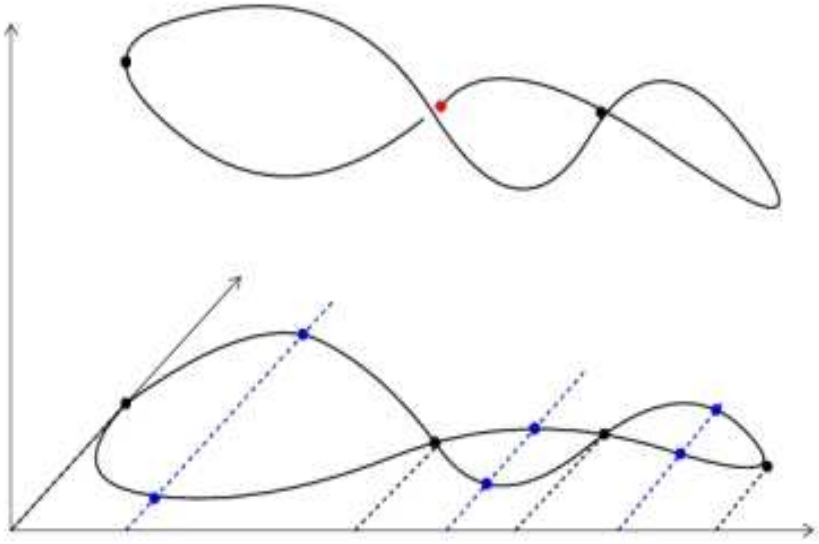

FIG. 4.3 – Calcul de la topologie de la projection

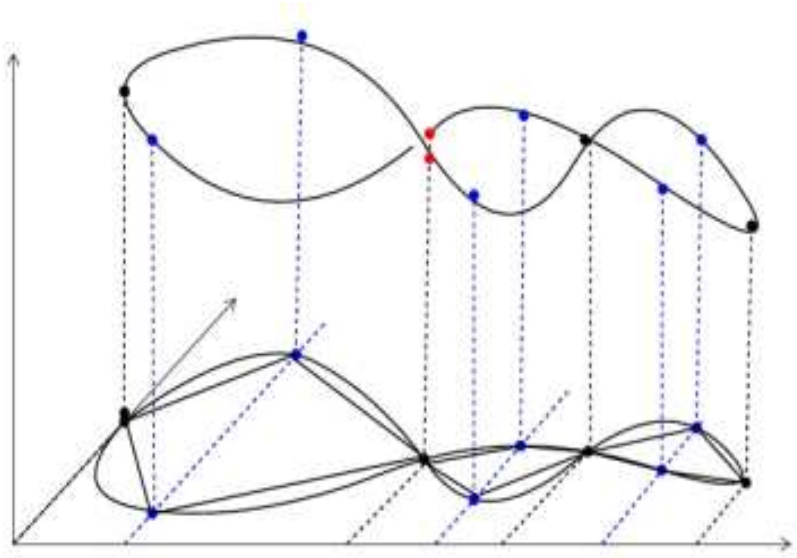

FIG. 4.4 – Relèvement des fibres

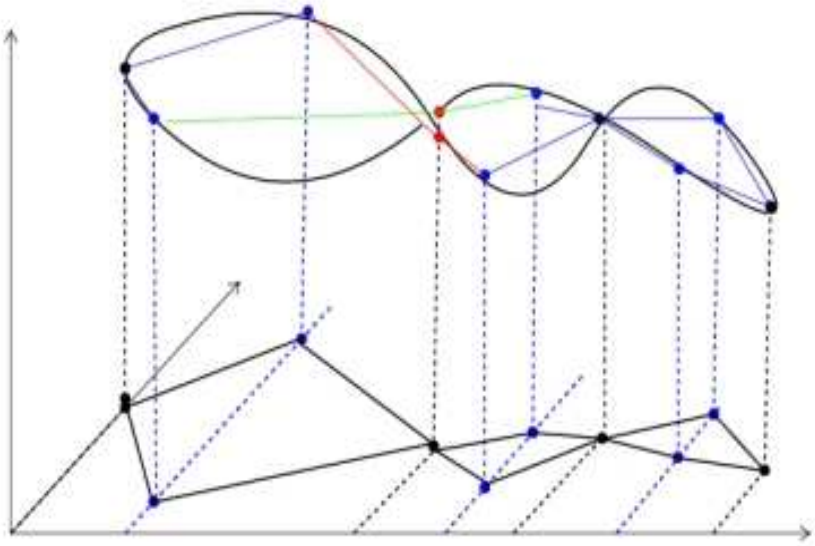

FIG. 4.5 – Phase de connection

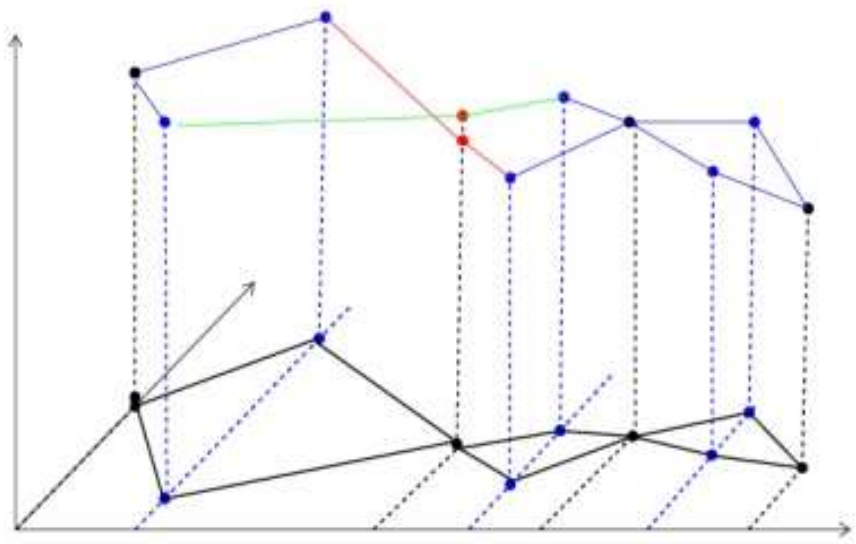

FIG. 4.6 – Complexe simplicial obtenu

L'objectif de la section suivante est de définir, puis de caractériser la notion de "bonne position" employée ci-dessus.

4.3.2 Conditions de généricité de $\mathcal{C}_{\mathbb{R}}$

Pour qu'une courbe spatiale soit dans "une bonne position", elle doit remplir trois conditions. Dans cette sous-section, nous définissons ces conditions, puis élaborons des algorithmes certifiés permettant de tester si une courbe donnée les remplit.

Pseudo-généricité de la position de $\mathcal{C}_{\mathbb{R}}$

Soit $\Pi : (x,y,z) \in \mathbb{C}^3 \longmapsto (x,y) \in \mathbb{C}^2$ et $\Pi|_{\mathcal{C}}$ la restriction de Π à l'ensemble $\mathcal{C}$.

Définition 4.3.1 *La courbe réelle $\mathcal{C}_{\mathbb{R}}$ est en position pseudo-générique par rapport au plan (x,y) si, pour presque tout point $(\alpha,\beta) \in \Pi|_{\mathcal{C}}(\mathcal{C})$, l'ensemble $\Pi|_{\mathcal{C}}^{-1}(\alpha,\beta)$ est réduit à un point. Autrement dit, $\mathcal{C}_{\mathbb{R}}$ est en position pseudo-générique si et seulement si l'ensemble* App*, défini par* App $:= \{(\alpha,\beta) \in \Pi|_{\mathcal{C}}(\mathcal{C}) \mid \#(\Pi|_{\mathcal{C}}^{-1}(\alpha,\beta)) > 1\}$*, est fini.*

Admettons que $\deg_Z(P_1) = \deg(P_1)$ et $\deg_Z(P_2) = \deg(P_2)$ (on peut toujours se ramener à cette hypothèse par un changement de coordonnées). Soit f la partie sans facteur carré du résultant de P_1 et P_2 par rapport à la variable Z et $m := \min(\deg(P_1), \deg(P_2))$. Pour tout $i \in [\![0,m]\!]$, soit $\mathrm{Sr}_i(X,Y,Z) = \sum_{j\in[\![0,i]\!]} \mathrm{sr}_{i,j}(X,Y)Z^j$ le i^{eme} sous-résultant associé à P_1 et P_2 considérés comme polynômes en Z. Soit $(\Delta_i(X,Y))_{i\in[\![0,m]\!]}$ la séquence d'éléments de $\mathbb{Q}[X,Y]$ inductivement définie ci-dessous :

$$\Delta_0(X,Y) = 1, \Theta_0(X,Y) = f(X,Y);$$

$$\forall i \in [\![1,m]\!], \Theta_i(X,Y) = \mathrm{pgcd}(\Theta_{i-1}(X,Y), \mathrm{sr}_{i,i}(X,Y)).$$

$$\forall i \in [\![1,m]\!], \Delta_i(X,Y) = \frac{\Theta_{i-1}(X,Y)}{\Theta_i(X,Y)}$$

Pour tout $i \in [\![1,m]\!]$, soient :

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

$$\mathcal{C}(f) := \{(x,y) \in \mathbb{R}^2 : f(x,y) = 0\}.$$

La proposition suivante permet de classer les composantes de $\mathcal{C}(f)$, projection de $\mathcal{C}_\mathbb{R}$ sur le plan (x,y), selon leur multiplicité. De plus, pour une classe de composantes de $\mathcal{C}(f)$ de multiplicité i, elle fournit une paramétrisation rationnelle permettant de relever les points réguliers de cette classe de composantes.

Proposition 4.3.2

1. $f(X,Y) = \prod_{i\in[\![1,m]\!]} \Delta_i(X,Y)$.
2. $\mathcal{C}(f) = \bigcup_{i\in[\![1,m]\!]} \mathcal{C}(\Delta_i)$.
3. *$\mathcal{C}_\mathbb{R}$ est en position pseudo-générique par rapport au plan (x,y) si et seulement si pour tout $(\alpha,\beta) \in \mathbb{C}^2$ et tout $i \in [\![1,m]\!]$ tel que $\mathrm{sr}_{i,i}(\alpha,\beta) \neq 0$ et $\Delta_i(\alpha,\beta) = 0$ on a :*

$$\mathrm{Sr}_i(\alpha,\beta,Z) = \sum_{j\in[\![0,i]\!]} \mathrm{sr}_{i,j}(\alpha,\beta)Z^j = \mathrm{sr}_{i,i}(\alpha,\beta)(Z-\gamma)^i, \text{ avec } \gamma = -\frac{\mathrm{sr}_{i,i-1}(\alpha,\beta)}{i\,\mathrm{sr}_{i,i}(\alpha,\beta)}$$

Démonstration

1. Comme pour tout $i \in [\![1,m]\!]$, $\Delta_i(X,Y) = \frac{\Theta_{i-1}(X,Y)}{\Theta_i(X,Y)}$, alors par récurrence on a :

$$\prod_{i=1}^{m} \Delta_i(X,Y) = \frac{\Theta_0(X,Y)}{\Theta_m(X,Y)} = \frac{f(X,Y)}{\Theta_m(X,Y)}.$$

   Comme $\deg_Z(P_1) = \deg(P_1)$ et $\deg_Z(P_2) = \deg(P_2)$ alors $\mathrm{sr}_{m,m}(X,Y) \in \mathbb{Q}^*$ par suite $\Theta_m(X,Y) = \mathrm{pgcd}(\Theta_{m-1}(X,Y), \mathrm{sr}_{m,m}(X,Y)) = 1$ et $f(X,Y) = \prod_{i\in[\![1,m]\!]} \Delta_i(X,Y)$.

2. Comme $f(X,Y)=\prod_{i\in[\![1,m]\!]}\Delta_i(X,Y)$, alors il est clair que $\mathcal{C}(f)=\bigcup_{i\in[\![1,m]\!]}\mathcal{C}(\Delta_i)$.
3. Supposons que $\mathcal{C}_{\mathbb{R}}$ soit en position pseudo-générique par rapport au plan (x,y). Soient $(\alpha,\beta)\in\mathbb{C}^2$ et $i\in[\![1,m]\!]$ tels que $\Delta_i(\alpha,\beta)=0$ et $\mathrm{sr}_{i,i}(\alpha,\beta)\neq 0$. Comme $\Delta_i(X,Y)=\frac{\Theta_{i-1}(X,Y)}{\Theta_i(X,Y)}$, alors $\Theta_{i-1}(\alpha,\beta)=0$. Or $\Theta_{i-1}(X,Y)=\mathrm{pgcd}(\Theta_{i-2}(X,Y),\mathrm{sr}_{i-1,i-1}(X,Y))$, donc $\Theta_{i-2}(\alpha,\beta)=0$ et $\mathrm{sr}_{i-1,i-1}(\alpha,\beta)=0$. Répétant le même raisonnement, nous montrons que $\mathrm{sr}_{i-2,i-2}(\alpha,\beta)=\ldots=\mathrm{sr}_{0,0}(\alpha,\beta)=0$. Ainsi on a, $\mathrm{sr}_{i-1,i-1}(\alpha,\beta)=\ldots=\mathrm{sr}_{0,0}(\alpha,\beta)=0$ et $\mathrm{sr}_{i,i}(\alpha,\beta)\neq 0$, et par le théorème fondamental des sous-résultants :

$$\mathrm{pgcd}(P_1(\alpha,\beta,Z),P_2(\alpha,\beta,Z))=\mathrm{Sr}_i(\alpha,\beta,Z)=\sum_{j\in[\![0,i]\!]}\mathrm{sr}_{i;j}(\alpha,\beta)Z^j.$$

Comme $\mathcal{C}_{\mathbb{R}}$ est en position pseudo-générique par rapport au plan (x,y), le polynôme $\mathrm{Sr}_i(\alpha,\beta,Z)$ admet une unique racine, qui s'écrit, d'après les relations entre coefficients et racines d'un polynôme, $\gamma=-\frac{\mathrm{sr}_{i,i-1}(\alpha,\beta)}{i\,\mathrm{sr}_{i,i}(\alpha,\beta)}$, d'où le résultat.

Réciproquement, supposons que pour tout $(\alpha,\beta)\in\mathbb{C}^2$ et tout $i\in[\![1,m]\!]$ tels que $\mathrm{sr}_{i,i}(\alpha,\beta)\neq 0$ et $\Delta_i(\alpha,\beta)=0$ on a :

$$\mathrm{Sr}_i(\alpha,\beta,Z)=\sum_{j\in[\![0,i]\!]}\mathrm{sr}_{i,j}(\alpha,\beta)Z^j=\mathrm{sr}_{i,i}(\alpha,\beta)(Z-\gamma)^i,\ \text{avec}\ \gamma=-\frac{\mathrm{sr}_{i,i-1}(\alpha,\beta)}{i\,\mathrm{sr}_{i,i}(\alpha,\beta)}.$$

Soit alors $(\alpha,\beta)\in\mathcal{C}(f)$. Comme $\mathcal{C}(f)=\bigcup_{i\in[\![1,m]\!]}\mathcal{C}(\Delta_i)$, il existe $i\in[\![1,m]\!]$ tel que $\Delta_i(\alpha,\beta)=0$. Si $\mathrm{sr}_{i,i}(\alpha,\beta)\neq 0$, en posant $\gamma=-\frac{\mathrm{sr}_{i,i-1}(\alpha,\beta)}{i\,\mathrm{sr}_{i,i}(\alpha,\beta)}$, nous avons $\mathrm{Sr}_i(\alpha,\beta,\gamma)=0$, ainsi (α,β,γ) est l'unique point de $\mathcal{C}$ se projetant sur (α,β). Sachant par ailleurs, qu'il n'y a qu'un nombre fini de points de $\mathcal{C}(f)$ solutions du système $\Delta_i(x,y)=\mathrm{sr}_{i,i}(x,y)=0$, alors presque tous les points de $\mathcal{C}(f)$ ont une et une seule pré-image par $\Pi|_{\mathcal{C}}$. La courbe $\mathcal{C}_{\mathbb{R}}$ est donc en position pseudo-générique.

□

Proposition 4.3.3 *Soient $P_1,P_2\in\mathbb{Z}[X,Y,Z]$, $d=\max(\deg(P_1),\deg(P_2))$ et $\tau=\mathcal{L}(P_1,P_2)$. La séquence $(\Delta_i(X,Y))_{i\in[\![1,m]\!]}$ se calcule avec une complexité binaire de $\tilde{O}_B(d^{12}\tau)$.*

Démonstration En effet, par le Théorème 2.3.10, le calcul de la séquence $(\mathrm{sr}_{i,i}(X,Y))_{i\in[\![1,m]\!]}$ s'effectue avec un coût binaire de $\tilde{O}_B(d^6\tau)$, de plus, pour tout $i\in[\![1,m]\!]$ $\mathcal{L}(\mathrm{sr}_{i,i})=O(d\tau)$ et $\deg(\mathrm{sr}_{i,i})=O(d^2)$. $\Theta_0(X,Y)$ étant par définition la partie sans facteur carré de $\mathrm{sr}_{0,0}(X,Y)$, alors $\deg(\Theta_0)=O(d^2)$ et $\mathcal{L}(\Theta_0)=O(d\tau)$. Par ailleurs comme $\Theta_0(X,Y)=\prod_{i=1}^{m-1}\Delta_i(X,Y)$ alors $\sum_{i=1}^{m}\deg(\Theta_i)=O(d^2)$ et $\mathcal{L}(\Theta_i)=O(d\tau)$. Pour calculer la séquence $(\Delta_i(X,Y))_{i\in[\![1,m]\!]}$, nous réalisons $O(d)$ calcul de pgcd de polynômes bivariés de degrés $O(d^2)$ (les polynômes $\Theta_i(X,Y)$ et $\mathrm{sr}_{i,i}(X,Y)$) et dont les coefficients sont de tailles binaires $O(d\tau)$. Sachant que

chaque calcul de pgcd à un coût binaire de $\tilde{O}_B(d^{11}\tau)$ d'après le Théorème 2.3.10, il vient que la complexité binaire de l'algorithme calculant la séquence $(\Delta_i(X,Y))_{i\in[\![1,m]\!]}$ est de $\tilde{O}_B(d^{12}\tau)$. □

Théorème 4.3.4 *La courbe $\mathcal{C}_{\mathbb{R}}$ est en position pseudo-générique par rapport au plan (x,y) si et seulement si pour tout $i\in[\![1,m-1]\!]$, pour tout $j\in[\![1,i-1]\!]$ on a :*

$$i(i-j)\,\mathrm{sr}_{i,j}(X,Y)\,\mathrm{sr}_{i,i}(X,Y)-(j+1)\,\mathrm{sr}_{i,i-1}(X,Y)\,\mathrm{sr}_{i,j+1}(X,Y)=0 \bmod \Delta_i(X,Y).$$

Démonstration Supposons que $\mathcal{C}_{\mathbb{R}}$ soit en position pseudo-générique. Soient $(i,j)\in[\![1,m-1]\!]\times[\![0,i-1]\!]$ et $(\alpha,\beta)\in\mathbb{C}^2$ tels que $\Delta_i(\alpha,\beta)=0$.
Si $\mathrm{sr}_{i,i}(\alpha,\beta)=0$, alors par la Proposition 2.3.6, $\mathrm{sr}_{i,i-1}(\alpha,\beta)=0$. Par suite :

$$i(i-j)\,\mathrm{sr}_{i,j}(\alpha,\beta)\,\mathrm{sr}_{i,i}(\alpha,\beta)-(j+1)\,\mathrm{sr}_{i,i-1}(\alpha,\beta)\,\mathrm{sr}_{i,j+1}(\alpha,\beta)=0.$$

Si $\mathrm{sr}_{i,i}(\alpha,\beta)\neq 0$, si nous posons $\gamma=-\frac{\mathrm{sr}_{i,i-1}(\alpha,\beta)}{i\,\mathrm{sr}_{i,i}(\alpha,\beta)}$, par la Proposition 4.3.2 (3) on a alors :

$$\mathrm{Sr}_i(\alpha,\beta,Z)=\sum_{j\in[\![0,i]\!]}\mathrm{sr}_{i,j}(\alpha,\beta)Z^j=\mathrm{sr}_{i,i}(\alpha,\beta)(Z-\gamma)^i$$

En développant $(Z-\gamma)^i$ on obtient :

$$\mathrm{Sr}_i(\alpha,\beta,Z)=\sum_{j\in[\![0,i]\!]}\mathrm{sr}_{i,j}(\alpha,\beta)Z^j=\mathrm{sr}_{i,i}(\alpha,\beta)\sum_{j\in[\![0,i]\!]}\binom{i}{j}(-\gamma)^{i-j}Z^j.$$

Alors par identification on obtient : pour tout $i\in[\![1,m-1]\!]$, $j\in[\![1,i-1]\!]$ et $(\alpha,\beta)\in\mathbb{C}^2$, $\Delta_i(\alpha,\beta)=0$ implique $i(i-j)\,\mathrm{sr}_{i,j}(\alpha,\beta)\,\mathrm{sr}_{i,i}(\alpha,\beta)-(j+1)\,\mathrm{sr}_{i,i-1}(\alpha,\beta)\,\mathrm{sr}_{i,j+1}(\alpha,\beta)=0$.
Réciproquement, supposons que pour tout $i\in[\![1,m-1]\!]$ et tout $j\in[\![1,i-1]\!]$,

$$i(i-j)\,\mathrm{sr}_{i,j}(X,Y)\,\mathrm{sr}_{i,i}(X,Y)-(j+1)\,\mathrm{sr}_{i,i-1}(X,Y)\,\mathrm{sr}_{i,j+1}(X,Y)=0 \bmod \Delta_i(X,Y) \quad (1)$$

Soit $(\alpha,\beta)\in\mathcal{C}(f)$ et $i\in[\![1,m-1]\!]$ tel que $\Delta_i(\alpha,\beta)=0$ et $\mathrm{sr}_{i,i}(\alpha,\beta)\neq 0$. Alors par (1) on a $\forall j\in[\![1,i-1]\!]$:

$$i(i-j)\,\mathrm{sr}_{i,j}(\alpha,\beta)\,\mathrm{sr}_{i,i}(\alpha,\beta)-(j+1)\,\mathrm{sr}_{i,i-1}(\alpha,\beta)\,\mathrm{sr}_{i,j+1}(\alpha,\beta)=0 \quad (2)$$

En multipliant (2) par $\binom{i}{j}$ et en utilisant l'égalité $(j+1)\binom{i}{j+1}=(i-j)\binom{i}{j}$, on obtient :

$$\forall j\in[\![0,i-1]\!], i\binom{i}{j+1}\mathrm{sr}_{i,j}(\alpha,\beta)\,\mathrm{sr}_{i,i}(\alpha,\beta)-\binom{i}{j}\mathrm{sr}_{i,i-1}(\alpha,\beta)\,\mathrm{sr}_{i,j+1}(\alpha,\beta)=0 \quad (3)$$

Comme $\mathrm{sr}_{i,i}(\alpha,\beta)\neq 0$, on peut diviser l'égalité (3) par $i(\mathrm{sr}_{i,i}(\alpha,\beta))$. Ainsi on obtient pour tout $j\in[\![0,i-1]\!]$:

$$\binom{i}{j+1}\mathrm{sr}_{i,j}(\alpha,\beta)+\binom{i}{j}\gamma(\alpha,\beta)\,\mathrm{sr}_{i,j+1}(\alpha,\beta)=0 \text{ avec } \gamma(\alpha,\beta)=\frac{-\mathrm{sr}_{i,i-1}(\alpha,\beta)}{i(\mathrm{sr}_{i,i}(\alpha,\beta))}$$

De cette dernière égalité on déduit par récurrence, que $\forall j \in [\![0,i]\!]$:

$$\mathrm{sr}_{i,j}(\alpha,\beta) = \binom{i}{j} \mathrm{sr}_{i,i}(\alpha,\beta)(-\gamma(\alpha,\beta))^{i-j}.$$

D'où, $\sum_{j\in[\![0,i]\!]} \mathrm{sr}_{i,j}(\alpha,\beta)Z^j = \sum_{j\in[\![0,i]\!]} \binom{i}{j} \mathrm{sr}_{i,i}(\alpha,\beta)(-\gamma(\alpha,\beta))^{i-j}Z^j = \mathrm{sr}_{i,i}(\alpha)(Z-\gamma(\alpha,\beta))^i$.
Ainsi par la Proposition 4.3.2, $\mathcal{C}_{\mathbb{R}}$ est en position pseudo-générique. □

L'algorithme suivant, fondé sur le Théorème 4.3.4, permet de certifier la pseudo-généricité de la position de la courbe $\mathcal{C}_{\mathbb{R}}$.

Algorithme 4.3.1 : `PseudoGenericTest`

Entrées : $P_1, P_2 \in \mathbb{Q}[X,Y,Z]$ tels que $\mathrm{pgcd}(P_1,P_2) = 1$
Etape 1 : Rendre $\mathrm{lc}(P_1)$ et $\mathrm{lc}(P_2)$ éléments de $\mathbb{Q}^*$.
Si $\deg_Z(P_2) \neq \deg(P_2)$ ou $\deg_Z(P_1) \neq \deg(P_1)$ faire le changement de variables $(X,Y,Z) \leftarrow (X+\lambda Z, Y+\mu Z, Z)$ dans P_1 et P_2, avec $\lambda,\mu \in \mathbb{Q}^*$.
Etape 2 Calcul des polynôms $\Delta_i(X,Y)$.
Calcul de la séquence des sous-résultants associée à P_1 et P_2
$\mathrm{Sr}_i(X,Y,Z) = \sum_{j=0}^{i} \mathrm{sr}_{i,j}(X,Y)Z^j, i \in \{0,\ldots,m\}$.
$f(X,Y) := \mathrm{squarefree}(\mathrm{sr}_{0,0}(X,Y))$,
$\Theta_1(X,Y) = \mathrm{pgcd}(f(X,Y), \mathrm{sr}_{1,i}(X,Y))$,
$\Delta_1(X,Y) = \frac{f(X,Y)}{\Theta_1(X,Y)}$,
pour i allant de 1 à m faire :
$\Theta_i(X,Y) = \mathrm{pgcd}(\Theta_{i-1}(X,Y), \mathrm{sr}_i(X,Y))$,
$\Delta_i(X,Y) = \frac{\Theta_{i-1}(X,Y)}{\Theta_i(X,Y)}$
fin faire.
Etape 3 Test de pseudo-généricité.
Pour i allant de 1 à m faire :
si $\Delta_i(X,Y) \neq 0$ alors
pour j allant de 0 à $i-1$ faire :
$(i(i-j)\,\mathrm{sr}_{i,j}(X,Y)\,\mathrm{sr}_{i,i}(X,Y) - (j+1)\,\mathrm{sr}_{i,i-1}(X,Y)\,\mathrm{sr}_{i,j+1}(X,Y)) \bmod \Delta_i(X,Y)$.
Si le résultat est égal à zéro, continuer,
Sinon retourner Faux,
fin si,
fin faire,
fin si,
fin faire.
Retourner Vrai.

Théorème 4.3.5 *Soient $P_1,P_2 \in \mathbb{Z}[X,Y,Z]$, $d = \max(\deg(P_1),\deg(P_2))$ et $\tau = \mathcal{L}(P_1,P_2)$. L'algorithme* `PseudoGenericTest`*, teste la pseudo-généricité de la position de $\mathcal{C}_{\mathbb{R}}$ avec une*

complexité binaire de $\tilde{O}_B(d^{11}\tau)$.

Démonstration L'utilisation de l'algorithme `PseudoGenericTest` nécessite $O(d^2)$ appels de l'algorithme de division exacte de polynômes multivariés (voir [6]) avec en entrées un polynôme bivarié de degré borné par $O(d^2)$ (polynôme $\Delta_i(X,Y)$) et un de degré borné par $O(d^2)$ (produit de deux coefficients sous-résultants de degrés bornés par $O(d^2)$) et dont les coefficients sont de tailles binaires bornées par $\tilde{O}_B(d\tau)$. Comme la complexité de l'algorithme de division exact de deux polynômes bivariés de degrés p et q est $O(p^2q^2)$ (voir [6]) alors la complexité binaire de l'algorithme `PseudoGenericTest` est $O(d^2) \times O((d^2)^2 \times (d^2)^2) \times \tilde{O}_B((d\tau)) = \tilde{O}_B(d^{11}\tau)$. □

La proposition suivante découle de la Proposition 4.3.2.

Proposition 4.3.6 *Supposons que* $\mathcal{C}_{\mathbb{R}}$ *soit en position pseudo-générique et soit* $(\alpha,\beta,\gamma) \in \mathcal{C}_{\mathbb{R}}$ *tel que* (α,β) *soit un point régulier de* $\mathcal{C}(f)$. *Alors il existe un unique* $i \in [\![1,m]\!]$ *tel que* $\Delta_i(\alpha,\beta) = 0$ *et* $\mathrm{sr}_{i,i}(\alpha,\beta) \neq 0$. *De plus* $\gamma = -\frac{\mathrm{sr}_{i,i-1}(\alpha,\beta)}{i\,\mathrm{sr}_{i,i}(\alpha,\beta)}$.

Remarque 4.3.7 La proposition précédente est essentielle dans la phase de relèvement de la topologie de $\mathcal{C}(f)$ pour obtenir celle de $\mathcal{C}_{\mathbb{R}}$. En effet, les paramétrisations $\gamma = -\frac{\mathrm{sr}_{i,i-1}(\alpha,\beta)}{i\,\mathrm{sr}_{i,i}(\alpha,\beta)}$ permettent de calculer les troisièmes coordonnées des points réguliers de $\mathcal{C}(f)$ connaissant leurs coordonnées ainsi que l'indice i de l'unique composante $\mathcal{C}(\Delta_i)$ à laquelle ils appartiennent. Ces informations sont fournies par l'algorithme de calcul de topologie de $\mathcal{C}(f)$. En effet, les points réguliers de $\mathcal{C}(f)$ sont obtenus en choisissant une valeur régulière α entre deux valeurs x-critiques de $\mathcal{C}(f)$ puis en résolvant l'équation $f(\alpha,Y) = 0$ pour obtenir les deuxièmes coordonnées (voir section 3.3.3). Mais sachant que $f(X,Y) = \prod_{i\in[\![1,m]\!]} \Delta_i(X,Y)$, pour une valeur régulière donnée α, nous allons résoudre les équations $\Delta_1(\alpha,Y) = 0, \ldots, \Delta_m(\alpha,Y) = 0$. Ceci nous permettra d'obtenir la deuxième coordonnée et l'indice i de l'unique composante $\mathcal{C}(\Delta_i)$ à laquelle appartient le point régulier considéré. Ainsi, utilisant la paramétrisation $\gamma = -\frac{\mathrm{sr}_{i,i-1}(\alpha,\beta)}{i\,\mathrm{sr}_{i,i}(\alpha,\beta)}$, on relève aisément le point régulier de $\mathcal{C}(f)$ considéré.
Il reste maintenant à relever les points x-critiques de $\mathcal{C}(f)$. Cette opération est plus délicate et nécessite que l'on analyse l'origine et la nature de ces derniers. En effet tout les points x-critiques de $\mathcal{C}(f)$ ne sont pas des projections de points x-critiques de $\mathcal{C}_{\mathbb{R}}$.

La sous-section suivante introduit la notion de singularité apparente de $\mathcal{C}(f)$ puis celle de généricité d'une courbe algébrique spatiale.

Singularités apparentes et conditions de généricité de $\mathcal{C}_{\mathbb{R}}$

Théorème 4.3.8 *Soient $f \in \mathbb{Q}[X,Y]$ le résultant de P_1 et P_2 par rapport à la variable Z et $\mathcal{C}(f) := \{(x,y) \in \mathbb{R}^2, f(x,y) = 0\}$ la projection de $\mathcal{C}_{\mathbb{R}}$ sur le plan (x,y). Si (α,β,γ) est un point singulier de $\mathcal{C}_{\mathbb{R}}$, alors (α,β) est un singulier de $\mathcal{C}(f)$. La réciproque est fausse.*

Démonstration Voyons P_1 et P_2 comme polynômes en la variable Z :

$$P_1(X,Y,Z) = a_{d_1}(X,Y)Z^{d_1} + ... + a_0(X,Y)$$
$$P_2(X,Y,Z) = b_{d_2}(X,Y)Z^{d_2} + ... + b_0(X,Y)$$

Soit M la matrice de Sylvester de P_1 et P_2 :

$$M = \begin{pmatrix} a_0 & & & b_0 & & \\ \vdots & \ddots & & \vdots & \ddots & \\ a_{d_1} & & a_0 & b_{d_2} & & b_0 \\ & \ddots & \vdots & & \ddots & \vdots \\ & & a_{d_1} & & & b_{d_2} \end{pmatrix}$$

Par définition $f(X,Y) = \det(M)$. Soit $M^{'}$ la matrice obtenue à partir de M en multipliant le i^{eme} colonne de M par Z^{i-1}. On a : $\det(M^{'}) = Z^s \det(M) = Z^s f(X,Y)$ avec $s = \frac{1}{2}(d_1+d_2-1)(d_1+d_2)$. En ajoutant toutes les colonnes de $M^{'}$ à la première on obtient une matrice M'', dont la première colonne est la transposée de $(P_1(Z),\ldots,Z^{d_2-1}P(Z),P_2(Z),\ldots,Z^{d_1-1}P_2(Z))$. Pour calculer le déterminant de M'', on développe suivant la première colonne et on obtient alors :

$$\det(M^{'}) = \sum_{i=0}^{d_2-1} Z^i P_1(Z) m^{'}_{i+1,1}(Z) + \sum_{i=0}^{d_1-1} Z^i P_2(Z) m^{'}_{i+d_2+1,1}(Z)$$

où $m^{'}_{i,1}$ est le cofacteur d'ordre $(i,1)$ de $M^{'}$. Or $m^{'}_{i,1}(Z) = Z^s m_{i,1}$ (où $m_{i,1}$ est le cofacteur d'ordre $(i,1)$ de M) donc

$$\det(M^{'}) = Z^s(P_1(Z)\sum_{i=0}^{d_2-1} Z^i m_{i+1,1} + P_2(Z)\sum_{i=0}^{d_1-1} Z^i m_{i+d_2+1,1}).$$

Or $\det(M') = Z^s f(X,Y)$, donc

$$f(X,Y) = (P_1(Z)\sum_{i=0}^{d_2-1} Z^i m_{i+1,1} + P_2(Z)\sum_{i=0}^{d_1-1} Z^i m_{i+d_2+1,1}).$$

Posant $A=\sum_{i=0}^{d_2-1} Z^i m_{i+1,1}$ et $B=\sum_{i=0}^{d_1-1} Z^i m_{i+d_2+1,1}$, on obtient :

$$f(X,Y)=P_1(X,Y,Z)A(X,Y,Z)+P_2(X,Y,Z)B(X,Y,Z)$$

Quitte à effectuer le changement de variable $Z=Z-\gamma$, (le résultant est invariant par translation), on peut supposer que $\gamma=0$. Montrons que $\partial_Y f(\alpha,\beta)=0$.
$\partial_Y f=A\partial_Y P_1+P_1\partial_Y A+B\partial_Y P_2+P_2\partial_Y B$, comme $P_1(\alpha,\beta,\gamma)=P_2(\alpha,\beta,\gamma)=0$ alors
$\partial_y f(\alpha,\beta)=A(\alpha,\beta,\gamma)\partial_Y P_1(\alpha,\beta,\gamma)+B(\alpha,\beta,\gamma)\partial_y P_2(\alpha,\beta,\gamma)$.
Or $A=\sum_{i=0}^{d_2-1} Z^i m_{i+1,1}$ et $B=\sum_{i=0}^{d_1-1} Z^i m_{i+d_2+1,1}$, donc $A(\alpha,\beta,\gamma)=A(\alpha,\beta,0)=m_{1,1}(\alpha,\beta)$ et $B(\alpha,\beta,\gamma)=m_{1+d_2,1}(\alpha,\beta)$. Par ailleurs, comme $P_1(\alpha,\beta,\gamma)=P_2(\alpha,\beta,\gamma)=0$ et $\gamma=0$ alors $a_0(\alpha,\beta)=b_0(\alpha,\beta)=0$. Donc par développement suivant la première colonne on a :
$m_{1,1}(\alpha,\beta)=(-1)^{d_2+1}b_1(\alpha,\beta)C(\alpha,\beta)$ et $m_{1+d_2,2}(\alpha,\beta)=(-1)^{d_2+2}a_1(\alpha,\beta)C(\alpha,\beta)$, où C est le déterminant de la matrice obtenue en privant M de ses deux premières lignes et ses deux premières colonnes.
Ainsi $A(\alpha,\beta,\gamma)=(-1)^{d_2+1}b_1(\alpha,\beta)C(\alpha,\beta)$ et $B(\alpha,\beta,\gamma)=(-1)^{d_2+2}a_1(\alpha,\beta)C(\alpha,\beta)$, d'où $\partial_Y f(\alpha,\beta)=(-1)^{d_2+1}C(\alpha,\beta)b_1(\alpha,\beta)\partial_Y P_1(\alpha,\beta,\gamma)-a_1(\alpha,\beta)\partial_Y P_2(\alpha,\beta,\gamma)$. Comme $\gamma=0$, alors $a_1(\alpha,\beta)=\partial_Z P_1(\alpha,\beta,\gamma)$ et $b_1(\alpha,\beta)=\partial_Z P_2(\alpha,\beta,\gamma)$ par suite,

$$\partial_Y f(\alpha,\beta)=(-1)^{d_2+1}C(\alpha,\beta)\partial_Z P_2(\alpha,\beta,\gamma)\partial_Z P_1(\alpha,\beta,\gamma)-\partial_Z P_1(\alpha,\beta,\gamma)\partial_Y P_2(\alpha,\beta,\gamma).$$

Mais comme (α,β,γ) est un point singulier de $\mathcal{C}_{\mathbb{R}}$ alors

$$(\partial_Z P_2(\alpha,\beta,\gamma)\partial_Y P_1(\alpha,\beta,\gamma)-\partial_Z P_1(\alpha,\beta,\gamma)\partial_Y P_2(\alpha,\beta,\gamma))=0.$$

D'où $\partial_Y f(\alpha,\beta)=0$. De manière analogue on montre que $\partial_X f(\alpha,\beta)=0$. Ainsi (α,β) est un point singulier de $\mathcal{C}(f)$. □

Remarque 4.3.9 La projection d'un point singulier de $\mathcal{C}_{\mathbb{R}}$ étant un point singulier de $\mathcal{C}(f)$, nous pouvons retrouver les singularités de la courbe $\mathcal{C}_{\mathbb{R}}$ à partir de celles de $\mathcal{C}(f)$. Cependant, le problème des singularités apparentes se pose. En effet quand on projette une courbe, il arrive qu'il apparaisse d'autres singularités et il est essentiel de les distinguer parmi les singularités de $\mathcal{C}(f)$.

Rappelons que $\Pi:(x,y,z)\in\mathbb{C}^3\longmapsto(x,y)\in\mathbb{C}^2$ et $\Pi|_{\mathcal{C}_{\mathbb{R}}}$ est la restriction de Π à l'ensemble $\mathcal{C}_{\mathbb{R}}$.

Définition 4.3.10 *Soient $f\in\mathbb{Q}[X,Y]$ le résultant de $P_1(X,Y,Z)$ et $P_2(X,Y,Z)$ par rapport à la variable Z, $\mathcal{C}(f):=\{(x,y)\in\mathbb{R}^2, f(x,y)=0\}$ la projection de $\mathcal{C}_{\mathbb{R}}$ sur le plan (x,y) et (α,β) un point singulier de $\mathcal{C}(f)$.*

1. *On dit que (α,β) est une singularité apparente de $\mathcal{C}(f)$ lorsque l'ensemble $\Pi|_{\mathcal{C}_{\mathbb{R}}}^{-1}(\alpha,\beta)$ contient au moins deux points (voir figure 4.7).*

2. *On dit que* (α,β) *est une singularité réelle de* $\mathcal{C}(f)$ *lorsque l'ensemble* $\Pi\,|^{-1}_{\mathcal{C}_{\mathbb{R}}}(\alpha,\beta)$ *est réduit à un point (voir figure 4.7).*

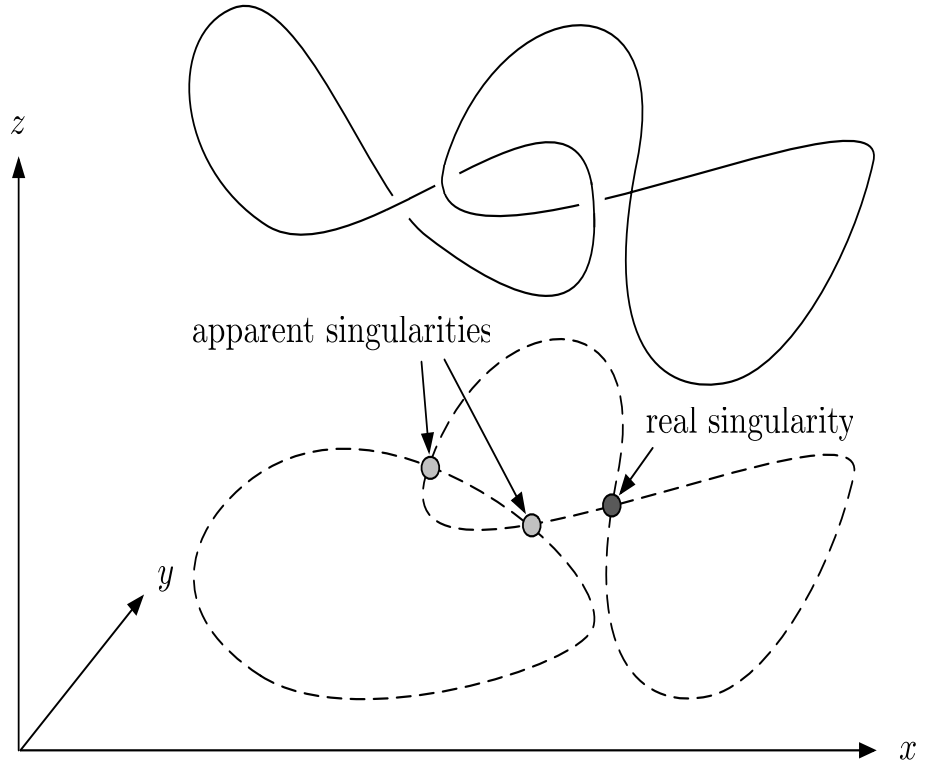

FIG. 4.7 – Distinction entre singularités apparentes et vraies singulariés

A présent nous allons définir la notion de position générique pour une courbe intersection de deux surfaces algébriques implicites.

Définition 4.3.11 *Soient* $P_1,P_2 \in \mathbb{Q}[X,Y,Z]$, $f \in \mathbb{Q}[X,Y]$ *le résultant de* P_1 *et* P_2 *par rapport à la variable Z,* $\mathcal{C}_{\mathbb{R}} = \{(x,y,z) \in \mathbb{R}^3 \mid P_1(x,y,z) = 0, P_2(x,y,z) = 0\}$ *et* $\mathcal{C}(f) := \{(x,y) \in \mathbb{R}^2, f(x,y) = 0\}$ *la projection de* $\mathcal{C}_{\mathbb{R}}$ *sur le plan* (x,y)*. On dira que* $\mathcal{C}_{\mathbb{R}}$ *est en position générique par rapport au plan* (x,y) *si et seulement si :*

1. $\mathcal{C}_{\mathbb{R}}$ *est en position pseudo-générique par rapport au plan* (x,y)*,*
2. *la courbe plane* $\mathcal{C}(f)$ *est en position générique,*
3. *toute singularité apparente de* $\mathcal{C}(f)$ *est un noeud.*

Nous avons fourni dans la sous-section précédente un algorithme permettant de tester la pseudo-généricité de la position de $\mathcal{C}_{\mathbb{R}}$. L'algorithme permettant de certifier la généricité de la position de la courbe plane $\mathcal{C}(f)$ a été donné dans le Chapitre 3.

Dans la sous-section suivante nous fournissons un algorithme modulaire permettant de distinguer les singularités apparentes de $\mathcal{C}(f)$ puis de tester si elles sont toutes des noeuds.

Calcul des singularités apparentes de $\mathcal{C}(f)$

Nous supposerons ici que $\mathcal{C}_{\mathbb{R}}$ est en position *pseudo-générique* et $\mathcal{C}(f) = \Pi_z(\mathcal{C}_{\mathbb{R}})$ est en position *générique*. Soit $(\Gamma_j(X))_{j\in[\![1,n]\!]}$ la séquence des polynômes associés à $\mathcal{C}(f)$ (voir section 3.3.2) et $(\beta_j(X))_{j\in[\![1,n]\!]}$ la séquence des paramétrisations polynômiales qui leur sont associées (voir section 3.3.3). Rappelons que $(\mathrm{Sr}_i(X,Y,Z))_{i\in[\![1,m]\!]}$ désigne la séquence des polynômes sous-résultants associés à $P_1, P_2 \in \mathbb{Q}[X,Y,Z]$.
Pour tout $(k,i) \in [\![1,m]\!] \times [\![0,k-1]\!]$, soit $R_{k,i}(X,Y)$ et le polynôme suivant :

$$R_{k,i}(X,Y) = k(k-i)\,\mathrm{sr}_{k,i}(X,Y)\,\mathrm{sr}_{k,k}(X,Y) - (i+1)\,\mathrm{sr}_{k,k-1}(X,Y)\,\mathrm{sr}_{k,i+1}(X,Y).$$

Nous avons le lemme suivant :

Lemme 4.3.12 *Soit $(a,b) \in \mathbb{R}^2$ tel que $\mathrm{sr}_{k,k}(a,b) \neq 0$. Le polynôme $\mathrm{Sr}_k(a,b,Z)$ a une et une seule racine si et seulement si pour tout $i \in [\![0,k-1]\!]$, $R_{k,i}(a,b) = 0$.*

Pour tout $j \in [\![1,n]\!]$, soit $(u_{k,j}(X))_{k\in[\![1,j]\!]}$ et $(v_{k,j}(X))_{k\in[\![2,j]\!]}$ les séquences d'éléments de $\mathbb{Q}[X]$ définies par :

- $u_{1,j}(X) := \mathrm{pgcd}(\Gamma_j(X), \mathrm{sr}_{1,1}(X, \beta_j(X)))$,
  $u_{k,j}(X) := \mathrm{pgcd}(\mathrm{sr}_{k,k}(X, \beta_j(X)), u_{k-1,j}(X))$,
- $v_{k,j}(X) := \mathrm{quo}(u_{k-1,j}(X), u_{k,j}(X))$.

De manière plus intuitive, pour un j fixé dans $[\![1,n]\!]$, α est racine de $v_{k,j}(X)$ si et seulement si :

1. $\deg_Y(\mathrm{pgcd}(f(\alpha,Y), \partial_Y f(\alpha,Y)) = j$,
2. $\deg_Z(\mathrm{pgcd}(P_1(\alpha,\beta_j(\alpha),Z), P_2(\alpha,\beta_j(\alpha),Z))) = k$.

Pour tout $(k,i) \in [\![2,j]\!] \times [\![0,k-1]\!]$, soit $(w_{k,i,j}(X))$, $(\Gamma_{j,k}(X))$ et $(\chi_{j,k}(X))$ les séquences d'éléments de $\mathbb{Q}[X]$ définies par :

- $w_{k,0,j}(X) := v_{k,j}(X)$, $w_{k,i+1,j}(X) := \mathrm{pgcd}(R_{k,i}(X, \beta_j(X)), w_{k,i,j}(X))$,
- $\Gamma_{j,1}(X) := \mathrm{quo}(\Gamma_j(X), u_{1,j}(X))$, $\Gamma_{j,k}(X) := w_{k,k,j}(X)$,
- $\chi_{j,k}(X) := \mathrm{quo}(w_{k,0,j}(X), \Gamma_{j,k}(X))$.

Théorème 4.3.13

1. *Pour toute racine α de $\Gamma_{j,k}(X)$ la fibre x-critique $(\alpha, \beta_j(\alpha))$ contient l'unique point $(\alpha, \beta_j(\alpha), \gamma_{j,k}(\alpha))$ avec $\gamma_{j,k}(\alpha) := -\frac{\mathrm{sr}_{k,k-1}(\alpha,\beta_j(\alpha))}{k\,\mathrm{sr}_{k,k}(\alpha,\beta_j(\alpha))}$.*

2. *Pour tout* α *racine de* $\chi_{j,k}(X)$, $(\alpha, \beta_j(\alpha))$ *est une singularité apparente de* $\mathcal{C}(f)$.

Démonstration

1. Soit α une racine de $\Gamma_{j,k}(X) := w_{k,k,j}(X) = \text{pgcd}(R_{k,k-1}(X, \beta_j(X)), w_{k,k-1,j}(X))$. Alors

$$w_{k,k-1,j}(\alpha) = R_{k,k-1}(\alpha, \beta_j(\alpha)) = 0.$$

   Comme $w_{k,k-1,j}(X) := \text{pgcd}(R_{k,k-2}(X, \beta_j(X)), w_{k,k-2,j}(X))$, on a :

$$w_{k,k-2,j}(\alpha) = R_{k,k-2}(\alpha, \beta_j(\alpha)) = 0.$$

   Ainsi par une récurrence immédiate on obtient :

$$\forall i \in [\![0, k-1]\!], w_{k,i,j}(\alpha) = R_{k,i}(\alpha, \beta_j(\alpha)) = 0.$$

   Comme $w_{k,0,j}(X) := v_{k,j}(X)$, nous en déduisons que :

$$v_{k,j}(\alpha) = 0.$$

   Comme $v_{k,j}(X) := \text{quo}(u_{k-1,j}(X), u_{k,j}(X))$ et que $u_{k,j}$ et $u_{k-1,j}$ sont sans facteur carré, alors $u_{k-1,j}(\alpha) = 0$ et $u_{k,j}(\alpha) \neq 0$. Comme $u_{k,j}(X) = \text{pgcd}(\text{sr}_{k,k}(X, \beta_j(X)), u_{k-1,j}(X))$ alors $\text{sr}_{k,k}(\alpha, \beta_j(\alpha)) \neq 0$. Par ailleurs $u_{k-1,j}(X) = \text{pgcd}(\text{sr}_{k-1,k-1}(X, \beta_j(X)), u_{k-2,j}(X))$ et $u_{k-1,j}(\alpha) = 0$, d'où $\text{sr}_{k-1,k-1}(\alpha, \beta_j(\alpha)) = u_{k-2,j}(\alpha) = 0$.
   Utilisant les même arguments, on montre par récurrence que :

$$\forall i \in [\![0, k-1]\!] \, \text{sr}_{i,i}(\alpha, \beta_j(\alpha)) = 0.$$

   Ainsi on a : $\text{sr}_{k,k}(\alpha, \beta_j(\alpha)) \neq 0$ et $\text{sr}_{k-1,k-1}(\alpha, \beta_j(\alpha)) = \ldots = \text{sr}_{0,0}(\alpha, \beta_j(\alpha)) = 0$ et par le théorème fondamental des sous résultants :

$$\text{pgcd}(P_1(\alpha, \beta_j(\alpha), Z), P_2(\alpha, \beta_j(\alpha), Z)) = \text{Sr}_k(\alpha, \beta_j(\alpha), Z) = \sum_{i=0}^{k} \text{sr}_{k,i}(\alpha, \beta_j(\alpha)) Z^i.$$

   Ainsi par le Lemme 4.3.12, $\text{pgcd}(P_1(\alpha, \beta_j(\alpha), Z), P_2(\alpha, \beta_j(\alpha), Z)$ admet une et une seule racine qui s'écrit $\gamma_j(\alpha) := -\frac{\text{sr}_{k,k-1}(\alpha, \beta_j(\alpha))}{k \, \text{sr}_{k,k}(\alpha, \beta_j(\alpha))}$.

2. Soit α une racine de $\chi_{j,k}(X) := \text{quo}(w_{k,0,j}(X), \Gamma_{j,k}(X))$. Alors $w_{k,0,j}(\alpha) = 0$ et $\Gamma_{j,k}(\alpha) = w_{k,k,j}(\alpha) \neq 0$ car $w_{k,0,j}(X)$ et $\Gamma_{j,k}(X)$ sont sans facteur carré. Sachant que pour tout $i \in [\![0, k-1]\!]$, $w_{k,i+1,j}(X) := \text{pgcd}(R_{k,i}(X, \beta_j(X)), w_{k,i,j}(X))$ alors $w_{k,0,j}(\alpha) = 0$ et $w_{k,k,j}(\alpha) \neq 0$ implique l'existence de $i \in \{0, \ldots, k-1\}$ tel que $R_{k,i}(\alpha, \beta_j(\alpha)) \neq 0$. Alors par Lemme 4.3.12, le polynôme $\text{Sr}_k(\alpha, \beta_j(\alpha), Z) = \sum_{i=0}^{k} \text{sr}_{k,i}(\alpha, \beta_j(\alpha)) Z^i$ admet au moins deux racines distinctes. Sachant que $\text{pgcd}(P_1(\alpha, \beta_j(\alpha), Z), P_2(\alpha, \beta_j(\alpha), Z)) = \text{Sr}_k(\alpha, \beta_j(\alpha), Z)$,
   alors $(\alpha, \beta_j(\alpha))$ est une singularité apparente.

□

Proposition 4.3.14 *Soient* $(j,k) \in [\![1,n]\!]\times[\![2,j]\!]$ *et* α *une racine de* $\chi_{j,k}(X)$. *La singularité apparente de* $\mathcal{C}(f)$ $(\alpha,\beta_j(\alpha))$ *est un noeud si et seulement si :*

$$(\partial^2_{XY} f(\alpha,\beta_j(\alpha)))^2 - \partial^2_{X^2} f(\alpha,\beta_j(\alpha))\partial^2_{Y^2} f(\alpha,\beta_j(\alpha)) \neq 0$$

Démonstration Soit $(j,k) \in [\![1,n]\!]\times[\![2,j]\!]$ et α une racine de $\chi_{j,k}(X)$. Soit $f(X+\alpha, Y+\beta_j(\alpha)) = F_1 + \ldots + F_n$, où $F_i \in \mathbb{Q}[\alpha][X,Y]$ est un polynôme homogène de degré i. La singularité apparente $(\alpha,\beta_j(\alpha))$ est un point double si et seulement si $F_2 \neq 0$. Il est bien connu que $F_2 = 1/2(\partial^2_{Y^2} f(\alpha,\beta_j(\alpha))Y^2 + 2\partial^2_{XY} f(\alpha,\beta_j(\alpha))XY + \partial^2_{X^2} f(\alpha,\beta_j(\alpha))X^2)$ et que les facteurs de F_2 donne le cône tangent de $\mathcal{C}(f)$ en $(\alpha,\beta_j(\alpha))$. Ainsi la singularité apparente $(\alpha,\beta_j(\alpha))$ est un noeud si et seulement si le discriminant du polynôme $F_2(1,Y)$ est non nul, d'où le résultat. □

Pour tout $j \in [\![1,n]\!]$, $T_j(X) := (\partial^2_{XY} f(X,\beta_j(X)))^2 - \partial^2_{X^2} f(X,\beta_j(X))\partial^2_{Y^2} f(X,\beta_j(X))$. La proposition précédente implique le théorème suivant :

Théorème 4.3.15 *Toutes les singularités apparentes de* $\mathcal{C}(f)$ *sont des noeuds si et seulement si pour tout* $(j,k) \in [\![1,n]\!]\times[\![2,j]\!]$ *les polynômes* $\chi_{j,k}(X)$ *et* $T_j(X)$ *sont premiers entre eux.*

4.3.3 Relèvement de la topologie de la courbe plane $\mathcal{C}(f)$

Dans cette section, nous supposons que $\mathcal{C}_{\mathbb{R}}$ est en position générique, c'est-à-dire que $\mathcal{C}_{\mathbb{R}}$ est en position pseudo-générique, que la courbe plane $\mathcal{C}(f) = \Pi_z(\mathcal{C}_{\mathbb{R}})$ est en position générique et toutes ses singularités apparentes sont des noeuds. Comme nous l'avons déjà mentionné, pour calculer la topologie de $\mathcal{C}_{\mathbb{R}}$, notre stratégie consiste à calculer la topologie de sa projection sur le plan (x,y), puis de relever dans l'espace la topologie obtenue dans le plan (x,y). Soit $\tilde{\mathcal{C}}(f)$ la topologie de $\mathcal{C}(f)$; $\tilde{\mathcal{C}}(f)$ est une structure linéaire par morceaux isotope à $\mathcal{C}(f)$ composée des fibres x-critiques de $\mathcal{C}(f)$, d'une fibre régulière entre deux fibres x-critiques consécutives et des segments reliant ces fibres entre elles. Parmi les fibres x-critiques de $\tilde{\mathcal{C}}(f)$ nous distinguerons les fibres contenant des singularités apparentes de $\mathcal{C}(f)$. Relever la topologie de $\mathcal{C}(f)$ revient à calculer, dans un premier temps, les pré-images $\Pi|_{\mathcal{C}}^{-1}(\alpha,\beta)$ où (α,β) est soit un point régulier de $\tilde{\mathcal{C}}(f)$, soit une singularité apparente de $\tilde{\mathcal{C}}(f)$, soit un point x-critique de $\tilde{\mathcal{C}}(f)$. Puis dans un second temps, il faut déterminer les connections entre ces pré-images calculées. Le calcul des pré-images des points x-critiques qui ne sont pas des singularités apparentes s'effectue aisément avec les paramétrisations données par le Théorème 4.3.13 (1). Les pré-images des points réguliers s'obtiennent sans difficulté par les

paramétrisations données par la Proposition 4.3.6. Dans la sous-section suivante on explique comment obtenir des connections entre les pré-images des points réguliers et les pré-images des points x-critiques qui ne sont pas des singularités apparentes.

Connections entre les pré-images des points réguliers et celles des points x-critiques de $\mathcal{C}_{\mathbb{R}}$

Pour une courbe $\mathcal{C}_{\mathbb{R}}$ en position générique, les connections entre les points réguliers (pré-images des points réguliers de $\tilde{\mathcal{C}}(f)$) et les points x-critiques de $\mathcal{C}_{\mathbb{R}}$, sont exactement celles obtenues lors du calcul de la topologie $\tilde{\mathcal{C}}(f)$ de $\mathcal{C}(f)$ par l'algorithme `TopolCourbe2D` décrit dans le chapitre précédent (voir figure 4.8).

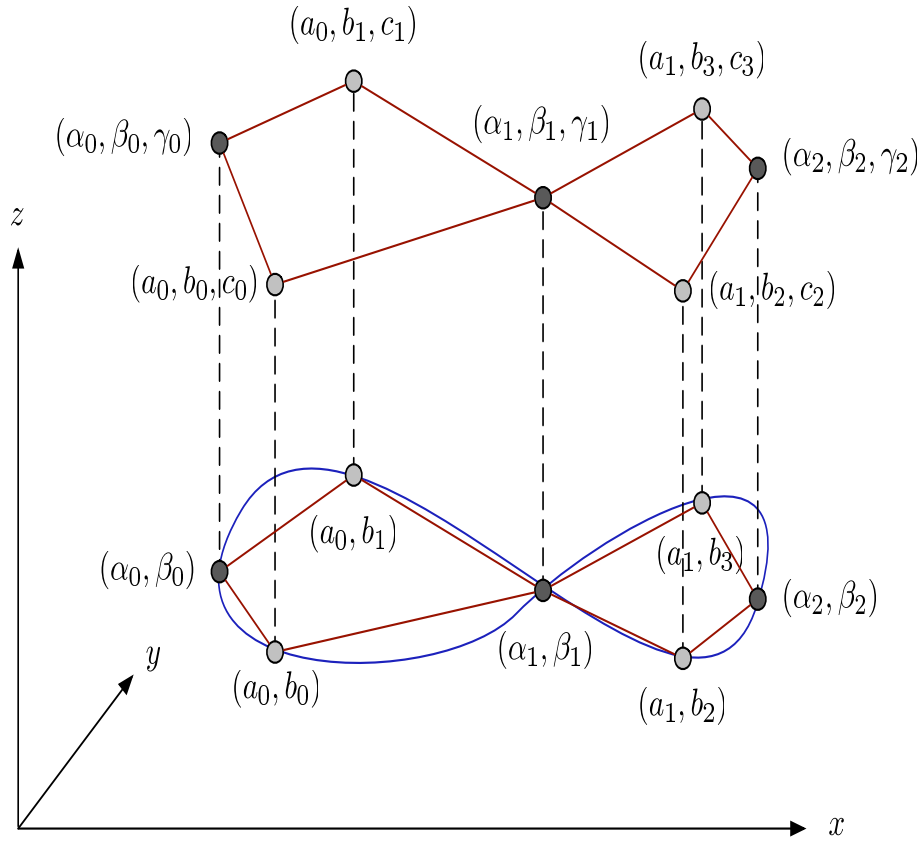

FIG. 4.8 – Relèvement des connections

La sous-section suivante traite du cas particulier des singularités apparentes. Nous y présentons une methode permettant à la fois de relever les singularités apparentes de $\tilde{\mathcal{C}}(f)$ et de déterminer les connections entre leurs pré-images et les pré-images des points réguliers de $\tilde{\mathcal{C}}(f)$ auxquels elles étaient connectées.

Relèvement des singularités apparentes de $\mathcal{C}(f)$

Le relèvement des singularités apparentes de $\mathcal{C}(f)$ est un peu plus complexe que celui de ses autres points x-critiques. En effet, pour les autres points x-critiques de $\mathcal{C}(f)$, les paramétrisations rationnelles, données par le Théorème 4.3.13 (1), facilitent le calcul de leur troisième coordonnée. De plus, au-dessus des singularités apparentes se pose un autre le problème : celui de la détermintion de la position des deux branches de la courbe. Nous solutionnons ce problème en analysant la géométrie de la courbe au voisinage d'une singularité apparente.
Par la Proposition 4.3.2, $\mathcal{C}(f) = \bigcup_{i\in[\![1,m]\!]} \mathcal{C}(\Delta_i)$, donc lorsque $\mathcal{C}_\mathbb{R}$ est en position générique, une singularité apparente est un point de croisement, par effet de projection, d'une branche de $\mathcal{C}(\Delta_i)$ et d'une branche de $\mathcal{C}(\Delta_j)$ avec $(i,j) \in [\![1,m]\!] \times [\![1,m]\!]$. Donc nous avons la proposition suivante :

Proposition 4.3.16 *En position générique, si (α,β) est une singularité apparente de $\mathcal{C}(f)$ telle que $\Delta_i(\alpha,\beta) = \Delta_j(\alpha,\beta) = 0$, alors le polynôme* $\operatorname{pgcd}(P_1(\alpha,\beta,Z), P_2(\alpha,\beta,Z)) \in \mathbb{R}[Z]$ *est de degré $(i+j)$.*

Démonstration Soit (α,β) une singularité apparente de $\mathcal{C}(f)$ telle que $\Delta_i(\alpha,\beta) = \Delta_j(\alpha,\beta) = 0$ et $D := \deg_Z(\operatorname{pgcd}(P_1(\alpha,\beta,Z), P_2(\alpha,\beta,Z)))$, alors $D \geqslant (i+j)$. Montrons que $D = (i+j)$. Si on avait $D > (i+j)$ alors il existerait $k \in [\![1, D-(i+j)]\!]$ tel que $\Delta_k(\alpha,\beta) = 0$. Par suite, (α,β) serait un point de croisement d'une branche de $\mathcal{C}(\Delta_i)$, d'une branche de $\mathcal{C}(\Delta_j)$ et d'une branche de $\mathcal{C}(\Delta_k)$ et donc ne serait pas un noeud. Ceci est impossible car, en position générique, toutes les singularités apparentes sont des noeuds. Par conséquent $D = (i+j)$. □

Soit (α,β) une singularité apparente de $\mathcal{C}(f)$ tel que $\Delta_i(\alpha,\beta) = \Delta_j(\alpha,\beta) = 0$. Soit (α,β,γ_1) et (α,β,γ_2) les pré-images de (α,β). Par la proposition 4.3.6, pour tout $(a,b,c) \in \mathcal{C}_\mathbb{R}$ tel que $\Delta_i(a,b) = 0$ et $\operatorname{sr}_{i,i}(a,b) \neq 0$, nous avons $c = -\frac{\operatorname{sr}_{i,i-1}(a,b)}{i\operatorname{sr}_{i,i}(a,b)}$. Donc la fonction $(x,y) \longmapsto Z_i(x,y) := -\frac{\operatorname{sr}_{i,i-1}(x,y)}{i\operatorname{sr}_{i,i}(x,y)}$ donne la troisième coordonnée de tout point $(a,b,c) \in \mathcal{C}_\mathbb{R}$ tel que $\Delta_i(a,b) = 0$ et $\operatorname{sr}_{i,i}(a,b) \neq 0$. Peut-on utiliser directement la fonction Z_i pour calculer γ_1 ou γ_2 ? La réponse est non car par la Proposition 4.3.16 et le théorème fondamental des polynômes sous-résultants : $\operatorname{sr}_{0,0}(\alpha,\beta) = \ldots = \operatorname{sr}_{i,i}(\alpha,\beta) = \ldots = \operatorname{sr}_{j,j}(\alpha,\beta) = \ldots. = \operatorname{sr}_{i+j-1,i+j-1}(\alpha,\beta) = 0$. Par contre tout n'est pas perdu, car la fonction Z_i est prolongeable par continuité en (α,β). En effet soit u_1 la pente de la droite tangente à $\mathcal{C}(\Delta_i)$ en (α,β) et $t \in \mathbb{R}^*$. Soit $\gamma_i(t) := Z_i(\alpha,\beta+tu_1) = -\frac{\operatorname{sr}_{i,i-1}(\alpha,\beta+tu_1)}{i\operatorname{sr}_{i,i}(\alpha,\beta+tu_1)}$, sachant que la courbe algébrique réelle $\mathcal{C}_\mathbb{R}$ n'admet aucune discontinuité, il vient $\lim_{t\to 0^+}\gamma_i(t) = \lim_{t\to 0^-}\gamma_i(t) = \gamma_1$. Par le même raisonnement, si nous notons u_2 la pente de la droite tangente à $\mathcal{C}(\Delta_j)$ en (α,β) et $\gamma_j(t) := Z_j(\alpha,\beta+tu_2) = -\frac{\operatorname{sr}_{j,j-1}(\alpha,\beta+tu_2)}{j\operatorname{sr}_{j,j}(\alpha,\beta+tu_2)}$, nous obtenons $\lim_{t\to 0^+}\gamma_j(t) = \lim_{t\to 0^-}\gamma_j(t) = \gamma_2$.
Maintenant que nous savons calculer les pré-images des singularités apparentes, il reste à déterminer comment les connections s'effectuent au dessus des singularités apparentes. Soit

(a, b_1, c_1) et (a, b_2, c_2) les points réguliers de $\mathcal{C}_{\mathbb{R}}$ que nous devons connecter aux points $(\alpha, \beta, \gamma_1)$ et $(\alpha, \beta, \gamma_2)$. Le problème est de savoir : "qui connecter à qui ?" (voir figure 4.9). La solution tient au fait que γ_1 est associé à u_1 et γ_2 à u_2. Sachant que u_1 est la pente de la droite tangente à $\mathcal{C}(\Delta_i)$ en (α, β) et u_2 celle de la droite tangente à $\mathcal{C}(\Delta_j)$ en (α, β), alors il vient que $(\alpha, \beta, \gamma_1)$ sera connecté à (a, b_1, c_1) si (a, b_1) est sur la branche associée à u_1. Si (a, b_1) n'est pas sur la branche associée à u_1 alors il est sur la branche associée à u_2 donc $(\alpha, \beta, \gamma_2)$ sera connecté à (a, b_1, c_1) (voir figure 4.10).

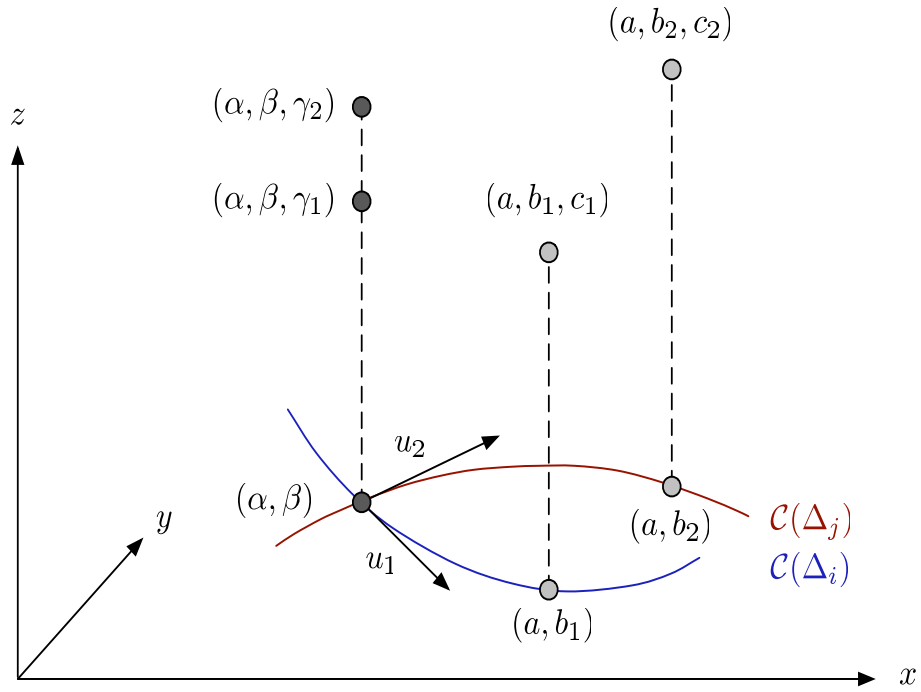

FIG. 4.9 – Relèvement d'une singularité apparente

Remarque 4.3.17 Pour une courbe en position générique, toutes les singularités apparentes sont des noeuds, donc les pentes u_1 et u_2 sont toujours distinctes en une singularité apparente.

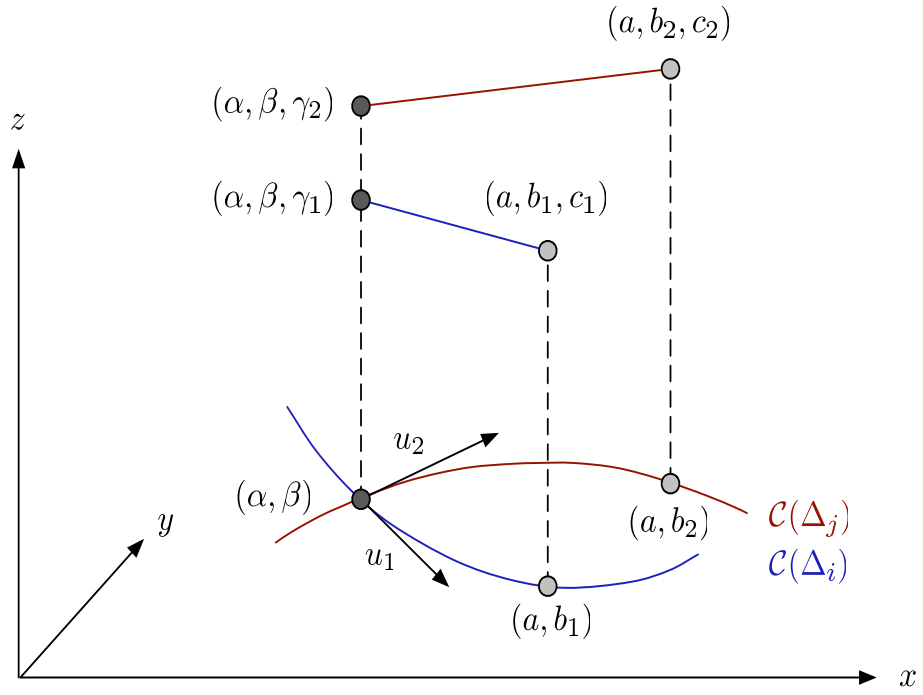

FIG. 4.10 – Connections au-dessus d'une singularité apparente

4.3.4 Description globale de l'algorithme `TopolCourbe3D`

Algorithme 4.3.2 : `TopolCourbe3D`

Entrées : $P_1, P_2 \in \mathbb{Q}[X, Y, Z]$ polynômes sans facteur carré de degré d
Sorties : Topologie de la courbe $\mathcal{C}_{\mathbb{R}}$

1. Tester la pseudo-généricité de la position de $\mathcal{C}_{\mathbb{R}}$ avec `PseudoGenericTest`,
2. Calculer la topologie de la projection $\mathcal{C}(f)$ de $\mathcal{C}_{\mathbb{R}}$ avec `TopolCourbe2D`.
3. Distinguer les singularités apparentes de $\mathcal{C}(f)$ de ses autres points x-critiques.
4. Relever les singularités apparentes de $\mathcal{C}(f)$.
5. Relever les autres points x-critiques de $\mathcal{C}(f)$.
6. Relever les fibres régulières de $\mathcal{C}(f)$.
7. Connecter les points en suivant les connections données par la courbe plane.

4.3.5 Complexité de l'algorithme `TopolCourbe3D`

Nous rappelons que $\tilde{O}_B$ désigne la complexité binaire en ignorant les facteurs logarithmiques, $\mathcal{L}(a) := \lceil \log_2 |a| \rceil$ désigne la taille binaire d'un entier donné a et pour P polynôme à coeffients entiers $(a_0, \ldots, a_n)$ (en une ou plusieurs variables) $\mathcal{L}(P)$ désigne :

$$\mathcal{L}(P) := \max(\mathcal{L}(a_0), \ldots, \mathcal{L}(a_n))$$

L'algorithme de calcul de topologie d'une courbe algébrique implicite spatiale que nous venons de décrire, comporte essentiellement quatre phases :

1. une phase d'élimination où nous calculons la séquence des polynômes sous-résultants associée aux polynômes P_1 et P_2.
2. une phase où nous testons si la courbe $\mathcal{C}_{\mathbb{R}}$ est en position générique.
3. une phase où nous calculons la topologie de $\mathcal{C}(f)$, projection de $\mathcal{C}_{\mathbb{R}}$ sur le plan (x,y).
4. une phase de relèvement de la topologie de $\mathcal{C}(f)$.

Théorème 4.3.18 *Soient $P_1, P_2 \in \mathbb{Z}[X,Y,Z]$, $d := \max(\deg(P_1), \deg(P_2))$, $\tau := \mathcal{L}(P_1,P_2)$ et $\mathcal{C}_{\mathbb{R}}$ la courbe d'intersection des surfaces définies par P_1 et P_2. La topologie de $\mathcal{C}_{\mathbb{R}}$ se calcule avec une complexité binaire probabiliste en $\tilde{O}_B(d^{21}\tau)$ et déterministe en $\tilde{O}_B(d^{21}\tau)$.*

Démonstration La première étape de l'algorithme consiste à calculer la séquence des sous-résultants $(\mathrm{Sr}_i(P_1,P_2))_{i\in[\![0,d]\!]}$ associée à P_1 et P_2 par rapport à la variable Z. D'aprés le Théoreme 2.3.10, ce calcul s'effectue avec une complexité binaire de $\tilde{O}_B(d^7\tau)$ et pour tout $i \in [\![0,d]\!]$, $\mathcal{L}(\mathrm{Sr}_i(P_1,P_2)) = O(d\tau)$. La deuxième est celle du calcul de la suite $(\Delta_i(X,Y))_{i\in[\![1,m]\!]}$. Par la Proposition 4.3.3 son coût binaire est de $\tilde{O}_B(d^{12}\tau)$. Ensuite vient la phase de test et de mise en position pseudo-générique de $\mathcal{C}_{\mathbb{R}}$. D'aprés le Théorème 4.3.5, ce calcul s'effectue avec une complexité de $\tilde{O}_B(d^{11}\tau)$. Ensuite vient la phase de calcul de la topologie de la projection $\mathcal{C}(f)$ de $\mathcal{C}_{\mathbb{R}}$. Comme $\deg(f) = O(d^2)$ et $\mathcal{L}(f) = O(d\tau)$ alors par le Théorème 3.4.3, ce calcul s'effectue avec une complexité binaire déterministe en $\tilde{O}_B((d^2)^{10} \times (d\tau)) = \tilde{O}_B(d^{21}\tau)$ et probabiliste en $\tilde{O}_B((d^2)^{10} \times (d\tau)) = \tilde{O}_B(d^{21}\tau)$. Le coût de la phase de relèvement de la topologie de $\mathcal{C}(f)$ est négligeable car s'effectue à l'aide des paramétrisations rationnelles. Ainsi le calcul de la topologie de $\mathcal{C}_{\mathbb{R}}$ s'effectue avec une complexité binaire déterministe en $\tilde{O}_B(d^7\tau + d^{12}\tau + d^{11}\tau + d^{21}\tau) = \tilde{O}_B(d^{21}\tau)$ et probabiliste en $\tilde{O}_B(d^7\tau + d^{12}\tau + d^{11}\tau + d^{21}\tau) = \tilde{O}_B(d^{21}\tau)$. □

Remarque 4.3.19 La complexité binaire de l'algorithme `TopolCourbe3D` donnée par le Théorème 4.3.18, est trés encourageant comparé à celui de décomposition cylindrique algébrique. En effet, par le Théorème 2.4.21, la complexité arithmétique de l'algorithme de décomposition

cylindrique algébrique pour le calcul de topologie variétés semi-algébriques réelles est de $O(m^{2^n} d^{n2^{n+1}})$ où m est le nombre de polynômes définissant la variété, d le maximum des degrés totaux de ces polynômes et n leur nombre de variables. Dans le contexte de l'intersection de deux surfaces, $n = 3$ et $m = 2$, d'où une complexité arithmétique de $O(d^{48})$.

4.4 Implémentation et expérimentation

L'algorithme `TopolCourbe3D` a été entièrement implémenté avec MATHEMAGIX. Dans cette section, nous fournissons quelques exemples de topologies calculées ainsi qu'un tableau indiquant les temps de calculs.

Courbes	P_1	P_2	Temps (s)
1	$x^2+y^2+z^2-1$	x^2-y^2-z+1	0.032
2	$x^2+y^2+z^2-1$	$x^3+3x^2z+3xz^2+$ $z^3+y^3-xyz-yz^2$	0.659
3	$(x-2y+2z)^2+y^2+z-1$	$z^3-z-(x-2y+2z)^3$ $+3(x-2y+2z)y^2$	2.125
4	$(x-2y+2z)^2+y^2+z^2-1$	$y^3-(x-2y+2z)^3$ $-(x-2y+2z)yz$	1.031
5	$(x-y+z)^2+y^2+z^2-1$	$y^2-(x-y+z)^2-(x-y+z)z)^2$ $-z^2((x-y+z)^2+y^2)$	1.6963
6	$(x-y+z)^2+y^2+z^2-1$	$((x-y+z)^2+y^2+z^2)^2$ $-4((x-y+z)^2+y^2)$	2.228
7	$(x-y+z)^2+y^2-2(x-y+z)$	$((x-y+z)^2+y^2+z^2)^2$ $-4((x-y+z)^2+y^2)$	2.875
8	$x^2+y^2+z^2-1$	$(x^3+y^3-xyz)*$ $(-4(z^3-z-x^3+3xy^2)$	6.575

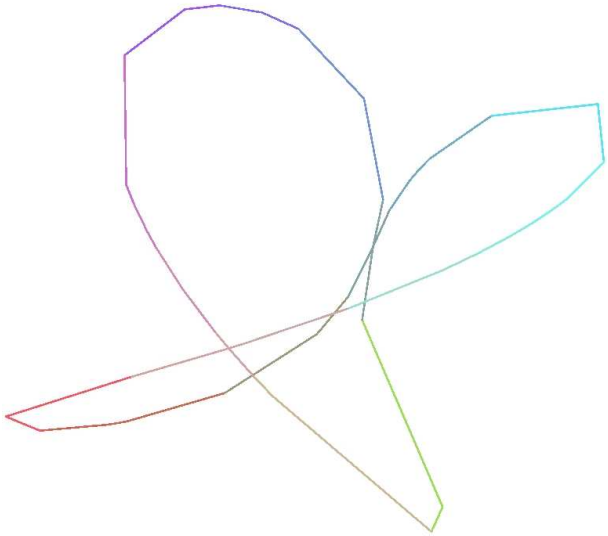

FIG. 4.11 – Courbe 7

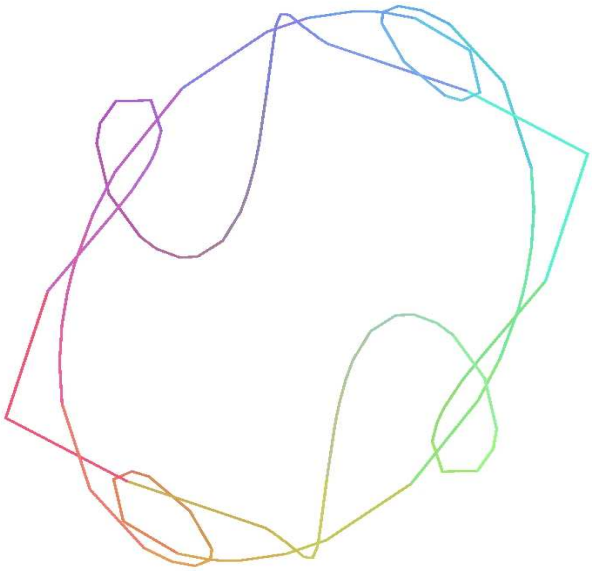

FIG. 4.12 – Courbe 8

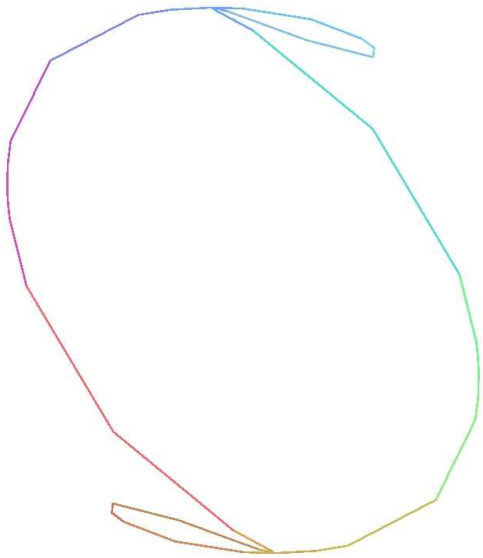

FIG. 4.13 – Courbe 4

Deuxième partie

Topologie de surfaces algébriques

Chapitre 5

Triangulation isotopique d'une surface algébrique implicite

5.1 Introduction

Soit $P \in \mathbb{Q}[X,Y,Z]$ un polynôme sans facteur carré et $\mathcal{S}$ le lieu de ses zéros réels :

$$\mathcal{S} := \{(\alpha,\beta,\gamma) \in \mathbb{R}^3 | P(\alpha,\beta,\gamma) = 0\}$$

Le problème auquel nous nous intéressons dans ce chapitre est celui du calcul d'une triangulation de la surface $\mathcal{S}$. La triangulation des variétés (semi)-algébriques réelles est un problème récurrent et fondamental en géométrie algébrique réelle. La triangulation a été beaucoup étudiée d'un point de vue théorique [38], [39]. Dans les travaux [10], [15], [6], le problème de la triangulation des variétés semi-algébriques est abordé d'un point de vue effectif, via la décomposition cylindrique algébrique et l'encodage de Thom des nombres algébriques. Mais l'algorithme qui en découle est pénalisé par sa très grande complexité, même lorsqu'on cherche à traiter des ensembles semi-algébriques en petite dimension $(n \leqslant 3)$. Ainsi comme pour le cas des courbes en petite dimension, le cas des surfaces algébriques a fait l'objet de plusieurs travaux [30], [29], [12], [2]. Mais ces traveaux ne traitent que le cas des surfaces *lisses*. Dans [4], les auteurs proposent un algorithme qui nécessite le calcul des sections de la surface en les points singuliers de sa "silhouette" pour pouvoir reconstruire sa topologie. Cette opération est très difficile à certifier. En effet elle revient à calculer la topologie de la courbe algébrique plane d'équation $P(\alpha,Y,Z) = 0$ où α est un nombre algébrique.
Dans ce chapitre, nous proposons un algorithme certifié calculant la triangulation d'une surface algébrique implicite. Notre approche consiste à calculer dans un premier temps la topologie d'une "silhouette" de la surface $\mathcal{S}$. Cette "silhouette" partitionne l'espace en des cylindres connexes, à l'intérieur desquels le nombre de nappes est constant. Ensuite, nous effectuons,

grâce à des sections de la surface $\mathcal{S}$, le maillage des nappes à l'intérieur de chaque cylindre. Concernant la phase de connection des différentes nappes, nous proposons un nouvel algorithme, ne nécessitant pas le calcul de la topologie de sections de la surface en les points x-critiques de sa silhouette. La connection est entièrement guidée par la topologie de la silhouette calculée au départ. Une implémentation de l'algorithme a été effectuée avec MATHEMAGIX. Il est essentiel de remarquer qu'il s'agit du premier code disponible, complet et certifié, calculant la topologie d'une surface algébrique implicite singulière. La complexité binaire de l'algorithme est dominée par la phase de calcul d'une silhouette de la surface et est de $\tilde{O}_B(d^{21}\tau)$ où d est le degré du polynôme définissant la surface et τ la taille binaire de ses coefficients.

5.2 Description géométrique de l'algorithme

Notre objectif est de calculer une triangulation "correcte" de la surface algébrique $\mathcal{S}$ lieu des zéros réels de $P \in \mathbb{Q}[X,Y,Z]$. Trianguler une surface consiste en un processus de calcul d'une représentation de celle-ci par des morceaux de surfaces lisses. "Correcte" signifie que le résultat doit conserver la topologie de la surface et si possible sa géométrie. Les définitions suivantes combinent ces exigences topologiques et geométriques.

Définition 5.2.1 *Une isotopie de $\mathbb{R}^3$ est une application $\varphi : \mathbb{R}^3 \times [0,1] \longrightarrow \mathbb{R}^3$, telle que $\varphi(\cdot,0) = \mathrm{Id}_{\mathbb{R}^3}$ et pour tout $t \in]0,1]$, $\varphi(\cdot,t)$ est un homéomorphisme.*

Définition 5.2.2 *Soient $\Delta, \Omega \subset \mathbb{R}^3$, on dit que Δ est isotope à Ω s'il existe une isotopie φ de $\mathbb{R}^3$ telle que $\varphi(\Delta,1) = \Omega$.*

Notre stratégie pour construire une triangulation de $\mathcal{S}$ consiste à trouver des régions uniformes dans le plan (x,y), où la surface $\mathcal{S}$ peut être vue comme une famille de graphes de fonctions du type $z = h(x,y)$. Une manière d'obtenir de telles régions consiste à couper la surface en ses points d'auto-intersection et en ses points où l'espace tangent est un plan orthogonal au plan (x,y). L'ensemble de ces points forme ce que nous appelerons la silhouette de la surface.

Définition 5.2.3 *Soit $P \in \mathbb{Q}[X,Y,Z]$ un polynôme sans facteur carré et $\mathcal{S}$ la surface algébrique réelle définie par P. Nous appelerons **silhouette** de $\mathcal{S}$ la variété algébrique suivante :*

$$\mathcal{P} := \{(\alpha,\beta,\gamma) \in \mathbb{R}^3 | P(\alpha,\beta,\gamma) = \partial_Z P(\alpha,\beta,\gamma) = 0\}$$

Le principe de l'algorithme de calcul de la topologie de la surface algébrique $\mathcal{S}$ est le même que celui utilisé pour obtenir la topologie d'une courbe algébrique plane. Il consiste à bal-

ayer la surface par un plan puis à détecter les positions où la topologie de l'intersection de la surface avec le plan de balayage change. Si, pour une courbe algébrique plane les changements de topologie s'observent au niveau des points x-critiques de celle-ci, pour une surface algébrique les changements de topologie s'observent au niveau de sa silhouette, plus particulièrement en les points x-critiques de celle-ci. Comme pour les courbes algébriques planes, où la topologie de l'intersection d'une droite avec la courbe ne varie pas entre deux points x-critiques, la topologie de l'intersection de la surface avec un plan orthogonal à l'axe des abscisses ne varie pas entre deux points x-critiques consécutifs de la silhouette $\mathcal{P}$ de $\mathcal{S}$. Donc, en calculant les topologies des sections de $\mathcal{S}$ au niveau des points x-critiques de sa silhouette et une section entre deux sections x-critiques consécutives, nous disposerons de toute l'information topologique nécessaire pour trianguler la surface.
Pour mieux visualiser l'algorithme de triangulation de $\mathcal{S}$ que nous allons décrire, il est essentiel de comprendre intuitivement que si nous enlevons de la surface $\mathcal{S}$ sa silhouette $\mathcal{P}$, celle-ci se décompose en plusieurs morceaux de surfaces lisses que nous appelerons des nappes.
Lorsque nous coupons la surface $\mathcal{S}$ par un plan orthogonal à l'axe des abscisses, nous obtenons une courbe plane. Nous montrerons que ses points y-critiques appartiennent à la silhouette $\mathcal{P}$ et que ses arcs (au sens de la Définition 3.2.9) représentent les nappes de la surface. Les sections de $\mathcal{S}$ que nous calculerons sont donc des arcs ordonnés dont les supports sont des points de la silhouette $\mathcal{P}$. La question essentielle qui se pose maintenant est la suivante : d'une section de $\mathcal{S}$ à une autre, quels sont les arcs qui appartiennent à une même nappe ? Lorsque la surface est en position générique, l'étude de la topologie de sa silhouette permet de répondre à cette question. L'idée est que deux arcs de même position, dans deux sections consécutives de $\mathcal{S}$, dont les supports sont reliés par des arcs lisses de la sihouette, appartiennent à la même nappe de $\mathcal{S}$.

La section suivante porte sur le calcul de la topologie de la silhouette $\mathcal{P}$ et sur celui des sections de la surface $\mathcal{S}$ nécessaire à la reconstruction de sa topologie et à l'ordonnancement des arcs d'une section de la surface.

5.3 Topologie de la silhouette et des sections de $\mathcal{S}$

Comme le polynôme P définissant la surface $\mathcal{S}$ est sans facteur carré, alors sa silhouette $\mathcal{P}$ est une courbe algébrique implicite spatiale. Le calcul de sa topologie nécessite que la surface soit dans une position générique.

Définition 5.3.1 *La surface $\mathcal{S}$ est en position générique si et seulement si sa silhouette $\mathcal{P}$ est en position générique au sens de la Définition 4.3.11.*

La généricité de la position de $\mathcal{S}$ sera assurée lors de la phase de calcul de la topologie de sa silhouette $\mathcal{P}$. Cela s'effectue en appelant l'algorithme `TopolCourbe3D` avec $P_1 := P$ et $P_2 = \partial_Z P$. L'algorithme retourne une approximation polygonale de $\mathcal{P}$ qui lui est isotope.
Soit $(c_i := (\alpha_i, \beta_i, \gamma_i))_{i\in[\![1,n]\!]}$ la liste ordonnée des points x-critiques de $\mathcal{P}$ et $(r_i)_{i\in[\![1,n+1]\!]}$ une séquence de nombres réels vérifiant $r_1 < \alpha_1 < r_2 < \alpha_2 < \ldots \alpha_{n-1} < r_n < \alpha_n < r_{n+1}$. Pour tout $i \in [\![1, n+1]\!]$, soit $\mathcal{R}_{r_i} := \{(y,z) \in \mathbb{R}^2 | P(r_i, y, z) = \partial_Z P(r_i, y, z) = 0\}$ l'intersection de $\mathcal{P}$ avec le plan d'équation $x = r_i$ et $n_i = \#\mathcal{R}_{r_i}$. Nous noterons $(p_1^{r_i}, \ldots, p_{n_i}^{r_i})$ la séquence des points de $\mathcal{R}_{r_i}$, ordonnés par rapport à leur deuxième coordonnée.

Remarque 5.3.2 La topologie de $\mathcal{P}$ est décrite par la donnée des listes de points $(c_i := (\alpha_i, \beta_i, \gamma_i))_{i\in[\![1,n]\!]}$, $((p_1^{r_i}, \ldots, p_{n_i}^{r_i}))_{i\in[\![1,n+1]\!]}$ et des connections existant entre ces points.

Après le calcul de la topologie de la silhouette $\mathcal{P}$ de notre surface, il est nécessaire de calculer quelques sections de la surface par des plans orthogonaux à l'axe des abscisses. A la différence de l'approche décrite dans [4], ces sections ne seront pas réalisées en les points x-critiques de la silhouette $\mathcal{P}$ mais seulement en "certains" de ses points réguliers. Ensuite guidés par la topologie de la silhouette $\mathcal{P}$ de $\mathcal{S}$, nous procéderons à la connection des sections calculées.
Pour tout $i \in [\![1, n+1]\!]$, soit $\mathcal{C}_{r_i} := \{(y,z) \in \mathbb{R}^2 | P(r_i, y, z) = 0\}$ la courbe algébrique plane, intersection de la surface $\mathcal{S}$ avec le plan d'équation $x = r_i$. Les courbes $\mathcal{C}_{r_i}$ constituent les sections de la surface $\mathcal{S}$ nécessaires à la reconstruction de sa topologie. Ces courbes sont obtenues avec une version simplifiée de l'algorithme de calcul de topologie de courbe algébrique plane `TopolCourbe2D`. En effet nous n'aurons ni besoin de tester la généricité de la position des courbes $\mathcal{C}_{r_i}$, ni de calculer leurs points y-critiques.

Proposition 5.3.3 *Si $\mathcal{S}$ est en position générique alors pour tout $i \in [\![1, n+1]\!]$, les points y-critiques de la courbe plane $\mathcal{C}_{r_i}$ sont exactement les points d'intersection de la silhouette $\mathcal{P}$ avec le plan d'équation $x = r_i$, c'est-à-dire $(p_1^{r_i}, \ldots, p_{n_i}^{r_i})$.*

Démonstration Soit $i \in [\![1, n+1]\!]$. Par définition, les points y-critiques de la courbe plane $\mathcal{C}_{r_i} := \{(y,z) \in \mathbb{R}^2 : P(r_i, y, z) = 0\}$ sont les solutions du système $P(r_i, y, z) = \partial_z P(r_i, y, z) = 0$. Or les solutions de ce système sont exactement les points d'intersection, $(p_1^{r_i}, \ldots, p_{n_i}^{r_i})$, de la silhoutte $\mathcal{P}$ avec le plan d'équation $x = r_i$. □

Proposition 5.3.4 *Si $\mathcal{S}$ est en position générique alors pour tout $i \in [\![1, n+1]\!]$, la courbe algébrique plane $\mathcal{C}_{r_i} := \{(y,z) \in \mathbb{R}^2 : P(r_i, y, z) = 0\}$ est en position générique.*

Remarque 5.3.5 Pour tout $i \in [\![1, n+1]\!]$, la Proposition 5.3.4 montre qu'il ne sera pas nécessaire de tester la généricité de la courbe plane $\mathcal{C}_{r_i}$ lors du calcul de sa topologie. La Proposition 5.3.3 indique que le calcul de la topologie de $\mathcal{P}$ fournit les points y-critiques nécessaires pour

le calcul de la topologie $\mathcal{C}_{r_i}$. Ceci constitue un gain non négligeable pour l'efficacité globale de l'algorithme de maillage d'une surface car les phases de test de généricité et de calcul des points y-critiques sont les plus coûteuses dans l'algorithme de calcul de la topologie d'une courbe algébrique plane (voir chapitre 3).

Pour tout $i \in [\![1, n+1]\!]$, la topologie de la courbe plane $\mathcal{C}_{r_i}$ sera décrite par la donnée, d'une part, de ses points y-critiques, et d'autre part, de celle des listes d'arcs (ou branches) reliant ces points. Ci-dessus nous rappelons les définitions des notions d'arc et de support d'un arc introduites dans la section 3.2 puis nous introduisons une relation d'ordre permettant de classer les arcs d'une courbe algébrique plane.

Définition 5.3.6 *Pour tout $i \in [\![1, n+1]\!]$ nous rappelons qu'un arc de la courbe algébrique plane $\mathcal{C}_{r_i}$ est un morceau de courbe lisse de $\mathcal{C}_{r_i}$ reliant deux points y-critiques de $\mathcal{C}_{r_i}$ (voir section 3.2).*

Remarque 5.3.7 Comme les points y-critiques de $\mathcal{C}_{r_i}$ sont $p_1^{r_i}, \ldots, p_{n_i}^{r_i}$, alors les arcs de $\mathcal{C}_{r_i}$ sont des branches lissent de $\mathcal{C}_{r_i}$, reliant deux points de la liste $(p_1^{r_i}, \ldots, p_{n_i}^{r_i})$.

Définition 5.3.8 *Soient s_1 et s_2 deux points distincts de la liste $(p_1^{r_i}, \ldots, p_{n_i}^{r_i})$ des points y-critiques de $\mathcal{C}_{r_i}$ et $\mathcal{A}$ la liste des arcs de $\mathcal{C}_{r_i}$ reliant s_1 et s_2. Nous appelons support de $\mathcal{A}$ le bipoint (s_1, s_2).*

Un arc de $\mathcal{C}_{r_i}$ de support (s_1, s_2) sera représenté par la donnée des trois points $s_1 Q s_2$ où Q est un point quelconque de l'arc de support (s_1, s_2). Les arcs de $\mathcal{C}_{r_i}$ ayant le même suppport sont naturellement ordonnés. La relation permettant de les ordonner est la suivante :

Définition 5.3.9 *Soient qQ_1g et qQ_2g deux arcs distincts de $\mathcal{C}_{r_i}$ de support (q, g). Nous définissons la relation $\succ$ sur l'ensemble des arcs de support (q, g) par $qQ_1g \succ qQ_2g$ si et seulement si $z_{Q_1} > z_{Q_2}$ (voir figure 5.1).*

Il est clair que $\succ$ est une relation d'ordre sur tout ensemble d'arcs de $\mathcal{C}_{r_i}$ de même support.

Soit $q_1Q_1g_1$ et $q_2Q_2g_2$ deux arcs de $\mathcal{C}_{r_i}$ de supports différents. Comme par définition les arcs sont des morceaux de courbes lisses alors soit $[y_{q_1}, y_{g_1}] \subseteq [y_{q_2}, y_{g_2}]$, soit $[y_{q_2}, y_{g_2}] \subseteq [y_{q_1}, y_{g_{21}}]$, soit $[y_{q_1}, y_{g_1}] \cap [y_{q_2}, y_{g_2}] = \{\}$. La relation $\succ$ s'étend aux arcs $q_1Q_1g_1$ et $q_2Q_2g_2$ de $\mathcal{C}_{r_i}$ dont le support vérifie la contrainte $[y_{q_1}, y_{g_1}] \subseteq [y_{q_2}, y_{g_2}]$ ou $[y_{q_2}, y_{g_2}] \subseteq [y_{q_1}, y_{g_{21}}]$.

Définition 5.3.10 *Soit $q_1Q_1g_1$ et $q_2Q_2g_2$ deux arcs de $\mathcal{C}_{r_i}$ tels que $[y_{q_1}, y_{g_1}] \subseteq [y_{q_2}, y_{g_2}]$. La relation $\succ$ définie par : $q_1Q_1g_1 \succ q_2Q_2g_2$ si et seulement si $z_{Q_1} > z_{Q_2}$ est une relation d'ordre (voir figure 5.2).*

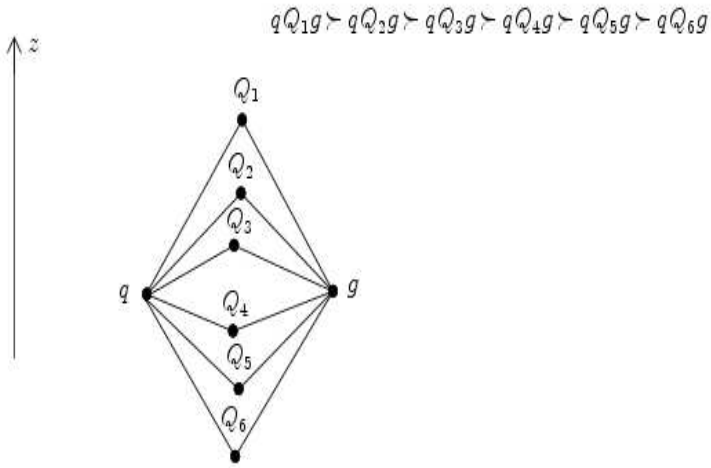

FIG. 5.1 – Arcs ordonnés de même support

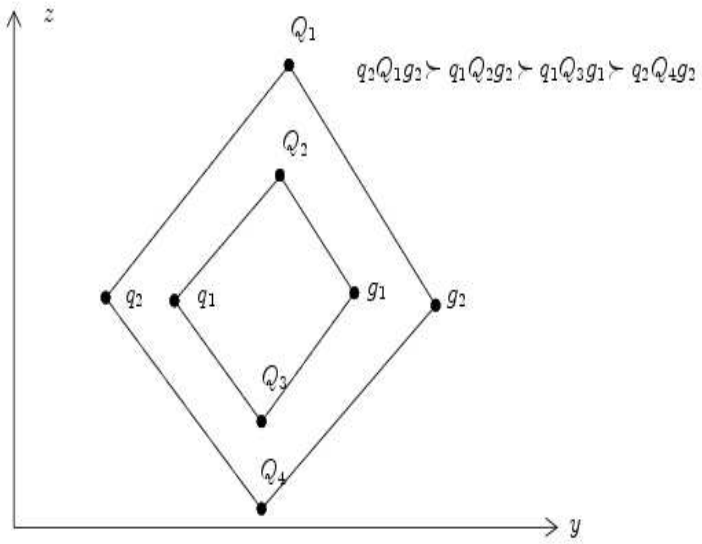

FIG. 5.2 – Arcs ordonnés de supports différents

Une fois la topologie de la silhouette $\mathcal{P}$ et celle des sections $(\mathcal{C}_{r_i})_{i\in[\![1,n+1]\!]}$ de $\mathcal{S}$ calculées, arrive l'étape de connection des différentes structures obtenues. Dans la section suivante, nous décrivons l'algorithme permettant de connecter deux sections consécutives de $\mathcal{S}$.

5.4 Connection de deux sections consécutives de $\mathcal{S}$

Afin d'alléger les notations, nous décrirons l'algorithme de connnection en considérant les sections consécutives $\mathcal{C}_{r_1}$ et $\mathcal{C}_{r_2}$.
Rappelons que $\mathcal{R}_{r_1} := \{(y,z) \in \mathbb{R}^2 | P(r_1,y,z) = \partial_Z P(r_1,y,z) = 0\}$
(resp. $\mathcal{R}_{r_2} := \{(y,z) \in \mathbb{R}^2 | P(r_2,y,z) = \partial_Z P(r_2,y,z) = 0\}$) désigne la section de la silhouette $\mathcal{P}$ par le plan d'équation $x = r_1$ (resp $x = r_2$), $n_1 = \#\mathcal{R}_{r_1}$ (resp. $n_2 := \#\mathcal{R}_{r_2}$), $(p_1^{r_1}, \ldots, p_{n_1}^{r_1})$ (resp. $(p_1^{r_2}, \ldots, p_{n_2}^{r_2})$) est la séquence ordonnée par rapport à leur deuxième coordonnée des points de $\mathcal{R}_{r_1}$ (resp.$\mathcal{R}_{r_2}$).
Nous noterons $c := (\alpha, \beta, \gamma)$ l'unique point x-critique de $\mathcal{P}$ tel que $r_1 < \alpha < r_2$. Soit UpPoints $:=$ $\{z \in \mathbb{R} | P(\alpha,\beta,z) = 0 \text{ et } z > \gamma\}$ la séquence ordonnée des points de la surface $\mathcal{S}$ appartenant à la fibre (α,β) et situés au-dessus du point x-critique $c := (\alpha,\beta,\gamma)$ et DownPoints $:= \{z \in \mathbb{R} | P(\alpha,\beta,z) = 0 \text{ et } z < \gamma\}$ ceux situés en dessous de $c := (\alpha,\beta,\gamma)$. Ainsi la fibre x-critique de $\mathcal{S}$ contenant c est complètement décrite par la donnée de l'ensemble $\{\text{UpPoints}, c, \text{DownPoints}\}$.
Rappelons que la topologie de la section $\mathcal{C}_{r_1}$ (resp. $\mathcal{C}_{r_2}$) est décrite par la donnée de ses points y-critiques $(p_1^{r_1}, \ldots, p_{n_1}^{r_1})$ (resp. $(p_1^{r_2}, \ldots, p_{n_2}^{r_2})$) et des classes d'arcs reliant ces points. Soit $(\mathcal{A}_1, \ldots, \mathcal{A}_{m_1})$ (resp. $(\mathcal{B}_1, \ldots, \mathcal{B}_{m_2})$) la liste des classes d'arcs de $\mathcal{C}_{r_1}$ (resp. $\mathcal{C}_{r_2}$). L'objectif est de connecter les classes d'arcs de la séquence $(\mathcal{A}_1, \ldots, \mathcal{A}_{m_1})$ à celles de $(\mathcal{B}_1, \ldots, \mathcal{B}_{m_2})$ en s'appuyant sur la structure de la fibre {UpPoints, c, DownPoints} et les connections entre les séquences $(p_1^{r_1}, \ldots, p_{n_1}^{r_1})$ et $(p_1^{r_2}, \ldots, p_{n_2}^{r_2})$ données par la topologie de la silhouette $\mathcal{P}$. Les connections doivent produire des triangles qui ne s'intersectent pas.
Au cours de l'algorithme de connection, nous aurons besoin essentiellement de savoir faire trois opérations élémentaires au cours desquelles les triangles de notre maillage seront construits :

1. connecter directement un arc $p_i^{r_1} Q_1 p_j^{r_1}$ *à un arc* $p_k^{r_2} Q_2 p_l^{r_2}$;
2. connecter directement un arc $p_i^{r_1} Q_1 p_j^{r_1}$ à un point C ;
3. connecter un arc $p_i^{r_1} Q_1 p_j^{r_1}$ *à un arc* $p_k^{r_2} Q_2 p_l^{r_2}$ en passant par un point C.

Dans les trois petits algorithmes qui suivent, nous donnons une description géométrique de la manière de réaliser ces connections.

Algorithme 5.4.1 : `ConnectArcToArc`

Entrées : $p_i^{r_1} Q_1 p_j^{r_1}$ et $p_k^{r_2} Q_2 p_l^{r_2}$ deux arcs donnés
Sorties : Complexe représentant la connection des deux arcs(voir figure 5.3)

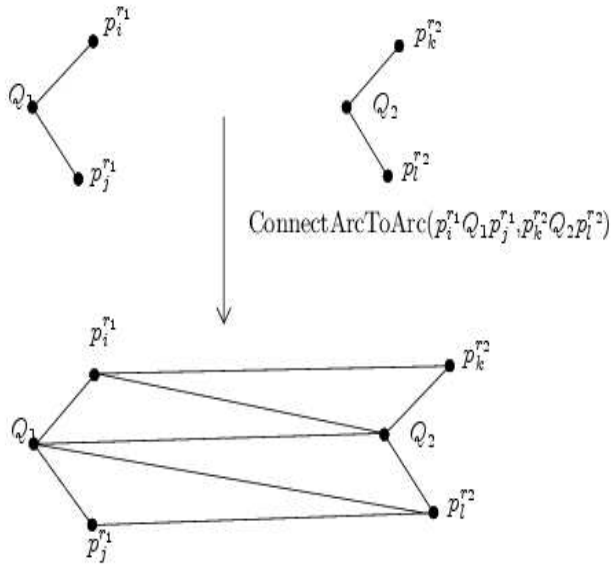

FIG. 5.3 – Connection d'un arc à un arc

Algorithme 5.4.2 : `ConnectArcToPoint`

Entrées : $p_i^{r_1}Q_1p_j^{r_1}$ un arc et C un point

Sorties : Complexe représentant la connection de l'arc au point (voir figure 5.4)

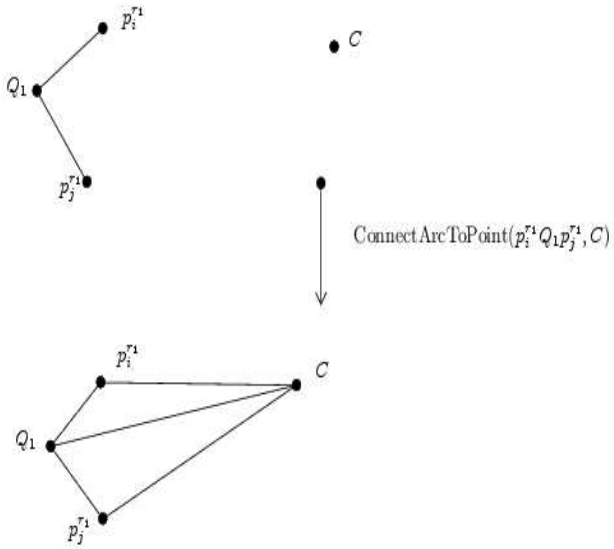

FIG. 5.4 – Connection d'un arc à un point

Algorithme 5.4.3 : `ConnectArcToPointToArc`

Entrées : $p_i^{r_1}Q_1p_j^{r_1}$, $p_k^{r_2}Q_2p_l^{r_2}$ deux arcs et C un point

Sorties : Complexe représentant la connection des deux arcs en passant par le point (voir figure 5.5)

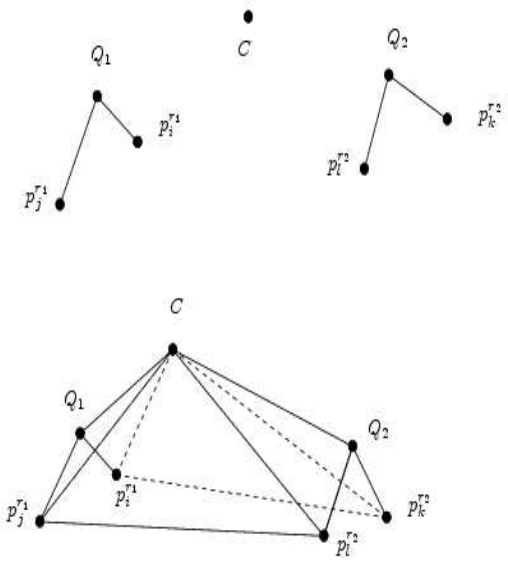

FIG. 5.5 – Connection d'un arc à un arc en passant par un point

Pour $j \in [\![1, m_1]\!]$, soit (μ_1, μ_2) le support de la classe d'arcs $\mathcal{A}_j$ de $\mathcal{C}_{r_1}$ et (θ_1, θ_2) les points de $(p_1^{r_2}, \ldots, p_{n_2}^{r_2})$ respectivement connectés à μ_1 et μ_2 lors du calcul de la topologie de la silhouette $\mathcal{P}$. La connection des arcs de support (μ_1, μ_2) à ceux de support (θ_1, θ_2) sera guidée par la valeur de l'entier $\varphi_c(\Pi_z(\mu_1)) * \varphi_c(\Pi_z(\mu_2))$ ou φ_c est la fonction définie dans la Remarque 3.3.16 et Π_z l'application de projection sur le plan (x,y). En effet l'entier $\varphi_c(\Pi_z(\mu_1)) * \varphi_c(\Pi_z(\mu_2))$ ne peut prendre que trois valeurs, $\{-1, 0, 1\}$. A chacune de ces valeurs correspond une configuration géométrique nécessitant un traitement particulier des arcs.

1. $\varphi_c(\Pi_z(\mu_1)) * \varphi_c(\Pi_z(\mu_2)) = -1$: alors $\varphi_c(\Pi_z(\mu_1)) = -1$ et $\varphi_c(\Pi_z(\mu_2)) = 1$ ou $\varphi_c(\Pi_z(\mu_1)) = 1$ et $\varphi_c(\Pi_z(\mu_2)) = -1$. Cette situation correspond à la configuration géométrique de la figure 5.6 :

   Lors de la première étape de l'algorithme de connection, nous collectons dans un ensemble $\mathcal{K}$ (resp $\mathcal{L}$) les classes d'arcs de $\mathcal{C}_{r_1}$ (resp. $\mathcal{C}_{r_2}$) vérifiant cette contrainte, puis nous les ordonnons suivant la relation d'ordre de la Définition 5.3.10. La connection de ces arcs est imposée par la structure de la fibre x-critique $\{\text{UpPoints}, c, \text{DownPoints}\}$. La deuxième phase consiste à connecter les #UpPoints premiers arcs de $\mathcal{K}$ aux #UpPoints premiers arcs de $\mathcal{L}$, en passant à chaque fois par un point de UpPoints. Ensuite nous connectons

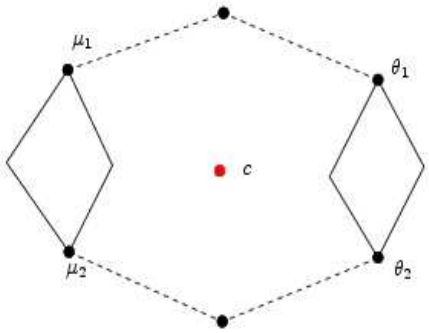

FIG. 5.6 – $\varphi_c(\Pi_z(\mu_1)) * \varphi_c(\Pi_z(\mu_2)) = -1$

les #DownPoints derniers arcs de $\mathcal{K}$ aux #DownPoints derniers arcs de $\mathcal{L}$ en passant à chaque fois par un point de Downpoints. Pour finir, nous connectons le reste des arcs dans $\mathcal{K}$ et $\mathcal{L}$ au point x-critique c.

2. $\varphi_c(\Pi_z(\mu_1)) * \varphi_c(\Pi_z(\mu_2)) = 1$: alors $\varphi_c(\Pi_z(\mu_1)) = -1$ et $\varphi_c(\Pi_z(\mu_2)) = -1$ ou $\varphi_c(\Pi_z(\mu_1)) = 1$ et $\varphi_c(\Pi_z(\mu_2)) = 1$. Cette situation correspond à la configuration géométrique de la figure 5.7 :

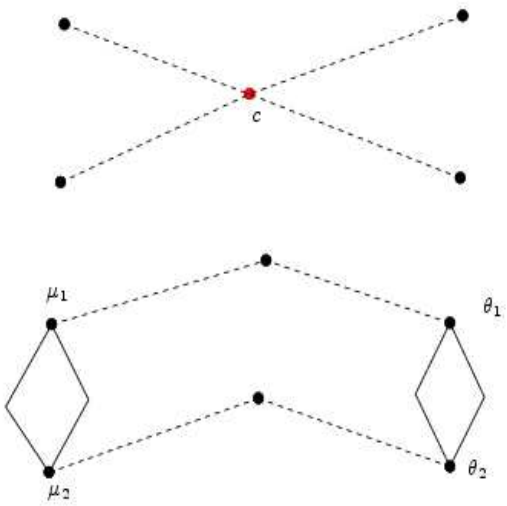

FIG. 5.7 – $\varphi_c(\Pi_z(\mu_1)) * \varphi_c(\Pi_z(\mu_2)) = 1$

Dans cette configuration, le nombre d'arcs de support (μ_1, μ_2) est égal à celui des arcs de support (θ_1, θ_2). Il suffit alors d'ordonner les arcs dans chaque classe puis les connecter suivant leur position.

3. $\varphi_c(\Pi_z(\mu_1)) * \varphi_c(\Pi_z(\mu_2)) = 0$: cette situation correspond aux configurations géométriques des figures 5.8 et 5.9 :

   Lorsque $\varphi_c(\Pi_z(\mu_1)) * \varphi_c(\Pi_z(\mu_2)) = 0$, il suffit de connecter tous les arcs de support (μ_1, μ_2) au point *x*-critique *c*.

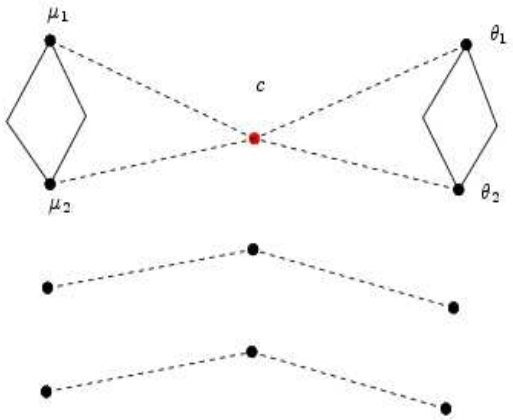

FIG. 5.8 – $\varphi_c(\Pi_z(\mu_1)) = 0$ and $\varphi_c(\Pi_z(\mu_2)) = 0$

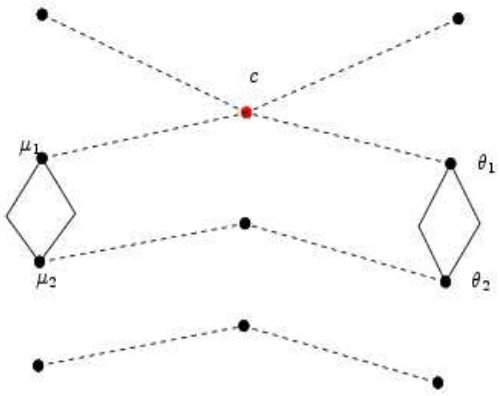

FIG. 5.9 – $\varphi_c(\Pi_z(\mu_1)) = 0$ and $\varphi_c(\Pi_z(\mu_2)) = 1$

Algorithme 5.4.4 : `Connection de deux sections consécutives de la surface`

Entrées : $(\mathcal{A}_1,\ldots,\mathcal{A}_{m_1})$,$(\mathcal{B}_1,\ldots,\mathcal{B}_{m_2})$, $\{\text{UpPoints}, c, \text{DownPoints}\}$, $\mathcal{P}$ et φ_c

Sorties : Complexe représentant la connection de $(\mathcal{A}_1,\ldots,\mathcal{A}_{m_1})$ à $(\mathcal{B}_1,\ldots,\mathcal{B}_{m_2})$

→ $\mathcal{E} := (\mathcal{B}_1,\ldots,\mathcal{B}_{m_2})$; $j := 1$; $\mathcal{K} := \{\}$; $\mathcal{L} := \{\}$;

→ Tant que $j < m_1$ faire

- $\Omega := \mathcal{A}_j$, $(\mu_1,\mu_2) :=$ support des arcs de la classe $\mathcal{A}_j$,
- Si $\varphi_c(\Pi_z(\mu_1)) * \varphi_c(\Pi_z(\mu_2)) = -1$ alors faire {
  $\mathcal{K} := \mathcal{K} \bigcup \Omega$; $(\theta_1,\theta_2) :=$ les points de $(p_1^{r_2},\ldots,p_{n_2}^{r_2})$ connectés à (μ_1,μ_2),
  $\Lambda :=$ l'élément de $\mathcal{E} := (\mathcal{B}_1,\ldots,\mathcal{B}_{m_2})$ de support (θ_1,θ_2),
  $\mathcal{L} := \mathcal{L} \bigcup \Lambda$; $\mathcal{E} := \mathcal{E} \backslash \Lambda$}
- Si $\varphi_c(\Pi_z(\mu_1)) * \varphi_c(\Pi_z(\mu_2)) = 1$ alors faire {
  $(\theta_1,\theta_2) :=$les points de $(p_1^{r_2},\ldots,p_{n_2}^{r_2})$ connectés à (μ_1,μ_2),
  $\Lambda :=$ l'élément de $\mathcal{E} := (\mathcal{B}_1,\ldots,\mathcal{B}_{m_2})$ de support (θ_1,θ_2),
  Pour k allant de 1 à $\#\Omega$ faire {`ConnectArcToArc`$(\Omega[k],\Lambda[k])$,}
  $\mathcal{E} := \mathcal{E} \backslash \Lambda$,}
- Si $\varphi_c(\Pi_z(\mu_1)) * \varphi_c(\Pi_z(\mu_2)) = 0$, alors faire
  pour k allant de 1 à $\#\Omega$ faire {`ConnectArcToPoint`$(\Omega[k],c)$,}

→ Fin Tant que.

→ Si $\#\mathcal{E} \neq 0$ alors pour i allant de 1 à $\#\mathcal{E}$ faire { $\Lambda := \mathcal{E}[i]$,
pour k allant de 1 à $\#\Lambda$ faire {`ConnectArcToPoint`$(\Lambda[k],c)$, } }

→ Ordonner les arcs dans $\mathcal{K}$ puis ceux dans $\mathcal{L}$ par la relation d'ordre de la Définition 5.3.10, puis faire :

1. $\Sigma_1 :=$ la séquence ordonnée des points de UpPoints,
2. $\Sigma_2 :=$ la séquence ordonnée des points de DownPoints,
3. Pour k allant de 1 à $\#\Sigma_1$ faire {`ConnectArcToPointToArc`$(\mathcal{K}[k],\Sigma_1[k],\mathcal{L}[k])$,}
4. Pour k allant de 1 à $\#\Sigma_2$ faire
   {`ConnectArcToPointToArc`$(\mathcal{K}[(\#\mathcal{K})-k],\Sigma_2[\#(\Sigma_2)-k],\mathcal{L}[\#(\mathcal{L})-k])$,}
5. Pour k allant de $\#\Sigma_1+1$ à $\#\mathcal{K}-\#\Sigma_2$ faire {`ConnectArcToPoint`$(\mathcal{K}[k],c)$,}
6. Pour k allant de $\#\Sigma_1+1$ à $\#\mathcal{L}-\#\Sigma_2$ faire {
   `ConnectArcToPoint`$(\mathcal{L}[k],c)$,}

5.5 L'algorithme de triangulation de la surface $\mathcal{S}$

5.5.1 Description globale de l'algorithme `TopolSurface`

Algorithme 5.5.1 : `TopolSurface`

Entrées : $P \in \mathbb{Q}[X,Y,Z]$ polynôme sans facteur carré de degré d

Sorties : Complexe simplicial isotope à $\mathcal{S} := \{(\alpha,\beta,\gamma) \in \mathbb{R}^3 | P(\alpha,\beta,\gamma) = 0\}$

1. Calcul de la topologie de la silhouette $\mathcal{P}$ de $\mathcal{S}$ avec l'algorithme `TopolCourbe3D`.
   - $\mathcal{P} :=$ TopolCoube$3D(P(X,Y,Z), \partial_Z P(X,Y,Z))$;
   - Soit $(c_i := (\alpha_i, \beta_i, \gamma_i))_{i \in [\![1,n]\!]}$ la liste ordonnée des points x-critiques de $\mathcal{P}$ et $(r_i)_{i \in [\![1,n+1]\!]}$ une séquence de nombres réels vérifiant $r_1 < \alpha_1 < r_2 < \alpha_2 < \ldots \alpha_{n-1} < r_n < \alpha_n < r_{n+1}$.
2. Calcul des fibres de la surface $\mathcal{S}$ passant par les points x-critiques de la silhouette $\mathcal{P}$.
   Pour i allant de 1 à n faire $\{\text{Fib}_{c_i} := \{\text{UpPoints}(c_i), c_i, \text{DownPoints}(c_i)\};\}$
3. Calcul des topologies des sections $(\mathcal{C}_{r_1}, \ldots, \mathcal{C}_{r_{n+1}})$ de la surface $\mathcal{S}$.
   Pour i allant de 1 à $n+1$ faire $\{\mathcal{C}_{r_i} :=$ `TopolCourbe2D`$(P(r_i,Y,Z));\}$
4. Connection des différentes sections de la surface $\mathcal{S}$.
   $\mathcal{K} := \{\}$;
   Pour i allant de 1 à n faire $\{\mathcal{K} := \mathcal{K} \cup$ `Connection`$(\mathcal{C}_{r_i}, \text{Fib}_{c_i}, \mathcal{C}_{r_{i+1}})\}$
5. Retourner $\mathcal{P} \cup \mathcal{K}$

5.5.2 Preuve de l'algorithme `TopolSurface`

Pour prouver que l'algorithme est correcte, nous allons utiliser certains des résultats de la théorie de Morse stratifiée. On peut se réfèrer à [34, 37, 18, 11], pour plus de détails. La notion fondamentale est celle de stratification de Withney. C'est une décomposition de la variété en parties lisses qui s'assemblent de manière régulière. Commençons par rappeler quelques définitions.

Définition 5.5.1 *Une stratification d'une variété (semi-algébrique) $A \subset \mathbb{R}^n$ est une partition localement finie de A en sous-variétés lisses appelées strates.*

Définition 5.5.2 *Soit (X,Y) deux strates et $p \in \bar{X} \cap Y \subset \mathbb{R}^n$. X est Whitney-régulier en p le long de Y si pour toutes suites $x_n \in X$, $y_n \in Y$ convergeant vers p, $l = \lim_{n \longrightarrow +\infty} x_n y_n \subset \mathcal{T} =$*

$\lim_{\longrightarrow+\infty} T_{x_n}X$, *où* T_xX *est l'espace tangent de* X *au point* x.

Définition 5.5.3 *Une stratification de Whitney d'une variété S est une stratification de S telle que tous les couples de strates soient Whitney-réguliers*

Notons que l'on a pas évoqué la condition aux frontières pour les strates alors qu'elle est souvent exigées. Mais nous avons besoin seulement du lemme de Thom et cette propriété ne joue pas de rôle dans sa démonstration [11].

Proposition 5.5.4 *Toute strate semi-algébrique d'une variété S est Whitney régulière relativement à une strate de dimension 0.*

Démonstration L'idée est d'utiliser le lemme de selection de courbes. Voir [18]. □

Définition 5.5.5 *Une application différentiable* $f : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ *est une submersion en un point p de* $\mathbb{R}^m$*si la différentielle de* f *en p est surjective.*

Définition 5.5.6 *Une application continue* $f : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ *est propre si l'image inverse de tout compact de* $\mathbb{R}^m$ *est un compact de* $\mathbb{R}^n$.

Le principal théorème que nous utilisons est le lemme d'isotopie de Thom :

Théorème 5.5.7 (***Lemme d'isotopie de Thom***). *Soit* Z *une stratification de Whitney d'un sous-ensemble de* $\mathbb{R}^m$ *et* $\pi : Z \longrightarrow \mathbb{R}^n$ *une submersion propre et stratifiée. Alors il existe un homéomorphisme préservant les strates* $h : Z \longrightarrow (\pi^{-1}(0) \cap Z) \times \mathbb{R}^n$ *qui est lisse sur chaque strate et qui commute avecla projection sur* $\mathbb{R}^n$.

Cela implique que Z est homéomorphe à un cylindre de base $\pi^{-1}(0) \cap Z$. Dans notre cas, nous appliquons le théorème avec $Z := \mathcal{S} \cap B($ où B est une boule de $\mathbb{R}^3$ de rayon suffisamment grand), $m = 3$, $n = 1$ et π la projection sur l'axe des x qui est propre puisque nous travaillons dans une boule B qui est compacte. Soit $\mathcal{C} := \{(\alpha,\beta) \in \mathbb{R}^2 | \operatorname{Res}_Z(P, \partial_Z P)(\alpha,\beta) = 0\}$ la projection de la silhouette $\mathcal{P}$ de $\mathcal{S}$ sur le plan (x,y).

Théorème 5.5.8 *[42, 4] Pour une surface* $\mathcal{S}$ *en position générique, soient*

- $\mathcal{S}^0$ *l'ensemble des points de la silhouette* $\mathcal{P}$ *de* $\mathcal{S}$ *qui se projettent en des points singuliers de* $\mathcal{C}$ *(chaque point est considéré comme une strate),*
- $\mathcal{S}^1$ *l'ensemble des composante connexes de* $\mathcal{P} - \mathcal{S}^0$ *(chaque composante connexe est une strate),*
- $\mathcal{S}^2$ *l'ensemble des composante connexes de* $\mathcal{S} - \mathcal{P}$ *(chaque composante connexe est une strate),*

– $\mathcal{S}^3 = \mathbb{R}^3 - \mathcal{S}$

Alors $(\mathcal{S}^0, \mathcal{S}^1, \mathcal{S}^2, \mathcal{S}^3)$ *est une stratification de Whitney de* $\mathcal{S}$ *et elle vérifie les hypothèses du lemme de Thom pour la projection sur l'axe des x entre les abscisses des points de* $\mathcal{S}^0$.

En effet, la régularité de Whitney est vérifiée pour toute strate relativement à $\mathcal{S}^3$ (car l'espace tangent à un point de $\mathcal{S}^3$ est tout l'espace). De la Proposition 5.5.4, on déduit que montrer que $(\mathcal{S}^0, \mathcal{S}^1, \mathcal{S}^2, \mathcal{S}^3)$ est une stratification de Whitney revient à montrer que $(\mathcal{S}^1, \mathcal{S}^2)$ est Whitney-régulier.
Selon que l'on considère le polynôme P définissant $\mathcal{S}$ au dessus de $\mathbb{R}$ ou de $\mathbb{C}$, on obtient une variété réelle $\mathcal{S} = \mathcal{S}_{\mathbb{R}}$ ou complexe $\mathcal{S}_{\mathbb{C}}$, comme ensemble des zéros de P. Nous allons utiliser la notion d'équisingularité au dessus de $\mathbb{C}$ et la notion de projection "permissible" pour prouver le théorème précédent. Speder à donné dans [59] une définition de projection permissible, plus forte que l'originale donnée par Zariski [62]. Comme nous allons uniquement considérer le cas de la codimension 1, pour lequel les deux définitions coincident, nous n'allons considérer que la défintion de projection permissible de Zariski :

Définition 5.5.9 *Une direction permissible de projection pour le couple* (X, Y)*avec*$Y \subset X$ *en* $Q \in Y$ *est un élément de* $\mathbb{PC}^3$ *tel que la droite passant par Q définie par cette direction n'est ni incluse dans un voisinage de Q ni dans l'espace tangent à Y en Q.*

Proposition 5.5.10 *Pour une surface algébrique* $\mathcal{S}$*, une direction de projection générique permissible pour le couple* $(\mathcal{S}^1, \mathcal{S}^2)$ *en tout point de* $\mathcal{S}^1$.

Démonstration Pour une variété algébrique, le fait qu'une droite soit localement incluse dans une surface est équivalent à son inclusion globale. On en déduit que les directions de projection à éviter sont incluses dans l'union des :

– directions de droite incluse dans la surface

– directions des tangentes à la partie lisse du lieu singulier de la variété.

On considère le premier ensemble de directions des droites incluses dans la surface $\mathcal{S}$, définie par l'équation $P = 0$. Si on plonge la surface dans l'espace projectif, les directions des droites incluses dans $\mathcal{S}$, considérées comme des points de l'espace projectif, sont incluses dans l'intersection de $\mathcal{S}$ avec l'hyperplan à l'infini, qui est une courbe projective. Les directions correspondant aux premiers ensembles sont donc incluses dans un ensemble de dimension 1 et sont ainsi génériquement évitées.

Considérons maintenant le deuxième ensemble. On considère un arc de la partie lisse de la silhouette de la surface (il existe un nombre fini de tels arcs pour une surface algébrique). On considère une paramétrisation semi-algébrique de cet arc $(x(s), y(s), z(s))$. On obtient une

paramétrisation semi-algébrique $(x'(s), y'(s), z'(s))$ d'un ensemble de vecteurs unités correspondant aux directions des tangentes à la courbe. On en déduit un ensemble à éviter (pour la condition de tangence) corespondant à une courbe semi-algébrique sur la sphère unité de $\mathbb{R}^3$ et est génériquement évité. □

Proposition 5.5.11 *Si la surface $\mathcal{S}$ est en position générique au sens de la Définition 5.3.1, alors la projection π_z parallèlement à l'axe des z est une projection permissible.*

Démonstration Tout d'abord, il n'y a pas de droite parallèle à l'axe des z dans $\mathcal{S}$ car si c'était le cas, cette droite verticale serait incluse dans la silhouette $\mathcal{P}$ de $\mathcal{S}$ et nous ne serions pas en position générique. Le second point à vérifier est que la direction z ne correspond pas à la direction d'une tangente de $\mathcal{S}^1$. C'est le cas puisque par construction les points de la silhouette avec des tangentes verticale sont dans $\mathcal{S}^0$. □

On rappelle la notion d'équisingularité :

Définition 5.5.12 *Soit $X \subset \mathbb{C}^n$ une hypersurface, Y une sous-variété lisse de X de codimension c, p un point de Y. On dit que X est équisingulier en p le long de Y si $c = 0$ et X est lisse ou bien si $c > 0$, $Y \subset X_{\text{sing}}$ et qu'il existe une projection permissible π_z telle que $\Delta(\pi_z, X)$ est équisingulière en $\pi_z(p)$ le lond de $\pi_z(Y)$(voir [62]).*

Le principal résultat que nous utilisons est le suivant :

Proposition 5.5.13 *Si l'hypersurface X est équisingulière le long de Y (en codimension 1) alors le couple $(X_{\text{smooth}} - Y, Y)$ remplit les conditions de Whitney le long de Y (voir [62]).*

Cela nous permet de vérifier les conditions de Whitney sur $\mathbb{C}$. Pour le vérifier sur $\mathbb{R}$ nous utilisons le lemme suivant dont une preuve est donnée dans [4] :

Lemme 5.5.14 *Si X et Y sont deux Strates d'une stratification de $\mathcal{S}_{\mathbb{C}}$ avec $\dim(X) = 2$ et $\dim(Y) = 1$, alors$X_{\mathbb{R}} = X \cap \mathbb{R}^3$ et $Y_{\mathbb{R}} = Y \cap \mathbb{R}^3$ sont Whitney réguliers.*

Démonstration du Théorème 5.5.8. Comme nous l'avons précédemment mentionné, par application de la Proposition 5.5.4, nous avons seulement besoins de vérifier la condition de Whitney pour une strate de dimention 1 $S^1_{\mathbb{R}}$ de $\mathcal{S}$ et une strate de dimension 2 $S^2_{\mathbb{R}}$ de $\mathcal{S}$. Soit $p \in S^1_{\mathbb{R}} \cap S^2_{\mathbb{R}}$. Si p est un point lisse de $\mathcal{S}$, la condition de Whitney est trivialement satisfaite. Si p est singulier, par la Proposition 5.5.13, la condition de Whitney est vérifiée pour $(S^1_{\mathbb{C}}, S^2_{\mathbb{C}})$ en p. Et en appliquant le Lemme précédent, on en déduit la condition de Whitney pour $(S^1_{\mathbb{R}}, S^2_{\mathbb{R}})$ en p. Cela prouve que $(\mathcal{S}^0, \mathcal{S}^1, \mathcal{S}^2, \mathcal{S}^3)$ est une stratification de Whitney de $\mathcal{S}$.

En appliquant le Théorème 5.5.8 et en utilisant le lemme de Thom, on déduit qu'entre deux sections consécutives de $\mathcal{S}$ contenant un point x-critique de sa silhouette $\mathcal{P}$ la topologie des sections est constante. Nous avons calculé la topologie de sections régulières entre deux sections x-critiques. D'un point de vue topologique, nous définissons les bonnes connections car le maillage est réalisé de façon à ne pas créer de nouvelles auto-intersections. Ainsi l'algorithme TopoloSurface retourne bien une structure simpliciale isotope à la surface de départ $\mathcal{S}$

5.5.3 Complexité de l'algorithme `TopolSurface`

Théorème 5.5.15 *Soient $P \in \mathbb{Z}[X,Y,Z]$, $d := \deg(P)$, $\tau := \mathcal{L}(P)$ la taille binaire des coefficients de P, et $\mathcal{S}$ le lieu des zéros réels de P. L'algorithme `TopolSurface` calcule une triangulation de $\mathcal{S}$ avec une complexité binaire de $\tilde{O}_B(d^{21}\tau)$.*

Démonstration La première étape de l'algorithme est le calcul de la topologie de la silhouette $\mathcal{P}$ de la surface $\mathcal{S}$. D'après le Théorème 4.3.18, ce calcul s'effectue avec une complexité de $\tilde{O}_B(d^{21}\tau)$. Ensuite vient la phase de calcul des $(n+1)$ sections de $\mathcal{S}$. Comme $\deg(P) = d$, alors il est clair que $n = O(d^4)$. Comme d'après le Théorème 3.3.12, le calcul de chaque section s'effectue avec une complexité binaire de $\tilde{O}_B(d^{10}\tau)$ alors le calcul de l'ensemble des sections nécessaires s'effectue avec une complexité binaire de $O(d^4) \times \tilde{O}_B(d^{10}\tau) = \tilde{O}_B(d^{14}\tau)$. Le coût de la phase de connection est clairement négligeable. Ainsi la triangulation de $\mathcal{S}$ s'effectue avec une complexité binaire de $\tilde{O}_B(d^{21}\tau + d^{14}) = \tilde{O}_B(d^{21}\tau)$. □

5.5.4 Implémentation et expérimentation

Une implémentation de `TopolSurface` a été réalisée avec MATHEMAGIX et les résultats visualisés avec le modeler géométrique AXEL. Le tableau suivant montre les temps de calculs de quelques surfaces implicites sur une machine Intel(R) 2GHz avec 1GB de RAM.

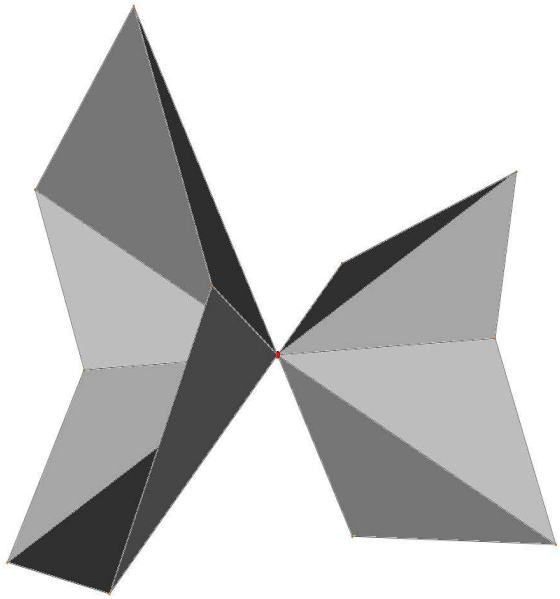

FIG. 5.10 – Surface 3

Surface	$P(x,y,z)$	Temps (s)
1	$x^4-y^4-z^2$	0.33
2	$x^5-y^2-z^2$	0.36
3	$x^4+y^2-z^2$	0.31
4	$-xz^2-z^3+y^2$	0.40
5	$x^5+y^2-z^2$	0.32
6	$z(x^2+y^2+z^2-1)(x^2+4x+y^2+z^2+3)$	0.82
7	$-x^2z-2xyz+2yz^2+z^3+x^2+$ $2xy+2y^2+2yz+2z^2-1$	0.90
8	$x^4z^3-x^4z^2-2x^4z+y^2z^3-z^5-$ $y^2z^2+z^4-2y^2z+2z^3$	0.98

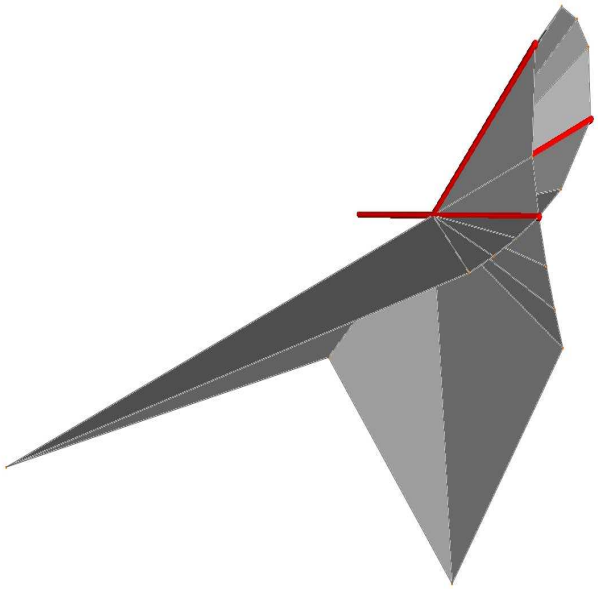

FIG. 5.11 – Surface 4

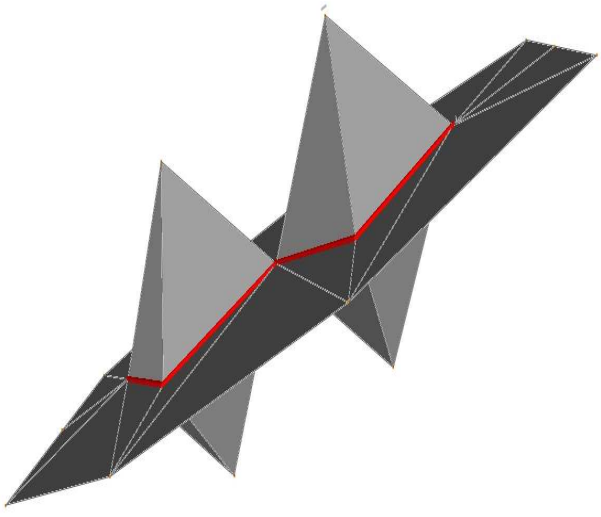

FIG. 5.12 – Surface 6

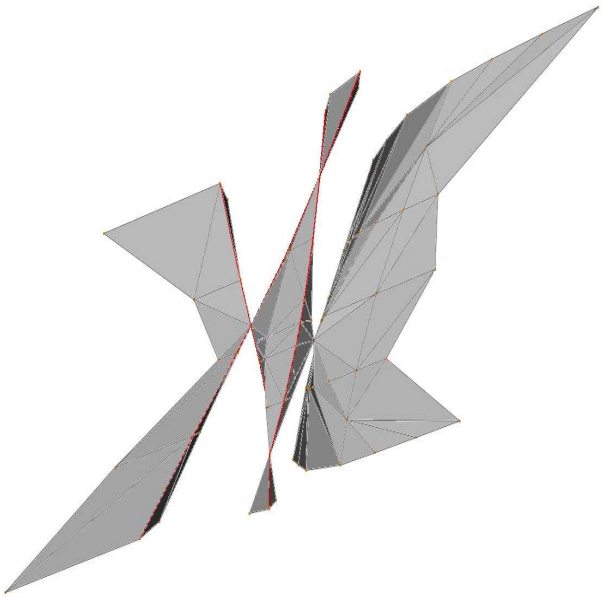

FIG. 5.13 – Surface 7

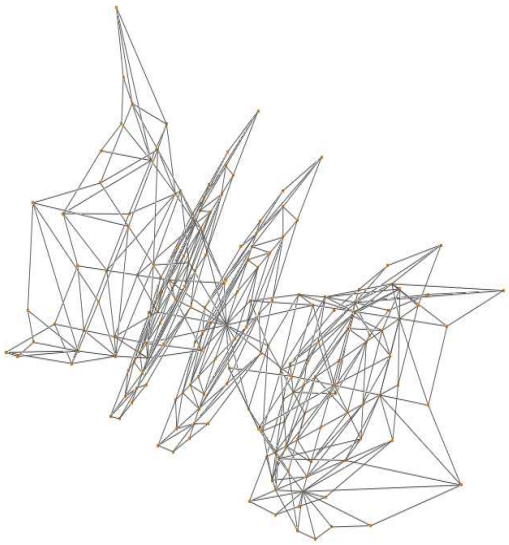

FIG. 5.14 – Surface 8

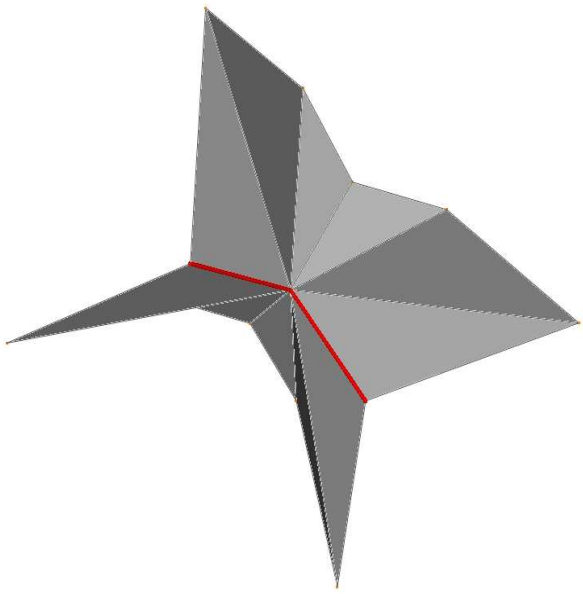

FIG. 5.15 – Surface 5

Chapitre 6

Perspectives : Calcul d'arrangement de quadriques

6.1 Introduction

Soient $Q_1,\ldots,Q_n \in \mathbb{Z}[X,Y,Z]$ tels que pour tout $i \in [\![1,n]\!]$ $\deg(Q_i) \leqslant 2$. Soit $(\mathcal{S}_1,\ldots,\mathcal{S}_n)$ la famille de quadriques définie par les polynômes $(Q_1,\ldots,Q_n)$:

$$\forall i \in [\![1,n]\!], \mathcal{S}_i := \{(\alpha,\beta,\gamma) \in \mathbb{R}^3 | Q_i(\alpha,\beta,\gamma) = 0\}$$

Dans ce chapitre nous évoquons notre travail en cours sur le problème du calcul de l'arrangement de la famille de quadriques $(\mathcal{S}_1,\ldots,\mathcal{S}_n)$ dans $\mathbb{R}^3$. Le calcul d'arrangement de courbes et de surfaces est un problème fondamental dans les domaines de l'informatique notamment la modélisation de solides et la géométrie algorithmique. Par exemple en modélisation [40], le calcul d'arrangement de courbes et surfaces intervient généralement lors de l'éxécution d'opérations booléennes sur les quadriques, qui jouent un rôle important dans la conception de pièces mécaniques. En robotique, les arrangements de quadriques interviennent lors de la planification de trajectoire de robots. Dans l'article [36], Halperin insiste sur l'intérêt du calcul d'arrangement d'objets linéaires en géométrie algorithmique. La manipulation de quadriques offre un compromis entre le traitement dans un maillage d'un très grand nombre d'objets simples, les triangles et un nombre plus restreint d'objets plus complexes mais potentiellement plus riches en informations, des objets algébriques.
Par définition, l'arrangement d'un ensemble $\mathcal{E}$ d'objets semi-algébriques dans $\mathbb{R}^n$ est la décomposition de $\mathbb{R}^n$ en composantes connexes de dimensions $0,1,\ldots,n$ où les polynômes définissant les objets sont de signes constants. Un outil classique pour la décomposition d'ensemble semi-algébriques est la décomposition cylindrique algébrique. Mais sa très grande

complexité a motivé le développement de nombreux approches alternatives en géométrie algorithmique. Ainsi dans [50], les auteurs utilisent une technique consistant à balayer l'espace par un plan orthogonal à l'axe des abscisses. L'intersection du plan de balayage avec la famille de quadriques en une position $x = x_0$ fixée, donne un arrangement de coniques dans le plan (y,z). Les cellules sont calculées via une décomposition en "trapézoides" de la section $x = x_0$. Dans [58] les auteurs ont présenté deux méthodes pour calculer une cellule dans un arrangement de quadriques. La première utilise des techniques de projection basées sur les résultants, alors que la seconde utilise des techniques de modélisation géométrique de volumes. Si les auteurs soulignent eux mêmes les limites de la méthode utilisant les techniques de modélisation géométrique de volumes, les difficultés de la phase de relèvement qui apparaissent lorsqu'on procéde par projection (distinction des singularités apparentes, gestion certifiée des connections au dessus des singularités apparentes) n'ont pas été traitées. Notre stratégie consiste à calculer sur chaque quadrique $\mathcal{S}_\setminus$ de la famille $(\mathcal{S}_1,\ldots,\mathcal{S}_n)$, toutes les courbes d'intersection de $\mathcal{S}$ avec les $(n-1)$ quadriques restantes ainsi que sa silhouette. Pour y parvenir, l'ensemble de ces courbes sera projeté sur le plan (x,y) conduisant ainsi à un calcul de sous-arrangements de courbes planes. Afin de simplifier la phase de relèvement et la gestion des singularités apparentes, nous introduisons des conditions de généricité, similaires à celles décrites dans le Chapitre 4, qui conduirons à l'existence de paramétrisations rationnelles très simples (car les surfaces ici sont des quadriques), permettant le relèvement des courbes projetées. Ensuite, pour le calcul de sous-arrangements de courbe algébrique plane, nous utilisons l'algorithme décrite dans [1]. Dans la section suivante, nous donnons les grandes lignes d'un travail encours dont la phase la plus difficile sera sûrement celle de l'implémentation.

6.2 L'algorithme de calcul d'arrangement de quadriques

6.2.1 Conditions de généricité et phase de projection

Soit $\mathcal{S}$ une quadrique de la famille $(\mathcal{S}_1,\ldots,\mathcal{S}_n)$ que nous supposerons être le n^{ieme}. Pour tout $i \in [\![1,n-1]\!]$, soit $\mathcal{C}_i := \mathcal{S} \cap \mathcal{S}_i$ la courbe intersection de la quadrique $\mathcal{S}$ avec la quadrique $\mathcal{S}_i$. Soit $\mathcal{P}$ la silhouette de $\mathcal{S}$ au sens de la Définition 5.2.3 et $\mathcal{C} := \mathcal{P} \cup \mathcal{C}_1 \cup \ldots \cup \mathcal{C}_{n-1}$.

Définition 6.2.1 *La quadrique $\mathcal{S}$ est en position générique si et seulement si la courbe spatiale $\mathcal{C}$ définie comme réunion des courbes $\mathcal{C}_i$ et $\mathcal{P}$ est en position pseudo-générique au sens de la Définition 4.3.1.*

Supposons que la quadrique $\mathcal{S}$ est en position générique. Cette hypothèse peux être testée par une version simplifiée, du test de pseudo-généricité proposé dans le Chapitre 4, tenant compte du fait que les surfaces sont ici des quadriques. Dans les cas où $\mathcal{S}$ n'est pas en position générique, nous effectuerons un changement de variable sur l'ensemble des quadriques pour se mettre dans une position adéquate.
Il est clair que si $\mathcal{C} := \mathcal{P} \cup \mathcal{C}_1 \cup \ldots \cup \mathcal{C}_{n-1}$ est en position pseudo-générique, alors toutes les courbes d'intersection $\mathcal{C}_i$ et la silhouette $\mathcal{P}$ de $\mathcal{S}$ sont en position pseudo-générique. Comme toutes ces courbes sont des intersections de surfaces quadriques alors en appliquant la Proposition 4.3.2 à chaque courbe on obtient le Proposition suivante :

Proposition 6.2.2 *Pour tout $i \in [\![1, n-1]\!]$, nous noterons $\mathrm{sr}_0(Q, Q_i) \in \mathbb{Q}[X,Y]$ le résultant des polynômes Q et Q_i, $\mathrm{sr}_{1,1}(Q, Q_i), \mathrm{sr}_{1,0}(Q, Q_i) \in \mathbb{Q}[X,Y]$ les coefficients du polynôme sous-résultant d'ordre 1 associé à Q et Q_i. Alors si la quadrique $\mathcal{S}$ est en position générique, alors pour tout $i \in [\![1, n-1]\!]$, $\mathcal{C}_i := \{(\alpha,\beta,\gamma) \in \mathbb{R}^3 | \, \mathrm{sr}_0(Q, Q_i)(\alpha,\beta) = 0, \gamma = \frac{-\mathrm{sr}_{1,0}(Q,Q_i)(\alpha,\beta)}{\mathrm{sr}_{1,1}(Q,Q_i)(\alpha,\beta)}\}$ et*

$$\mathcal{P} := \{(\alpha,\beta,\gamma) \in \mathbb{R}^3 | \, \mathrm{sr}_0(Q, \partial_Z Q)(\alpha,\beta) = 0, \gamma = \frac{-\mathrm{sr}_{1,0}(Q,\partial_Z Q)(\alpha,\beta)}{\mathrm{sr}_{1,1}(Q,\partial_Z Q)(\alpha,\beta)}\}.$$

La proposition précédente montre que par projection, le calcul de la courbe $\mathcal{C}$ se ramène à celui de l'arrangement des courbes algébriques planes d'équations
$(\mathrm{sr}_0(Q, Q_1), \ldots, \mathrm{sr}_0(Q, Q_{n-1}), \mathrm{sr}_0(Q, \partial_Z Q))$. Le calcul d'un tel arrangement peut s'effectuer avec l'algorithme décrit dans [1].

6.2.2 Phase de relèvement

La phase de relèvement est gérée de la même façon que dans le Chapitre 4. En effet les paramétrisations rationnelles données dans la Proposition 6.2.2 permettent de relever de façon indépendant chaque courbe $\mathcal{C}_i$. Les singularités apparentes sont détectées et relevées avec des adaptations des algorithmes décrites dans le Chapitre 4. Concernant la reconstruction de $\mathcal{S}$, on utilise l'algorithme décrit dans le Chapitre 5. Ce travail est en cours et nous souhaitons mettre en place avec MATHEMAGIX un code certifié de calcul d'arrangement de quadriques.

Chapitre 7

Conclusion

Le but de cette thèse était de construire des algorithmes certifiés calculant la topologie de courbes et surfaces algébriques réelles puis de les implémenter. Nous avons développé trois algorithmes symboliques-numériques certifiés dont les complexités binaires, rappelées ci-dessous, représentent les meilleures parmi les algorithmes traitant ces questions. Nos algorithmes ont été implémentés avec MATHEMAGIX.

Le premier est fortement basé sur les propriétés des polynômes sous-résultants, et permet le calcul de la topologie d'une courbe algébrique plane. Cet algorithme d'une complexité binaire de $\tilde{O}_B(d^{10}\tau)$ (d étant le degré du polynôme définissant la courbe étudiée, et τ la taille binaire de ses coefficients) est une amélioration de l'algorithme décrit dans [32] dont la complexité binaire est de $\tilde{O}_B(d^{16}\tau)$.

Le deuxième algorithme résoud le problème du calcul de la topologie d'une courbe algébrique spatiale définie comme intersection de deux surfaces algébriques implicites avec un coût binaire de $\tilde{O}_B(d^{21}\tau)$.

Le troisième est un algorithme de maillage de surfaces implicites. C'est le premier algorithme certifié et entièrement implémenté qui traite le problème du maillage isotopique de surfaces implicites singulières. Sa complexité binaire est de $\tilde{O}_B(d^{21}\tau)$.

Dans cette thése les algorithmes que nous proposons améliorent les complexités théoriques connues et sont tous certifiés. Néamoins, en pratique, ils sont limités par la croissance exponentielle des coefficients des polynômes lors des phases d'élimination de variables et par la densification des polynômes qu'engendre les changements de variables lorsqu'on recherche une position génerique. Sur le problème des courbes gauches, nous poursuivons nos efforts pour tenter d'affaiblir le plus possible, sans perdre la certification des résultats retournés, les conditions de généricité requises. Si un tel travail aboutit, les répercutions seront immédiates sur le traitement des surfaces algébriques et des arrangements de quadriques.

Bibliographie

[1] L. Alberti, B. Mourrain, and J. Wintz. Topology and arrangement computation of semi-algebraic planar curves. *Comput. Aided Geom. Design*, 25(8) :631–651, 2008.

[2] Lionel Alberti, Georges Comte, and Bernard Mourrain. Meshing implicit algebraic surfaces : the smooth case. In L.L. Schumaker M. Maehlen, K. Morken, editor, *Mathematical Methods for Curves and Surfaces : Tromso'04*, pages 11–26. Nashboro, 2005.

[3] Lionel Alberti and Bernard Mourrain. Visualisation of implicit algebraic curves. In Marc Alexa, Steven Gortler, and Tao Ju, editors, *Visualisation of implicit algebraic curves.*, pages 303–312. IEEE Computer Society, 2007.

[4] Lionel Alberti, Bernard Mourrain, and Jean P. Tecourt. Isotopic triangulation of a real algebraic surface. In *Preprint*. 2009.

[5] Juan Gerardo Alcázar and J. Rafael Sendra. Computation of the topology of real algebraic space curves. *J. Symbolic Comput.*, 39(6) :719–744, 2005.

[6] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, second edition, 2006.

[7] Riccardo Benedetti and Jean-Jacques Risler. *Real algebraic and semi-algebraic sets*. Actualités Mathématiques. [Current Mathematical Topics]. Hermann, Paris, 1990.

[8] Marshall W. Bern, David Eppstein, Pankaj K. Agarwal, Nina Amenta, L. Paul Chew, Tamal K. Dey, David P. Dobkin, Herbert Edelsbrunner, Cindy Grimm, Leonidas J. Guibas, John Harer, Joel Hass, Andrew Hicks, Carroll K. Johnson, Gilad Lerman, David Letscher, Paul E. Plassmann, Eric Sedgwick, Jack Snoeyink, Jeff Weeks, Chee-Keng Yap, and Denis Zorin. Emerging challenges in computational topology. *CoRR*, cs.CG/9909001, 1999.

[9] Dario Andrea Bini. Numerical computation of polynomial zeros by means of Aberth's method. *Numer. Algorithms*, 13(3-4) :179–200 (1997), 1996.

[10] J. Bochnak, M. Coste, and M.-F. Roy. *Géométrie Algébrique Réelle*. Springer-Verlag, Heidelberg, 1987.

[11] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy. *Real algebraic geometry*, volume 36 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1998. Translated from the 1987 French original, Revised by the authors.

[12] Jean-Daniel Boissonnat, David Cohen-Steiner, and Gert Vegter. Isotopic implicit surface meshing. In *Proceedings of the 36th Annual ACM Symposium on Theory of Computing*, pages 301–309 (electronic), New York, 2004. ACM.

[13] Jinsan Cheng, Sylvain Lazard, Luis Penaranda, Marc Pouget, Fabrice Rouillier, and Tsigaridas Elias. On the topology of planar algebraic curve. Submitted, 2008.

[14] George E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In *Automata theory and formal languages (Second GI Conf., Kaiserslautern, 1975)*, pages 134–183. Lecture Notes in Comput. Sci., Vol. 33. Springer.

[15] Michel Coste. An introduction to semi-algebraic geometry. RAAG network school, 2002.

[16] Michel Coste and Marie-Françoise Roy. Thom's lemma, the coding of real algebraic numbers and the computation of the topology of semi-algebraic sets. *J. Symbolic Comput.*, 5(1-2) :121–129, 1988.

[17] Daouda Niang Diatta, Olivier Ruatta, and Bernard Mourrain. On the computation of the topology of a non-reduced space curve. In *ISSAC 2008*, pages 47–54. ACM, 2008.

[18] Alexandru Dimca. *Singularities and topology of hypersurfaces*. Universitext. Springer-Verlag, New York, 1992.

[19] Dimitrios I. Diochnos, Ioannis Z. Emiris, and Elias P. Tsigaridas. On the complexity of real solving bivariate systems. In *ISSAC 2007*, pages 127–134. ACM, New York, 2007.

[20] Dimitrios I. Diochnos, Ioannis Z. Emiris, and Elias P. Tsigaridas. On the complexity of real solving bivariate systems. In *ISSAC 2007*, pages 127–134. ACM, New York, 2007.

[21] Lionel Ducos. Optimizations of the subresultant algorithm. *J. Pure Appl. Algebra*, 145(2) :149–163, 2000.

[22] Arno Eigenwillig, Michael Kerber, and Nicola Wolpert. Fast and exact geometric analysis of real algebraic plane curves. In *ISSAC 2007*, pages 151–158. ACM, New York, 2007.

[23] Mohab Safey El Din. Algorithmes efficaces en géométrie algébrique réelle. Journées Nationales du Calcul Formel 2007, 2007.

[24] M'hammed El Kahoui. Topology of real algebraic space curves. *J. Symbolic Comput.*, 43(4) :235–258, 2008.

[25] Mohamed Elkadi and Bernard Mourrain. *Introduction à la résolution des systèmes polynomiaux*, volume 59 of *Mathématiques & Applications (Berlin) [Mathematics & Applications]*. Springer, Berlin, 2007.

[26] Ioannis Z. Emiris and Bernard Mourrain. Matrices in elimination theory. *J. Symbolic Comput.*, 28(1-2) :3–44, 1999. Polynomial elimination—algorithms and applications.

[27] Ioannis Z. Emiris, Bernard Mourrain, and Elias P. Tsigaridas. Real algebraic numbers : Complexity analysis and experimentation. In *Reliable Implementation of Real Number Algorithms*, pages 57–82, 2008.

[28] J. C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *J. Symbolic Comput.*, 16(4) :329–344, 1993.

[29] Elisabetta Fortuna, Patricia M. Gianni, and Domenico Luminati. Algorithmical determination of the topology of a real algebraic surface. *J. Symb. Comput.*, 38(6) :1551–1567, 2004.

[30] Elisabetta Fortuna, Patricia M. Gianni, Paola Parenti, and Carlo Traverso. Algorithms to compute the topology of orientable real algebraic surfaces. *J. Symb. Comput.*, 36(3-4) :343–364, 2003.

[31] Gregory Gatellier, Abder. Labrouzy, Bernard. Mourrain, and Jean Pierre. Técourt. Computing the topology of three-dimensional algebraic curves. In *Computational methods for algebraic spline surfaces*, pages 27–43. Springer, Berlin, 2005.

[32] Laureano González-Vega and M'Hammed El Kahoui. An improved upper complexity bound for the topology computation of a real algebraic plane curve. *J. Complexity*, 12(4) :527–544, 1996. Special issue for the Foundations of Computational Mathematics Conference (Rio de Janeiro, 1997).

[33] Laureano Gonzalez-Vega and Ioana Necula. Efficient topology determination of implicitly defined algebraic plane curves. *Comput. Aided Geom. Design*, 19(9) :719–743, 2002.

[34] Mark Goresky and Robert MacPherson. *Stratified Morse theory*, volume 14 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1988.

[35] Thomas A. Grandine. Applications of contouring. *SIAM Rev.*, 42(2) :297–316 (electronic), 2000.

[36] Dan Halperin. Arrangements. In *Handbook of discrete and computational geometry*, CRC Press Ser. Discrete Math. Appl., pages 389–412. CRC, Boca Raton, FL, 1997.

[37] Helmut A. Hamm. On stratified Morse theory. *Topology*, 38(2) :427–438, 1999.

[38] Robert M. Hardt. Triangulation of subanalytic sets and proper light subanalytic maps. *Invent. Math.*, 38(3) :207–217, 1976/77.

[39] H. Hironaka. Triangulations of algebraic sets. In *Algebraic geometry (Proc. Sympos. Pure Math., Vol. 29, Humboldt State Univ., Arcata, Calif., 1974)*, pages 165–185. Amer. Math. Soc., Providence, R.I., 1975.

[40] Christoph M. Hoffmann and George Vaněček, Jr. Fundamental techniques for geometric and solid modeling. In *Control and dynamic systems, Vol. 48*, pages 101–165. Academic Press, San Diego, CA, 1991.

[41] Hoon Hong. An efficient method for analyzing the topology of plane real algebraic curves. *Math. Comput. Simulation*, 42(4-6) :571–582, 1996. Symbolic computation, new trends and developments (Lille, 1993).

[42] J. R. Sendra J. G. Alcazar, J. Schicho. A delineability-based method for computing critical sets of algebraic surfaces. *J.Symb.Comp.*, 42(6) :678–691, 2007.

[43] Thomas Lickteig and Marie-Françoise Roy. Sylvester-Habicht sequences and fast Cauchy index computation. *J. Symbolic Comput.*, 31(3) :315–341, 2001.

[44] Henri Lombardi, Marie-Françoise Roy, and Mohab Safey El Din. New structure theorem for subresultants. *J. Symbolic Comput.*, 29(4-5) :663–690, 2000. Symbolic computation in algebra, analysis, and geometry (Berkeley, CA, 1998).

[45] Maurice Mignotte and Doru Ştefănescu. *Polynomials*. Springer Series in Discrete Mathematics and Theoretical Computer Science. Springer-Verlag Singapore, Singapore, 1999. An algorithmic approach.

[46] B. Mourrain. A new criterion for normal form algorithms. In *Applied algebra, algebraic algorithms and error-correcting codes (Honolulu, HI, 1999)*, volume 1719 of *Lecture Notes in Comput. Sci.*, pages 430–443. Springer, Berlin, 1999.

[47] B. Mourrain and J. P. Pavone. Subdivision methods for solving polynomial equations. *J. Symbolic Comput.*, 44(3) :292–306, 2009.

[48] B. Mourrain, M. N. Vrahatis, and J. C. Yakoubsohn. On the complexity of isolating real roots and computing with certainty the topological degree. *J. Complexity*, 18(2) :612–640, 2002. Algorithms and complexity for continuous problems/Algorithms, computational complexity, and models of computation for nonlinear and multivariate problems (Dagstuhl/South Hadley, MA, 2000).

[49] Bernard Mourrain, Fabrice Rouillier, and Marie-Françoise Roy. The Bernstein basis and real root isolation. In *Combinatorial and computational geometry*, volume 52 of *Math. Sci. Res. Inst. Publ.*, pages 459–478. Cambridge Univ. Press, Cambridge, 2005.

[50] Bernard Mourrain, Jean-Pierre Técourt, and Monique Teillaud. On the computation of an arrangement of quadrics in 3D. *Comput. Geom.*, 30(2) :145–164, 2005.

[51] Bernard Mourrain and Philippe Trébuchet. Algebraic methods for numerical solving. *An. Univ. Timişoara Ser. Mat.-Inform.*, 39(Special Issue) :149–169, 2001. Symbolic and numeric algorithms on scientific computing (Timişoara, 2001).

[52] Bernard Mourrain and Philippe Trébuchet. Stable normal forms for polynomial system solving. *Theoret. Comput. Sci.*, 409(2) :229–240, 2008.

[53] John C. Owen and Alyn P. Rockwood. Intersection of general implicit surfaces. In *Geometric modeling*, pages 335–345. SIAM, Philadelphia, PA, 1987.

[54] Victor Y. Pan. Optimal and nearly optimal algorithms for approximating polynomial zeros. *Comput. Math. Appl.*, 31(12) :97–138, 1996.

[55] Daniel Reischert. Asymptotically fast computation of subresultants. In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI)*, pages 233–240 (electronic), New York, 1997. ACM.

[56] Fabrice Rouillier. Solving zero-dimensional systems through the rational univariate representation. *Appl. Algebra Engrg. Comm. Comput.*, 9(5) :433–461, 1999.

[57] Olivier Ruatta. A multivariate Weierstrass iterative rootfinder. In *Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation*, pages 276–283 (electronic), New York, 2001. ACM.

[58] Elmar Schömer and Nicola Wolpert. An exact and efficient approach for computing a cell in an arrangement of quadrics. *Comput. Geom.*, 33(1-2) :65–97, 2006.

[59] J. P. Speder. Équisingularité et conditions de Whitney. *Amer. J. Math.*, 97(3) :571–588, 1975.

[60] Jan Verschelde and Ronald Cools. Symbolic homotopy construction. *Appl. Algebra Engrg. Comm. Comput.*, 4(3) :169–183, 1993.

[61] Joachim von zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, second edition, 2003.

[62] Oscar Zariski. Studies in equisingularity. II. Equisingularity in codimension 1 (and characteristic zero). *Amer. J. Math.*, 87 :972–1006, 1965.