Algorithmes efficaces en géométrie algébrique réelle

Mohab Safey El Din

Journées Nationales du Calcul Formel 2007

Algorithmes efficaces en géométrie algébrique réelle

Mohab Safey El Din

Université Pierre et Marie Curie
Laboratoire d'Informatique de Paris 6
Département Calcul Scientifique
Équipe SPIRAL
(Systèmes Polynomiaux, Implantations et Résolutions ALgébriques),
Projet INRIA/LIP6 SALSA
(Software for ALgebraic Systems and Applications)

Janvier 2007

Table des matières

1 Introduction

Ce document constitue les notes d'un cours dispensé lors des *Journées Nationales de Calcul Formel 2007* organisées par F. Chyzak, O. Ruatta et E. Thomé. Je remercie les organisateurs de cette invitation.

Ce cours, intitulé *Algorithmes efficaces en géométrie algébrique réelle*, traîte de l'étude des solutions réelles des systèmes polynomiaux à coefficients rationnels de *dimension positive* (c'est-à-dire dont le nombre de solutions complexes est infini). L'accent est mis sur les techniques permettant d'obtenir des *algorithmes efficaces en pratique*. Les objets étudiés relèvent de la géométrie algébrique réelle. Il nous reste ici à préciser ce qu'on entend par l'étude des solutions réelles des systèmes polynomiaux de dimension positive et sa traduction en terme de spécification d'algorithmes.

La ou plutôt *les* réponses à cette question proviennent des applications provenant de domaines aussi variés que la reconnaissance de formes, la robotique, la mécanique céleste, la chimie ou la géométrie algorithmique. La question la plus fréquemment posée est de décider du vide de l'ensemble des solutions réelles d'un système d'équations polynomiales, avec ou sans contraintes. En plus de déterminer l'existence de solutions réelles, on peut bien évidemment en demander des approximations numériques ou des informations de nature topologique : décider si des points donnés sont situés sur une même composante connexe du lieu-solution, décrire ces composantes connexes, etc. Une question qui apparaît aussi régulièrement est de déterminer l'existence de solutions réelles *régulières* (c'est-à-dire des solutions réelles au voisinage desquelles le lieu-solution réel est difféomorphe à un sous-espace vectoriel de dimension la dimension du lieu-solution complexe[1]). Nous donnons ci-après des exemples d'applications illustrant ces *spécifications*.

1.1 Plan du cours

Les algorithmes que nous présentons dans ce document ramènent (presque) tous les problèmes étudiés à la résolution de systèmes d'équations polynomiales ayant un nombre fini de solutions complexes et/ou le comptage et l'isolation des solutions réelles d'un polynôme en une variable. Bien qu'il ne soit pas nécessaire de connaître les algorithmes traitant de ces questions pour suivre ce cours, le lecteur pourra avantageusement consulter [21] pour compléter ses connaissances.

Chapitre 2 : Les objets de la géométrie algébrique réelle. Nous introduisons dans ce chapitre les objets géométriques étudiés par les algorithmes présentés plus loin ainsi que leurs propriétés. Les ensembles algébriques réels sont des ensembles de solutions communes à des polynômes à coefficients dans un corps réel clos (dans la suite on travaillera avec $\mathbb{R}$). Les ensembles semi-algébriques sont des unions de solutions réelles de systèmes d'équations et d'inégalités polynomiales à coefficients dans $\mathbb{R}$. On donne ensuite des propriétés de ces objets (notamment leur comportement par projection), une notion de dimension ainsi qu'un théorème de structure, qu'on appelle théorème de trivialité semi-algébrique de Hardt. Les algorithmes que nous étudions dans la suite du document permettent de décider du vide et de calculer au moins un point par composante connexe dans des ensembles algébriques réels ou des ensembles semi-algébriques.

Chapitre 3 : La décomposition cylindrique algébrique. L'algorithme de décomposition cylindrique algébrique décompose les ensembles semi-algébriques de $\mathbb{R}^n$ en un nombre fini de cellules homéomorphes à $]0,1[^i$ (pour $i \in \{0,\ldots,n\}$). Le fait qu'une telle décomposition existe est directement corrélé au théorème de trivialité semi-algébrique de Hardt, la décomposition cylindrique algébrique en étant en quelque sorte une version effective. Cet algorithme commence par projeter dans $\mathbb{R}^{n-1}$ les semi-algébriques étudiés et étudie récursivement cette projection en la projetant dans $\mathbb{R}^{n-2}$ et ainsi de suite. La sortie de cet algorithme est un ensemble de points représentatifs de chacune des cellules (sur lesquelles les polynômes donnés en entrée et définissant le semi-algébrique étudié sont de signe constant). Chaque cellule est obtenue en découpant des cylindres construits au-dessus de semi-algébriques de $\mathbb{R}^{n-1}$ homéomorphes à des pavés, par des graphes de fonctions semi-algébriques continues. Ces derniers sont obtenus de manière similaire en découpant des cylindres construits au-dessus de semi-algébriques connexes vivant dans $\mathbb{R}^{n-2}$ et ainsi de suite. La sortie de cet algorithme est très forte : elle permet de déterminer toutes les conditions de signe satisfaites par une famille de polynômes donnée en entrée et de calculer au moins un point dans

[1] Nous préciserons le sens donné à ces notions de dimension.

chaque composante connexe des semi-algébriques ainsi définis. Un post-traitement permet aussi de décrire la topologie des semi-algébriques étudiés. Enfin, à quelques modifications près, cet algorithme résoud le problème d'élimination des quantificateurs dans une formule du premier ordre. Malheureusement, tout ceci se paie par une complexité doublement exponentielle en le nombre de variables dont on verra qu'elle est incontournable dès qu'on veut résoudre le probléme d'élimination des quantificateurs d'une part, et qu'elle est inhérente au procédé récursif de projection mis en œuvre dans cet algorithme d'autre part.

Chapitre 4 : Applications polynomiales, lieux critiques, et topologie. Afin d'éviter le procédé récursif de projection mis en œuvre dans la décomposition cylindrique algébrique, on considère les *lieux critiques d'applications polynomiales* restreintes à des variétés algébriques. Ces lieux sont les ensembles de points où la différentielle de l'application n'est pas surjective. L'image d'un point critique par l'application considérée est appelée valeur critique. Le théorème de Sard énonce que l'ensemble des valeurs critiques d'une application polynomiale est contenue dans un fermé de Zariski de l'espace d'arrivée. La définition même de points critiques et quelques résultats supplémentaires que nous donnons nous dit qu'en un point *générique* de l'espace d'arrivée on peut appliquer localement le théorème des fonctions implicites. Ceci n'est malheureusement pas suffisant pour obtenir un théorème de structure global garantissant des propriétés d'invariance topologique similaire à ce qui est énoncé par le théorème de trivialité semi-algébrique de Hardt. La notion de *propreté* d'une application polynomiale permet d'obtenir un énoncé similaire à celui de Hardt si l'application considérée est restreinte à une variété lisse. Pour aller au-delà, on doit étendre la notion de valeur critique en une notion de *valeur critique généralisée*. Nous étudions donc ces notions dans le cas d'applications polynomiales de $\mathbb{C}^n$ dans $\mathbb{C}$ puis dans le cas d'applications polynomiales restreintes à des variétés algébriques lisses et équi-dimensionnelles. Enfin, nous donnons des bornes sur les degrés des lieux critiques et des valeurs critiques généralisées : on constatera que celles-ci sont simplement exponentielles en le nombre de variables. Ces objets constituent donc de bons outils pour espérer obtenir des algorithmes permettant d'étudier des variétés algébriques réelles ou des ensembles semi-algébriques de complexité simplement exponentielle en le nombre de variables.

Chapitre 5 : Test du vide et calcul d'au moins un point par composante connexe d'une variété algébrique réelle. Les algorithmes que nous présentons dans ce chapitre permettent de tester le vide et donner au moins un point par composante connexe de l'ensemble des solutions réelles d'un systèmes d'équations polynomiales à coefficients rationnels. Les sorties de ces algorithmes sont des paramétrisations rationnelles encodant des ensembles finis de solutions complexes de systèmes d'équations. Ces algorithmes sont fondés sur des calculs de points critiques d'applications polynomiales restreintes aux variétés algébriques réelles étudiées et on verra que pour certains d'entre eux, leur complexité est polynomiale en D^n où D borne les degrés des polynômes donnés en entrée et n est le nombre de variables. Ils permettent d'obtenir des implantations permettant de résoudre des problèmes largement inatteignables par l'algorithme de décomposition cylindrique algébrique. La technique consiste à exhiber des applications polynomiales (projections ou carrés de la distance euclidienne à un point) atteignant leurs extrema sur chaque composante connexe de la variété étudiée. Ce premier point, lorsque la variété étudiée n'est pas compacte, n'est pas simple et on fait un usage intensif des notions d'applications polynomiales propres et dominantes introduites dans le chapitre précédent. Un deuxième problème se pose avec les caractérisations algébriques des points critiques d'applications polynomiales introduites dans le chapitre précédent : celles-ci sont valables uniquement sous certaines conditions (impliquant qu'il n'y a pas dégénérescence du rang de la jacobienne associée à la famille de polynômes donnés en entrée en chaque point de la variété). Plusieurs stratégies peuvent être mises en œuvre : certaines sont récursives et étudient des lieux singuliers imbriqués les uns dans les autres. D'autres simulent des déformations infinitésimales sur le système d'équations donné en entrée. Ce sont ces dernières qui permettent d'obtenir les résultats les plus intéressants en pratique.

Chapitre 6 : Test du vide et calcul d'au moins un point par composante connexe d'un ensemble semi-algébrique. Ce chapitre aborde le problème du calcul d'au moins un point par composante connexe d'un ensemble semi-algébrique défini par un système d'équations et d'inégalités polynomiales. Les algorithmes permettant d'effectuer de tels calculs et qui sont fondés sur la méthode des points critiques réduisent le problème initial au calcul d'au moins un point par composante connexe d'une famille d'ensembles algébriques réels. Historiquement, ces ensembles algébriques réels sont obtenus en procédant

à des déformations infinitésimales des polynômes donnés en entrée. L'introduction l'introduction de ces infinitésimaux par des rationnels après avoir effectuer un pré-calcul de valeurs critiques généralisées de certaines applications polynomiales (notion introduite dans le chapitre 4). On donne donc des algorithmes de calcul de valeurs critiques généralisées, puis on montre comment les utiliser pour calculer au moins un point par composante connexe d'un ensemble semi-algébrique.

1.2 Applications

Les applications de la géométrie algébrique réelle sont nombreuses et variées. Les algorithmes présentés dans ce cours permettent de tester le vide et donner au moins un point par composante connexe dans un ensemble algébrique réel ou un ensemble semi-algébrique. De tels algorithmes trouvent des applications dans des problémes de reconnaissance de formes, en analyse numérique, en géométrie algorithmique ou encore dans la résolution des systèmes polynomiaux paramétrés qui s'applique elle aussi à des problémes de robotique mécanique céleste, etc. Les applications que nous présentons ci-dessous illustrent l'utilité des algorithmes présentés dans ce document et ont déjà été traîtées plus ou moins partiellement mais cette liste n'est évidemment pas exhaustive.

Enfin, mentionnons qu'on trouve aussi couramment des problèmes se ramenant à des problèmes de connexité ou de topologie en géométrie algébrique réelle (notamment en planification de trajectoire avec des problèmes du type du déménageur de piano). Les algorithmes nécessaires à leur résolution sortant du cadre de ce cours, nous ne décrivons pas ce type d'applications dans la suite.

Problème de reconnaissance des formes. Soit $\mathcal{P}$ et $\mathcal{Q}$ deux objets géométriques d'un espace euclidien E, muni d'une fonction distance d sur de tels objets, et G un groupe de transformations. Étant donné un réel positif ε, le problème classique de reconnaissance de formes (*pattern-matching* en anglais) est de décider si il existe une transformation $g \in G$ tel que $d(\mathcal{P}, g\mathcal{Q}) < \varepsilon$.

Pour décrire le problème spécifique qui est étudié dans [91], on introduit les notations et définitions ci-dessous. Considérons une courbe polygonale $\mathcal{P}$ définie comme une fonction de $\{0, \ldots, m\}$ vers $\mathbb{R}^3$ telle que $\mathcal{P}(i) = p_i$ est le i-ième sommet de $\mathcal{P}$. On note $Mon(X, Y)$ l'ensemble de toutes les applications surjectives non strictement croissantes d'un ensemble X vers un ensemble Y, oú X et Y sont des sous-ensembles finis de $\mathbb{N}$. On utilise ces applications pour réindexer les sommets des courbes polygonales qu'on consière. De plus, si k et ℓ sont deux entiers avec $\ell \leqslant k$, l'ensemble $\{\ell, \ell+1, \ldots, k-1, k\}$ est noté $[\ell : k]$.

La distance discrète de Fréchet entre deux courbes polygonales $\mathcal{P}$ et $\mathcal{Q}$ est :

$$d_F(\mathcal{P}, \mathcal{Q}) = \min_{(\gamma,\lambda)} ||\mathcal{P} \circ \gamma - \mathcal{Q} \circ \lambda||_\infty$$

où les couples (γ, λ) parcourent $Mon_{m,n} = Mon([1 : m+n], [0 : m]) \times Mon([1 : m+n], [0 : n])$.
Dans la situation qui nous intéresse, $\mathcal{P}$ et $\mathcal{Q}$ sont des courbes polygonales de $\mathbb{R}^3$ representées par une liste de leur sommet, la distance que nous considérons est la distance discrète de Fréchet et $G = SO(3, \mathbb{R})$ est le groupe des rotations de $\mathbb{R}^3$. Notre problème ici est de décider si $G(\mathcal{P}, \mathcal{Q}, \varepsilon, d_F)$, l'ensemble de tous les éléments g de G tel que $d_F(\mathcal{P}, g\mathcal{Q}) \leqslant \varepsilon$, est vide. Afin de réduire la manipulation des courbes polygonales à la manipulation des sommets de ces courbes, on définit l'ensemble de (G, ε)-transporteur associé aux points p et q dans $\mathbb{R}^3$ comme

$$\tau_{p,q}^{G,\varepsilon} = \{g \in G \mid ||p - gq|| \leqslant \varepsilon\}$$

Dans [107, 106], les auteurs prouvent la relation suivante :

$$G(\mathcal{P}, \mathcal{Q}, \varepsilon, d_F) = \bigcup_{(\gamma,\lambda) \in Mon_{m,n}} \bigcap_{s \in [1:m+n]} \tau_{p_{\gamma(s)}, q_{\lambda(s)}}^{G,\varepsilon}$$

Décider le vide de $G(\mathcal{P}, \mathcal{Q}, \varepsilon, d_F)$ est donc équivalent à décider le vide de

$$\bigcap_{s \in [1:m+n]} \tau_{p_{\gamma(s)}, q_{\lambda(s)}}^{G,\varepsilon}$$

pour chaque γ, λ dans $Mon_{m,n}$.

Polynômes transporteurs. Il nous faut maintenant décrire $\tau^{G,\varepsilon}_{p_{\gamma(s)},q_{\lambda(s)}}$ à l'aide de polynômes. Pour ce faire, le groupe $SO(3,\mathbb{R})$ est paramétrisé par les *quaternions unitaires*. Plus précisément, on utilise l'application suivante :

$$\begin{array}{ccc} \mathbb{R}^3 & \rightarrow & \mathbb{H} \\ (x,y,z) & \mapsto & (1,x,y,z) \end{array}$$

La matrice de rotation $g_{(w,x,y,z)}$ est alors :

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & w^2+x^2-y^2-z^2 & 2xy-2wz & 2xz+2wy \\ 0 & 2xy+2wz & w^2-x^2+y^2-z^2 & 2yz-2wx \\ 0 & 2xz-2wy & 2yz+2wx & w^2-x^2-y^2+z^2 \end{bmatrix}$$

Un $(SO(3,\mathbb{R}),\varepsilon)$-polynôme transporteur pour p et q est calculé comme suit :

$$g^{\varepsilon}_{p,q} = \varepsilon^2 - ||(1,p_x,p_y,p_z) - g_{(w,x,y,z)}(1,q_x,q_y,q_z)||^2$$

où ε, (p_x,p_y,p_z), et (q_x,q_y,q_z) sont des rationnels. Ceci nous amène à considérer le système d'équations et d'inégalités polynomiales en 4 inconnues ci-dessous :

$$w^2+x^2+y^2+z^2 = 1,\ g^{\varepsilon}_{p_{\gamma(1)},q_{\lambda(1)}} \geqslant 0,\ \ldots,\ g^{\varepsilon}_{p_{\gamma(m+n)},q_{\lambda(m+n)}} \geqslant 0$$

pour chaque γ,λ dans $Mon_{m,n}$. D'autres paramétrisations de $SO(3,\mathbb{R})$ peuvent être utilisées. Par exemple, une rotation autour d'un vecteur u peut être décrite comme la composée de trois rotations autour des axes x, y, et z. Dans ce cas, la matrice associée à la rotation qu'on considère est la suivante :

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos\theta_y\cos\theta_z & -\cos\theta_y\sin\theta_z & \sin\theta_y \\ 0 & \sin\theta_x\sin\theta_y\cos\theta_z+\cos\theta_x\sin\theta_z & -\sin\theta_x\sin\theta_y\sin\theta_z+\cos\theta_x\cos\theta_z & -\sin\theta_x\cos\theta_y \\ 0 & -\cos\theta_x\sin\theta_y\cos\theta_z+\sin\theta_x\sin\theta_z & \cos\theta_x\sin\theta_y\sin\theta_z+\sin\theta_x\cos\theta_z & \cos\theta_x\cos\theta_y \end{bmatrix}$$

avec comme contrainte $\cos\theta_x^2+\sin\theta_x^2=1$, $\cos\theta_y^2+\sin\theta_y^2=1$, et $\cos\theta_z^2+\sin\theta_z^2=1$.

Autres groupes de transformation. On peut considérer aussi d'autres groupes de transformation, le tableau suivant donne les matrices et les contraintes utilisées pour représenter les translations et les homothéties et de manière plus générales les isomorphismes.

	Translation	Homothétie	Isomorphisme
Matrice	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ b & 0 & 1 & 0 \\ c & 0 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \lambda_x & 0 & 0 \\ 0 & 0 & \lambda_y & 0 \\ 0 & 0 & 0 & \lambda_z \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & x_{1,1} & x_{1,2} & x_{1,3} \\ 0 & x_{2,1} & x_{2,2} & x_{2,3} \\ 0 & x_{3,1} & x_{3,2} & x_{3,3} \end{bmatrix}$
Contraintes		$\lambda_x\lambda_y\lambda_z\Lambda = 1$	$det(M)D = 1$

Ces transformations peuvent être combinées et plusieurs systèmes d'équations et d'inégalités non-strictes peuvent ainsi être engendrés. Il s'agit alors de décider du vide de leur lieu-solution réel.

Problème d'interpolation de Birkhoff. Le problème qui consiste à interpoler une fonction inconnue $f : \mathbb{R} \longrightarrow \mathbb{R}$ par un polynôme univarié en connaissant les valeurs de f et de certaines de ses dérivées en des points de $\mathbb{R}$ est un problème classique d'analyse numérique et en théorie de l'approximation.

Deux cas d'interpolation classiques ont été étudiés et résolus : il s'agit de la formule d'interpolation de Lagrange et du problème d'interpolation de Hermite. Dans le premier cas, les valeurs de f en les points $x_0 < \ldots < x_n$ sont connues et la formule d'interpolation de Lagrange montre l'existence d'un unique polynôme de degré inférieur ou égal à n interpolant f en les x_i.

Le problème d'interpolation de Hermite généralise le cas précédent en incluant des informations sur les dérivées de f. Soit $x_1 < \ldots < x_n$ des points donnés et $\nu_1,\ldots,\nu_n$ des entiers positifs : le problème d'interpolation de Hermite est résolu en prouvant qu'il existe un unique polynôme P de degré inférieur

ou égale à $\nu_1 + \ldots + \nu_n - 1$ tel que pour tous $k \in \{1, \ldots, n\}$ et $j \in \{0, \ldots, \nu_k - 1\}$ l'égalité suivante est vérifiée :

$$f^{(j)}(x_k) = P^{(j)}(x_k).$$

Les problèmes d'interpolation peuvent être présentés de manière générale en décrivant les conditions d'interpolation en termes de *matrices d'incidence* : de telles matrices contiennent l'information connue sur f.

Définition 1. *Soit n et r deux entiers tels que $n \geqslant 1$ et $r \geqslant 0$. La matrice*

$$\mathcal{E} = \begin{pmatrix} e_{1,0} & \ldots & e_{1,r} \\ \vdots & & \vdots \\ e_{n,0} & \ldots & e_{n,r} \end{pmatrix}$$

est appelée matrice d'incidence si $e_{i,j} \in \{0, 1\}$ pour tout couple (i, j).

Pour une matrice d'incidence, on note $|\mathcal{E}|$ le nombre de 1 dans $\mathcal{E}$:

$$|\mathcal{E}| = \sum_{i,j} e_{i,j}$$

Dans le cas où $|\mathcal{E}|$ est égal au nombre de colonnes dans $\mathcal{E}$, on dira que $\mathcal{E}$ est une *matrice d'incidence normale*.

Soit $\chi = \{x_1, \ldots, x_n\}$ un ensemble de nombres réels tels que $x_1 < \ldots < x_n$ et $\mathcal{F}$ une matrice de nombres réels donnés ayant le même nombre de rangées et de colonnes que $\mathcal{E}$ et dont on notera les éléments $f_{i,j}$. Le problème de déterminer un polynôme P dans $\mathbb{R}[x_1, \ldots, x_n]$ de degré plus petit que r qui interpole $\mathcal{F}$ en $(\chi, \mathcal{E})$ c'est-à-dire qui vérifie les conditions :

$$P^{(j)}(x_i) = f_{i,j} \quad \text{ssi} \quad e_{i,j} = 1$$

est connu sous le nom de *problème d'interpolation de Birkhoff* qui est partiellement résolu dans [62] puis dans [121] et est intégralement étudié dans [125].

Définition 2. *Une matrice d'incidence normale $\mathcal{E}$ ayant n rangées et $r + 1$ colonnes est dite* équilibrée *si pour tout choix de noeuds $x_1 < \ldots < x_n$ et d'une matrice $\mathcal{F}$ il existe un unique polynôme P de degré inférieur ou égal à r qui interpole $\mathcal{F}$ en $(\chi, \mathcal{E})$.*

Un premier exemple de matrice d'incidence *équilibrée* est celle qui correspond à la Formule d'Interpolation de Lagrange (avec $r = n - 1$) :

$$\begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 1 & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & 0 & 0 & \ldots & 0 \end{pmatrix}$$

Un second exemple vient du problème d'interpolation de Lagrange : pour tout choix d'entiers positifs $\nu_1, \ldots, \nu_n$, la matrice ayant n rangées et $N = \nu_1 + \ldots + \nu_n$ colonnes telle que dans la i-ième rangée, il y ait ν_i 1 est équilibrée.

Voyons comment déterminer si une matrice d'incidence donnée est équilibrée en utilisant des techniques de Calcul Formel. Ceci revient en particulier à déterminer si un système d'équations linéaires (dont la matrice dépend de plusieurs paramètres qu'on appellera *noeuds*) a une unique solution. Soit $a_0, \ldots, a_r$ les indéterminées et $P_r(x)$ le polynôme générique de degré r

$$P_r(x) = a_r x^r + \cdots + a_0.$$

Alors, une matrice d'incidence $\mathcal{E}$ ayant n rangées et r colonnes est *équilibrée* si pour tout ensemble $\chi = \{x_1, \ldots, x_n\}$ de nombres réels tels que $x_1 < \ldots < x_n$ et pour toute matrice de nombres réels $\mathcal{F}$ (ayant n rangées et $r + 1$ colonnes) le système d'équations :

$$P_r^{(j)}(x_i) = f_{i,j} \quad \text{ssi} \quad e_{i,j} = 1$$

a une unique solution. Dans la suite, on note $\mathcal{M}_\mathcal{E}$ la matrice associée au système linéaire qui caractérise le polynôme d'interpolation de χ et $\mathcal{E}$.
La proposition ci-dessous montre comment on réduit le problème à l'étude des matrices d'incidence normales : les matrices $\mathcal{M}_\mathcal{E}$ à étudier sont toujours des matrices carrées.

Proposition 1. *Soit $\mathcal{E}$ une matrice d'incidence équilibrée ayant n rangées et $r+1$ colonnes. Alors, $\mathcal{E}$ est normale, c'est-à-dire que*

$$|\mathcal{E}| = r + 1.$$

Exemple. *Soit $\mathcal{E}$ la matrice d'incidence normale définie par :*

$$\mathcal{E} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Alors la matrice $\mathcal{M}_\mathcal{E}$ associée à $\mathcal{E}$ est

$$\mathcal{M}_\mathcal{E} = \begin{pmatrix} 1 & x_1 & x_1^2 & x_1^3 & x_1^4 & x_1^5 \\ 1 & x_2 & x_2^2 & x_2^3 & x_2^4 & x_2^5 \\ 0 & 1 & 2x_2 & 3x_2^2 & 4x_2^3 & 5x_2^4 \\ 0 & 1 & 2x_3 & 3x_3^2 & 4x_3^3 & 5x_3^4 \\ 0 & 0 & 2 & 6x_2 & 12x_2^2 & 20x_2^3 \\ 0 & 0 & 0 & 6 & 24x_1 & 60x_1^2 \end{pmatrix}$$

Exemple. *Soit $\mathcal{E}_\mathcal{L}$ la matrice d'incidence normale correspondante à la Formule d'Interpolation de Lagrange*

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}$$

Alors la matrice d'incidence $\mathcal{M}_{\mathcal{E}_\mathcal{L}}$ associée à $\mathcal{E}_\mathcal{L}$ est

$$\mathcal{M}_\mathcal{E} = \begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{pmatrix}$$

Soit $\mathcal{E}_\mathcal{H}$ la matrice d'incidence normale correspondante au problème d'interpolation de Hermite associé à $\nu_1, \dots, \nu_n$ ($N = \nu_1 + \dots + \nu_n$). Alors la matrice $\mathcal{M}_{\mathcal{E}_\mathcal{H}}$ a la structure suivante :

$$\mathcal{M}_{\mathcal{E}_\mathcal{H}} = \begin{pmatrix} \mathcal{P}_1 \\ \mathcal{P}_2 \\ \vdots \\ \mathcal{P}_n \end{pmatrix} \mathcal{P}_j = \left(\frac{\partial^k}{\partial x_j} \begin{bmatrix} 1 & x_j & x_j^2 & x_j^3 & \dots & x_j^{N-1} \end{bmatrix} \right)_{0 \leqslant k \leqslant \nu_k - 1}$$

La proposition réduit le problème de déterminer si une matrice d'incidence normale est équilibrée à un problème d'élimination des quantificateurs sur les réels.

Proposition 2. *Soit $\mathcal{E}$ une matrice d'incidence normale. Alors $\mathcal{E}$ est équilibrée si et seulement si le déterminant de $\mathcal{M}_\mathcal{E}$ ne s'annule pas pour tout ensemble de nombres réels $\chi = \{x_1, \dots, x_n\}$ tels que $x_1 < \dots < x_n$.*

Pour une matrice d'incidence normale $\mathcal{E}$ donnée, on note $\mathcal{D}_\mathcal{E}$ le déterminant de $\mathcal{M}_\mathcal{E}$. D'après la proposition précédente, déterminer si une matrice d'incidence normale $\mathcal{E}$ est équilibrée est un problème qui se réduit à trouver un ensemble de nombres réels $\chi = \{x_1, \dots, x_n\}$ tels que :

$$x_1 < \dots < x_n \quad \text{et} \quad \mathcal{D}_\mathcal{E}(x_1, \dots, x_n) = 0.$$

Simplification du problème. On est alors ramené à décider du vide d'ensembles de points réels définis par une équation et des inégalités polynomiales. On montre maintenant comment obtenir des simplifications spécifiques au problème d'interpolation de Birkhoff en obtenant plus d'informations sur le polynôme $\mathcal{D}_{\mathcal{E}}$.

Proposition 3. *Soit $\mathcal{E}$ une matrice d'incidence normale ayant n rangées et $r+1$ colonnes. Si $\ell_{i,j}$ $(1 \leqslant i < j \leqslant n)$ est le nombre de colonnes dans $\mathcal{E}$ telles que*

$$\mathcal{E}_{i,k} = 1, \quad \text{et} \quad \mathcal{E}_{j,k} = 1$$

alors $(x_i - x_j)^{\ell_{i,j}}$ divise le polynôme $\mathcal{D}_{\mathcal{E}}$.

La proposition ci-dessus montre que l'on peut simplifier le polynôme $\mathcal{D}_{\mathcal{E}}$ en le divisant par $(x_i - x_j)^{\ell_{i,j}}$, mais comme le montre l'exemple ci-dessous $\ell_{i,j}$ n'est pas la puissance maximale de $(x_i - x_j)$ divisant $\mathcal{D}_{\mathcal{E}}$.

Exemple. *Soit $\mathcal{E}$ la matrice d'incidence de l'exemple 1.2. Dans cet exemple le polynôme $\mathcal{D}_{\mathcal{E}}$ se factorise de la manière suivante :*

$$\mathcal{D}_{\mathcal{E}} = -36(x_2 - x_3)^2(x_1 - x_2)^4(6x_1^2 - 12x_1x_3 - x_2^2 + 2x_2x_3 + 5x_3^2).$$

Or, dans ce cas $\ell_{1,2} = 1$ et $\ell_{2,4} = 1$.

Ceci nous amène à introduire l'entier $L_{i,j}$ comme étant la plus grande puissance de $(x_i - x_j)$ qui divise $\mathcal{D}_{\mathcal{E}}$.

Définition 3. *Soit $\mathcal{E}$ une matrice d'incidence normale. L'indicateur d'équilibre de $\mathcal{E}$ est le polynôme à coefficients entiers :*

$$\widetilde{\mathcal{D}}_{\mathcal{E}} = \frac{\mathcal{D}_{\mathcal{E}}}{\prod_{1 \leqslant i < j \leqslant n}(x_j - x_i)^{L_{i,j}}}$$

On peut alors travailler avec l'*indicateur d'équilibre* d'une matrice d'incidence normale $\mathcal{E}$ pour déterminer si celle-ci est équilibrée. Revenons à l'exemple précédent. L'*indicateur d'équilibre* de $\mathcal{E}$ est alors :

$$\widetilde{\mathcal{D}}_{\mathcal{E}} = -36(6x_1^2 - 12x_1x_3 - x_2^2 + 2x_2x_3 + 5x_3^2).$$

Il est facile de voir qu'on a

$$\widetilde{\mathcal{D}}_{\mathcal{E}} = -36(6(x_1 - x_3)^2 - (x_2 - x_3)^2)$$

En effectuant la substitution :

$$x_2 - x_1 = t_1^2 \quad x_3 - x_2 = t_2^2 \Longrightarrow x_3 - x_1 = t_1^2 + t_2^2$$

on obtient

$$\widetilde{\mathcal{D}}_{\mathcal{E}}(t_1, t_2) = -36(5t_1^4 + 12t_1^2t_2^2 + 6t_2^4)$$

ce qui nous permet alors de conclure que $\mathcal{E}$ est équilibrée puisque pour tout $x_1 < x_2 < x_3$ le polynôme $\widetilde{\mathcal{D}}_{\mathcal{E}}$ est strictement négatif (ce qui implique que $\mathcal{D}_{\mathcal{E}}$ est strictement négatif).

Exemple. *Les déterminants des matrices $\mathcal{M}_{\mathcal{E}_{\mathcal{L}}}$ (issus de l'Interpolation de Lagrange) et des matrices $\mathcal{M}_{\mathcal{E}_{\mathcal{H}}}$ (issus de l'Interpolation de Hermite) sont*

$$\mathcal{D}_{\mathcal{E}_{\mathcal{L}}} = \prod_{i<j}(x_j - x_i) \quad \mathcal{D}_{\mathcal{E}_{\mathcal{H}}} = \prod_{k=1}^{n} \prod_{\lambda=0}^{\nu_k - 1} \lambda! \prod_{i<j}(x_j - x_i)^{\nu_j \nu_i}$$

Les indicateurs d'équilibre correspondants sont égaux à des nombres entiers non nuls.

Pour déterminer si une matrice d'incidence normale est équilibrée, on va suivre la méthode appliquée pour résoudre l'exemple 1.2.

Proposition 4. *Soit $\mathcal{E}$ une matrice d'incidence normale ayant n rangées et $r+1$ colonnes et soit $t_1, \ldots, t_{n-1}$ de nouvelles variables. Le polynôme*

$$\mathcal{H}_{\mathcal{E}} = \widetilde{\mathcal{D}}_{\mathcal{E}}(x_1, x_1 + t_1^2, x_1 + t_1^2 + t_2^2, \ldots, x_1 + \sum_{i=1}^{n-1} t_i^2)$$

est un polynôme dans $\mathbb{Z}[t_1, \ldots, t_{n-1}]$.

Proposition 5. *Soit $\mathcal{E}$ une matrice d'incidence normale ayant n rangées et $r+1$ colonnes. Alors le polynôme $\mathcal{H}_{\mathcal{E}}$ est homogène et son degré est strictement borné par $2nr$.*

Corollaire 1. *Soit $\mathcal{E}$ une matrice d'incidence normale. Alors, le polynôme $\mathcal{H}_{\mathcal{E}}$ a des racines réelles $(t_1, \ldots, t_{n-1})$ telles que $t_1 \ldots t_{n-1} \neq 0$ si et seulement si la matrice $\mathcal{E}$ est équilibrée.*

Puisque $\mathcal{H}$ est homogène et puisque on en cherche des solutions réelles dont aucune des coordonnées n'est nulle, le résultat suivant est immédiat.

Corollaire 2. *Soit $\mathcal{E}$ une matrice d'incidence normale. Le polynôme $\mathcal{H}_{\mathcal{E}}$ a des racines réelles de la forme $(1, t_2, \ldots, t_{n-1})$ telles que $t_2 \ldots t_{n-1} \neq 0$ si et seulement si la matrice $\mathcal{E}$ est équilibrée.*

Ainsi, si on fixe n et r la résolution du problème d'interpolation de Birkhoff est équivalente à décider si des hypersurfaces contiennent des points réels dont aucune des coordonnées n'est nulle. Ceci montre d'une part que le problème d'interpolation de Birkhoff pour n et r fixés est *décidable* et permet de donner des bornes de complexité pour ce problème.

Diagramme de Voronoï de trois droites. Le diagramme de Voronoi d'un ensemble d'objets disjoints est une décomposition de l'espace en cellules associées à un unique objet telles que la cellule associée à un objet est constituée de tous les points qui sont plus proches de l'objets associé que de tous les autres. On considère ici le diagramme de Voronoi de 3 droites de $\mathbb{R}^3$.

Soit $\mathcal{L} = \{\ell_1, \ldots, \ell_n\}$ une famille de n droites dans $\mathbb{R}^3$. Chaque droite est donnée par un point p_i et un vecteur v_i. Soit $d(p, \ell_i)$ la distance euclidienne de du point p à la droite ℓ_i. Le diagramme de Voronoi de $\mathcal{L}$, qu'on note $\mathcal{V}(\mathcal{L})$, est défini comme étant la décomposition de $\mathbb{R}^3$ en régions, $V(Q)$, pour tout sous-ensemble non-vide $Q \subsetneq \{\ell_1, \ell_2, \ldots, \ell_n\}$ qu'on définit de la manière suivante :

$$V(Q) = \{p \in \mathbb{R}^3 \mid d(p, \ell_i) = d(p, \ell_j) < d(p, \ell_k),\ \forall \ell_i, \ell_j \in Q,\ \ell_k \notin Q\}$$
$$V(i) = \{p \in \mathbb{R}^3 \mid d(p, \ell_i) < d(p, \ell_j),\ \forall j \neq i\},$$
$$V(i,j) = \{p \in \mathbb{R}^3 \mid d(p, \ell_i) = d(p, \ell_j) < d(p, \ell_k),\ k \notin \{i, j\}\},$$
$$V(i,j,k) = \{p \in \mathbb{R}^3 \mid d(p, \ell_i) = d(p, \ell_j) = d(p, \ell_k) < d(p, \ell_m),\ m \notin \{i, j, k\}\}.$$

On considère ici le diagramme de Voronoi de trois droites, ℓ_1, ℓ_2, et ℓ_3 en *position générale position.* Sans nuire à la généralité, on suppose que ℓ_1 et ℓ_2 sont toutes les deux horizontaleset qu'elles passent respectivement par les points $(0, 0, 1)$ et $(0, 0, -1)$ respectively, et leur vecteur directeur forment respectivement un angle horizontal γ et $-\gamma$ avec le vecteur directeur des abscisses. Plus précisément, on suppose que la droite $\ell_{\mathbf{1}}$ est définie par le point $\mathbf{p_1} = (\mathbf{0}, \mathbf{0}, \mathbf{1})$ et le vecteur $\mathbf{v_1} = (\mathbf{1}, \mathbf{a}, \mathbf{0})$ et que la droite $\ell_{\mathbf{2}}$ par le point point $\mathbf{p_2} = (\mathbf{0}, \mathbf{0}, -\mathbf{1})$ et le vecteur $\mathbf{v_2} = (\mathbf{1}, -\mathbf{a}, \mathbf{0})$, $a \in \mathbb{R}$. De plus, puisque les trois droites ne sont pas toutes parallèles à un même plan, ℓ_3 n'est pas parallèle au plan $z = 0$. Ainsi, on peut supposer que la **droite $\ell_{\mathbf{3}}$ est définie par le point $\mathbf{p_3} = (\mathbf{x}, \mathbf{y}, \mathbf{0})$ et le vecteur $\mathbf{v_3} = (\alpha, \beta, \mathbf{1})$**, avec $x, y, \alpha, \beta \in \mathbb{R}$.

Dans [48], on trouve une preuve du théorème ci-dessous qui caractérise la topologie des cellules du diagramme de Voronoi de trois droites dans $\mathbb{R}^3$:

Théorème 1. *Le trisecteur de 3 droites de $\mathbb{R}^3$ en position générales est constituée de 4 branches infinies lisses de :*

- *soit une courbe quadrique de genre 1*
- *ou l'union d'une droite et de 3 branches d'une skew cubique qui n'intersecte pas cette droite.*

De plus, la cellule du diagramme associée à une droite est constituée de deux composantes connexes bornées respectivement par 3 et 1 de ces branches.

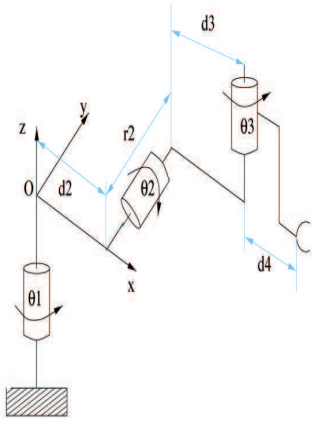

FIG. 1 – Robot cuspidal

Ce résultat a été initialement conjecturé par Koltun et Sharir [79] et a été partiellement obtenu en étudiant un problème classique de géométrie algébrique réelle : décider si un polynôme en plusieurs variables change de signe ou pas.

On note $\mathcal{H}_{i,j}$ le bi-secteur des droites ℓ_i et ℓ_j c'est-à-dire l'ensemble des points équi-distants de ℓ_i et ℓ_j. Dans [79], il est prouvé que $\mathcal{H}_{i,j}$ est un paraboloïde hyperbolique.

Ainsi, le tri-secteur de trois droites est l'intersection de deux paraboloïdes hyperboliques.

L'intersection de deux paraboloïdes hyperboliques peut être singulière ; une quartique nodale ou cuspidale, deux coniques sécantes, une cubique et une droite ou encore une conique et deux droites, etc. On montre que le tri-secteur est toujours non singulier en étudiant le polynôme caractéristique du traceé de $\mathcal{H}_{1,2}$ et $\mathcal{H}_{1,3}$.

Soit $Q_{1,2}$ et $Q_{1,3}$ les représentations matricielles de $\mathcal{H}_{1,2}$ et $\mathcal{H}_{1,3}$, *i.e.* la Hessienne de la forme quadratique associée à la quadrique considérée (voir [45]). On appelle *tracé* de $Q_{1,2}$ et $Q_{1,3}$ l'ensemble des combinaisons linéaires, $P(\lambda) = \{\lambda Q_{1,2} + Q_{1,3},\ \forall \lambda \in \bar{\mathbb{R}}\}$. The *polynôme caractéristique* du tracé est le déterminant, $\mathcal{D}(\lambda) = \det(P(\lambda))$, qui est de degré 4 en λ.

L'intersection de deux quadriques est une quartique non singulière dans $\mathbb{P}^3(\mathbb{C})$, si et seulement si le polynôme caractéristique n'a pas de racines multiples (in $\mathbb{C}$) [137] (voir aussi [46]). Une quartique non singulière de $\mathbb{P}^3(\mathbb{C})$ est, dans $\mathbb{P}^3(\mathbb{R})$, soit vide soit une quartique non singulière. Ainsi, puisque le tri-secteur de trois droites ne peut pas être vide dans $\mathbb{R}^3$, le tri-secteur est une quartique lisse de $\mathbb{P}^3(\mathbb{R})$ si et seulement si l'équation caractéristique du tracé n'a pas de racines multiples.

Ce polynôme caractéristique est plutôt compliqué (son affichage ne tient pas sur une page). Ceci dit, en effectuant le changement de variables $\lambda \to 2\,\lambda\,(1+\alpha^2+\beta^2)$ et en divisant le résultat obtenu par le facteur strictement positif $(1+a^2)^2(1+\alpha^2+\beta^2)^3$, le polynôme obtenu se simplifie en un polynôme qu'on continue de noter $\mathcal{D}(\lambda)$ pour simplifier notre propos.

$$\begin{aligned}\mathcal{D}(\lambda) = &\left(\alpha^2+\beta^2+1\right)a^2\lambda^4 - 2\,a\left(2\,a\beta^2 + a y\beta + a\alpha\,x - \beta\,\alpha + 2\,a + 2\,a\alpha^2 - \beta\,\alpha\,a^2\right)\lambda^3\\ &+\Big(\beta^2 + 6\,a^2\beta^2 - 2\,\beta\,x a^3 - 6\,\beta\,\alpha\,a^3 + 6\,y\beta\,a^2 - 6\,a\beta\,\alpha - 2\,a\beta\,x + 6\,\alpha\,x a^2 + y^2a^2 - 2\,a\alpha\,y + x^2a^2 - 2\,y\alpha\,a^3 + 6\,a^2\alpha^2 + a^4\alpha^2 + 4\,a^2\Big)\\ &\lambda^2 - 2\left(x a - y a^2 - 2\,\beta\,a^2 - \beta + 2\,a\alpha + \alpha\,a^3\right)(x a - y - \beta + a\alpha)\,\lambda + \left(1+a^2\right)(x a - y - \beta + a\alpha)^2 \qquad (1)\end{aligned}$$

On cherche donc à savoir si le discriminant de ce polynôme (par rapport à la variable λ) a des racines réelles qui n'en annulent pas le gradient.

Robots cuspidaux. Dans [40], les auteurs étudient la classification d'une famille de robots série à 3 degrés de liberté dont les articulations sont des liaisons pivots telles que les axes de deux liaisons successives soient orthogonaux comme l'illustre la figure 1.

Ces robots dépendent de paramètres (quatre exactement : r_2, d_3, d_4 et r_3). Dans [47], les auteurs montrent qu'une condition pour qu'un tel robot puisse changer de posture sans rencontrer le lieu singulier

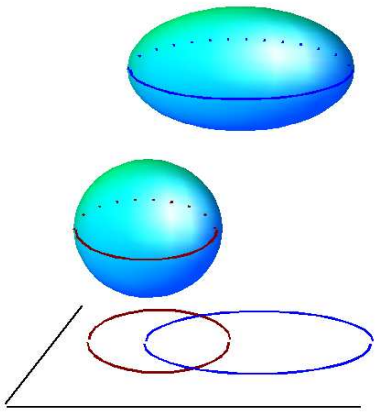

FIG. 2 – Résolution de systèmes paramétrés

de son espace articulaire est liée à l'apparition d'un point de rebroussement dans toute section verticale de son espace de travail. Si cette condition est vérifiée, on a un robot *cuspidal*. Cela se ramène à tester l'existence d'une racine triple d'un polynôme de degré 4. Ce polynôme est évidemment paramétré par r_2, d_3, d_4 et r_3. Dans le cadre d'une étude visant à classifier ces robots, il faut déterminer les paramètres donnant des robots cuspidaux, ce qui revient à résoudre un système à paramètres.

Dans [90], les auteurs donnent une méthode générale permettant de résoudre les systèmes polynomiaux à paramètres. Cette méthode consiste à calculer une *variété discriminante* dans l'espace des paramètres délimitant des zones connexes au-dessus desquelles toutes les fibres de la projection sur l'espace des paramètres sont homéomorphes. Comme l'illustre la figure 2 ceci revient *dans les cas simples* à calculer la projection des endroits en lesquels on ne peut pas appliquer le théorème des fonctions implicites.

Une fois qu'on a obtenu une variété discriminante, pour terminer l'étude, il faut au moins disposer d'au moins un point par composante connexe dans le complémentaire de cette variété.

2 Les objets de la géométrie algébrique réelle

Comme nous l'avons dit en introduction, l'objet de ce cours est l'étude des algorithmes permettant d'étudier les solutions réelles des systèmes d'équations et d'inégalités polynomiales. Les solutions réelles de tels systèmes sont des objets géométriques dont les propriétés sont exploitées par les algorithmes que nous présentons plus loin dans le document. Ce chapitre a pour vocation d'introduire la terminologie associée à de tels lieux-solutions ainsi que leurs propriétés. Les ouvrages [29, 21, 28, 41] ont été intensivement utilisés pour rédiger ce chapitre et contiennent les preuves de la majorité des résultats ci-dessous.

2.1 Les objets de base et leurs propriétés

Définition 4. *Un corps* $\mathbf{R}$ *est* réel *si* $-1 \in \mathbf{R}$ *n'est pas une somme de carrés d'éléments de* $\mathbf{R}$.

On peut montrer que les corps réels sont systématiquement de caractéristique nulle et que les corps ordonnés sont réels.

Les corps réels qui viennent immédiatement à l'esprit sont évidemment $\mathbb{Q}$ et $\mathbb{R}$. Le corps $\mathbb{R}_{\text{alg}}$ des racines réelles de polynômes à coefficients dans $\mathbb{Q}$ est lui aussi réel. Mentionnons aussi qu'étant donné un corps réel $\mathbf{R}$, le corps de séries de Puiseux en la variable ε à coefficients dans $\mathbf{R}$

$$\mathbf{R}\langle\varepsilon\rangle = \{\sum_{i \geqslant i_0} a_i \varepsilon^{i/q} \mid i_0 \in \mathbb{Z},\ q \in \mathbb{N}^\star,\ a_i \in \mathbf{R}\}$$

est lui aussi réel.

Définition 5. *Un corps réel* $\mathbf{R}$ *est* clos *si il est ordonné, tout élément positif de* $\mathbf{R}$ *s'écrit comme somme de carrés d'éléments de* $\mathbf{R}$ *et tout polynôme de* $\mathbf{R}[X]$ *de degré impair a au moins une racine dans* $\mathbf{R}$.

Évidemment $\mathbb{Q}$ n'est pas un corps réel clos, alors que $\mathbb{R}$ et $\mathbb{R}_{\text{alg}}$ le sont. Par ailleurs, si $\mathbf{R}$ est réel clos, alors $\mathbf{R}\langle\varepsilon\rangle$ est lui aussi réel clos. Ainsi, $\mathbb{R}\langle\varepsilon\rangle$ est un corps réel clos. Nous verrons que ce dernier point est important dans le cadre des algorithmes de la géométrie algébrique réelle.

Définition 6. *Soit* $\mathbf{R}$ *un corps réel clos et* $n \in \mathbb{N}^\star$. *Un ensemble inclus dans* $\mathbf{R}^n$ *est algébrique réel s'il existe un système d'équations polynomiales à coefficients dans* $\mathbf{R}$ *dont il est le lieu-solution.*

Du fait que $\mathbf{R}$ soit réel clos, on déduit que tout ensemble algébrique réel peut être défini par une seule équation (on prend la somme des carrés des polynômes du système définissant l'ensemble algébrique réel considéré). Ceci constitue une différence essentielle par rapport au cas algébriquement clos. Ainsi, l'origine est définie tant par $x^2+y^2=0$ que par $x=y=0$. Dans cet exemple, la variété algébrique définie par $x=y=0$ est la plus petite variété algébrique contenant le lieu réel de l'hypersurface définie par $x^2+y^2=0$. Étant donné un ensemble algébrique $\mathcal{E} \subset \mathbb{R}^n$, on appelle *complexifié (ou clôture de Zariski) de* $\mathcal{E}$ la plus petite variété algébrique contenant $\mathcal{E}$. Dans la suite, on considérera les *composantes irréductibles d'une variété algébrique* V comme étant les variétés algébriques associées aux idéaux premiers de l'idéal associé à V (qui est l'ensemble de tous les polynômes qui s'annulent sur V). La dimension de V coïncide avec celle de son idéal associé.

Définition 7. *Soit* $\mathcal{E} \subset \mathbb{R}^n$ *un ensemble algébrique réel,* $\mathcal{V} \subset \mathbb{C}^n$ *son complexifié,* I *l'idéal des polynômes s'annnulant sur* $\mathcal{V}$, *et* $\{f_1, \ldots, f_s\} \subset \mathbb{R}[X_1, \ldots, X_n]$ *un système de générateurs de* I.

La co-dimension de $\mathcal{V}$ *est égale au maximum du rang de la jacobienne de* $(f_1, \ldots, f_s)$

$$\begin{bmatrix} \frac{\partial f_1}{\partial X_1} & \cdots & \frac{\partial f_1}{\partial X_n} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_s}{\partial X_1} & \cdots & \frac{\partial f_s}{\partial X_n} \end{bmatrix}$$

évaluée en les points de $\mathcal{V}$.

La co-dimension de $\mathcal{E}$ *est égale au maximum du rang de la jacobienne de* $(f_1, \ldots, f_s)$ *évaluée en les points de* $\mathcal{E}$.

La co-dimension de $\mathcal{E}$ *est égale à celle de* $\mathcal{V}$.

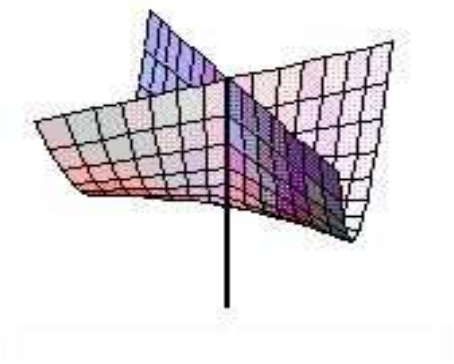

FIG. 3 – Parapluie de Whitney

Si $\mathcal{V}$ est équi-dimensionnelle[2]*, un point de $\mathcal{E}$ est dit régulier si et seulement si le rang de la jacobienne de $(f_1, \ldots, f_s)$ évaluée en ce point est égale à la co-dimension de $\mathcal{E}$.*

Soit $y \in \mathcal{E}$ un point régulier. L'espace co-tangeant à $\mathcal{E}$ en y est le noyau de l'application linéaire définie par la jacobienne de $(f_1, \ldots, f_s)$ évaluée en y.

Dans la définition ci-dessus, le fait que $\mathcal{V}$ soit le complexifié de $\mathcal{E}$ est crucial. L'exemple $x^2 + y^2 = 0$ l'illustre bien. Le complexifié est ici défini par $x = 0, y = 0$. La jacobienne associée à x, y est de rang 2 en l'origine alors que la jacobienne associée à $x^2 + y^2$ est de rang 0 en l'origine. Les exemples de systèmes algébriques n'ayant pas de solution réelle mais ayant des solutions complexes l'illustrent encore mieux.

Remarquons que pour que la définition ci-dessus devienne *effective*, il faut a priori se doter d'un algorithme permettant de calculer le complexifié d'un ensemble algébrique réel. Ceci dit, étant donné une variété algébrique *irréductible* $\mathcal{V} \subset \mathbb{C}^n$, si $\mathcal{V}$ contient un point réel *régulier*, alors $\mathcal{V}$ est le complexifié de $\mathcal{V} \cap \mathbb{R}^n$. Nous verrons dans le chapitre suivant comment la décomposition cylindrique algébrique permet de calculer la dimension d'un ensemble algébrique réel.

Enfin, étant donnée une variété algébrique $\mathcal{V} \subset \mathbb{C}^n$, l'ensemble des points réels réguliers n'est pas dense dans $\mathcal{V} \cap \mathbb{R}^n$ alors que l'ensemble des points réguliers (complexes) est dense dans $\mathcal{V}$. Le parapluie de Whitney est une surface qui illustre bien cela (voir figure 3) : le lieu singulier est constituée d'une droite et, sur une partie (qu'on appelle *manche du parapuie* et qui est une demi-droite) de celle-ci, tout point singulier admet un voisinage ne contenant aucun point régulier du parapluie de Whitney.

La projection d'un ensemble algébrique sur un sous-espace affine n'est pas algébrique mais *constructible* (c'est-à-dire définie par un système d'équations et d'inéquations polynomiales). De la même manière, la projection d'un ensemble algébrique réel n'est pas algébrique réel. Ceci nous amène à considérer des *ensembles semi-algébriques*.

Définition 8. *Soit $\mathbf{R}$ un corps réel clos et $n \in \mathbb{N}^\star$. Un ensemble $\mathcal{S} \subset \mathbf{R}^n$ est* semi-algébrique *si il existe un nombre fini de systèmes d'équations et d'inégalités polynomiales en n variables et à coefficients dans $\mathbf{R}$ tels que $\mathcal{S}$ est l'union de leur lieu-solutions.*

Donnons quelques exemples. Les semi-algébriques de $\mathbb{R}$ sont donc des réunions *finies* d'intervalles et de points. Évidemment, tout ensemble algébrique réel est semi-algébrique. Si $\mathcal{A} \subset \mathbb{R}^n$ et $\mathcal{B} \subset \mathbb{R}^n$ sont semi-algébriques alors $\mathcal{A} \cap \mathcal{B}$ est semi-algébrique. Il en est de même pour l'union de deux semi-algébriques et plus généralement pour toute union *finie* de semi-algébriques. On a aussi que si $\mathcal{A} \subset \mathbb{R}^n$ et $\mathcal{B} \subset \mathbb{R}^k$ sont semi-algébriques alors $\mathcal{A} \times \mathcal{B} \subset \mathbb{R}^n \times \mathbb{R}^k$ est semi-algébrique.

On peut aussi définir les semi-algébriques grâce au langage des *formules du premier ordre*. Une formule du premier ordre est obtenue par les règles suivantes :

- Si $f \in \mathbb{R}[X_1, \ldots, X_n]$ alors $f = 0$ et $f > 0$ sont des formules.
- Si φ et ψ sont des formules, alors $\varphi \wedge \psi$, $\varphi \vee \psi$ et $\neg\varphi$ sont des formules.
- Si φ est une formule, et X une variable réelle, alors $\exists X \varphi$ et $\forall X \varphi$ sont des formules.

[2]au sens où toutes ses composantes irréductibles sont de même dimension.

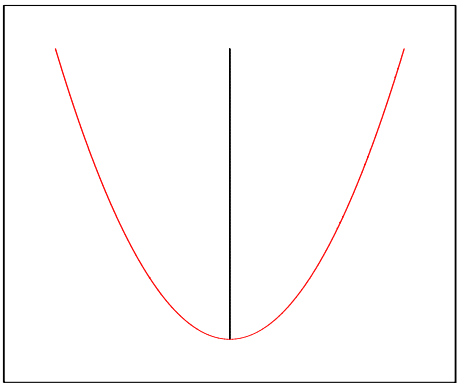

FIG. 4 – Parabole et sa projection

Dans ce cadre, un ensemble $\mathcal{S} \subset \mathbb{R}^n$ est semi-algébrique si et seulement si il existe une formule du premier ordre φ sans quantificateur telle que :

$$(x_1, \ldots, x_n) \in \mathcal{S} \Leftrightarrow \varphi(x_1, \ldots, x_n) \text{ est vraie}$$

C'est ce que montre le Théorème de Tarski-Seidenberg. Il est important car il permet d'aborder les problèmes d'élimination des quantificateurs.

Théorème 2 (Théorème de Tarski-Seidenberg). *Si φ est une formule du premier ordre, l'ensemble des $(x_1, \ldots, x_n) \in \mathbb{R}^n$ qui satisfont $\varphi(x_1, \ldots, x_n)$ est un ensemble semi-algébrique de $\mathbb{R}^n$.*

Ainsi, décrire l'ensemble semi-algébrique $\mathcal{S}$ des points de $\mathbb{R}^n$ qui satisfont une formule du premier ordre donnée φ revient à fournir une formule sans quantificateurs définissant $\mathcal{S}$. C'est ce qu'on appelle communément l'*élimination des quantificateurs*.

Entre autres conséquences importantes du théorème de Tarski-Seidenberg, on a que l'adhérence $\overline{\mathcal{S}}$ d'un semi-algébrique $\mathcal{S} \subset \mathbb{R}^n$ (pour la topologie induite par la norme euclidienne) est semi-algébrique. En effet, on peut exprimer facilement l'appartenance à $\overline{\mathcal{S}}$ par la satisfiabilité d'une formule du premier ordre.

Revenons un instant sur la manière dont on a défini les formules du premier ordre. Le fait que les quantificateurs portent sur des variables réelles est crucial. En effet, considérons le sous-ensemble de $\mathbb{R}^2$

$$\{(x, y) \in \mathbb{R}^2 \mid \exists n \in \mathbb{N} \;\; y = nx\}.$$

Celui-ci n'est pas semi-algébrique. Raisonnons par l'absurde et supposons qu'il soit semi-algébrique. Dans ce cas, son intersection avec la droite définie par $x + y + 1 = 0$, qui est constituée d'une infinité de points est semi-algébrique. La projection de ces points sur l'axe des abscisses est constituée d'une infinité de points et devrait être un semi-algébrique de $\mathbb{R}$. Or, on a vu qu'un semi-algébrique de $\mathbb{R}$ est une réunion *finie* d'intervalles et de points.

Un résultat important concernant les ensembles semi-algébriques est que l'image d'un semi-algébrique est semi-algébrique (c'est une conséquance du théorème de Tarski-Seidenberg). C'est ce qu'énonce la proposition ci-dessous.

Proposition 6. *Soit $k \in \mathbb{N}$, $\Pi : \mathbf{R}^n \to \mathbf{R}^k$ une projection sur un sous-espace affine de $\mathbf{R}^n$ de dimension k, $\mathcal{S}$ un ensemble semi-algébrique et $\mathcal{E}$ un ensemble algébrique réel.*

L'image de $\mathcal{E}$ par Π est semi-algébrique. L'image de $\mathcal{S}$ par Π est semi-algébrique.

Exemple. *Considérons la parabole définie dans $\mathbb{R}^2$ par $y - x^2 = 0$. Il s'agit d'un ensemble algébrique réel. Sa projection sur l'axe des orodonnées est l'ensemble semi-algébrique de $\mathbb{R}$ défini par $y \geqslant 0$ (voir figure 4).*

Si on considère l'hyperbole dans $\mathbb{R}^2$ définie par $xy - 1 = 0$. Sa projection sur l'axe des abscisses est l'ensemble semi-algébrique de $\mathbb{R}$ défini par $x \neq 0$ (voir figure 5).

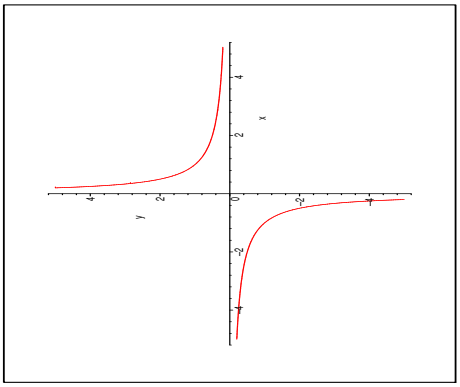

FIG. 5 – Hyperbole et sa projection

La dimension d'un ensemble semi-algébrique $\mathcal{S}$ peut être définie de manière similaire à celle d'un ensemble algébrique réel en considérant le complexifié de $\mathcal{S}$ c'est-à-dire la plus petite variété algébrique $\mathcal{V}$ contenant $\mathcal{S}$.

Définition 9. *La dimension d'un ensemble semi-algébrique $\mathcal{S}$ est égale à celle de son complexifié.*

La dimension vérifie des propriétés évidentes : la dimension d'une union finie de semi-algébriques est le maximum des dimensions des semi-algébriques. La dimension d'un produit cartésien de semi-algébriques est la somme des dimensions des semi-algébriques du produit cartésien. La dimension de l'adhérence d'un semi-algébrique est égale à la dimension du semi-algébrique considéré, et la dimension de sa frontière est inférieure strictement à sa dimension.

2.2 Fonctions semi-algébriques

Définition 10. *Soit $\mathcal{A} \subset \mathbb{R}^n$ et $\mathcal{B} \subset \mathbb{R}^k$ deux semi-algébriques. Une fonction $f : \mathcal{A} \to \mathcal{B}$ est semi-algébrique si et seulement si son graphe est semi-algébrique.*

De telles fonctions sont munies d'importantes propriétés. Ainsi, grâce au théorème de Tarski-Seidenberg, on peut montrer que l'image d'un semi-algébrique par une fonction semi-algébrique est semi-algébrique. Il en est de même pour l'image réciproque. On a aussi que la composée de deux fonctions semi-algébriques est semi-algébrique.

Les exemples de fonctions semi-algébriques ne manquent pas : toute fonction polynomiale (ou rationnelle) d'un semi-algébrique vers un semi-algébrique est semi-algébrique. Plus généralement, toute fonction d'un semi-algébrique $\mathcal{A}$ vers un semi-algébrique $\mathcal{B}$ dont l'image se décrit par une formule du premier ordre est semi-algébrique. En effet, dans ce cas le graphe de f peut être défini par une formule du premier ordre.

Les fonctions semi-algébriques ont un comportement classique vis-à-vis de la dimension. Plus précisément, si $\mathcal{S} \subset \mathbb{R}^n$ est un semi-algébrique, et $f : \mathcal{S} \to \mathbb{R}^k$ une fonction semi-algébrique, alors la dimension de $f(\mathcal{S})$ est inférieure ou égale à celle de $\mathcal{S}$, l'égalité étant assurée si f est injective.

Le résultat ci-dessous, qu'on appelle Inégalité de Lojasiewicz, renseigne sur la croissance comparée de deux fonctions semi-algébriques continues restreintes à un semi-algébrique compact.

Proposition 7. *Soit $\mathcal{S} \subset \mathbb{R}^n$ un ensemble semi-algébrique compact et $f, g : \mathcal{S} \to \mathbb{R}$ deux fonctions semi-algébriques continues telles que :*

$$\{x \in \mathcal{S} \mid f(x) = 0\} \subset \{x \in \mathcal{S} \mid g(x) = 0\}$$

Alors, il existe $N \in \mathbb{N}$ et une constante $C \geqslant 0$ tels que

$$\forall x \in \mathcal{S} \quad |g(x)|^N \leqslant C|f(x)|$$

Du fait de la compacité de $\mathcal{S}$ requise dans l'énoncé ci-dessus, celui-ci est un peu restrictif. Il peut être généralisé comme suit :

Proposition 8. *Soit $\mathcal{S} \subset \mathbb{R}^n$ un ensemble semi-algébrique fermé et $f, g : \mathcal{S} \to \mathbb{R}$ deux fonctions semi-algébriques continues telles que :*

$$\forall x \in \mathcal{S} \quad g(x) = \frac{1}{1+|x|^2} \qquad et \qquad \{x \in \mathcal{S} \mid f(x) = 0\} = \varnothing$$

Alors, il existe $N \in \mathbb{N}$ et une constante $C \geqslant 0$ tels que

$$\forall x \in \mathcal{S} \quad |g(x)|^N \leqslant C|f(x)|$$

Le lemme de sélection des courbes ci-dessous nous dit qu'étant donné un ensemble semi-algébrique $\mathcal{S}$ et un point dans la clôture de $\mathcal{S}$ (pour la topologie euclidienne), on peut construire un chemin semi-algébrique passant par ce point et inclus dans $\mathcal{S}$.

Lemme 1 (Lemme de sélection des courbes). *Soit $\mathcal{S} \subset \mathbb{R}^n$ un ensemble semi-algébrique et $x \in \overline{\mathcal{S}}$. Alors il existe une fonction semi-algébrique $\gamma : [0,1] \to \mathbb{R}^n$ telle que :*
- *$\gamma(0) = x$;*
- *la restriction de γ à $]0,1]$ est continue ;*
- *$\gamma(]0,1]) \subseteq \mathcal{S}$.*

Si on suppose que $\mathcal{S}$ est connexe, le lemme de sélection de courbes nous dit qu'on peut relier par un chemin semi-algébrique n'importe quel point de sa clôture à n'importe quel point de $\mathcal{S}$.

Le résultat ci-dessous, qu'on appelle lemme de sélection des courbes à l'infini, s'obtient par une compactification semi-algébrique de $\mathbb{R}^n$, et le lemme classique de sélection des courbes classique ci-dessus.

Lemme 2 (Lemme de sélection des courbes à l'infini). *Soit $\mathcal{S} \subset \mathbb{R}^n$ un ensemble semi-algébrique et $\varphi : \mathcal{S} \to \mathbb{R}^q$ une fonction semi-algébrique. S'il existe une suite de points $(x_\ell)_{\ell \in \mathbb{N}} \subset \mathcal{S}$ telle que $||x_\ell||$ tend vers l'infini quand ℓ tend vers l'infini et $\varphi(x_\ell)$ tend vers $y \in \mathbb{R}^q$ quand ℓ tend vers l'infini, alors il existe une fonction semi-algébrique continue $\gamma :]0,1[\to \mathbb{R}^n$ telle que :*
- *$||\gamma(t)||$ tend vers l'infini quand t tend vers 1 ;*
- *$\gamma(]0,1[) \subset \mathcal{S}$;*
- *$\varphi(\gamma(t))$ tend vers y quand t tend vers 1.*

On a vu que l'image d'un ensemble semi-algébrique $\mathcal{S} \subset \mathbb{R}^n$ par une fonction semi-algébrique $\varphi : \mathcal{S} \to \mathbb{R}^k$ est semi-algébrique. Le théorème des fonctions implicites donne des informations locales sur la topologie de $\mathcal{S}$ et des fibres de φ. Le théorème des fonctions implicites est valable dans un contexte analytique hors on travaille ici avec des objets définis à l'aide de polynômes. Il est alors naturel de se demander si on peut extraire des informations globales de nature topologique sur $\mathcal{S}$ et les fibres de φ.

Considérons l'exemple du semi-algébrique $\mathcal{S} \subset \mathbb{R}^2$ défini par $x^2 + y^2 - 1 \neq 0$ et prenons comme application la projection π sur l'axe des abscisses (voir Figure 6). L'image de π par $\mathcal{S}$ est $\mathbb{R}$ tout entier. On remarque qu'en partitionnant $\mathbb{R}$ en $]-\infty,-1[$, $\{-1\}$, $]-1,1[$, $\{1\}$, $]1,\infty[$, on a les propriétés suivantes :
- La pré-image de $]-\infty,-1[$ (resp. $]1,\infty[$) est égale (et donc homéomorphe) à $]-\infty,-1[\times\mathbb{R}$ (resp. $]1,\infty[\times\mathbb{R}$) ; remarquons ici que $\mathbb{R}$ est précisément la pré-image par π d'un point de $]-\infty,-1[$ (resp. $]1,\infty[$) ;
- La pré-image de $]-1,1[$ est constituée des trois composantes connexes définies par $x^2+y^2-1 > 0, y < 0$, $x^2+y^2-1 < 0$ et $x^2+y^2-1 > 0, y > 0$; remarquons que la pré-image (qu'on note$F$) par π d'un point de $]-1,1[$ est constituée de deux demi-droites et d'un segment ouvert (évidemment contenues dans les composantes connexes qu'on vient de définir) ; de plus il apparaît que ces composantes connexes sont homéomorphes à $]-1,1[\times F$.

Finalement, sur cet exemple, on a partitionné l'image de $\mathcal{S}$ en cinq composantes connexes $C_1, \ldots, C_5$ telles que les pré-images de ces composantes connexes sont homéomorphes au produit cartésien de C_i et de la pré-image par π d'un point choisi dans C_i (pour $i = 1, \ldots, 5$).

Le théorème ci-dessous, connu sous le nom de théorème de trivialité semi-algébrique de Hardt, montre que ce qu'on vient de voir sur un exemple se généralise complètement. En effet, il montre qu'étant donné un semi-algébrique $\mathcal{S}$ et une fonction semi-algébrique $\varphi : \mathcal{S} \to \mathbb{R}^k$, on peut partitionner l'espace d'arrivée $\mathbb{R}^k$ en un nombre *fini* de sous-ensembles semi-algébriques C_i tels qu'au dessus de chaque C_i, $\mathcal{S}$ est homéomorphe à un produit cartésien $C_i \times F_i$ où F_i est un semi-algébrique de $\mathbb{R}^n$. On dit aussi que $\mathcal{S}$ est trivial au-dessus de chaque C_i. Dans le cas où $\mathcal{S}$ est difféomorphe au produit cartésien $C_i \times F_i$, on dit aussi que φ réalise une fibration localement triviale sur $\mathcal{S} \cap \varphi^{-1}(C_i)$.

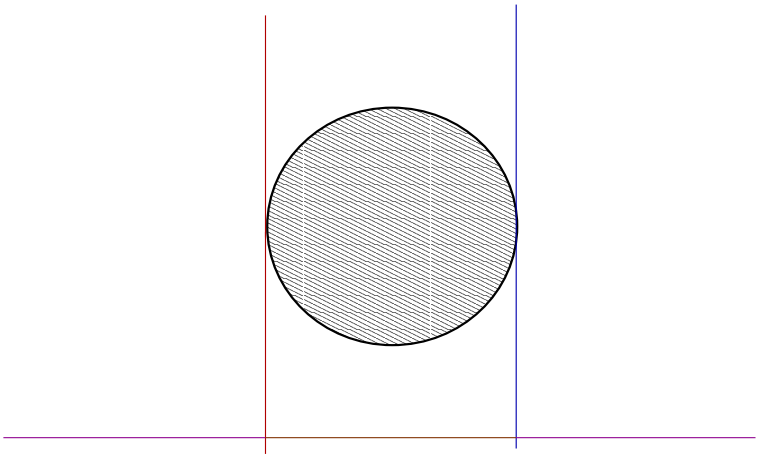

FIG. 6 – Illustration du théorème de Hardt appliqué à $x^2 + y^2 - 1 \neq 0$

Théorème 3. (Trivialité semi-algébrique de Hardt) *Soit $\mathcal{S} \subset \mathbb{R}^n$ un ensemble semi-algébrique et soit $\varphi : \mathcal{S} \to \mathbb{R}^k$ une fonction semi-algébrique continue. Alors, il existe une partition de $\mathbb{R}^k$ en un nombre fini de sous-ensembles semi-algébriques $C_1, \ldots, C_\ell$ et pour tout $i = 1, \ldots, \ell$ un sous ensemble semi-algébrique $F_i \subset \mathbb{R}^n$ et un homéomorphisme $h_i : \varphi^{-1}(C_i) \to C_i \times F_i$ tels que le diagramme suivant commute :*

$$\begin{array}{ccc} \varphi^{-1}(C_i) \subset \mathcal{S} & \xrightarrow{h_i} & C_i \times F_i \\ & \searrow^{\varphi} & \downarrow \pi \\ & & C_i \subset \mathbb{R}^k \end{array}$$

où π est la projection qui envoie $(x, y) \in C_i \times F_i$ sur x.

Les conséquences de ce théorème sont nombreuses. Ce théorème intervient dans la preuve du fait que le nombre de composantes connexes d'un ensemble semi-algébrique est fini.

De plus, si on se donne y et y' dans le même semi-algébrique C_i, alors $\varphi^{-1}(y)$ et $\varphi^{-1}(y')$ sont tous deux semi-algébriquement homéomorphes à F_i et donc semi-algébriquement homéomorphes entre eux. D'ailleurs chaque F_i peut être remplacé par $\varphi^{-1}(y)$ pour un choix quelconque de $y \in C_i$.

Une première conséquence sur la dimension est que si $y \in C_i$,

$$\dim(\varphi^{-1}(y)) = \dim(F_i) = \dim(\varphi^{-1}(C_i)) - \dim(C_i) \leqslant \dim(\mathcal{S}) - \dim(C_i)$$

ce qui permet de montrer que, étant donné $d \in \mathbb{N}$,

$$\{y \in \mathbb{R}^k \mid \dim(\varphi^{-1}(y)) = d\}$$

est un sous-ensemble semi-algébrique de dimension inférieure ou égale à $\dim(\mathcal{S}) - d$.

2.3 Discussion

Nous avons introduit les objets de base de la géométrie algébrique réelle. Du point de vue algorithmique, les premières questions auxquelles on voudrait répondre sont naturellement le test du vide des ensembles algébriques réels ou des semi-algébriques, ainsi que le calcul de la dimension de l'ensemble considéré.

Répondre à de telles questions portant sur un ensemble algébrique $\mathcal{V} \subset \mathbb{C}^n$ se fait en procédant à une réécriture du système polynomial définissant $\mathcal{V}$ (sous une forme triangulaire par exemple). Citons entre autres exemples les algorithmes de calcul de bases de Gröbner [32, 50, 51], d'ensembles triangulaires [88, 76, 152], et de résolution géométrique [61, 94]. Une quantité importante dans ce contexte est le *degré* d'une variété algébrique. Ceci peut être défini comme la somme du nombre de points obtenus quand on intersecte chaque composante équi-dimensionnelle de dimension d de $\mathcal{V}$ avec d hyperplans choisis

génériquement[3]. Ce degré est borné par la borne de Bézout (qui est, dans les cas non surcontraints, le produit des degrés des polynômes du système définissant $\mathcal{V}$). L'algorithme donné dans [94] est polynomial en cette quantité. Dans de nombreux cas, le calcul de bases de Gröbner l'est aussi [83, 84, 67, 16].

Le passage au contexte réel est problématique à plus d'un titre. L'approche la plus naturelle consiste à utiliser la définition de *dimension* d'un semi-algébrique (ou d'un algébrique réel) au pied de la lettre. Mais il faut alors pouvoir calculer le complexifié du semi-algébrique considéré. Rien que dans le cas des algébriques réels, cela revient dans un premier temps à effectuer une décomposition en idéaux premiers de l'idéal engendré par le système donné en entrée. Une fois ceci effectué, il faut tester s'il existe des points réels réguliers, ce qui revient à tester le vide d'un semi-algébrique, etc. Ainsi, le calcul de dimension par l'intermédiaire d'un calcul de complexifié est délicat.

Mentionnons également que la notion de degré des variétés algébriques n'est pas transposable au cas des ensembles algébriques réels. En effet, dans ce cas, pour obtenir un nombre maximal de points réels, nos hyperplans doivent être choisis en dehors d'un semi-algébrique qui est parfois de co-dimension nulle. L'exemple du cercle dans le plan illustre bien cet état de fait dès lors que l'intersection des droites choisies avec l'axe des abscisses n'appartient pas à $]-1,1[$. On pourrait alors vouloir se réfugier derrière le degré du complexifié de l'ensemble algébrique réel considéré. Mais, ce dernier peut être bien supérieur à la borne de Bézout calculée à partir des polynômes définissant la variété qu'on étudie. Le polynôme ci-dessous :

$$\sum_{i=1}^{n} \left(\prod_{j=1}^{D} (X_i - j) \right)^2 = 0$$

qui est de degré $2D$ (c'est ici la borne de Bézout et le degré de l'hypersurface étudiée) illustre bien cela : le lieu-solution réel a un complexifié de degré D^n. De plus, cette dernière quantité est purement algébrique et ne reflètera pas systématiquement la complexité géométrique du lieu-solution réel.

C'est une situation dont il faudra s'accomoder. Les algorithmes que nous allons étudier relèvent du Calcul Formel, ils feront usage d'algorithmes d'élimination algébrique. Pour en mesurer la complexité (ou, à défaut, la taille de la sortie), des quantités purement algébriques interviendront sans que celles-ci reflètent systématiquement la complexité du lieu-solution réel.

Le point de départ est une version *effective* du théorème de trivialité semi-algébrique de Hardt. Nous allons montrer comment décomposer un semi-algébrique $\mathcal{S} \subset \mathbb{R}^n$ en un sous-famille finie de semi-algébriques homéomorphes à des hypercubes $]0,1[^d$ pour $d = 1, \ldots, n$. Ceci revient à construire ce que nous appellerons une décomposition cylindrique algébrique. Pour ce faire, nous remplacerons φ dans l'enoncé du théorome de trivialité par une projection sur un sous-espace affine de dimension $n-1$ et raisonnerons par récurrence sur chacun des $C_i \subset \mathbb{R}^{n-1}$ en appliquant toujours le même théroème mais avec une projection sur un sous-espace affine de dimension $n-2$, etc. Ceci nous permettra de décrire complètement la topologie d'un ensemble semi-algébrique et donc d'en tester le vide, d'en donner la dimension, d'en exhiber au moins un point par composante connexe, etc.

[3] Il existe un fermé de Zariski tel que pour tout choix d'hyperplans effectués en dehors de ce fermé, ce nombre de points obtenus à l'intersection est constant est maximal

3 Décomposition Cylindrique Algébrique

Ce chapitre est consacré à l'algorithme de décomposition cylindrique algébrique. Comme indiqué plus haut, il s'agit d'obtenir une version effective du théorème de trivialité semi-algébrique de Hardt. À quelques modifications près, cet algorithme permet aussi de résoudre le "problème d'élimination des quantificateurs" c'est-à-dire :

- décider si une formule du premier ordre avec quantificateurs est vraie ;
- obtenir une description du semi-algébrique défini par une formule du premier ordre avec quantificateurs (c'est ici que réside véritablement l'"élimination" des quantificateurs).

En ce sens, l'algorithme d'élimination des quantificateurs est aussi une version effective du théorème de Tarski-Seidenberg. C'est pourquoi il est fondamental en géométrie algébrique réelle effective.

Initialement, Tarski propose dans [141] un algorithme résolvant le problème d'élimination des quantificateurs. Néanmoins, la complexité de cet algorithme n'est pas élémentairement récursive. Nous verrons dans ce chapitre que l'algorithme de décomposition cylindrique algébrique est de complexité doublement exponentielle en le nombre de variables. Cette complexité qui peut paraître terrifiante constitue donc une amélioration conséquente du résultat de Tarski. De plus, nous verrons qu'il est illusoire d'espérer une meilleure complexité : le problème d'élimination des quantificateurs est intrinsèquement doublement exponentiel en le nombre de variables.

Dans la suite, nous commençons par définir une décomposition cylindrique adaptée à un ensemble de polynômes en tant qu'objet et indépendamment de tout algorithme. Nous donnons aussi les résultats qui permettent d'en déduire un algorithme calculant une telle décomposition. Dans la seconde section de ce chapitre, nous présentons l'algorithme et abordons les questions algorithmiques soulevées par ses implantations. Puis, nous montrons comment modifier l'algorithme de décomposition cylindrique pour résoudre le problème d'élimination des quantificateurs et expliquons pourquoi ce problème est intrinsèquement doublement exponentiel en le nombre de variables.

3.1 La décomposition cylindrique algébrique en tant qu'objet

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 $1 \leqslant i \leqslant n$, $\mathcal{S}_i$ est une décomposition de $\mathbb{R}^i$ en sous-ensembles semi-algébriques connexes (que nous appellerons *cellules*), ayant les propriétés suivantes :

- a) Toute cellule $S \in \mathcal{S}_1$ est soit un point soit un intervalle ouvert.
- b) Pour tout $1 \leqslant i \leqslant n$ et toute cellule $S \in \mathcal{S}_i$, il existe un nombre fini de fonctions semi-algébriques continues

$$\xi_{S,1} < \ldots < \xi_{S,\ell_S} \ : \ S \longrightarrow R$$

telles que le cylindre $S \times \mathbb{R}$ est l'union disjointe de cellules de $\mathcal{S}_{i+1}$ qui sont :

- soit le graphe $\Gamma_{S,j}$ d'une des fonctions $\xi_{S,j}$ pour $j \in \{1, \ldots, \ell_S\}$:

$$\Gamma_{S,j} = \{(x', x_{j+1}) \in S \times R \mid x_{j+1} = \xi_{S,j}(x')\}$$

- soit une *bande* $B_{S,j}$ du cylindre borné par les graphes des fonctions $\xi_{S,j}$ et $\xi_{S,j+1}$ pour $j \in \{0, \ldots, \ell_S\}$, où on prend par convention $\xi_{S,0} = -\infty$ et $\xi_{i,\ell_S+1} = +\infty$:

$$B_{S,j} = \{(x', x_{j+1}) \in S \times R \mid \xi_{S,j}(x') < x_{j+1} < \xi_{S,j+1}(x')\}$$

Exemple. *Une décomposition cylindrique algébrique de $\mathbb{R}^2$ est donnée par la suite $\mathcal{S}_1, \mathcal{S}_2$ où :*

- *$\mathcal{S}_1$ est la partition de $\mathbb{R}$ constituée de $]-\infty, -1], \{-1\},]-1, 1[, \{1\},]1, +\infty[$.*
- *$\mathcal{S}_2$ est la partition de $\mathbb{R}^2$ constituée des semi-algébriques connexes $S_1, S_2, S_3, S_4, S_5, S_6, S_7$ où :*
  - *S_1 est l'ensemble des points $\{(x, y) \in \mathbb{R}^2 \mid x \in]-\infty, -1[\}$*
  - *S_2 est la demi-droite $\{(x, y) \in \mathbb{R}^2 \mid x = -1, y < 0\}$*
  - *S_3 est la demi-droite $\{(x, y) \in \mathbb{R}^2 \mid x = -1, y = 0\}$*
  - *S_4 est la demi-droite $\{(x, y) \in \mathbb{R}^2 \mid x = -1, y > 0\}$*
  - *S_5 est l'ensemble des points $\{(x, y) \in \mathbb{R}^2 \mid x \in]-1, 1[\}$*
  - *S_6 est la droite $\{(x, y) \in \mathbb{R}^2 \mid x = 1\}$*
  - *S_7 est l'ensemble des points $\{(x, y) \in \mathbb{R}^2 \mid x \in]1, \infty[\}$*

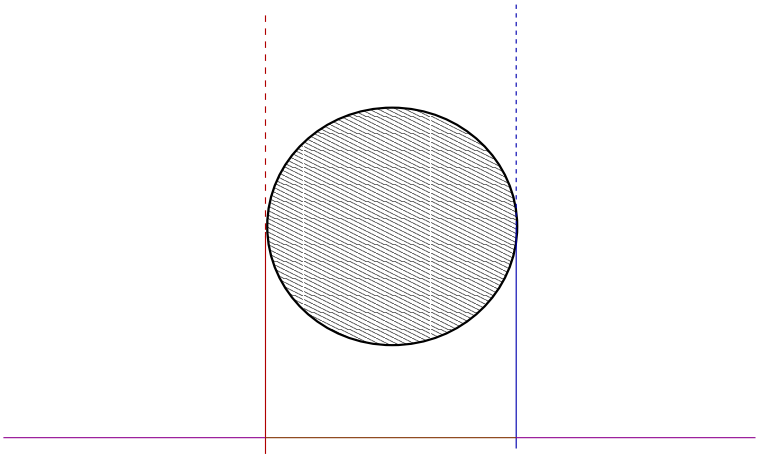

FIG. 7 – Décomposition de $\{x^2 + y^2 - 1\}$-invariante

Dans cet exemple, $S_2 \cup S_3 \cup S_4$ par exemple est le cylindre $\{-1\} \times \mathbb{R}$ (les fonctions ξ qui sont associées à -1 sont $\xi_{\{-1\},0} = -\infty$, $\xi_{\{-1\},1} = 0$ et $\xi_{\{-1\},2} = +\infty$).

Proposition 9. *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 $\mathbb{Q}[X_1, \ldots, X_n]$, 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. Dans la suite de ce chapitre 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. On parlera alors de décomposition cylindrique algébrique $\mathcal{P}$-invariante.

Soit S un ensemble semi-algébrique. Une décomposition cylindrique algébrique adaptée à S est une décomposition cylindrique algébrique de $\mathbb{R}^n$ telle que S est une union finie de cellules de cette décomposition. Il est clair que si $\mathcal{P}$ est une famille de polynômes telle que S est la réalisation d'une formule sans quantificateurs avec atomes dans $\mathcal{P}$, une décomposition cylindrique algébrique adaptée à $\mathcal{P}$ *contient* une décomposition cylindrique algébrique adaptée à S.

Exemple. *Considérons le polynôme $f = x^2+y^2-1 \in \mathbb{Q}[x,y]$ et l'ensemble semi-algébrique $S \subset \mathbb{R}^2$ défini par $f < 0$. Nous allons exhiber une décomposition cylindrique algébrique adaptée à S S en construisant une décomposition cylindrique algébrique $\{f\}$-invariante (voir figure 7).*

Cette dernière est donnée par la suite $\mathcal{S}_1, \mathcal{S}_2$ où :

- *$\mathcal{S}_1$ est la partition de $\mathbb{R}$ constituée de $]-\infty,-1], \{-1\},]-1,1[, \{1\},]1,+\infty[$.*
- *$\mathcal{S}_2$ est la partition de $\mathbb{R}^2$ constituée des semi-algébriques connexes $C_{2,i}$ pour $i = 1, \ldots, 13$ où :*
  - $C_{2,1} = \{(x,y) \in \mathbb{R}^2 \mid x < -1\}$
  - $C_{2,2} = \{(x,y) \in \mathbb{R}^2 \mid x = -1, y < 0\}$
  - $C_{2,3} = \{(x,y) \in \mathbb{R}^2 \mid x = -1, y = 0\}$
  - $C_{2,4} = \{(x,y) \in \mathbb{R}^2 \mid x = -1, y > 0\}$
  - $C_{2,5} = \{(x,y) \in \mathbb{R}^2 \mid -1 < x < 1, x^2 + y^2 - 1 > 0, y < 0\}$
  - $C_{2,6} = \{(x,y) \in \mathbb{R}^2 \mid -1 < x < 1, x^2 + y^2 - 1 = 0, y < 0\}$
  - $C_{2,7} = \{(x,y) \in \mathbb{R}^2 \mid -1 < x < 1, x^2 + y^2 - 1 < 0\}$
  - $C_{2,8} = \{(x,y) \in \mathbb{R}^2 \mid -1 < x < 1, x^2 + y^2 - 1 = 0, y > 0\}$
  - $C_{2,9} = \{(x,y) \in \mathbb{R}^2 \mid -1 < x < 1, x^2 + y^2 - 1 > 0, y > 0\}$
  - $C_{2,10} = \{(x,y) \in \mathbb{R}^2 \mid x = 1, y < 0\}$
  - $C_{2,11} = \{(x,y) \in \mathbb{R}^2 \mid x = 1, y = 0\}$
  - $C_{2,12} = \{(x,y) \in \mathbb{R}^2 \mid x = 1, y > 0\}$
  - $C_{2,13} = \{(x,y) \in \mathbb{R}^2 \mid x > -1\}$

Les semi-algébriques $C_{2,i}$ (pour $i = 1, \ldots, 13$) sont les cellules de notre décomposition cylindrique algébrique qui est $\{f\}$-invariante. Penchons-nous sur le cylindre $]-1,1[\times\mathbb{R}$. Une décomposition cylindrique

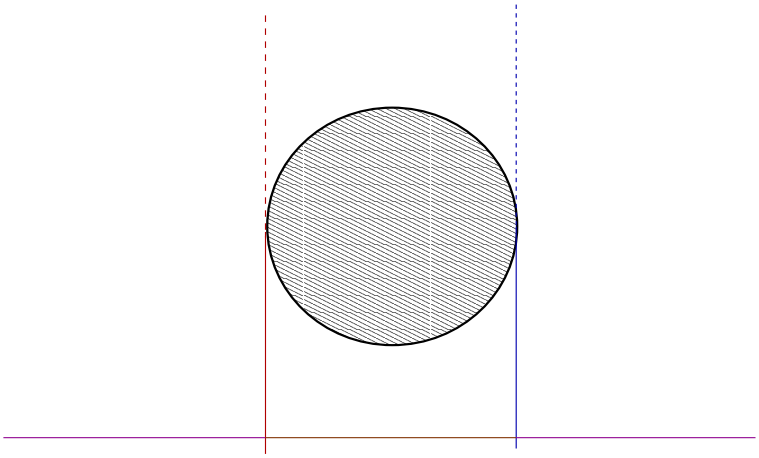

FIG. 8 – Décomposition de $\{x^2+y^2-1\}$-invariante

algébrique adaptée à S est contenue dans celle que nous venons d'exhiber et est constituée de $C_{2,7}$. Il est la réunion des cellules $C_{2,5}, C_{2,6}, C_{2,7}, C_{2,8}$ et $C_{2,9}$. Considérons les fonctions semi-algébriques :

- $\xi_0 : \begin{array}{ccc}]-1,1[& \to & \mathbb{R} \\ x & \mapsto & -\infty \end{array}$
- $\xi_1 : \begin{array}{ccc}]-1,1[& \to & \mathbb{R} \\ x & \mapsto & \sqrt{1-x^2} \end{array}$
- $\xi_2 : \begin{array}{ccc}]-1,1[& \to & \mathbb{R} \\ x & \mapsto & -\sqrt{1-x^2} \end{array}$
- $\xi_3 : \begin{array}{ccc}]-1,1[& \to & \mathbb{R} \\ x & \mapsto & +\infty \end{array}$

On vérifie aisément qu'on a les relations suivantes :

- *$C_{2,5}$ est la bande $\{(x,y) \in \mathbb{R}^2 \mid x \in]-1,1[, \xi_0(x) < y < \xi_1(x)\}$;*
- *$C_{2,6}$ est le graphe $\{(x,y) \in \mathbb{R}^2 \mid x \in]-1,1[, y = \xi_1(x)\}$;*
- *$C_{2,7}$ est la bande $\{(x,y) \in \mathbb{R}^2 \mid x \in]-1,1[, \xi_1(x) < y < \xi_2(x)\}$;*
- *$C_{2,8}$ est le graphe $\{(x,y) \in \mathbb{R}^2 \mid x \in]-1,1[, y = \xi_2(x)\}$;*
- *$C_{2,9}$ est la bande $\{(x,y) \in \mathbb{R}^2 \mid x \in]-1,1[, \xi_2(x) < y < \xi_3(x)\}$;*

Remarquons que les fonctions ξ_1 et ξ_2 associent à x une racine de $x^2+y^2-1=0$ qui évolue continument lorsque x varie. Enfin, notons que la décomposition cylindrique adaptée au semi-algébrique considéré S est constituée ici d'une seule cellule homéomorphe à $\mathbb{R}^2$ et que 2 est la dimension du semi-algébrique considéré.

Savoir construire une décomposition cylindrique algébrique adaptée à un ensemble semi-algébrique permet de répondre à de nombreuses questions. Tout d'abord, il est clair d'après la définition que tout semi-algébrique de $\mathbb{R}^n$ décrit par une combinaison booléenne d'égalités et d'inégalités polynomiales est réunion de certaines cellules d'une décomposition cylindrique algébrique adaptée à la famille constituée de ces polynômes. On peut donc décider du vide, donner au moins un point par composante connexe et *in fine* démonter le semi-algébrique concerné en cellules homéomorphes à des pavés $]0,1[^i$. De plus, l'arrangement cylindrique des cellules permet d'observer que n'importe quel ensemble semi-algébrique S de $\mathbb{R}^p$ décrit par une formule $Q_1 X_{p+1} Q_2 X_{p+2} \cdots Q_n X_{p+n} \Phi$ où quantificateurs $Q_1, \ldots, Q_n$ sont des quantificateurs et Φ une formule du premier ordre sans quantificateurs est une réunion de certaines cellules dans $\mathbb{R}^p$. On voit ici qu'on pourra en déduire une formule du premier ordre sans quantificateurs décrivant S.

Maintenant, voyons comment construire une décomposition cylindrique algébrique adaptée à une famille de polynômes $\{f_1, \ldots, f_s\} \subset \mathbb{Q}[X_1, \ldots, X_n]$. L'exemple donné ci-dessus fait ressortir le rôle crucial joué par les fonctions dont les graphes découpent les cylindres donnant ainsi les cellules de la décomposition cylindrique algébrique qu'on cherche à construire. Ces cellules devant être $\{f_1, \ldots, f_s\}$-invariantes, ces fonctions décrivent, en fonction de $(x_1, \ldots, x_{n-1}) \subset \mathbb{R}^{n-1}$ les racines réelles des polynômes f_i (où les

variables $X_1, \ldots, X_{n-1}$ sont instantiées en $x_1, \ldots, x_{n-1}$). Le résultat ci-dessous est une première étape allant dans ce sens.

Proposition 10. *Soit f un polynôme de $\mathbb{R}[X_1, \ldots, X_n]$, $k \in \mathbb{N}$ et $C \subset \mathbb{R}^{n-1}$ un sous-ensemble semi-algébrique connexe tel que pour tout $a = (a_1, \ldots, a_{n-1}) \in C$, le nombre de racines réelles ou complexes distinctes de $f(a, X_n)$ soit égal à k. Alors, il existe $\ell \leqslant k$ fonctions continues semi-algébriques $\xi_1, \ldots, \xi_\ell : C \to \mathbb{R}$ telles que, pour tout point $a \in C$, l'ensemble des racines réelles de $f(a, X_n)$ soit exactement $\{\xi_1(a), \ldots, \xi_\ell(a)\}$.*

Il faut aussi s'assurer que les racines des f_i ne se mélangent pas :

Proposition 11. *Soit f et g deux polynômes de $\mathbb{R}[X_1, \ldots, X_n]$ et C un sous-ensemble semi-algébrique connexe de $\mathbb{R}^{n-1}$. On suppose que :*

- *le nombre de racines réelles ou complexes distinctes de $g(a, X_n)$ est constant pour $a \in C$;*
- *le nombre de racines réelles ou complexes distinctes de $g(a, X_n)$ est constant pour $a \in C$;*
- *le degré du pgcd de $f(a, X_n)$ et $g(a, X_n)$ est constant pour tout $a \in C$.*

Soit $\xi, \zeta : C \to \mathbb{R}$ deux fonctions semi-algébriques continues telles que $f(a, \xi(a)) = 0$ et $g(a, \zeta(a)) = 0$ pour tout $a \in C$. Alors, pour tout $a \in C$ on a soit $\xi(a) = \zeta(a)$, soit $\xi(a) < \zeta(a)$ soit $\xi(a) > \zeta(a)$.

Ainsi, d'après les deux propositions ci-dessus, étant donné un sous-ensemble semi-algébrique connexe C de $\mathbb{R}^{n-1}$ tel que pour tout $a \in C$, le nombre de racines réelles de chacun des $f_i(a, X_n)$ est constant ainsi que le degré du pgcd de $f_i(a, X_n)$ et de $f_j(a, X_n)$ pour tout $(i, j) \in \{1, \ldots, s\}^2$ (avec $i \neq j$), on sait décrire les cellules d'une décomposition cylindrique algébrique $\{f_1, \ldots, f_s\}$-invariante puisque les fonctions semi-algébriques continues découpant les bandes du cylindre $C \times \mathbb{R}$ décrivent l'évolution des racines réelles $f_i(a, X_n)$ pour tout $i \in \{1, \ldots, s\}$ quand a varie dans C. Ceci constitue l'énoncé du théorème ci-dessous :

Théorème 4. *Soit $\mathcal{P}$ une famille de polynômes dans $\mathbb{R}[X_1, \ldots, X_n]$ et S une composante semi-algébriquement connexe de $\mathbb{R}^{n-1}$ telle que*

- *pour tout $x' \in S$, et pour tout $f \in \mathcal{P}$, le nombre de racines distinctes de $f(x', X_n)$ dans $\mathbb{C}$ et dans $\mathbb{R}$ est constant,*
- *pour tout $x' \in S$, et pour tout $f \in \mathcal{P}$, le degré de $f(x', X_n)$ est constant.*
- *pour tout $x' \in S$, et pour tout couple $(f, g) \in \mathcal{P} \times \mathcal{P}$, le degré du pgcd de $f(x', X_n)$ et de $g(x', X_n)$ est constant.*

Alors, pour tout $f \in \mathcal{P}$, il existe ℓ fonctions semi-algébriques continues $\xi_1, \ldots, \xi_\ell : S \to R$ telles que $\forall x' \in S$, l'ensemble des racines réelles de $f(x', X_n)$ est exactement $\{\xi_1(x'), \ldots, \xi_\ell(x')\}$ et les cellules délimitées par les graphes des ξ_i sont $\mathcal{P}$-invariantes.

Explicitons maintenant le lien entre une décomposition cylindrique algébrique $\mathcal{S}_1, \ldots, \mathcal{S}_{n-1}, \mathcal{S}_n$ (avec $\mathcal{S}_i \subset \mathbb{R}^i$) adaptée à un ensemble semi-algébrique $S \subset \mathbb{R}^n$ et le théorème de trivialité semi-algébrique de Hardt dont nous rappelons l'énoncé ci-dessous : *Soit $\mathcal{S} \subset \mathbb{R}^n$ un ensemble semi-algébrique et soit $\varphi : \mathcal{S} \to \mathbb{R}^k$ une fonction semi-algébrique continue. Alors, il existe une partition de $\mathbb{R}^k$ en un nombre fini de sous-ensembles semi-algébriques $C_1, \ldots, C_\ell$ et pour tout $i = 1, \ldots, \ell$ un sous ensemble semi-algébrique $F_i \subset \mathbb{R}^n$ et un homéomorphisme $h_i : \varphi^{-1}(C_i) \to C_i \times F_i$ tels que le diagramme suivant commute :*

$$\begin{array}{ccc} \varphi^{-1}(C_i) \subset \mathcal{S} & \xrightarrow{h_i} & C_i \times F_i \\ & \searrow^{\varphi} & \downarrow \pi \\ & & C_i \subset \mathbb{R}^k \end{array}$$

où π est la projection qui envoie $(x, y) \in C_i \times F_i$ sur x.

Supposons que dans l'énoncé ci-dessus, φ soit la projection $\Pi : (x_1, \ldots, x_n) \in \mathbb{R}^n \to (x_1, \ldots, x_n)$. On sait alors que l'on peut partitionner $\mathbb{R}^{n-1}$ en sous-ensembles semi-algébriques connexes $C_1, \ldots, C_\ell$ tels que le diagramme de l'énoncé ci-dessus commute. Hors, considérons les cellules de $\mathcal{S}_{n-1} = (C'_1, \ldots, C'_p) \subset \mathbb{R}^{n-1}$. Pour chacune d'entre elles, les cylindres $(C'_i \times \mathbb{R}) \cap \mathcal{S}$ sont semi-algébriquement homéomorphes à $C'_i \times F_i$ où $F_i = \Pi^{-1}(a_i) \cap \mathcal{S}$ avec $a_i \in C'_i$. C'est parce que les cylindres $(C'_i \times \mathbb{R}) \cap \mathcal{S}$ sont réunion de cellules de $\mathcal{S}_n$ et qu'on a un algorithme (voir le paragraphe suivant) calculant $\mathcal{S}_n$ qu'on dit que la décomposition cylindrique algébrique fournit une version effective du théorème de trivialité semi-algébrique de Hardt.

Enfin, mentionnons que le calcul d'une décomposition cylindrique algébrique adaptée un ensemble semi-algébrique permet d'en déduire la dimension.

Proposition 12. *Soit $S \subset \mathbb{R}^n$ un ensemble semi-algébrique et $\mathcal{D} = \{C_1, \ldots, C_k\}$ une décomposition cylindrique algébrique associée à S. Pour toute cellule C_i de $\mathcal{D}$, on note* $\dim(i)$ *la dimension de C_i. On a alors que C_i est homéromorphe à $\mathbb{R}^i$ et que la dimension de S est égale au maximum des dimensions des C_i pour $i = 1, \ldots, k$.*

3.2 L'algorithme de décomposition cylindrique algébrique

On se donne une famille de polynômes $\{f_1, \ldots, f_s\}$ dans $\mathbb{Q}[X_1, \ldots, X_n]$. L'algorithme calculant une décomposition cylindrique algébrique $\{f_1, \ldots, f_s\}$-invariante se divise en deux étapes. La première d'entre elles consiste à calculer récursivement des ensembles de polynômes, dits ensembles de projection, permettant de vérifier les hypothèses des résultats du paragraphe précédent. On part donc d'une famille de polynômes dans $\mathbb{Q}[X_1, \ldots, X_n]$ et on construit des ensembles de polynômes dans $\mathbb{Q}[X_1, \ldots, X_i]$ pour $i = n-1, \ldots, 1$. C'est l'étape dite de projection.

Puis, vient l'étape dite de remontée qui va construire au moins un point par cellule de la décomposition cylindrique algébrique $\{f_1, \ldots, f_s\}$-invariante : pour ce faire, on construit les partitions de $\mathbb{R}^i$ (pour $i = 1, \ldots, n$) en isolant les racines réelles de chacun des polynômes des ensembles de projection dans $\mathbb{Q}[X_1, \ldots, X_i]$ instantiées en des points *représentatifs* des cellules partitionnant $\mathbb{R}^{i-1}$.

Il résulte de cette section le résultat suivant :

Théorème 5. *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 $\mathcal{P}$.*

3.2.1 L'étape de projection

Pour rendre effectif les résultats du paragraphe précédent caractérisant les cellules d'une décomposition cylindrique algébrique $\{f_1, \ldots, f_s\}$-invariante où $f_1, \ldots, f_s$ sont des polynômes de $\mathbb{Q}[X_1, \ldots, X_n]$, on doit, en un certain sens, *contrôler* les degrés des pgcd des couples (f_i, f_j) (pour $i \neq j$) ainsi que le nombre de solutions réelles de chacun des f_i pour diverses instantiations des variables $X_1, \ldots, X_{n-1}$. Ceci peut se faire de diverses manières [98, 96, 97]. Elles mettent toutes en œuvre l'algorithme d'Euclide (ou des variantes). Pour des raisons qu'on ne détaillera pas ici, mais qui relèvent de préoccupations calculatoires (coût de l'arithmétique, croissance de la taille des coefficients) la variante de l'algorithme d'Euclide qu'on utilise calcule les *polynômes sous-résultants* associés à deux polynômes. Cette variante permet d'effectuer les calculs dans l'anneau engendré par les coefficients des deux polynômes considérés tout en gardant un bon contrôle sur la croissance des données.

Considérons donc les polynômes $f = a_0X^d + \cdots + a_dX^d$ et $g = b_0X^d + \cdots + b_eX^e$ avec $a_d \neq 0$ et $b_e \neq 0$. Le résultant de f et g est le déterminant de la matrice de Sylvester ci-dessous (qui est carrée de taille $d+e$).

$$\begin{pmatrix}
a_0 & a_1 & a_2 & \cdots & \cdots & a_d & 0 & & \cdots & 0 \\
0 & a_0 & a_1 & \cdots\cdots & & a_{d-1} & a_d & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & \cdots & \cdots & & 0 & a_0 & a_1 & a_2 & \cdots & a_d \\
b_0 & b_1 & b_2 & \cdots & \cdots & b_{e-1} & b_e & 0 & \cdots & 0 \\
0 & b_0 & b_1 & b_2 & \cdots & \cdots & b_e & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & \cdots & \cdots & 0 & b_0 & b_1 & b_2 & \cdots & \cdots & b_e
\end{pmatrix}$$

Le résultant est nul si et seulement si f et g ont un facteur commun. Pour $0 \leqslant j < \inf(d, e)$, on appelle *coefficient sous-résultant principal* d'ordre j de f et g (qu'on note $\mathrm{CSRes}_j(f, g)$) le mineur de taille $d+e-2j$ de la matrice de Sylvester de f et g obtenu en enlevant les j dernières lignes de coefficients de f, les j dernières lignes de coefficients de g et les $2j$ dernières colonnes.

Proposition 13. *Soit ℓ un entier tel que $0 \leqslant \ell < \inf(d, e)$. Le pgcd de f et g est de degré strictement supérieur à ℓ si et seulement si*

$$\mathrm{CSRes}_0(f, g) = \cdots = \mathrm{CSRes}_\ell(f, g) = 0$$

On a aussi le résultat suivant :

Proposition 14. *Les propriétés suivantes sont équivalentes :*
- *f a r racines distinctes réelles ou complexes*
- $\mathrm{CSRes}_{d-r}(f, \frac{\partial f}{\partial X}) \neq 0$ *et pour* $0 \leqslant \ell < d-r$, *on a* $\mathrm{CSRes}_\ell(f, \frac{\partial f}{\partial X}) = 0$

On sait maintenant calculer le nombre de racines réelles ou complexes distinctes d'un polynôme f ainsi que le degré du pgcd de deux polynômes f et g d'après les signes des coefficients sous-résultants principaux $\mathrm{CSRes}_\ell(f, \frac{\partial f}{\partial X_n})$ et $\mathrm{CSRes}_\ell(f, g)$ tant que les coefficients dominants de f et g ne s'annulent pas. Pour les valeurs des variables $X_1, \ldots, X_{n-1}$ où ces coefficients dominants s'annulent, il faut recalculer les coefficients sous-résultants principaux pour les polynômes tronqués.

Soit f un polynôme de $\mathbb{R}[X_1, \ldots, X_n]$ vu comme un polynôme univarié en X_n à coefficients polynomiaux dans $\mathbb{R}[X_1, \ldots, X_{n-1}]$. On note $\mathrm{Coeff}_i(f)$ le coefficient de X_n^i dans f et $\mathrm{TR}_i(f)$ le polynôme f tronqué aux termes de degré inférieurs ou égaux à i.

En s'inspirant des propositions du paragraphe précédent, on définit alors naturellement un ■opérateur■ de projection $\mathrm{PROJ}(\{f_1, \ldots, f_s\})$ comme étant la liste formée des polynômes en $X_1, \ldots, X_{n-1}$ suivants :
- tous les $\mathrm{Coeff}_i(f_j)$ pour $j \in \{1, \ldots, s\}$ et $i \in \{1, \ldots, \deg(f_j, X_n)\}$;
- tous les $\mathrm{CSRes}_i(\mathrm{TR}_k(f_j), \frac{\partial \mathrm{TR}_k(f_j)}{\partial X_n})$ pour $j \in \{1, \ldots, s\}$, $k \in \{2, \ldots, \deg(f_j, X_n)\}$ et $i \in \{0, \ldots, j\}$;
- tous les $\mathrm{CSRes}_i(\mathrm{TR}_k(f_j), \mathrm{TR}_\ell(f_p))$ pour $(j, p) \in \{1, \ldots, s\}^2$ avec $j \neq p$, $k \in \{2, \ldots, \deg(f_j, X_n)\}$, $\ell \in \{2, \ldots, \deg(f_p, X_n)\}$ et $i \in \{0, \ldots, \inf(k, \ell)\}$.

On a alors le résultat suivant :

Théorème 6. *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 $\xi_1 < \ldots < \xi_\ell : S \to \mathbb{R}$ telles que $\forall x' \in S$, l'ensemble de points $\{\xi_1(x'), \ldots, \xi_\ell(x')\}$ est exactement l'ensemble des racines de réelles de tous les polynômes non nuls $f(x', X_n)$ avec $f \in \mathcal{P}$. Le graphe de chaque fonction ξ_i ainsi que chaque bande du cylindre $S \times \mathbb{R}$ borné par ces graphes, sont des ensembles semi-algébriques semi-algébriquements connexes, et semi-algébriquements 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 $\mathrm{PROJ}(\mathcal{P})$ et S vérifiant les hypothèses du théorème précédent, les cellules de cette décomposition cylindrique algébrique, on voit alors qu'il existe une décomposition cylindrique algébrique de $\mathbb{R}^n$ adaptée à $\mathcal{P}$.
On définit récursivement des sous-ensembles finis de polynômes $\mathcal{P}_i$ tels que :
- $\mathcal{P}_n = \mathcal{P}$,
- Pour tout $i \in \{1, \ldots, n-1\}$, $\mathcal{P}_i = \mathrm{PROJ}(\mathcal{P}_{i+1})$.

Dans le cas où l'ensemble semi-algébrique étudié $S \subset \mathbb{R}^n$ est un ouvert de $\mathbb{R}^n$ (pour la topologie euclidienne), comme c'est le cas par exemple s'il est défini par une combinaison booléenne d'inégalités polynomiales strictes, l'opérateur de projection peut être simplifié. En effet, dans ce cas, tout cellule d'une décomposition cylindrique algébrique adaptée à S est homéomorphe à $]0, 1[^n$. Ceci implique que la construction des cellules au-dessus des $\mathrm{COEFF}_i(f_j)$ est inutile pour $i < \deg(f_j, X_n)$. Il en est de même de tous les coefficients sous-résultants principaux associés à deux polynômes qui ne sont pas le polynôme résultant de ces deux polynômes. Ainsi, on obtient ce qu'on appelle une décomposition cylindrique algébrique *ouverte* en modifiant l'opérateur de projection de manière telle qu'il ne contient plus que :
- tous les $\mathrm{Coeff}_{\deg(f_j, X_n)}(f_j)$ pour $j \in \{1, \ldots, s\}$ et $i = \deg(f_j, X_n)$} ;
- tous les $\mathrm{CSRes}_0(f_j, \frac{\partial f_j}{\partial X_n})$ pour $j \in \{1, \ldots, s\}$;
- tous les $\mathrm{CSRes}_0(f_j, f_p)$ pour $(j, p) \in \{1, \ldots, s\}^2$ avec $j \neq p$.

Dans [103], l'auteur montre que l'opérateur de projection ci-dessus permet aussi d'obtenir une décomposition cylindrique algébrique adaptée à un semi-algébrique S même lorsque celui-ci n'est pas un ouvert de $\mathbb{R}^n$.

3.2.2 L'étape de remontée

Il est alors 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 des polynômes de

$\mathcal{P}_1 : \{\alpha_{1,1}, \ldots, \alpha_{1,s_1}\}$ et donner un point dans chaque intervalle $]\alpha_{1,i}, \alpha_{1,i+1}[$ pour $i \in \{0, \ldots, s_1+1\}$ (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 $\mathcal{S}_1$.

Ceci pose le problème du codage des nombres algébriques réelles et de leur manipulation. En effet, parmi les cellules d'une décomposition cylindrique algébrique adaptée à $\mathcal{S}_1$, on trouve les racines réelles des polynômes de $\mathcal{P}_1$. Schématiquement, ce qu'on veut c'est pouvoir instantier la variable X_1 dans les polynômes de $\mathcal{P}_2$ en chacune de ces racines et calculer les racines réelles des polynômes ainsi obtenus.

Une possibilité est que les coordonnées en X_1, X_2 des points qu'on cherche à construire soient donnés en fonction d'un élément primitif de l'extension de $\mathbb{Q}$ qu'elles engendrent (cet élément primitif étant alors donné par son polynôme minimal et un intervalle à extrémités rationnelles qui l'isole). Une alternative à cette technique qui, en pratique s'avère couteuse, est donnée par le codage à la Thom des nombres algébriques réels. Cette dernière n'est pas plus efficace en pratique mais est utilisable dès lors qu'on travaille sur des corps non-archimédiens. En fait, la plupart des implantations modernes de l'algorithme de décomposition cylindrique algébrique travaillant sur des polynômes à coefficients *rationnels* exploitent la structure *triangulaire* des ensembles de projection ainsi que des techniques d'arithmétique d'intervalle.

Plus précisément, on commence par isoler les racines réelles des polynômes de $\mathcal{P}_1$. Soit donc $I =]\alpha_{1,i}, \alpha_{1,i+1}[$ un tel intervalle (avec extrêmités rationnelles) isolant une racine α_i. Soit f un polynôme de $\mathcal{P}_2$. On cherche alors à donner des intervalles isolant les racines réelles de $f(x, X_2)$ pour tout $x \in I$. Si $f(\alpha, X_2)$ est séparable, et que $\alpha_{i+1} - \alpha_i$ est suffisamment petit, on peut utiliser des variantes de l'algorithme d'Uspensky avec arithmétique d'intervalles pour arriver à nos fins. Si non, il faut calculer la partie séparable de f (quand X_1 est instantiée à α). Ce genre de procédé met en œuvre des calculs de pgcd au-dessus de tours d'extensions algébriques. Un tel processus – qui s'avère être particulièrement technique – peut être itéré pour produire un point dans chaque cellule de la décomposition cylindrique algébrique qu'on cherche à calculer. Le lecteur désirant avoir plus de détails peut se référer à [21].

L'algorithme de décomposition cylindrique de Collins est alors la succession de l'étape de projection et de l'étape de remontée décrites ci-dessus.

On peut extraire d'une décomposition cylindrique algébrique $\mathcal{S}$ adaptée à une famille de polynômes $\mathcal{P}$ une liste de points représentant chaque cellule de $\mathcal{S}$. On a la propriété suivante :

Théorème 7. *Soit $\mathcal{P}$ une famille de polynômes dans $\mathbb{R}[X_1, \ldots, X_n]$ et $\mathcal{S}$ une décomposition cylindrique algébrique adaptée à $\mathcal{P}$. Pour toute condition de signe σ vérifiée par $\mathcal{P}$, on note D_σ une composante semi-algébriquement connexe du lieu des points vérifiant σ. Il existe au moins une cellule de $\mathcal{S}$ telle que tout point de cette cellule est contenue dans D_σ.*

Donc, non seulement l'algorithme de décomposition cylindrique algébrique permet de décider toutes les conditions de signe réalisables simultanément par une famille de polynômes, mais elle permet aussi d'exhiber au moins un point dans chaque composante connexe des semi-algébriques ainsi définis.

3.3 Complexité théorique

On se concentre sur la complexité de l'opérateur de projection.

Soit D le maximum des degrés totaux des polynômes de $\mathcal{P}$. On note s le nombre de polynômes dans $\mathcal{P}$. Par ailleurs, on suppose que la multiplication de polynômes univariés dont le degré est borné par D est log-linéaire en D. Dans PROJ($\mathcal{P}$), on a :

- $s(D-1)$ polynômes de degré maximal $2D^2$ correspondant aux coefficients sous-résultants des polynômes de $\mathcal{P}$ et de leur dérivée par rapport à une variable.
- $\binom{s}{2}(D-1)$ polynômes de degré maximal $2D^2$ correspondant aux coefficients sous-résultants de chaque couple de polynômes dans $\mathcal{P}$.
- $s(D+1)$ polynômes de degré maximal D correspondant aux coefficients de chaque polynôme de $\mathcal{P}$.
- $s(D-1)^2$ polynômes de degré maximal $2D^2$ correspondant aux coefficients sous-résultants des polynômes *tronqués* de $\mathcal{P}$ et de leur dérivée par rapport à une variable.
- $\binom{s(D-1)}{2}(D-1)$ polynômes de degré maximal $2D^2$ correspondant aux coefficients sous-résultants de chaque couple de polynômes *tronqués* dans $\mathcal{P}$.

Donc PROJ($\mathcal{P}$) contient $\mathcal{O}(s^2D^2)$ polynômes de degré maximal $\mathcal{O}(D^2)$. Par ailleurs en utilisant des algorithmes "à la Schönage" pour le calcul des coefficients sous-résultants (voir [96]), ce calcul se fait

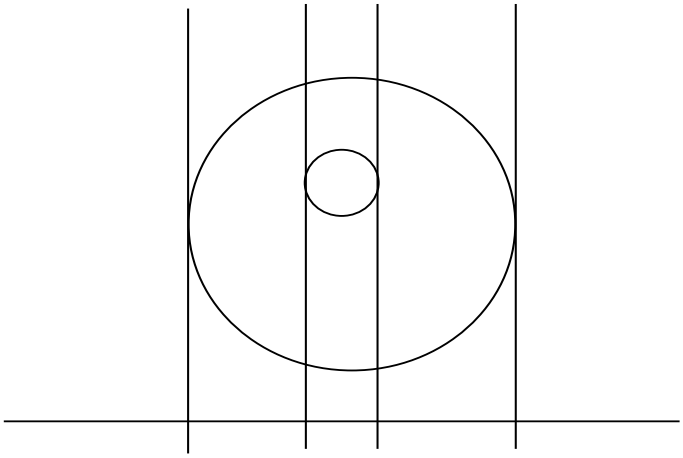

FIG. 9 – Décomposition cylindrique algébrique de deux cercles

en $\mathcal{O}(D \log^2 D \log\log D)$ opérations dans $\mathbb{Q}[X_1, \ldots, X_{n-1}]$. Comme chaque opération arithmétique dans $\mathbb{Q}[X_1, \ldots, X_{n-1}]$ entre des polynômes de degré D a un coût qui est au plus log-linéaire en D^{n-1} et qu'on a $\mathcal{O}(s^2 D)$ calculs de coefficients sous-résultants à effectuer, le coût de la première étape de projection est $\mathcal{O}(s^2 D^{4+(n-1)})$ aux facteurs logarithmiques près. L'ensemble de projection obtenu contient $\mathcal{O}(s^2 D^2)$ polynômes de degré $\mathcal{O}(D)$. Ainsi, si on note

- s_i le nombre de polynômes de l'ensemble de projection $\mathcal{P}_i$ obtenu après i étapes de projection,
- D_i le degré maximal des polynômes de $\mathcal{P}_i$
- et c_i le nombre d'opérations arithmétiques dans $\mathbb{Q}$ effectuées pour calculer $\mathcal{P}_i$

on a les relations suivantes :

$$s_{i+1} = (s_i D_i)^2/2 + s_i^2(D_i - 1) + s_i(D_i - 1), \quad D_{i+1} = 2D_i^2, \quad c_i = \mathcal{O}(s_{i+1}^2 D_i^{2+n-i}) + c_{i-1}$$

On a donc finalement $s_n \leqslant 3^n s^{2^n}/2^n$, $D_n = 2^n D^{2^n}$ et $c_n = \mathcal{O}(n 3^n s^{2^n} D^{n2^n})$

Nous obtenons donc une complexité théorique doublement exponentielle en le nombre de variables. Si on s'était concentré sur la complexité binaire de l'algorithme de décomposition cylindrique algébrique, nous aurions obtenu un résultat similaire. Enfin, les modifications apportées à l'opérateur de projection dans le cas du calcul d'une décomposition cylindrique algébrique ouverte ne changent en rien le caractére doublement exponentiel en le nombre de variables de l'étape de projection.

D'un point de vue pratique, l'algorithme de décomposition cylindrique algébrique 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 cruciale. Les résultats de [117, 116] ont constitué une avancée notable dans ce domaine, mais les problèmes qui restent à résoudre résident dans le nombre de points retournés qui est trop grand d'une part et les calculs de pgcd mentionnés dans la section précédente nécessaire à la remontée.

Ainsi, il arrive très souvent que pour des problèmes de plus de trois ou quatre variables la phase de projection nécessite des ressources que les ordinateurs actuels ne fournissent pas. Même lorsque cette dernière termine, la phase de remontée est aussi bloquante du fait du nombre de points réels qui doivent être manipulés.

3.4 Généralisation à l'élimination des quantificateurs

Nous montrons maintenant comment l'algorithme de décomposition cylindrique algébrique permet de résoudre le *problème d'élimination des quantificateurs*. Étant donnée une formule du premier ordre avec quantificateurs en n variables, le théorème de Tarski nous dit que l'ensemble des points de $\mathbb{R}^n$ qui réalisent cette formule est un ensemble semi-algébrique de $\mathbb{R}^n$. Ce dernier peut donc être décrit par une

formule du premier ordre sans quantificateurs. Trouver une telle formule est ce que nous entendons par la *résolution* du problème d'élimination des quantificateurs.

On considère une famille de polynômes $\mathcal{P}$ dans $\mathbb{Q}[X_1, \ldots, X_n]$ et une décomposition cylindrique algébrique $\mathcal{P}$-invariante ainsi qu'une formule

$$\Phi = (Q_1 X_1) \cdots (Q_n X_n) \varphi(X_1, \ldots, X_n)$$

où φ est une combinaison booléenne d'égalités et d'inégalites polynomiales sans quantificateurs et $Q_i \in \{\exists, \forall\}$ pour $i = 1, \ldots, n$. L'exemple ci-dessous illustre le fait qu'une décomposition cylindrique algébrique $\mathcal{P}$-invariante "classique" n'est pas suffisante pour résoudre le problème d'élimination des quantificateurs.

Exemple. *On considère la famille de polynômes $\mathcal{P} = \{f, g\} \subset \mathbb{Q}[x, y]$ avec $f = y^2 - x(x+1)(x-2)$ et $g = y^2 - (x+2)(x-1)(x-3)$. L'ensemble de projection* $\mathrm{PROJ}(\mathcal{P})$ *calculé par l'algorithme de décomposition cylindrique algébrique – après factorisation – est constitué des polynômes $p_1 = x(x+1)(x-2)$, $p_2 = (x+2)(x-1)(x-3)$ et $p_3 = (x^2 + 3x - 6)^2$. Dans la suite, on note $\{a, b\}$ les deux racines réelles de p_3 (avec $a < b$).*

Les ensembles de solutions de $f = 0$ et de $g = 0$ sont deux cubiques qui ne s'intersectent pas. Considérons maintenant l'ensemble semi-algébrique de $\mathbb{R}$ ainsi défini :

$$\{x \in \mathbb{R} \mid \exists y \in \mathbb{R}, \quad f < 0 \text{ et } g > 0\}$$

qui est égal à $]2, +\infty[$ est bien l'union de composantes connexes d'ensembles semi-algébriques définis par des conditions de signe sur les polynômes de $\mathrm{PROJ}(\mathcal{P})$ *mais ne peut pas être défini comme une formule sans quantificateurs construite uniquement avec ces polynômes. En effet, on a :*

- $\{-1, 0\} = \{x \in \mathbb{R} \mid p_1 = 0 \text{ et } p_2 > 0 \text{ et } p_3 > 0\}$
- $]-1, 0[\cup]3, +\infty[= \{x \in \mathbb{R} \mid p_1 > 0 \text{ et } p_2 > 0 \text{ et } p_3 > 0\}$
- $]-2, -1[\cup]0, 1[= \{x \in \mathbb{R} \mid p_1 < 0 \text{ et } p_2 > 0 \text{ et } p_3 > 0\}$
- $\{3\} = \{x \in \mathbb{R} \mid p_1 > 0 \text{ et } p_2 = 0 \text{ et } p_3 > 0\}$
- $\{-2, 1\} = \{x \in \mathbb{R} \mid p_1 < 0 \text{ et } p_2 = 0 \text{ et } p_3 > 0\}$
- $\{2\} = \{x \in \mathbb{R} \mid p_1 = 0 \text{ et } p_2 < 0 \text{ et } p_3 > 0\}$
- $]2, 3[= \{x \in \mathbb{R} \mid p_1 > 0 \text{ et } p_2 < 0 \text{ et } p_3 > 0\}$
- $]-\infty - 2[\cup]1, 2[\setminus \{a, b\} = \{x \in \mathbb{R} \mid p_1 < 0 \text{ et } p_2 < 0 \text{ et } p_3 > 0\}$
- $\{a, b\} = \{x \in \mathbb{R} \mid p_1 < 0 \text{ et } p_2 < 0 \text{ et } p_3 = 0\}$

Le problème provient du fait que les cellules qu'on construit dans l'algorithme de décomposition cylindrique algébrique (tel que présenté dans les sections précédentes) ne sont pas décrites par des combinaisons booléennes d'égalités et d'inégalités polynomiales des *polynômes calculés par l'opérateur de projection*. Pour accéder à une telle représentation, on doit faire usage du lemme de Thom. Ce résultat indique que si une famille de polynômes univariés est close par différentiation, alors les cellules définies par cette famille de polynômes peuvent être décrites par des conditions de signe sur la famille de polynômes considérée. Dans la suite, si σ est un ensemble de conditions de signe $\{> 0, = 0, < 0\}$ sur une famille de polynômes, on note $\overline{\sigma}$ l'ensemble des conditions de signe en relâchant les conditions de σ (les inégalités strictes sont transformées en inégalités larges). Aussi, on notera $\mathrm{Real}_{\mathcal{P}}(\sigma)$ l'ensemble des points réels qui satisfont les conditions de signe σ portant sur une famille de polynômes $\mathcal{P}$

Lemme 3 (Lemme de Thom). *Soit $\mathcal{P}$ une famille de polynômes dans $\mathbb{R}[X]$ qu'on suppose close par dérivation et σ un ensemble de conditions de signe sur $\mathcal{P}$. Alors,*

- $\mathrm{Real}_{\mathcal{P}}(\sigma)$ *est soit vide, soit un point, soit un intervalle ;*
- *Si* $\mathrm{Real}_{\mathcal{P}}(\sigma)$ *est vide, alors* $\mathrm{Real}_{\mathcal{P}}(\overline{\sigma})$ *est soit vide soit un point.*
- *Si* $\mathrm{Real}_{\mathcal{P}}(\sigma)$ *est un point, alors* $\mathrm{Real}_{\mathcal{P}}(\sigma) = \mathrm{Real}_{\mathcal{P}}(\overline{\sigma})$
- *Si* $\mathrm{Real}_{\mathcal{P}}(\sigma)$ *est un intervalle ouvert alors* $\mathrm{Real}_{\mathcal{P}}(\overline{\sigma})$ *est la clôture de cet intervalle.*

L'utilisation *récursive* de ce lemme permet d'adapter l'opérateur de projection de la décomposition cylindrique algébrique à l'élimination des quantificateurs de la manière suivante :

- Ajouter à l'entrée $\mathcal{P}$ toutes les dérivées partielles des polynômes de $\mathcal{P}$ par rapport à la variable X_n. On obtient l'ensemble $\overline{\mathcal{P}}_n$
- Pour i allant de n à 2 calculer $\mathcal{P}_{i-1} = \mathrm{PROJ}(\overline{\mathcal{P}}_i)$ et poser $\overline{\mathcal{P}_{i-1}} = \{\frac{\partial^k f}{\partial X_i^k} \mid f \in \mathcal{P}_{i-1}, k = 0, \ldots, \deg(f, X_{i-1})\} \cup \mathcal{P}_{i-1}$

L'opérateur de projection étant ainsi modifié, l'algorithme de décomposition cylindrique algébrique permet l'élimination des quantificateurs.

Une analyse de complexité – similaire à celle du paragraphe précédent – de l'algorithme de décomposition cylindrique algébrique modifié comme ci-dessus pour permettre l'élimination des quantificateurs montre que celle-ci est doublement exponentielle en le nombre de variables. Il est naturel ici de se demander si une telle complexité n'est pas inhérente au problème d'élimination des quantificateurs.

Pour ce faire, on doit se donner une notion de *taille* d'une formule du premier ordre. La taille d'une formule atomique ($f = 0$ ou $f < 0$ ou $f > 0$) est le nombre de monômes de f. Puis on définit récursivement la taille d'une formule du premier de la manière suivante :

- la taille de $\varphi_1 \vee \varphi_2$ (resp. $\varphi_1 \wedge \varphi_2$) est égale à $\text{taille}(\varphi_1) + \text{taille}(\varphi_2) + 1$;
- la taille de $\neq \varphi_1$ est $\text{taille}(\varphi_1) + 1$;
- les tailles de $(\exists \varphi_1)$ (ou $\forall X \varphi_1$) valent $\text{taille}(\varphi_1) + 2$.

On va maintenant exhiber un exemple de formule du premier ordre avec quantificateurs telle que toute formule sans quantificateur définissant le même semi-algébrique S est de taille au moins doublement exponentielle en le nombre de variables.

On considère pour cela deux variables complexes $z = x + iy$ et w, et nous construisons récursivement un prédicat $\psi_n(w, z)$ qui n'est vrai que si $w = z^{2^n}$:

$$\begin{array}{lcl} \psi_0(w,z) & := & (w - z^2 = 0) \\ \psi_n(w,z) & := & (\exists u)\ (\forall a\ \forall b)\ \ (((a = w \wedge b = u)\ \vee\ (a = u \vee b = z)) \Rightarrow \psi_{n-1}(a,b)) \end{array}$$

Remarquons que la taille de $\psi_n(w, z)$ évolue linéairement en fonction de n. On définit maintenant $\varphi_n(x, y)$ comme étant la formule ψ_n dans laquelle on a spécialisé w à 1, remplacé z par $x + iy$ et procédé aux identifications entre parties complexes et parties imaginaires. On vérifie aussi que la taille de φ_n évolue linéairement en fonction de n.

On considère maintenant $\theta_n(x, y)$ une formule équivalente à $\varphi_n(x, y)$ sans quantificateurs et $\mathcal{P}_n$ l'ensemble des polynômes apparaissant dans $\mathcal{P}_n$. La taille de θ_n est supérieure à la somme des degrés de ces polynômes. Hors, l'ensemble semi-algébrique défini par θ_n est constitué de 2^{2^n} points isolés (qui correspondent aux 2^{2^n} racines complexes de l'unité). Des résultats dérivés de la théorie de Morse (voir [21]) montrent que le nombre de composantes connexes d'un tel semi-algébrique est bornée par un polynôme en la somme des degrés des polynômes de $\mathcal{P}_n$. Ceci permet alors de montrer que la taille de θ_n est au moins doublement exponentielle en le nombre de variables.

Théorème 8. *La résolution du probléme d'élimination des quantificateurs dans le pire cas est au moins doublement exponentielle en le nombre de variables.*

3.5 Notes bibliographiques et commentaires

L'algorithme de décomposition cylindrique algébrique est dû à Collins [38]. Des implantations de l'algorithme de décomposition cylindrique algébrique (incluant des optimisations des algorithmes présentés dans cette section) sont disponibles soit dans des systèmes de Calcul Formel (tel `Mathematica` [5] ou `Reduce`) [6] soit sous la forme de programmes autonomes. Mentionnons les quatre implantations suivantes :

- `QEPCAD` : programme autonome écrit en `C` et fondé sur la bibliothèque de Calcul Formel `SACLib` est dû initialement à Hoon Hong puis enrichi par de nombreux autres, dont G. Collins. À ma connaissance, ce programme n'a que peu évolué ces dernières années.
- `QEPCAD-B` : programme autonome présenté comme le successeur de `QEPCAD`. Il est écrit en `C++` par C. Brown et contient de nombreuses optimisations (dont des implantations de décomposition cylindrique algébrique *partielle*). Ce programme, ainsi que la `SACLib` sont disponibles à l'URL :
  `http ://www.cs.usna.edu/~qepcad`
- `RLCAD` : il s'agit d'une implantation supervisée par T. Sturm qui est incluse dans le système `Reduce` [6].
  `http ://www.uni-koeln.de/REDUCE/`
- `Mathematica` : il s'agit d'une implantation due à A. Strzebonski. Les fonctionnalités offertes sont assez riches (consulter la documentation pour les détails).

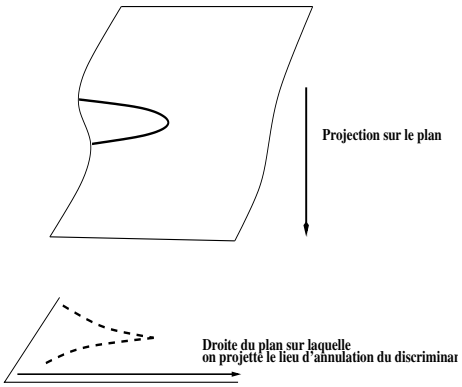

FIG. 10 –

– `CAD` : il s'agit d'un paquetage dû à R. Rioboo fourni initialement dans `ScratchPAD` (ancêtre d'`Axiom` [2]) puis implanté en `Axiom` et en `Aldor` [1]. Ces paquetages bénéficient des avancées concernant la gestion des nombres algébriques réels obtenues par l'auteur en y intégrant les techniques de calcul d'évaluation dynamique à la D5 [44].

La donnée d'une décomposition cylindrique algébrique $\mathcal{P}$-invariante (où $\mathcal{P}$ est une famille de polynômes dans $\mathbb{Q}[X_1, \ldots, X_n]$) permet d'identifier tous les signes que les polynômes de $\mathcal{P}$ peuvent avoir simultanément et de donner au moins un point par composante connexe dans chacun des ensembles semi-algébriques ainsi définis. Il s'agit donc d'une sortie extrêmement forte. Avec un post-traitement adéquat, la topologie de ces semi-algébriques peut même être identifiée. En revanche, si on cherche à décider du vide d'un ensemble semi-algébrique défini par un système d'équations et d'inégalités polynomiales $f_1 = \cdots = f_i = 0, \quad f_{i+1} > 0, \ldots, f_s > 0$, il n'existe pas à ma connaissance de modifications générales à l'algorithme de Collins qui permette de construire autre chose que *toutes les cellules* $\{f_1, \ldots, f_s\}$-invariantes. En faisant abstraction de sa complexité, l'exhaustivité de l'algorithme exposé dans ce chapitre est à la fois un atout et un talon d'Achille : trop de données sont calculées eu égard à certaines applications, notamment la plupart de celles évoquées au début de ce document.

De plus, comme mentionné plus haut, le caractère doublement exponentiel de l'algorithme de décomposition cylindrique algébrique est intrinsèque au fait qu'il résout, à de légères modifications près, le problème d'élimination des quantificateurs. Concrètement, ce caractère doublement exponentiel provient du fait que l'algorithme de décomposition cylindrique algébrique projette un semi-algébrique et itère récursivement son étude sur le projeté calculé. Si on se donne un polynôme $f \in \mathbb{Q}[X_1, \ldots, X_n]$ de degré D et qu'on se contente simplement de vouloir appliquer récursivement le théorème des fonctions implicites, on doit calculer le discriminant de f par rapport à X_n qui est de degré $\mathcal{O}(D^2)$ et travailler récursivement sur ce discriminant. En faisant abstraction des factorisations intervenant dans les discriminants itérés, on aboutit ici fatalement à une complexité $\mathcal{O}(D^{2^n})$.

La figure 10 illustre bien ce point de vue. Le discriminant du polynôme dont la surface dessinée est le lieu d'annulation a comme lieu-solution une courbe contenant une singularité (le *cusp*). Itérer notre étude sur cette courbe en considérant une projection sur une droite dans le plan dessiné nous amène à considérer cette singularité (nous sommes ici amené à partitionner notre droite en 3 cellules, deux d'entre elles étant homémomorphe à $]0, 1[$, l'autre correspondant à la projection du cusp sur la droite étant homéomorphe à $]0, 1[^0$. Néanmoins, si on considère directement la projection sur une telle droite restreinte à la surface qu'on désire étudier, on se rend compte que toutes les fibres sont difféomorphes. Autrement dit, dans cette situation, la partition de la droite qu'on est amené à considérer dans le théorème de trivialité semi-algébrique de Hardt est la droite toute entière alors que l'étude récursive de la projection nous a contraint à considérer partitionner cette droite en deux cellules.

Nous voyans dans le chapitre qui suit comment, en évitant ces étapes de projection intermédiaire, nous pouvons obtenir des complexités simplement exponentielles en le nombre de variables pour des problèmes de tests du vide, de calcul d'au moins un point par composante connexe dans un semi-algébrique et bien d'autres encore. Ici, l'idée consiste à ne considérer la projection du semi-algébrique étudié que sur une droite.

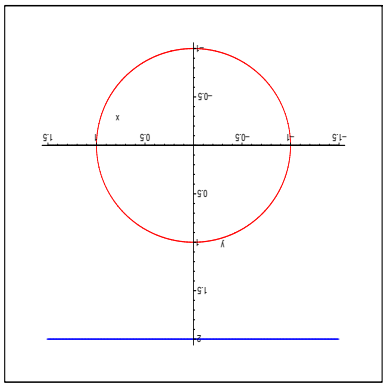

FIG. 11 –

4 Applications polynomiales, lieux critiques et topologie

Considérons une variété algébrique réelle $V \subset \mathbb{R}^n$ et une application polynomiale $\varphi : V \to \mathbb{R}^p$. Le théorème de trivialité semi-algébrique de Hardt décompose $\mathbb{R}^p$ en composantes C_i telles qu'il existe un homéomorphisme h entre $\varphi^{-1}(C_i)$ et $C_i \times F_i$ où F_i est la pré-image d'un point de C_i par φ. On s'intéresse aux composantes C_i qui sont de dimension maximale, et plus précisément on cherche un moyen d'identifier de telles composantes. Dans le cas, de la courbe $\mathcal{C}$ qui est l'union du cercle défini par l'équation $x^2 + y^2 - 1 = 0$ et de la droite définie par $y + 2 = 0$ et la projection $\pi : (x, y) \to x$ (voir figure 11), il s'agit des composantes $]-\infty, -1[$, $]-1, 1[$ et $]1, +\infty[$.

À l'intérieur de ces composantes, on doit au moins pouvoir appliquer le théorème des fonctions implicites. Ainsi, dans l'exemple qu'on considère la différentielle de π en chaque point de la pré-image de $]-1, 1[$ (qu'on identifie à l'application linéaire qui envoie un vecteur tangent à la courbe sur sa première coordonnée) est surjective. Notons qu'ici, le théorème des fonctions implicites nous dit que, étant donné $x \in \mathbb{R} \setminus \{-1, 1\}$, il existe un voisinage U de x tel que π réalise une fibration localement triviale sur $\mathcal{C} \cap \pi^{-1}(U)$. On constate sur cet exemple, qu'en fait, π réalise une fibration localement triviale sur $\mathbb{R} \setminus \{-1, 1\}$.

Cet exemple montre qu'il peut être pertinent d'étudier le lieu des points où la différentielle d'une application polynomiale n'est pas surjective pour identifier les composantes de dimension maximale intervenant dans le théorème de trivialité semi-algébrique de Hardt. Dans l'exemple que nous avons considéré, il s'agit des points $(-1, 0)$ et $(1, 0)$. Derrière cette approche, des difficultés (ou plutôt des limites apparaissent immédiatement) : en plus d'être passé d'un cadre semi-algébrique à un cadre algébrique, on doit maintenant assurer l'existence des différentielles des applications polynomiales considérées en chaque point de la variété étudiée. Celle-ci est conditionnée par le fait que chaque point de la variété est *régulier*, ou encore que la variété sur laquelle on travaille est lisse. Sous ces hypothèses, les points de la variété où la différentielle de l'application polynomiale considérée n'est pas surjective sont appelés *points critiques*. L'ensemble de leurs images par l'application polynomiale considérée est appelé ensemble des *valeurs critiques*.

Ces points sont caractérisables algébriquement : le fait qu'en ces points la différentielle de l'application polynomiale considérée n'est pas surjective se traduit, dans les cas où la variété étudiée est équi-dimensionnelle, par l'annulation de mineurs d'une matrice jacobienne. Dans les cas non équi-dimensionnels, on peut caractériser les points critiques par une formulation lagrangienne qui exprime explicitement des relations de co-linéarité entre des vecteurs gradients. On dispose donc de résultats permettant d'identifier clairement les points critiques (et les valeurs critiques) d'une application polynomiale.

Dans le cas où la variété étudiée V est compacte, il est montré que pour chaque composante connexe U du complémentaire de l'ensemble des valeurs critiques d'une application polynomiale φ restreinte à V, φ réalise une fibration localement triviale sur $V \cap \varphi^{-1}(U)$ ce qui correspond aux informations données par le théorème de trivialité semi-algébrique de Hardt. Ceci dit, le cas compact est un peu restrictif. Pour s'en défaire on considère des applications polynomiales restreintes à une variété V propres : en tout point

de l'image, il existe un voisinage U tel que la pré-image de U intersectée avec V est compacte. Dans ce cas aussi, on sait que l'application polynomiale considérée réalise une fibration localement triviale au-dessus de chaque composante connexe du complémentaire de l'ensemble de ses valeurs critiques. En fait, cette notion de propreté permet de garantir qu'aucun phénomène induisant un changement de topologie ne peut intervenir "à l'infini" (c'est pourquoi on a dans le cas des applications polynomiales propres un résultat identique à celui que nous avons dans le cas des applications restreintes à des variétés compactes).

On ne pourra malheureusement pas toujours choisir les applications polynomiales qu'on doit considérer pour les applications qui nous intéressent. En particulier, on doit pouvoir aussi obtenir des résultats de nature topologique, similaires à ceux fournis par le théorème de trivialité semi-algébrique de Hardt dans des situations non propres. Dans ce cas, on doit adjoindre à l'ensemble des valeurs critiques de l'application considérée un ensemble de points afin de tenir compte des changements de topologie des fibres intervenant à cause de phénomènes "à l'infini". Cet ensemble de points s'appelle *valeurs critiques asymptotiques*.

Dans la suite, on commence par donner les définitions et résultats relatifs à la notion de propreté pour les applications polynomiales. Puis on donne les définitions et propriétés des points et valeurs critiques d'applications polynomiales restreintes à des variétés algébriques (réelles ou pas). On donne aussi les différentes caractérisations algébriques possibles des points et valeurs critiques d'une application polynomiale ainsi que les énoncés relatifs aux propriétés topologiques de ces points et valeurs critiques dans le cas des applications propres. Pour pouvoir obtenir des énoncés similaires dans le cas des applications polynomiales non propres, on introduit les notions de valeur critique asymptotique et de valeur critique généralisée, d'abord dans le cas des applications polynomiales de $\mathbb{C}^n$ dans $\mathbb{C}$ puis dans le cas des applications polynomiales restreintes à des variétés algébriques lisses et équi-dimensionnelles. Enfin, on termine cette section en donnant des bornes sur les degrés des lieux critiques d'applications polynomiales ainsi que sur les degrés des valeurs critiques généralisées qui nous seront utiles dans la suite.

4.1 Notion de propreté

Définition 11. *Soit V et W des espaces topologiques et $f : V \to W$ une application de V dans W. L'application f est* propre *en $w \in W$ si il existe un voisinage B de w tel que $f^{-1}(\overline{B})$ est compact, où $\overline{B}$ est la clôture de B.*

Le lieu de non-propreté de f est l'ensemble des points $y \in W$ tels que f n'est pas propre en y.

On dira qu'une application $f : V \to W$ est propre *(resp.* non propre*) si son lieu de non-propreté est vide (resp. non vide).*

.

Dans le contexte qui nous intéresse, nous utiliserons des applications entre des variétés algébriques ou des variétés algébriques réelles. La notion de propreté sera alors relative aux topologies métriques induites par $\mathbb{C}$ ou $\mathbb{R}$.

Exemple. *Considérons l'hyperbole $\mathcal{H} \subset \mathbb{R}^2$ définie par $xy - 1 = 0$ et la projection $\pi_1 : (x, y) \in \mathcal{H} \to x$. En tout point $y \in \mathbb{R} \setminus \{0\}$, la projection π_1 est propre en y. En revanche, π_1 n'est pas propre en 0. Dans ce cas, le lieu de non-propreté de π_1 restreinte à $\mathcal{H}$ est $\{0\}$ (voir Figure 12). En revanche, si on considère la projection $\pi_2 : (x, y) \in \mathcal{H} \to x + y$, on constate que le lieu de non-propreté de π_2 est vide (voir Figure 13).*

En fait, dans la famille des projections sur des droites de $\mathbb{R}^2$ passant par l'origine, les deux seules qui ont un lieu de non-propreté non vide sont les projections sur les droites définies par $x = 0$ et $y = 0$.

Ainsi dans l'exemple ci-dessus, on constate que les lieux de non-propreté des projections restreintes à la courbe qu'on a considérée sont contenus dans un fermé de Zariski. Ce constat se généralise comme suit :

Proposition 15. *Soit $V \subset \mathbb{C}^n$ et $W \subset \mathbb{C}^n$ deux variétés algébriques et $f : V \to W$ une application polynomiale. Le lieu de non-propreté de f est soit vide soit un fermé algébrique de co-dimension 1 dans $f(V)$.*

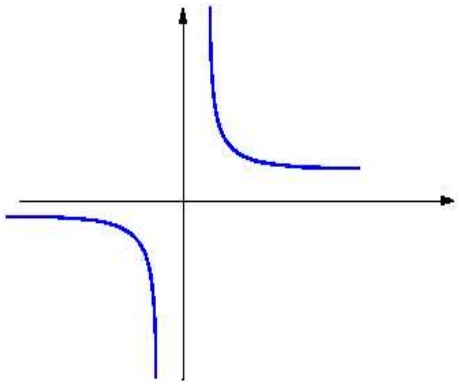

FIG. 12 – Lieu de propreté de π_1

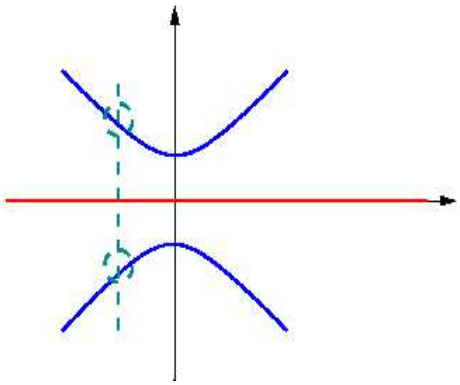

FIG. 13 – π_2 a un lieu de non-propreté vide

Ce résultat est faux dans le cas réel. En effet, si on considère l'hypersurface $\mathcal{H} \subset \mathbb{C}^3$ définie par $(x^2+y^2)z-1=0$ et la projection $\pi : (x,y,z) \in \mathcal{H} \cap \mathbb{R}^3 \to (x,y) \in \mathbb{R}^2$, on constate que le lieu de non-propreté est constitué de l'origine uniquement ; il est donc non vide mais n'est pas de co-dimension 1 dans $\mathbb{R}^2$. Il est évidemment contenu dans le lieu de non-propreté de $\widetilde{\pi} : (x,y,z) \in \mathcal{H} \to (x,y) \in \mathbb{C}^2$ qui est défini par $x^2+y^2=0$ et est bien de co-dimension 1 dans $\mathbb{C}^2$.

L'intérêt de la notion de propreté réside dans le fait qu'elles permet de garantir qu'une application polynomiale propre restreinte à une variété algébrique réelle atteint ses extrema sur chaque composante connexe de la variété considérée.

Proposition 16. *Soit $V \subset \mathbb{R}^n$ une variété algébrique réelle, D une composante connexe de V, E un sous-espace linéaire de $\mathbb{R}^n$ et $f : V \to E$ une projection propre. Soit $y \in E$ un point de la frontière de $f(D)$. Alors il existe $x \in V$ tel que $f(x) = y$.*

Ainsi, en garantissant qu'une projection restreinte à une variété algébrique donnée est propre, on s'assure que la projection considérée atteint ses extrema sur chaque composante connexe de la variété algébrique qu'on veut étudier. Nous verrons dans le chapitre suivant comment s'assurer qu'une projection restreinte à une variété algébrique donnée est propre. Ce test est basé sur le calcul du lieu de non-propreté de la projection considérée, pour lequel on donne une caractérisation algébrique dans la section suivante.

Définition 12. *Une application $f : V \to W$ où V et W sont des variétés algébriques irréductibles est* dominante *si son image est dense dans W, i.e. si la dimension de $f(V)$ en tant qu'ensemble constructible est égale à la dimension de W. On étend cette définition au cas $f : V \to W$, où V n'est pas nécessairement irréducible. Dans ce cas, la restriction de f à chaque composante irréductible de V est dominante.*

Considérons la droite de $\mathbb{C}^2$ définie par $x = 0$. La restriction de la projection π sur x restreinte à cette droite n'est évidemment pas dominante puisque l'image de la droite est ici un point. Remarquons que dans ce cas π n'est pas propre. Ceci se généralise comme suit.

Proposition 17. *Soit V et W deux variétés algébriques telles que $\dim(W) \leqslant \dim(V)$ et $f : V \to W$ une application. Si f n'est pas dominante, alors le lieu de non-propreté de f est non vide.*

La notion d'application dominante est donc importante : une application qui n'est pas dominante ne peut pas être propre. On verra aussi dans le paragraphe suivant que cette notion permet d'obtenir des propriétés sur la dimension du lieu critique des applications polynomiales qu'on considère.

4.2 Valeurs et lieux critiques d'applications polynomiales

Définition 13. *Soit $V \subset \mathbb{C}^n$ une variété algébrique, et $I(V) \subset \mathbb{Q}[X_1, \ldots, X_n]$ l'idéal associé à V (c'est-à-dire l'ensemble des polynômes qui s'annulent sur V).*

- *Si f est un polynôme de $\mathbb{Q}[X_1, \ldots, X_n]$, la* partie linéaire *de f en un point $p = (p_1, \ldots, p_n) \in \mathbb{C}^n$ (qu'on appelle aussi* différentielle de f en p*), notée $d_p(f)$, est définie par $d_p(f) = \frac{\partial f}{\partial X_1}(X_1 - p_1) + \ldots + \frac{\partial f}{\partial X_n}(X_n - p_n)$.*
- *Si $\varphi_1, \ldots, \varphi_q$ sont des polynômes de $\mathbb{Q}[X_1, \ldots, X_n]$, la différentielle de l'application polynomiale $\varphi : x \in \mathbb{C}^n \to (\varphi_1(x), \ldots, \varphi_q(x))$ en un point p, notée $d_p\varphi$, est définie comme étant l'application linéaire qui à $x \in \mathbb{C}^n$ associe $(d_p\varphi_1(x), \ldots, d_p\varphi_q(x))$.*
- *L'espace tangent à V en $p \in V$, noté $T_p(V)$, est l'ensemble des zéros communs de $d_p(f)$ pour $f \in I(V)$).*
- *Pour $p \in V$, la dimension de V en p, notée $\dim_p(V)$ est la dimension maximale des composantes irréductibles de V contenant p.*
- *Un point $p \in V$ est dit* régulier *(ou* non-singulier*) si $\dim(T_p(V)) = \dim_p(V)$. Un point* singulier *est un point non régulier.*
- *Une variété algébrique $V \subset \mathbb{C}^n$ est lisse si et seulement si tous les points $p \in V$ sont des points réguliers.*

Dans la suite, on notera $\mathrm{Reg}(V)$ (resp. $\mathrm{Sing}(V)$) l'ensemble des points réguliers (resp. singuliers) de V.

Nous pouvons maintenant donner les définitions de points et valeurs critiques d'une application polynomiale restreinte au lieu régulier d'une variété algébrique.

Définition 14. *Soit $V \subset \mathbb{C}^n$ une variété algébrique,* $\mathrm{Reg}(V)$ *l'ensemble des points réguliers de V, et $\varphi : V \to \mathbb{C}^p$ une application polynomiale.*

L'ensemble des points critiques de φ restreinte à $\mathrm{Reg}(V)$ *est l'ensemble des points x de* $\mathrm{Reg}(V)$ *tels que $d_x\varphi : T_x(V) \to \mathbb{C}^p$ n'est pas surjective.*

L'ensemble des valeurs critiques de φ restreinte à $\mathrm{Reg}(V)$ *est l'ensemble des images par φ des points critiques de φ restreinte à* $\mathrm{Reg}(V)$*.*

Considérons maintenant une variété algébrique $V \subset \mathbb{C}^n$ et $I(V) \subset \mathbb{Q}[X_1, \ldots, X_n]$ le plus grand idéal (pour l'inclusion) des polynômes de $\mathbb{Q}[X_1, \ldots, X_n]$ s'annulant sur V. Cet idéal est radical et on en considère un ensemble fini de générateurs $f_1, \ldots, f_s$.

En tout point régulier $x = (x_1, \ldots, x_n)$ de V, l'espace tangent à V en x est l'ensemble des zéros communs de $d_x f_1, \ldots, d_x f_s$. C'est donc le noyau de l'application linéaire de $\mathbb{C}^n$ dans $\mathbb{C}^s$ dont la matrice associée est l'évaluation de la jacobienne associée à $f_1, \ldots, f_s$ au point x :

$$\begin{bmatrix} \frac{\partial f_1}{\partial X_1}(x) & \ldots & \frac{\partial f_1}{\partial X_n}(x) \\ \vdots & \vdots & \vdots \\ \frac{\partial f_s}{\partial X_1}(x) & \ldots & \frac{\partial f_s}{\partial X_n}(x) \end{bmatrix}$$

On remarque immédiatement que l'espace vectoriel $\mathrm{Vect}(\mathbf{grad}_x(f_1), \ldots, \mathbf{grad}_x(f_s))$ engendré par les vecteurs gradients de $f_1, \ldots, f_s$ évalués au point p est normal à l'espace tangent à V en x. On appelle cet espace vectoriel, l'*espace co-tangent* à V en x.

Soit $p \in \mathbb{N}^\star$ et considérons une application polynomiale $\varphi : V \to \mathbb{C}^p$. La différentielle de φ au point x est l'application linéaire qui associe à un vecteur $\mathbf{v} \in T_x(V)$ le vecteur $(d_x\varphi_1(\mathbf{v}), \ldots, d_x\varphi_p(\mathbf{v}))$. Ainsi pour tout vecteur $\mathbf{v} = (v_1, \ldots, v_n)$ de $T_x(V)$, son image par $d_x\varphi$ est le vecteur

$$\begin{pmatrix} \frac{\partial \varphi_1}{\partial X_1}(x)v_1 + \cdots + \frac{\partial \varphi_1}{\partial X_n}(x)v_n \\ \vdots \\ \frac{\partial \varphi_p}{\partial X_1}(x)v_1 + \cdots + \frac{\partial \varphi_p}{\partial X_n}(x)v_n \end{pmatrix}$$

Dire que x est un point critique de φ c'est donc dire que $d_x(T_x(V))$ est de dimension inférieure ou égale à $p-1$. Donc, le noyau de $d_x\varphi$ est de dimension supérieure ou égale à 1, ce qui implique qu'il existe $(\lambda_1, \ldots, \lambda_n) \neq (0, \ldots, 0)$ tels que :

$$\begin{cases} \frac{\partial \varphi_1}{\partial X_1}(x)\lambda_1 + \cdots + \frac{\partial \varphi_1}{\partial X_n}(x)\lambda_n &= 0 \\ \vdots & \vdots \\ \frac{\partial \varphi_p}{\partial X_1}(x)\lambda_1 + \cdots + \frac{\partial \varphi_p}{\partial X_n}(x)\lambda_n &= 0 \end{cases}$$

sous les contraintes :

$$\begin{cases} \frac{\partial f_1}{\partial X_1}(x)\lambda_1 + \cdots + \frac{\partial f_1}{\partial X_n}(x)\lambda_n &= 0 \\ \vdots & \vdots \\ \frac{\partial f_s}{\partial X_1}(x)\lambda_1 + \cdots + \frac{\partial f_s}{\partial X_n}(x)\lambda_n &= 0 \end{cases}$$

Comme le noyau de $\mathrm{Jac}(f_1, \ldots, f_s)$ est de dimension $n-d$, on obtient que x est un point critique de la restriction de φ à V si

$$\dim(\mathbf{grad}_x(\varphi_1), \ldots, \mathbf{grad}_x(\varphi_p)) + \dim(\mathbf{grad}_x(f_1), \ldots, \mathbf{grad}_x(f_s)) < n - d + p$$

Dans le cas où la variété V définie par $f_1 = \cdots = f_s = 0$ est *lisse* et *équi-dimensionnelle* (toujours sous l'hypothèse que l'idéal $\langle f_1, \ldots, f_s \rangle$), ceci revient à dire que tous les mineurs $(n-d+p, n-d+p)$ de la matrice jacobienne $\mathrm{Jac}(f_1, \ldots, f_s, \varphi_1, \ldots, \varphi_p)$:

$$\begin{bmatrix} \frac{\partial f_1}{\partial X_1}(x) & \ldots & \frac{\partial f_1}{\partial X_n}(x) \\ \vdots & \vdots & \vdots \\ \frac{\partial f_s}{\partial X_1}(x) & \ldots & \frac{\partial f_s}{\partial X_n}(x) \\ \frac{\partial \varphi_1}{\partial X_1}(x) & \ldots & \frac{\partial \varphi_1}{\partial X_n}(x) \\ \vdots & \vdots & \vdots \\ \frac{\partial \varphi_s}{\partial X_1}(x) & \ldots & \frac{\partial \varphi_s}{\partial X_n}(x) \end{bmatrix}$$

s'annulent en x si et seulement si x est un point critique de la restriction de φ à V. Ceci donne une première caractérisation algébrique des points critiques de la restriction de φ à $\mathrm{Reg}(V)$.

Lemme 4. *Soit $f_1, \ldots, f_s$ des polynômes de $\mathbb{Q}[X_1, \ldots, X_n]$ engendrant un idéal radical, $V \subset \mathbb{C}^n$ la variété algébrique définie par $f_1 = \cdots = f_s = 0$ qui est supposée* lisse *et* équi-dimensionnelle *et $\varphi : x \in \mathbb{C}^n \to (\varphi_1(x), \ldots, \varphi_p(x)) \in \mathbb{C}^p$ une application polynomiale.*

L'ensemble des points critiques de la restriction de φ à V est l'ensemble des solutions du système d'équations polynomiales formé de :

- *les équations $f_1 = \cdots = f_s = 0$;*
- *pour tout $(n-d)$-uplet $\{i_1, \ldots, i_{n-d}\}$ de $\{1, \ldots, s\}$, tous les mineurs $(n-d+p, n-d+p)$ des matrices jacobiennes* $\mathrm{Jac}(f_{i_1}, \ldots, f_{i_{n-d}}, \varphi_1, \ldots, \varphi_p)$

Chaque hypothèse du lemme ci-dessus est importante.

- Si $\langle f_1, \ldots, f_s \rangle$ n'est pas radical, le lemme tombe en défaut car pour $x \in V$, $\mathbf{grad}_x(f_1), \ldots, \mathbf{grad}_x(f_s)$ n'engendre plus l'espace co-tangent à V en x. Par exemple, considérons le cercle défini par $f = (x^2+y^2-1)^2 = 0$ et la projection $\pi : (x, y) \to x$. En tout point du cercle, le gradient de f s'annule, et donc le système construit dans le lemme 4 est

$$\left\{ \begin{array}{rcl} (x^2+y^2-1)^2 & = & 0 \\ 2y(x^2+y^2-1) & = & 0 \end{array} \right.$$

  ce qui laisserait à penser que tous les points du cercle sont des points critiques de la restriction de la projection sur x à ce cercle.
- Si la variété V n'est pas équi-dimensionnelle, alors l'ensemble des solutions du système construit dans le lemme 4 peut être *strictement* contenu dans l'ensemble des points critiques de l'application polynomiale considérée. Par exemple, considérons le polynôme $f = x^2+y^2+z^2-1$, les polynômes $g_1 = z$ et $g_2 = x^2+y^2-1/2$, la variété algébrique $V \subset \mathbb{C}^n$ définie par :

$$\left\{ \begin{array}{rcl} fg_1 & = & 0 \\ fg_2 & = & 0 \end{array} \right.$$

  et la projection $\pi : (x, y, z) \to x$. la variété V est de dimension 2 : c'est la réunion d'une sphère et d'un cercle. Elle n'est donc pas équidimensionnelle. Le système par le lemme 4 est alors :

$$\left\{ \begin{array}{rcl} fg_1 & = & 0 \\ fg_2 & = & 0 \\ 2\,yz & = & 0 \\ 3\,z^2+x^2+y^2-1 & = & 0 \\ 2\,y\left(x^2+y^2-1/2\right)+2\,\left(x^2+y^2+z^2-1\right)y & = & 0 \\ 2\,z\left(x^2+y^2-1/2\right) & = & 0 \end{array} \right.$$

  Ce système se résoud à la main et on trouve que l'ensemble de ses solutions se réécrit sous la forme triangulaire :

$$\left\{ \begin{array}{rcl} z & = & 0 \\ y & = & 0 \\ x^2-1 & = & 0 \end{array} \right.$$

  On trouve ici les points critiques de la restriction de π à la composante de dimension 2 de V, mais pas ceux de la composante de dimension 1.
- Si la variété V n'est pas lisse, le système construit dans le lemme 4 peut contenir le lieu singulier de V. Par exemple, en tout point singulier d'une hypersurface définie par $f = 0$ avec $f \in \mathbb{Q}[X_1, \ldots, X_n]$, le gradient de f s'annule si bien que quelque soit l'application polynomiale considérée, les mineurs construits s'annulent.

L'hypothèse d'équi-dimensionnalité du lemme 4 peut néanmoins être levée en construisant un système dit de Lagrange.

Lemme 5. *Soit $V \subset \mathbb{C}^n$ une variété algébrique lisse définie par s polynômes $f_1, \ldots, f_s$ de $\mathbb{Q}[X_1, \ldots, X_n]$. Supposons que $\langle f_1, \ldots, f_s \rangle$ soit radical, et soit f_{s+1} un polynôme de $\mathbb{Q}[X_1, \ldots, X_n]$ et φ l'application :*

$$\begin{array}{rccc} \varphi : & V \subset \mathbb{C}^n & \longrightarrow & \mathbb{C} \\ & (x_1, \ldots, x_n) & \mapsto & f_{s+1}(x_1, \ldots, x_n) \end{array}$$

Étant donné un point $p \in V$, p est point critique de $\widetilde{f}_{s+1}$ si et seulement si il existe un point $(\lambda_1, \ldots, \lambda_s)$ dans $\mathbb{C}^s$ tel que $(\lambda_1, \ldots, \lambda_s, p) \in \mathbb{C}^s \times \mathbb{C}^n$ est une solution du système d'équations polynomiales dans $\mathbb{Q}[\ell_1, \ldots, \ell_s, X_1, \ldots, X_n]$:

$$\begin{cases} f_1 = \cdots = f_s = 0 \\ \ell_1 \frac{\partial f_1}{\partial X_1} + \cdots + \ell_s \frac{\partial f_s}{\partial X_1} = \frac{\partial f_{s+1}}{\partial X_1} \\ \ell_1 \frac{\partial f_1}{\partial X_2} + \cdots + \ell_s \frac{\partial f_s}{\partial X_2} = \frac{\partial f_{s+1}}{\partial X_2} \\ \qquad \vdots \\ \ell_1 \frac{\partial f_1}{\partial X_n} + \cdots + \ell_s \frac{\partial f_s}{\partial X_n} = \frac{\partial f_{s+1}}{\partial X_n} \end{cases}$$

où $\ell_1, \ldots, \ell_s$ sont des nouvelles variables.

Exemple.

- *Considérons une variété algébrique lisse $V \subset \mathbb{C}^n$, $\varphi_1, \ldots, \varphi_p$ des polynômes de $\mathbb{Q}[X_1, \ldots, X_n]$, et une application polynomiale $\varphi : x \in \mathbb{C}^n \to (\varphi_1(x), \ldots, \varphi_p(x)) \in \mathbb{C}^p$ avec $p > n$. Alors l'ensemble des points critiques de la restriction de φ à V est la variété V toute entière.*
  En effet, en tout point x de V, la dimension de l'espace tangent est inférieure ou égale à n, si bien que si $p > n$, son image par la différentielle de φ en x est forcément non surjective.
- *Considérons l'hyperplan H défini par $X_1 = 0$ dans $\mathbb{C}^n$ et la projection $\pi : x = (x_1, \ldots, x_n) \in \mathbb{C}^n \to x_1$. Dans ce cas aussi, l'ensemble des points critiques de la restriction de π à H est H tout entier.*
- *Considérons la courbe définie par $xy = 0$ dans le plan et la projection $\pi : (x, y) \to x$. D'après la Définition 13, le seul et unique point singulier de V est l'origine $(0, 0)$. Parmi les points réguliers de V, ceux qui sont des points critiques de la restricition de π à V sont ceux qui satisfont $x = 0, y \neq 0$. Ici, l'ensemble des points critiques n'est pas un fermé de Zariski mais un constructible.*
- *Considérons la sphère définie par $x^2 + y^2 + z^2 - 1 = 0$ et la projection $\pi_2 : (x, y, z) \to (x, y)$. Ici, le lieu critique de la restriction de π_2 à la sphère est défini par*

  $$z = 0, \quad x^2 + y^2 - 1 = 0$$

  Considérons maintenant la projection $\pi_1 : (x, y, z) \to x$. Le lieu critique de la restriction de π_1 à la sphère est constitué des points de coordonnées $(-1, 0, 0)$ et $(1, 0, 0)$ et il est contenu dans le lieu critique de la restriction de π_2 à la sphère.

Dans les exemples ci-dessus, nous avons constaté que l'ensemble des points critiques de la restriction d'une application polynomiale à une variété algébrique V peut être la variété V toute entière. Le thèorème ci-dessous montre qu'en toute circonstance, l'ensemble des valeurs critiques est contenu dans un fermé de Zariski strict de l'espace d'arrivée.

Théorème 9 (Théorème de Sard – Version algébrique). *Soit $V \subset \mathbb{C}^n$ une variété algébrique et $\varphi : V \to \mathbb{C}^p$ une application polynomiale. L'ensemble des valeurs critiques de φ restreinte à $\mathrm{Reg}(V)$ est contenu dans un fermé de Zariski de $\mathbb{C}^p$ de co-dimension au moins 1.*

Dans tous les exemples qu'on a vus jusqu'à présent, l'ensemble des valeurs critiques d'une application polynomiale était un fermé de Zariski. Considérons maintenant la surface S définie par :

$$y^2 - z^2(x^2 - z) = 0$$

et la projection $\pi : (x, y, z) \to (x, y)$. La surface considérée a un lieu singulier qui est la droite définie par :

$$z = 0, \quad y = 0$$

Le lieu critique de la restriction de π à S est défini par :

$$z^3 - 2\,y^2 = 0, \quad 2\,x^2 - 3\,z = 0, \quad \text{et} \quad (y \neq 0 \ \text{ ou } \ z \neq 0)$$

Ainsi, l'ensemble des valeurs critiques de la restriction de π à S est l'ensemble constructible défini par :

$$4x^6 - 27y^2 = 0, \quad y \neq 0.$$

On s'intéresse maintenant aux propriétés topologiques des lieux critiques d'applications polynomiales. Soit $V \subset \mathbb{C}^n$ une variété algébrique, $\pi : (x_1, \ldots, x_n) \in V \to x_1 \in \mathbb{C}$ une projection, $x = (\xi_1, \ldots, \xi_n) \in V$ un point critique de φ restreinte à $\mathrm{Reg}(V)$ et $T_x(V)$ l'espace tangent à V en x. D'après le théorème des fonctions implicites, si d est la dimension de V au point x (c'est-à-dire la dimension de l'espace tangent à V en x), il existe un voisinage $U \subset \mathbb{R}^{n-d}$ de $(\xi_{n-d+1}, \ldots, \xi_n)$ et une application polynomiale $\varphi : U \to \mathbb{R}^d$ tels que

$$\Phi : \begin{array}{ccc} U & \to & V \\ x' = (x_{n-d+1}, \ldots, x_n) & \to & (\varphi(x'), x') \end{array}$$

est un difféomorphisme de U sur $\Phi(U)$.

Définition 15. *On dit que x est non-dégénéré si et seulement si la hessienne de π au point x :*

$$\left[\ \frac{\partial^2 \varphi}{\partial X_i \partial X_j} \ \right], \quad n - d + 1 \leqslant i, j \leqslant n$$

Une projection dont tous les points critiques sont non-dégénérés est une fonction de Morse.

Des résultats montrent que dans l'ensemble des projections sur une droite, l'ensemble de celles qui ne sont pas de Morse est un fermé de Zariski.

Plusieurs propriétés concernant les lieux et valeurs critiques d'applications peuvent être exhibées.

Proposition 18. *Soit $V \subset \mathbb{C}^n$ une variété algébrique lisse. Étant donné $a = (a_1, \ldots, a_n) = \mathbb{Q}^d$, on note π_a la projection qui associe à $x = (x_1, \ldots, x_n) \in \mathbb{C}^n$ le point $a_1 x_1 + \cdots + a_n x_n \in \mathbb{C}$. Il existe un fermé de Zariski $\mathcal{Z} \subset \mathbb{C}^n$ tel que pour tout $a \in \mathbb{Q}^d \setminus \mathcal{Z}$, les valeurs critiques de la restriction de π_a à V sont toutes distinctes. C'est en particulier le cas des fonctions de Morse.*

Le résultat ci-dessous renseigne sur le caractère dominant d'une application polynomiale en fonction de la dimension du lieu critique.

Proposition 19. *Soit $V \subset \mathbb{C}^n$ une variété algébrique irréductible de dimension d, et $\varphi : V \to \mathbb{C}^p$ une application polynomiale. Alors si le lieu critique de φ restreinte à $\mathrm{Reg}(V)$ est de dimension inférieure ou égale à $p - 1$, la restriction de φ à V est dominante.*

Dans certains cas, c'est le caractère dominant d'une application polynomiale qui renseigne sur la dimension du lieu critique.

Proposition 20. *Soit $V \subset \mathbb{C}^n$ une variété algébrique irréductible de dimension d, et $\varphi : V \to \mathbb{C}^d$ une application polynomiale. Alors si la restriction de φ à V est dominante, le lieu critique de φ restreinte à $\mathrm{Reg}(V)$ est de dimension inférieure ou égale à $p - 1$.*

Les exemples de lieux critiques que nous avons donnés précédemment illustrent bien la proposition ci-dessus. Intéressons-nous maintenant aux propriétés topologiques associées aux lieux et valeurs critiques d'une application polynomiale.

Le résultat ci-dessous est à la base d'algorithmes [34, 36, 20, 104] permettant de répondre à des questions de connexité relatives aux variétés algébriques réelles, notamment le comptage de ses composantes connexes ou bien décider si deux points de cette variété appartiennent à la même composante.

Proposition 21. *Soit $V \subset \mathbb{C}^n$ une variété algébrique lisse, $\varphi : x \in \mathbb{C}^n \to f(x)$ une application polynomiale avec $f \in \mathbb{Q}[X_1, \ldots, X_n]$, $(a, b) \in \mathbb{R}^2$ un couple avc $a < b$ tel que $[a, b]$ ne contienne au plus qu'une seule valeur critique de la restriction de φ à V et C une composante connexe de $\left(\varphi^{-1}([a, b]) \cap V\right) \cap \mathbb{R}^n$.*

- *Si $[a, b]$ ne contient aucune valeur critique de la restriction de φ à V, alors pour tout $e \in [a, b]$, $\varphi^{-1}(e) \cap C$ est connexe.*
- *Si v est la seule valeur critique de la restriction de φ à V, alors $\varphi^{-1}(v) \cap C$ est connexe.*

Le fait que dans le second item du résultat ci-dessus, la connexité des fibres n'est assurée qu'au-dessus de la valeur critique v est illustrée par la figure 14.

Enfin, le résultat ci-dessous, renseigne sur les changements de topologie dans les fibres d'une application polynomiale restreinte à une variété algébrique (réelle ou pas) propre. Si $V \subset \mathbb{C}^n$ est une variété algébrique, $\varphi : V \to \mathbb{C}^p$ une application polynomiale et $\mathcal{K}(\varphi, V)$ l'ensemble des valeurs critiques de φ,

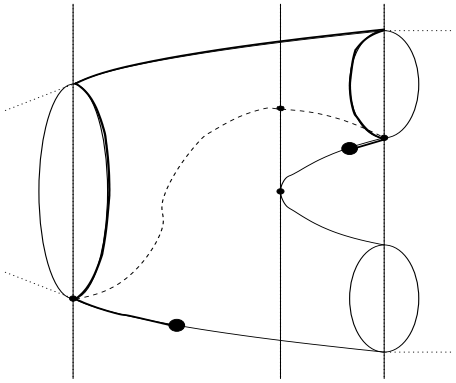

FIG. 14 – Connexité locale

l'énoncé assure que φ réalise une fibration localement triviale sur $V \setminus \varphi^{-1}(\mathcal{K}(\varphi, V))$ ce qui signifie que le diagramme suivant (où C est un ouvert simplement connexe de $\mathbb{R}^p \setminus \mathcal{K}(\varphi, V)$, h est un difféomorphisme et $F = \varphi^{-1}(x)$ pour x un point quelconque de C) commute :

$$\begin{array}{ccc} \varphi^{-1}(C) \subset V & \xrightarrow{h} & C \times F_i \\ & \searrow^{\varphi} & \downarrow \pi \\ & & C \subset \mathbb{R}^p \end{array}$$

Proposition 22. *Soit $V \subset \mathbb{C}^n$ une variété algébrique lisse, $\varphi : V \to \mathbb{C}^p$ une application polynomiale qu'on suppose propre et soit $\mathcal{K}(\varphi, V)$ l'ensemble des valeurs critiques de φ restreinte à V. Alors φ réalise une fibration localement triviale sur $V \setminus \varphi^{-1}(\mathcal{K}(\varphi, V))$.*

Le pendant réel de ce résultat s'énonce comme suit.

Proposition 23. *Soit $V \subset \mathbb{R}^n$ une variété algébrique réelle lisse, $\varphi : V \to \mathbb{R}^p$ une application polynomiale qu'on suppose propre et soit $\mathcal{K}(\varphi, V)$ l'ensemble des valeurs critiques de φ restreinte à V. Alors φ réalise une fibration localement triviale sur $V \setminus \varphi^{-1}(\mathcal{K}(\varphi, V))$.*

Cet énoncé est plus faible que le théorème de trivialité semi-algébrique de Hardt puisqu'il ne traîte que des cas des variétés algébriques lisses et d'applications polynomiales *propres*. Ceci dit, il nous indique que, dans ces cas-là, si on désire exhiber les cellules de dimension maximale d'une partition de l'espace d'arrivée de l'application polynomiale considérée, comme c'est fait dans le théorème de Hardt, il suffit de décrire les composantes connexes du complémentaire de l'ensemble des valeurs critiques de l'application polynomiale. Enfin, le résultat ci-dessus nous assure qu'on a fibration localement triviale, ce qui est plus fort qu'un résultat de trivialité assuré par le théorème de Hardt.

4.3 Valeurs critiques généralisées d'applications polynomiales

Nous avons vu que dans le cas des applications polynomiales propres, on pouvait assurer que de telles applications réalisent une fibration localement triviale au-dessus de chaque composante connexe de complémentaire de l'ensemble des valeurs critiques. C'est malheureusement faux lorsqu'on a affaire à des applications polynomiales non propres. Pour retrouver de telles propriétés topologiques, il faut adjoindre à l'ensemble des valeurs critiques des *valeurs critiques à l'infini* (qu'on appelle dans la suite *valeurs critiques asymptotiques*). L'union des valeurs critiques et des valeurs critiques asymptotiques est ce qu'on appelle *valeurs critiques généralisées*. Enfin, pour que tout ceci soit effectivement exploitable, il faut assurer que l'ensemble des valeurs critiques généralisées d'une application polynomiale φ est contenu dans un fermé de Zariski de l'espace d'arrivée de φ.

Dans la suite, on montre d'abord dans le cas d'applications polynomiales de $\mathbb{C}^n$ dans $\mathbb{C}$ puis de le cas d'applications polynomiales restreintes à des variétés algébriques lisses et équi-dimensionnelles comment définir correctement ces valeurs critiques généralisées pour garantir qu'elles sont effectivement incluses dans un fermé de Zariski de l'espace d'arrivée des applications considérées et avoir d'agréables propriétés topologiques similaires (des fibrations loccalement triviales donc).

4.3.1 Le cas des applications de $\mathbb{C}^n$ dans $\mathbb{C}$

Définition 16. *Soit $f \in \mathbb{Q}[X_1, \ldots, X_n]$ et l'application $\widetilde{f} : x \in \mathbb{C}^n \to f(x)$. L'ensemble des* valeurs critiques généralisées *de $\widetilde{f}$ est l'ensemble des valeurs complexes $c \in \mathbb{C}$ pour lesquelles il existe une suite de points $(x_\ell)_{\ell\in\mathbb{N}} \subset \mathbb{C}^n$ vérifiant les propriétés suivantes :*

- *$f(x_\ell) \to c$ quand $\ell \to \infty$*
- *pour tout $i \in \{1, \ldots, n\}$, $\frac{\partial f}{\partial X_i}(x_\ell) \to 0$ quand $\ell \to \infty$*
- *pour tout $(i, j) \in \{1, \ldots, n\}^2$, $\left(X_i \frac{\partial f}{\partial X_j}\right)(x_\ell) \to 0$ quand $\ell \to \infty$*

L'ensemble des valeurs critiques généralisées d'une application polynomiale $\widetilde{f} : x \in \mathbb{C}^n \to f(x)$ contient évidemment l'ensemble des valeurs critiques de $\widetilde{f}$, c'est-à-dire

$$\{c \in \mathbb{C} \mid \exists x \in \mathbb{C}^n \quad \frac{\partial f}{\partial X_1}(x) = \cdots = \frac{\partial f}{\partial X_n}(x) = 0, f(x) = c\}$$

qui est un fermé algébrique de $\mathbb{C}$ d'après le théorème de Sard.

Il contient aussi l'ensemble des valeurs critiques *asymptotiques* qui est l'ensemble des valeurs complexes $c \in \mathbb{C}$ pour lesquelles il existe une suite de points $(x_\ell)_{\ell\in\mathbb{N}} \subset \mathbb{C}^n$ vérifiant les propriétés suivantes :

- $f(x_\ell) \to c$ quand $\ell \to \infty$
- $||x_\ell|| \to \infty$ quand $\ell \to \infty$
- pour tout $i \in \{1, \ldots, n\}$, $\frac{\partial f}{\partial X_i}(x_\ell) \to 0$ quand $\ell \to \infty$
- pour tout $(i, j) \in \{1, \ldots, n\}^2$, $\left(X_i \frac{\partial f}{\partial X_j}\right)(x_\ell) \to 0$ quand $\ell \to \infty$

Exemple. *Considérons le polynôme $f = x(xy-1)$ et l'application polynomiale $\widetilde{f} : (x, y) \in \mathbb{C}^2 \to f(x, y)$. Cette application polynomiale n'a pas de valeur critique puisque le système d'équations polynomiales :*

$$\begin{cases} \frac{\partial f}{\partial x} = 2xy - 1 = 0 \\ \frac{\partial f}{\partial y} = x^2 = 0 \end{cases}$$

n'a pas de solutions. En revanche, si on considère la suite de points $(x_\ell, y_\ell) = (\frac{1}{2\ell}, \ell)$, on constate que

$$\begin{cases} \frac{\partial f}{\partial x}(x_\ell, y_\ell) = 2x_\ell y_\ell - 1 = 0 \\ \frac{\partial f}{\partial y}(x_\ell, y_\ell) = x_\ell^2 = \frac{1}{4\ell^2} \to 0 \qquad \textit{quand} \quad \ell \to \infty \end{cases}$$

et

$$\begin{cases} x_\ell \frac{\partial f}{\partial x}(x_\ell, y_\ell) = 2x_\ell^2 y_\ell - x_\ell = 0 \\ y_\ell \frac{\partial f}{\partial x}(x_\ell, y_\ell) = 2x_\ell y_\ell^2 - y_\ell = 0 \\ x_\ell \frac{\partial f}{\partial y}(x_\ell, y_\ell) = x_\ell^3 = \frac{1}{8\ell^3} \to 0 \qquad \textit{quand} \quad \ell \to \infty \\ y_\ell \frac{\partial f}{\partial y}(x_\ell, y_\ell) = y_\ell x_\ell^2 = \frac{1}{4\ell} \to 0 \qquad \textit{quand} \quad \ell \to \infty \end{cases}$$

tandis que $f(x_\ell, y_\ell) = -\frac{1}{4\ell}$ tend vers 0 quand ℓ tend vers ∞. Ainsi, 0 est une valeur critique asymptotique de l'application polynomiale $\widetilde{f}$.

C'est en fait la seule valeur critique généralisée de l'application $\widetilde{f}$. En effet, s'il existe une suite de points $(x_\ell, y_\ell)_{\ell\in\mathbb{N}} \subset \mathbb{C}^2$ satisfaisant les hypothèses de la Définition 16, $\frac{\partial f}{\partial x}(x_\ell, y_\ell) \to 0$ quand $\ell \to \infty$ ce qui implique que $x_\ell y_\ell$ tend vers $-\frac{1}{2}$. De plus, $\frac{\partial f}{\partial y}(x_\ell, y_\ell)$ doit aussi tendre vers 0 quand $\ell \to \infty$ ce qui implique que $x_\ell \to 0$ quand $\ell \to \infty$. Ainsi $f(x_\ell, y_\ell) = x_\ell(x_\ell y_\ell - 1)$ et $-\frac{1}{2}x_\ell$ ont la même limite qui est alors forcément 0.

Dans l'exemple étudié ci-dessus, l'ensemble des valeurs critiques asymptotiques est un fermé algébrique de $\mathbb{C}$, si bien que l'ensemble des valeurs critiques généralisées est un fermé de Zariski. Ceci est un résultat non spécifique à cet exemple.

Théorème 10. *[82] Soit $f \in \mathbb{Q}[X_1, \ldots, X_n]$ et considérons l'application polynomiale $\widetilde{f} : x \in \mathbb{C}^n \to f(x)$. L'ensemble des valeurs critiques généralisées de $\widetilde{f}$ est un fermé de Zariski dans $\mathbb{C}$.*

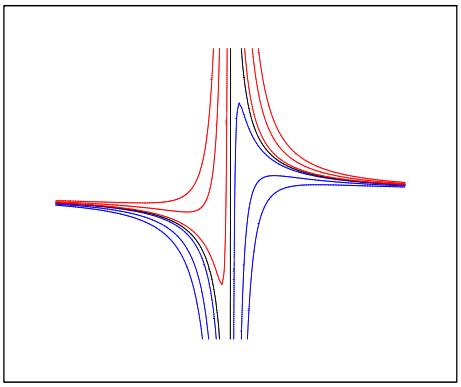

FIG. 15 – Existence de valeurs critiques généralisées et changement de topologie

Il est à noter que dans l'exemple étudié plus haut, nous avons pu définir une suite de points (x_ℓ, y_ℓ) caractérisant la présence d'une valeur critique asymptotique dans la courbe définie par $\frac{\partial f}{\partial x} = 0$. *In fine*, cette suite de points est une suite de points critiques de la projection $(x, y) \to y$ restreinte à l'hypersurface définie par $f + \frac{1}{2\ell} = 0$. Ce qui rend cette suite de points critiques un peu particulière est qu'elle ne converge pas.

À titre comparatif, si c est une valeur critique d'une application polynomiale $\widetilde{f} : x \in \mathbb{C}^n \to f(x) \in \mathbb{C}$ (où $f \in \mathbb{Q}[X_1, \ldots, X_n]$), on peut toujours, à changement linéaire de variables près, définir une suite de points $(x_\ell)_{\ell \in \mathbb{N}} \subset \mathbb{C}^n$ *convergente* (vers un point critique de $\widetilde{f}$) qui soit incluse dans la variété algébrique définie par :

$$\frac{\partial f}{\partial X_2} = \cdots = \frac{\partial f}{\partial X_n} = 0$$

Ces remarques sous-tendent qu'on peut éventuellement détecter une valeur critique *asymptotique* en considérant une suite de points critiques de projection sur une droite *bien choisie* qui tendrait vers l'infini, faisant intervenir ainsi un phénomène de non-propreté. Ceci sera étudié et précisé plus loin lorsque nous étudierons un algorithme de calcul des valeurs critiques généralisées.

De la même manière que les valeurs critiques ont des propriétés topologiques fortes dans le cas des applications propres, les valeurs critiques généralisées trouvent leur intérêt dans leurs propriétés topologiques et permettent de généraliser la proposition 22 au cas des applications non propres.

Théorème 11. *Soit $f \in \mathbb{Q}[X_1, \ldots, X_n]$, $K_{\mathbb{C}}(f)$ (resp. $K_{\mathbb{R}}(f)$) l'ensemble des valeurs critiques généralisées de l'application polynomiale $\widetilde{f_{\mathbb{C}}} : x \in \mathbb{C}^n \to f(x)$ (resp. $\widetilde{f_{\mathbb{R}}} : x \in \mathbb{R}^n \to f(x)$). Alors :*

- *$\widetilde{f_{\mathbb{C}}}$ réalise une fibration localement triviale sur $\mathbb{C}^n \setminus f^{-1}(K_{\mathbb{C}}(f))$*
- *$\widetilde{f_{\mathbb{R}}}$ réalise une fibration localement triviale sur $\mathbb{R}^n \setminus f^{-1}(K_{\mathbb{R}}(f))$*

Reprenons l'exemple du polynôme $f = x(xy - 1)$ et de l'application $\widetilde{f} : (x, y) \in \mathbb{R}^2 \to f(x, y)$ dont 0 est la seule valeur critique généralisée.

La fibre $\widetilde{f}^{-1}(0)$ est tracée en blanc sur la figure 15 et est consituée de trois composantes connexes. Sur la même figure, des fibres $\widetilde{f}^{-1}(e)$ sont tracées en bleu lorsque e est positif et en rouge lorsque e est négatif. Ces fibres sont constituées de deux composantes connexes. Il y a bel et bien eu un changement de topologie au niveau de la valeur critique généralisée. Il apparaît aussi que toutes les fibres $\widetilde{f}^{-1}(e)$ pour e positif (resp. e négatif) sont difféomorphes.

Néanmoins, la présence d'une valeur critique généralisée n'implique pas systématiquement un changement de topologie : une application polynomiale peut tout à fait réaliser une fibration localement triviale sur la pré-image d'un ouvert connexe U même si U contient une valeur critique généalisée. Pour illustrer ce fait, considérons le polynôme

$$f = -y(2x^2y^2 - 9xy + 12)$$

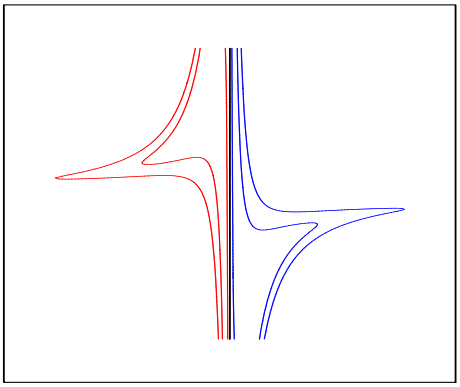

FIG. 16 – Existence de valeurs critiques généralisées sans changement de topologie

qui réalise une fibration localement triviale sur $f^{-1}(]-1,1[)$ (comme l'illustre la figure 16) alors que 0 est une valeur critique asymptotique de l'application polynomiale $\widetilde{f} : (x,y) \in \mathbb{R}^2 \to f(x,y)$.

Notons enfin l'importance de ce résultat de nature topologique pour la recherche d'au moins un point par composante connexe d'un semi-algébrique $\mathcal{S} \subset \mathbb{R}^n$ défini par $f > 0$ où $f \in \mathbb{Q}[X_1, \ldots, X_n]$. En effet, on montrera qu'il existe un réel suffisamment petit $e_0 \in]0, +\infty[$ tel que chaque composante connexe de $\mathcal{S}$ contient une composante connexe du lieu réel de l'hypersurface définie par $f - e_0 = 0$ et qu'il en est de même pour tout réel e compris entre 0 et e_0. On peut ainsi réduire la recherche d'un point par composante connexe dans $\mathcal{S}$ à la recherche d'un point par composante connexe dans le lieu réel d'une hypersurface si on sait déterminer e_0. Or, le fait que pour tout $e \in \mathbb{R}$ compris entre 0 et la plus petite valeur critique généralisée positive de l'application $\widetilde{f} : x \in \mathbb{R}^n \to f(x)$, les lieux réels des hypersurfaces définies par $f - e = 0$ sont difféomorphes implique qu'il suffit de calculer les valeurs critiques généralisées de $\widetilde{f}$ pour obtenir e_0. Nous reviendrons plus en détail sur ces aspects dans la suite du document.

Dans le paragraphe suivant, nous montrons comment étendre cette notion de valeur critique généralisée au cas des applications polynomiales restreintes à une variété algébrique lisse et équi-dimensionnelle qui sera elle aussi utile pour le calcul d'au moins un point par composante connexe dans un ensemble semi-algébrique (défini cette fois par un système d'équations et d'inégalités polynomiales).

4.3.2 Applications polynomiales restreintes à des variétés lisses

Soit $V \subset \mathbb{C}^n$ une variété algébrique lisse et équi-dimensionnelle de dimension d d, et $F = (f_1, \ldots, f_s)$ un ensemble de polynômes de $\mathbb{Q}[X_1, \ldots, X_n]$ engendrant l'idéal associé à V. On note $\mathrm{Jac}(f_1, \ldots, f_s)$ (ou $\mathrm{Jac}(F)$) la matrice jacobienne associée à $(f_1, \ldots, f_s)$:

$$\begin{bmatrix} \partial f_1/\partial X_1 & \ldots & \partial f_1/\partial X_n \\ \vdots & \vdots & \vdots \\ \partial f_s/\partial X_1 & \ldots & \partial f_s/\partial X_n \end{bmatrix}$$

Étant donnés $k \leqslant s$ polynômes $\varphi_1, \ldots, \varphi_k$ dans $\mathbb{Q}[X_1, \ldots, X_n]$, on note $\varphi : \mathbb{C}^n \to \mathbb{C}^k$ l'application polynomiale qui associe à $x \in V$ le point $(\varphi_1(x), \ldots, \varphi_k(x)) \in \mathbb{C}^k$.

Notation. *On utilise les notations suivantes :*

- *La matrice jacobienne associée à $(f_1, \ldots, f_s, \varphi_1, \ldots, \varphi_k)$ est notée $\mathrm{Jac}(F, \varphi)$;*
- *Étant donné un sous-ensemble $\mathcal{I} = \{i_1, \ldots, i_{n-d}\} \subset \{1, \ldots, s\}$ de cardinalité $n-d$ et un sous-ensemble $\mathcal{J} = \{j_1, \ldots, j_{n-d+k}\} \subset \{1, \ldots, n\}$ de cardinalité $n-d+k$, on note $M_{\mathcal{I},\mathcal{J}} \in \mathbb{Q}[X_1, \ldots, X_n]$ le mineur de $\mathrm{Jac}(F, \varphi)$ de taille $n-d+k$ construit en prenant les rangées $i_1, \ldots, i_{n-d}, s+1, \ldots, s+k$ et les colonnes $j_1, \ldots, j_{n-d+k}$ de $\mathrm{Jac}(F, \varphi)$;*
- *Étant donnés de tels sous-ensembles $\mathcal{I}$ et $\mathcal{J}$ comme ci-dessus et $i \in \mathcal{I}$ et $j \in \mathcal{J}$ on note $M_{\mathcal{I}\setminus\{i\},\mathcal{J}\setminus\{j\}}$ le mineur de $\mathrm{Jac}(F, \varphi)$ suivant la même contruction que précédemment. Si ce mineur est non nul on note $M^{i,j}_{\mathcal{I},\mathcal{J}}$ la fraction rationnelle $M_{\mathcal{I},\mathcal{J}}/M_{\mathcal{I}\setminus\{i\},\mathcal{J}\setminus\{j\}}$, sinon on pose $M^{i,j}_{\mathcal{I},\mathcal{J}} = 0$.*

Remarquons qu'il existe au plus $\binom{s}{n-d}$ (resp. $\binom{n}{n-d+k}$) choix possibles pour les sous-ensembles $\mathcal{I}$ (resp. $\mathcal{J}$), et que, étant donnés $\mathcal{I}$ et $\mathcal{J}$ il existe au plus $n-d$ (resp. $n-d+k$) choix pour i (resp. j).

De plus, puisque V est équi-dimensionnelle et que l'idéal $\langle f_1, \ldots, f_s \rangle$ est radical, $\mathcal{I}$ et $\mathcal{J}$ peuvent être choisis de manière telle que $M_{\mathcal{I},\mathcal{J}}$ n'est pas un diviseur de zéro dans $\mathbb{Q}[X_1, \ldots, X_n]/\langle f_1, \ldots, f_s \rangle$. De tels couples $\mathcal{I}, \mathcal{J}$ sont numérotés de 1 à N. Pour les mêmes raisons, étant donnés de tels sous-ensembles $\mathcal{I}$ et $\mathcal{J}$, il existe au moins un couple $(i,j) \in \mathcal{I} \times \mathcal{J}$ tel que $M^{i,j}_{\mathcal{I},\mathcal{J}}$ est non nul.

Dans la suite, on note $C = \{(i_1, j_1) \in \mathcal{I}_1 \times \mathcal{J}_1, \ldots, (i_N, j_N) \in \mathcal{I}_N \times \mathcal{J}_N\}$ un ensemble de couples tels que pour $\alpha = 1, \ldots, N$, le dénominateur de la fraction rationnelle $M^{i_\alpha, j_\alpha}_{\mathcal{I}_\alpha, \mathcal{J}_\alpha}$ n'est pas un diviseur de zéro dans $\mathbb{Q}[X_1, \ldots, X_n]/\langle f_1, \ldots, f_s \rangle$, et on note $\mathcal{C}$ l'ensemble de tels couples C. Étant donné $C = \{(i_\alpha, j_\alpha) \in \mathcal{I}_\alpha \times \mathcal{J}_\alpha \mid \alpha = 1, \ldots, N\} \in \mathcal{C}$, on note $\mathcal{M}^C$ l'ensemble des fractions rationnelles $M^{i_\alpha, j_\alpha}_{I_\alpha, J_\alpha}$ pour $\alpha = 1, \ldots, N$.

On peut maintenant définir les valeurs critiques généralisées d'une application polynomiale restreinte à une variété algébrique lisse et équi-dimensionnelle.

Définition 17. *Soit $V \subset \mathbb{C}^n$ une variété algébrique lisse et équi-dimensionnelle de dimension d, $f_1, \ldots, f_s$ une famille de polynômes dans $\mathbb{Q}[X_1, \ldots, X_n]$ engendrant $\mathcal{I}(V)$ et $\varphi : V \to \mathbb{C}^k$ une application polynomiale. En suivant les notations introduites et sous les hypothèses effectuées ci-dessus, un point $y \in \mathbb{C}^k$ est une valeur critique généralisée de φ restreinte à V si et seulement si il existe une suite de points $(x_\ell)_{\ell \in \mathbb{N}} \subset V$ et $C \in \mathcal{C}$ tels que :*

- *$\varphi(x_\ell)$ tend vers y quand ℓ tend vers ∞ ;*
- *pour tout $M \in \mathcal{M}^C$, $M(x_\ell)$ tend vers 0 quand ℓ tend vers ∞ ;*
- *pour tout $M \in \mathcal{M}^C$, les produits $(X_1.M)(x_\ell), \ldots, (X_n.M)(x_\ell)$ tendent vers 0 quand ℓ tend vers ∞ ;*

Si la norme de $(x_\ell)_{\ell \in \mathbb{N}} \subset V$ tend vers ∞ quand ℓ tend vers ∞, on dit que y est une valeur critique asymptotique.

L'ensemble des valeurs critiques généralisées de φ restreinte à V est noté dans la suite $K(\varphi, V)$. L'ensemble des valeurs critiques de φ restreinte à V est noté $K_0(\varphi, V)$, et l'ensemble des valeurs critiques asymptotiques est noté $K_\infty(\varphi, V)$.

Cette extension de la notion de valeur critique généralisée au cas des applications polynomiales restreintes à des variétés algébriques lisses est munie de propriétés topologiques agréables.

Théorème 12. *[82, 75] En gardant les notations et hypothèses introduites ci-dessus :*

- *l'ensemble des valeurs critiques généralisées $K(\varphi, V)$ de φ restreinte à V est une variété algébrique propre dans $\mathbb{C}^k$;*
- *l'application $\varphi : V \setminus \varphi^{-1}(K(\varphi, V)) \longrightarrow \mathbb{C}^k \setminus K(\varphi, V)$ est une fibration localement triviale ;*
- *l'application $\varphi : \big(V \setminus \varphi^{-1}(K(\varphi, V))\big) \cap \mathbb{R}^n \longrightarrow \mathbb{R}^k \setminus K(\varphi, V)$ est une fibration localement triviale.*

L'exemple de l'hypersurface $\mathcal{H}$ définie par $xyz - 1 = 0$ et de la projection sur x illustre bien le théorème ci-dessus. Pour tout réel α positif, $\mathcal{H} \cap \pi^{-1}(\alpha)$ est difféomorphe à une hyperbole définie par $yz - 1 = 0$. En 0, $\mathcal{H} \cap \pi^{-1}(0)$ est vide. Enfin, pour tout réel α négatif, $\mathcal{H} \cap \pi^{-1}(\alpha)$ est difféomorphe à une hyperbole définie par $yz + 1 = 0$.

4.4 Degré des lieux critiques et valeurs critiques généralisées

Le calcul de représentations algébriques encodant des lieux critiques constitue l'opération de base des algorithmes que nous présentons dans le paragraphe suivant. Afin de pouvoir effectuer des choix entre diverses stratégies possibles, il nous faut *au moins* avoir une idée précise de la taille de la sortie de nos algorithmes.

Puisque nous calculons des représentations algébriques de lieux critiques, qui sont – comme on l'a vu précédemment – des ensembles constructibles, avoir des informations précises sur la somme des degrés des composantes équi-dimensionnelles de la clôture de Zariski du lieu critique d'une application polynomiale est crucial. On est alors tenté d'appliquer le théorème de Bézout dans le contexte du lemme 4. Sous les conditions de ce lemme, en notant D le degré des polynômes définissant la variété considérée qui vit dans $\mathbb{C}^n$, d la dimension de la variété, on trouve $D^{n-d}\left((n-d)(D-1)\right)^d$. Cependant, plusieurs indicateurs laissent à penser que cette borne est une majoration grossière. On remarque facilement (voir les exemples ci-dessus) que ces systèmes sont sur-déterminés ; puisque bien souvent l'ensemble de leurs solutions n'est pas vide, ces systèmes ne sont pas *génériques* (l'ensemble des solutions communes de $n+1$ polynômes

génériques en n variables est vide), mais il est probable que la sur-détermination fasse chuter le degré[4]. Enfin, il suffit de quelques simulations effectuées sur machine pour se convaincre que la borne obtenue est une majoration brutale qu'on ne parvient pas à atteindre.

Pour mieux comprendre les phénomènes intervenant dans la complexité des lieux critiques, il faut revenir à la formulation du lemme 5. Les points critiques y sont caractérisés comme projection d'un ensemble algébrique. Appliquer directement la borne de Bézout au système de Lagrange donne D^{n+s} ce qui ne nous avance pas à grand chose. Ceci dit, on remarque que si les polynômes de départ sont homogènes et de même degré, le système de Lagrange est *presque* bi-homogène. On est donc tenté d'exploiter cette structure. En lui appliquant l'application

$$\begin{array}{rccl} \theta: & \mathbb{Q}[X_1,\ldots,X_n,\ell_1,\ldots,\ell_s] & \to & \mathbb{Q}[X_0,X_1,\ldots,X_n,\ell_0,\ell_1,\ldots,\ell_s] \\ & f & \to & X_0^{\deg_X(f)}\ell_0^{\deg_\ell(f)} f(\frac{X_1}{X_0},\ldots,\frac{X_n}{X_0},\frac{\ell_1}{\ell_0},\ldots,\frac{\ell_s}{\ell_0}) \end{array}$$

où X_0 (resp. ℓ_0) est une nouvelle variable et $\deg_X(f)$ (resp. $\deg_\ell(f)$) est le degré de f en $X_1,\ldots,X_n$ (resp. $\ell_1,\ldots,\ell_k$), on obtient un système bi-homogène.

Si on le suppose de dimension zéro dans le produit cartésien d'espaces projectifs $\mathbb{P}^{n+1}(\mathbb{C})\times\mathbb{P}^{s+1}(\mathbb{C})$ et qu'on lui applique les bornes de Bézout bi-homogène classiques (voir [53]) on obtient que le degré de l'ensemble des solutions du système bi-homogénéisé intersecté avec des formes linéaires affines en $X_0,\ldots,X_n$ d'une part et en $\ell_0,\ldots,\ell_n$ d'autre part est borné par $D^s(D-1)^{n-s}\binom{n}{n-s}$ ce qui est exactement ce qu'on obtient en pratique quand on considère une projection tirée au hasard restreinte à une variété algébrique définie par des polynômes eux aussi tirés au hasard ayant tous le même degré. Tout ceci n'est malheureusement pas si simple et dans le contexte du lemme 5, le système bi-homogène n'a aucune chance d'être équi-dimensionnelle puisque V ne l'est pas forcément. Il nous faut aussi définir une notion de *bi-degré* pour les idéaux bi-homogènes de dimension supérieure à 2. Dans [146], si $I\subset\mathbb{Q}[X_0,\ldots,X_n,\ell_0,\ldots,\ell_s]$ est un idéal bi-homogène de dimension supérieure à 2 cette notion est définie comme étant le degré de l'idéal affine $I+\langle u-1,v-1\rangle$ où u (resp. v) est une forme linéaire de $\mathbb{Q}[X_0,\ldots,X_n]$ ($\mathbb{Q}[\ell_0,\ldots,\ell_s]$) pour des choix génériques de u et v[5]. Dans le cas des idéaux non équi-dimensionnelles, on parle de bi-degré fort pour la somme des bi-degrés des composantes primaires isolées de l'idéal considéré.

Pour aboutir, nous devons utiliser les résultats suivants :

Théorème 13. *[134] Soit $k\in\{1,\ldots,n+s\}$ et $f_1,\ldots,f_k$ des polynômes bi-homogènes de l'anneau des polynômes $\mathbb{Q}[X_0,\ldots,X_n,\ell_0,\ldots,\ell_s]$ de bi-degrés respectifs (α_i,β_i) engendrant un idéal I. Supposons qu'il existe au plus n f_i tels que $\beta_i=0$ et au plus s f_i tels que $\alpha_i=0$. Alors, la somme des bi-degrés des idéaux premiers associés à $\sqrt{I}$ est bornée par*

$$\mathcal{B}(f_1,\ldots,f_k)=\sum_{\mathcal{I},\mathcal{J}}(\Pi_{i\in\mathcal{I}}\alpha_i).(\Pi_{j\in\mathcal{J}}\beta_j)$$

où $\mathcal{I}$ et $\mathcal{J}$ sont des sous-ensembles disjoints dont l'union est $\{1,\ldots,k\}$ et tels que $\mathcal{I}$ (resp. $\mathcal{J}$) est de cardinalité bornée par n (resp. s).

Le résultat ci-dessus nous permet de borner le bi-degré fort d'un idéal bi-homogène en fonction des bi-degrés d'un système de générateurs de cet idéal sous certaines conditions. Le résultat ci-dessous fait la correspondance entre la somme des degrés des composantes primaires isolées d'un idéal I de $\mathbb{Q}[X_1,\ldots,X_n,\ell_1,\ldots,\ell_s]$ et le bi-degré fort de l'idéal engendré par les bi-homogénénéisés $\theta(f)$ pour $f\in I$.

Théorème 14. *[134] Étant donné un idéal $I\subset\mathbb{Q}[X_1,\ldots,X_n,\ell_1,\ldots,\ell_k]$, on note $\theta(I)$ l'idéal engendré par $\{\theta(f)\mid f\in I\}\subset\mathbb{Q}[X_0,\ldots,X_n,\ell_0,\ldots,\ell_k]$.*

Alors, $\theta(I)$ est un idéal bi-homogène et la somme des degrés des composantes primaires isolées de I est bornée par le bi-degré fort de $\theta(I)$.

Enfin, on a :

[4]Cette situation intervient après tout dans de nombreuses applications, notamment en cryptanalyse algébrique, l'analyse des systèmes cryptographiques HFE effectuée par Bardet, Faugère et Salvy constitue un exemple édifiant

[5]Plus précisément, il existe un entier $\mathfrak{D}$ et un fermé de Zariski $\mathcal{Z}$ tel que pour tout choix de u et v hors de $\mathcal{Z}$ le degré de $I+\langle u-1,v-1\rangle$ est égale à $\mathfrak{D}$ et pour un choix de u ou v dans $\mathcal{Z}$ le degré de $I+\langle u-1,v-1\rangle$ est inférieur ou égale à $\mathfrak{D}$

Corollaire 3. *[134] Soit S une famille finie de polynômes dans $\mathbb{Q}[X_1,\ldots,X_n,\ell_1,\ldots,\ell_s]$ et I l'idéal engendré par S qu'on suppose radical. Considérons l'idéal J de $\mathbb{Q}[X_0,\ldots,X_n,\ell_0,\ldots,\ell_k]$ engendré par $\{\theta(f) \mid f \in S\}$.*

Alors la somme des degrés des composantes primaires isolées de I est bornée par le bi-degré fort de $\sqrt{J}$.

L'application de ces résultats au système de Lagrange nous permet alors d'énoncer :

Théorème 15. *[134] Soit $\{f_1,\ldots,f_s,f_{s+1}\} \subset \mathbb{Q}[X_1,\ldots,X_n]$ de degrés respectifs $D_1,\ldots,D_s,D_{s+1}$, $D = \max(D_i, i = 1,\ldots,s+1)$ et $V \subset \mathbb{C}^n$ la variété algébrique définie par*

$$f_1 = \cdots = f_s = 0$$

Supposons que l'idéal engendré par $f_1,\ldots,f_s$ soit radical et que V soit lisse. Alors, la somme des degrés des composantes équi-dimensionnelles du lieu critique de l'application polynomiale $\varphi : x \in V \to f_{s+1}(x)$ est bornée par

$$\left(\prod_{i=1}^{s} D_i\right)(D-1)^{n-s}\binom{n}{n-s}$$

On déduit aisément une borne sur le degré des valeurs critiques de ce résultat : puisqu'elles sont obtenues en évaluant f_{s+1} en les points critiques, la quantité ci-dessus borne le degré des valeurs critiques de φ.

Remarque. *Remarquons tout d'abord que dans le cas où $D = 2$, la borne ci-dessus est polynomiale en le nombre de variables et exponentielle en le nombre d'équations. Ceci laisse à penser que tout algorithme basé sur des calculs de points critiques et, géométriquement bien fondé, doit tomber dans une classe de complexité polynomiale en le nombre de variables et exponentielle en le nombre d'équations lorsque l'entrée est constituée de polynômes de degré au plus 2.*

Comparons maintenant la borne obtenue ci-dessus à l'aide d'une caractérisation des points critiques par le système de Lagrange à celle que nous obtenons en utilisant une caractérisation des points critiques par annulation de mineurs jacobiens. Notons tout d'abord que cette dernière n'est utilisable que dans le cas où la variété considérée est équidimensionnelle. Notons d cette dimension.

La borne obtenue en appliquant le théorème de Bézout sur la carctérisation à base de mineurs jacobiens est $D^{n-d}\left((n-d)(D-1)\right)^d$. Dans le cas où $s = n-d$, on constate que cette borne est toujours supérieure à la borne donnée plus haut obtenue par bi-homogénéisation du système de Lagrange.

Le résultat quantitatif ci-dessus n'est pas encore satisfaisant : en effet, il fait intervenir la quantité $D = \max(f_1,\ldots,f_s)$ ce qui n'est pas justifié géométriquement. Ceci se confirme par le calcul : lorsqu'on tire des polynômes au hasard $(f_1,\ldots,f_s)$ qui ne sont pas tous de même degré et qu'on calcule les points critiques de la restriction de la projection sur une variable à l'ensemble des zéros communs à $f_1,\ldots,f_s$ on trouve un ensemble de dimension zéro et de degré :

$$\prod_{i=1}^{s} D_i\left(\sum_{\alpha_1+\cdots+\alpha_s=n-s}\left(\prod_{i=1}^{s}(D_i-1)^{\alpha_i}\right)\right)$$

où D_i est le degré de f_i.

Savoir si ce constat expérimental peut devenir un résultat quantitatif est un problème ouvert sur lequel nous travaillons actuellement avec P. Trébuchet. Les motivations de ce travail sont expliquées dans la section suivante.

Théorème 16. *[75] Soit $f \in \mathbb{Q}[X_1,\ldots,X_n]$ et D son degré, $K_0(f)$ (resp. $\mathbb{K}_\infty(f)$) l'ensemble des valeurs critiques (resp. valeurs critiques asymptotiques) de l'application polynomiale qui à $x \in \mathbb{C}^n$ associe $f(x) \in \mathbb{C}$. Alors,*

$$\sharp K_0(f) + D\sharp K_\infty(f) \leqslant D^n - 1$$

Soit $V \subset \mathbb{C}^n$ une variété algébrique lisse équi-dimensionnelle de dimension d, $f_1,\ldots,f_s$ une famille de polynômes de $\mathbb{Q}[X_1,\ldots,X_n]$ de degrés bornés par D et $\varphi : x \in \mathbb{C}^n \to (\varphi_1(x),\ldots,\varphi_p(x)) \in \mathbb{C}^p$ une application polynomiale où φ_i est un polynôme de $\mathbb{Q}[X_1,\ldots,X_n]$ de degré borné par $\mathfrak{d}$ pour $i =$

$1, \ldots, p$. *On note* $K_0(\varphi, V)$ *(resp.* $K_\infty(\varphi, V)$*) l'ensemble des valeurs critiques (resp. valeurs critiques asymptotiques) de la restriction de* φ *à* V*. Alors,*

$$\sharp K_0(f) + \sharp K_\infty(f) \leqslant (\mathfrak{d} + k(p-1)(\mathfrak{d}-1) + (D-1)(n-d))^d D^{n-d}$$

où $k = \binom{n}{p+n-d}$.

Les bornes ci-dessus ont été obtenues en caractérisant des relations de dépendance linéaire entre vecteurs gradients par l'annulation de certains mineurs d'une matrice jacobienne. Il est opportun de mener à nouveau une étude sur ces degrés de valeurs critiques généralisées en essayant d'y intégrer l'usage de bornes bi-homogènes pour améliorer les bornes ci-dessus. Nous reviendrons plus loin dans le document sur ce problème.

4.5 Notes bibliographiques et commentaires

La plupart des définitions et résultats de ce chapitre sont classiques, excepté ce qui concerne les valeurs critiques généralisées et le degré des lieux critiques.

Voici un historique relatif à différents travaux concernant les valeurs critiques généralisées. Le *théorème de fibration d'Ehresmann* affirme qu'une submersion propre est une fibration localement triviale. Ainsi, $K_0(f)$ est un ensemble de bifurcation d'une application propre. Le théorème de fibration d'Ehresmann a été ensuite généralisé de différentes manières :

- Pour des applications non propres de $\mathbb{C}^n$ dans $\mathbb{C}$, R. S. Palais a introduit une condition, connue sous le nom de condition (C) de Palais.
- Pour des applications plus générales (d'une variété M dans une variété N), Rabier introduit la notion de submersion forte qui généralise la condition (C) de Palais. Dans ce cadre, la norme de la différentielle $d\ f$ de l'application considérée f est remplacée par $\nu(d\ f)$ (qui est simplement la distance de la différentielle de f à l'ensemble des opérateurs singuliers). Rabier montre alors que toute submersion forte est une fibration.
- Pour les applications de $\mathbb{C}^n$ dans $\mathbb{C}$ générales, il était déjà bien connu que l'ensemble de bifurcation de f est fini et contient $K_0(f)$ ainsi que quelques "valeurs critiques à l'infini". Plusieurs travaux ont consisté à donner une définition précise de ces valeurs critiques à l'infini.

Cependant, la difficulté était d'assurer un théorème de Sard pour les valeurs critiques à l'infini tout en préservant leurs propriétés topologiques. Les notions de valeurs critiques généralisées données dans ce chapitre sont issues de [82] et [74, 75]. Ces travaux s'inscrivent dans la lignée de ceux de Rabier. Ces notions préservent les propriétés de fibration localement triviale mais garantissent aussi un équivalent du théorème de Sard pour les valeurs critiques généralisées. De plus, des algorithmes permettant de calculer les valeurs critiques généralisées d'une application polynomiale ainsi que des bornes sur leur degré sont donnés. Nous en rediscutons plus loin dans ce document. Enfin, mentionnons que les valeurs critiques généralisées correspondent aux objets minimaux à calculer lorsqu'on veut résoudre un système d'équations polynomiales à paramètre (au sens de discuter le nombre de solutions réelles par exemple) (voir [89]). La notion de variété discriminante (voir [89]) coïncide avec celle de valeurs critiques généralisées dans les cas où on considère des projections :

- restreintes à des variétés algébriques lisses et équi-dimensionnelles
- les fibres génériques de ces projections sont de dimension zéro.

Mais les travaux de [89] permettent de gérer en plus les situations où on considère des variétés singulières ainsi que la présence d'inégalités. Néanmoins, la notion de variété discriminante telle que formulée dans [89] ne permet pas de gérer les situations où les fibres génériques des projections sont de dimension positive ce qu'autorisent les notions de valeurs critiques généralisées données dans ce chapitre.

Les bornes sur le degré des lieux critiques obtenues par l'analyse des systèmes de Lagrange sont directement issues de [134]. Comme indiqué dans le paragraphe correspondant, elles sont obtenues à partir d'un résultat bornant la somme des degrés des composantes équi-dimensionnelles d'une variété bi-projective. Ce résultat est montré dans [134]. On y trouve par ailleurs une analyse des propriétés des bi-séries de Hilbert. Ces travaux sont corrélés à ceux de [146, 113, 112, 68] qui traitent du cas équi-dimensionnel.

Nous disposons maintenant des notions de points et valeurs critiques d'applications polynomiales restreintes à des variétés algébriques, ainsi que d'une notion de valeur critique généralisée pour lesquelles

nous avons exhiber des résultats de nature topologique. Ceci permet d'utiliser *intelligemment* le théorème de trivialité semi-algébrique de Hardt : au lieu de procéder par projections itérées comme on l'a vu dans la décomposition cylindrique algébrique pour étudier une variété algébrique réelle, on peut directement calculer les points critiques (et parfois les valeurs critiques asymptotiques) de la projection sur une droite pour détecter les changements de topologie dans les pré-images de points de la droite considérée. Parmi ces changements de topologie, on trouve évidemment l'apparition de composantes connexes de l'ensemble algébrique réel étudié. De plus, les bornes exhibées dans le paragraphe précédent montrent que dans les situations non-dégénérées (non singulières) la taille des objets considérés est de l'ordre des bornes de Bézout (on a une croissance exponentielle en le nombre de variables[6]). Ceci est utilisé pour décider du vide et calculer au moins un point par composante connexe dans une variété algébrique réelle au moyen de ce qu'on appelle la méthode des points critiques.

[6]Ceci est à corréler à la croissance doublement exponentielle en le nombre de variables des degrés des polynômes apparaissant dans la décomposition cylindrique algébrique.

5 Tests du vide et calcul d'au moins un point par composante connexe d'une variété algébrique réelle

Nous abordons dans ce chapitre le problème du test du vide et du calcul d'au moins un point par composante connexe d'un ensemble algébrique réel donné par un système d'équations polynomiales. On verra dans le chapitre suivant que le calcul d'au moins un point par composante connexe d'un ensemble algébrique réel est une spécification importante dans la mesure où cela permet de tester *efficacement* le vide d'un ensemble semi-algébrique.

Les algorithmes que nous présentons dans ce chapitre permettent (ou ont permis) d'obtenir des implantations particulièrement efficaces pouvant traîter des problèmes très largement inatteignables par l'algorithme de décomposition cylindrique algébrique. Nous verrons que, pour certains d'entre eux, on sait prouver qu'ils ont une complexité théorique polynomiale en la borne de Bézout, c'est-à-dire, simplement exponentielle en le nombre de variables ce qui est à mettre en regard avec la complexité doublement exponentielle de l'algorithme de décomposition cylindrique algébrique.

Pour se donner une idée des méthodes mises en œuvre ici, considérons une hypersurface lisse $\mathcal{H} \subset \mathbb{C}^n$ définie par $f = 0$ (où $f \in \mathbb{Q}[X_1, \ldots, X_n]$ est sans facteurs carrés) et supposons, pour commencer, que son lieu réel $\mathcal{H} \cap \mathbb{R}^n$ soit compact. Considérons Π_1 la projection qui envoie $(x_1, \ldots, x_n) \in \mathbb{C}^n$ sur x_1. Puisque chaque composante connexe de $\mathcal{H} \cap \mathbb{R}^n$ est compacte, l'application polynomiale Π_1 est propre et d'après la proposition 16, Π_1 atteint ses extrema sur chaque composante connexe de $\mathcal{H} \cap \mathbb{R}^n$ (si elles existent). Ces extrema sont atteints en les points critiques de Π_1 restreinte à $\mathcal{H}$. D'après les caractérisations algébriques que nous avons vues dans le chapitre précédent (voir le lemme 4), ces points sont solutions du système d'équations polynomiales :

$$f = \frac{\partial f}{\partial X_2} = \cdots = \frac{\partial f}{\partial X_n} = 0$$

Si ce système d'équations polynomiales est zéro-dimensionnel (i.e. n'admet qu'un nombre fini de solutions complexes), on verra qu'on peut alors donner une paramétrisation rationnelle de ses solutions sous la forme :

$$\left\{ \begin{array}{rcl} X_n & = & \frac{q_n(T)}{q_0(T)} \\ & \vdots & \\ X_1 & = & \frac{q_1(T)}{q_0(T)} \\ q(T) & = & 0 \end{array} \right.$$

où T est une nouvelle variable et les polynômes $q_0, q, q_1, \ldots, q_n$ sont univariés en T à coefficients rationnels.

Le problème initial qui s'exprimait en plusieurs variables est ainsi réduit à un problème univarié (compter et isoler les racines réelles revient à étudier q et les fractions rationnelles $\frac{q_i}{q_0}$ pour $i = 1, \ldots, s$).

Il est important de noter ici que d'après le Théorème de Bézout (voir [53]) qui permet de borner le nombre de solutions d'un système d'équations polynomiales zéro-dimensionnel par le produit du degré des équations, le nombre de points critiques ainsi représenté est inférieur ou égale à $D(D-1)^{n-1}$ (où D est le degré de f). Sous réserve que les hypothèses qui ont émaillé cette discussion soient vérifiées, on vient d'exhiber un algorithme permettant de calculer au moins un point par composante connexe d'une hypersurface réelle compacte et sans singularités dont la sortie (le nombre de points représentés par la paramétrisation rationnelle) est bornée par le nombre de Bézout qui est simplement exponentiel en le nombre de variables. En terme de complexité, la difficulté est ramenée à savoir résoudre un système d'équations polynomiales zéro-dimensionnel avec une complexité polynomiale en la borne de Bézout dans le pire cas. On verra que de tels algorithmes existent. L'usage des concepts vus dans le chapitre précédent permet donc bien de contourner le caractère doublement exponentiel de la décomposition cylindrique algébrique. Les algorithmes fondés sur de tels calculs de points critiques relèvent de ce qu'on appelle dans la suite *la méthode des points critiques*.

On voit apparaître dans cette introduction les problèmes qu'il faut gérer pour obtenir un algorithme décidant du vide ou calculant au moins un point par composante connexe dans une variété algébrique réelle quelconque :

- *trouver une application polynomiale qui atteigne ses extrema sur chaque composante connexe* : dans notre exemple nous ne sommes pas confronté à cette difficulté, la variété algébrique réelle considérée étant supposée compacte. Mais, si l'on considère l'hyperbole définie par $xy - 1 = 0$ on constate sans

peine que la projection sur x n'atteint pas ses extrema sur chacune des deux composantes connexes de l'hyperbole : les deux composantes connexes se projettent sur des intervalles ouverts $(]-\infty, 0[$ et $]0, +\infty[)$ et la pré-image de 0 est évidemment vide.

– *s'assurer que le système définissant les points critiques de l'application considérée est zéro-dimensionnel* : c'est ce que nous avons supposé dans notre exemple, mais cette hypothèse est loin de pouvoir être garantie les yeux fermés. En effet, si l'on considère l'hypersurface $\mathcal{H}$ définie par $(x^2+1)(x^2+y^2-1)=0$ et la projection π sur x, le lieu critique de π restreint à $\mathcal{H}$ est défini par :

$$\begin{cases} y(x^2+1)=0 \\ (x^2+1)(x^2+y^2-1)=0 \end{cases}$$

qui n'est pas de dimension zéro. On peut aussi remarquer que si on choisit une autre projection (celle sur y par exemple) on obtient un lieu critique défini par :

$$\begin{cases} x(2x^2+y^2)=0 \\ (x^2+1)(x^2+y^2-1)=0 \end{cases}$$

qui, lui, est de dimension zéro.

– De plus, la caractérisation des points critiques donnée dans les lemmes 4 et 5 n'est valable que dans les cas où
  – l'idéal engendré par le système d'équations considéré est radical et la variété considérée est équi-dimensionnelle et lisse (si l'une de ces hypothèses n'est pas vérifiée, soit la caractérisation exhibée dans le lemme 4 définit systématiquement un ensemble algébrique de dimension positive, soit cette caractérisation n'est pas complète dans la mesure où les points critiques vivant sur les composantes équi-dimensionnelles de basse dimension sont oubliés) ;
  – l'idéal engendré par le système d'équations considéré est radical et la variété considérée est lisse dans le cas du lemme 5 mais cette caractérisation nécessite de faire intervenir plus de variables (les multiplicateurs de Lagrange) et ne peut être exploitée dans le cas d'idéaux non radicaux et/ou des variétés algébriques singulières.

  Ainsi, le cas général d'ensembles algébriques réels V donnés par un système S d'équations polynomiales tel que S n'engendre pas un idéal radical ou que V contient une infinité de points singuliers pose problème. En effet, dans ces cas, on ne peut pas caractériser les points critiques d'une application polynomiale restreinte à l'ensemble algébrique qu'on étudie via les lemmes 4 ou 5.

Pour gérer ces problèmes, les notions d'applications polynomiales propres et d'applications polynomiales dominantes introduites dans le chapitre précédent sont intensivement utilisées. Ce chapitre est structuré comme suit. Dans un premier temps, nous décrivons la sortie des algorithmes de résolution de systèmes polynomiaux que nous utilisons dans les diverses mises en œuvre de la méthode des points critiques. Nous portons une attention particulière aux ensembles triangulaires, aux bases de Gröbner et aux résolutions géométriques. Nous donnons aussi les complexités d'algorithmes permettant de calculer ces représentations.

Puis nous décrivons les stratégies générales de mise en œuvre de la méthode des points critiques en donnant d'abord un algorithme général de calcul d'au moins un point par composante connexe dans une variété algébrique réelle $V \subset \mathbb{R}^n$ définie comme étant le lieu des zéros réels communs d'une famille de polynômes $f_1, \ldots, f_s$ de $\mathbb{Q}[X_1, \ldots, X_n]$. Cet algorithme réduit ce problème au calcul d'au moins un point par composante connexe dans une hypersurface réelle compacte et lisse. Cette réduction est obtenue en considérant l'hypersurface $\mathcal{H} \subset \mathbb{C}^n$ qui est le lieu d'annulation de la somme des carrés des polynômes $f_1, \ldots, f_s$. Puis, l'étude est ramenée à celle d'une hypersurface lisse dont le lieu réel est compact en introduisant des infinitésimaux déformant l'hypersurface $\mathcal{H}$. La complexité de cet algorithme est bornée par $D^{\mathcal{O}(n)}$ où D borne le degré des polynômes définissant la variété algébrique réelle V et n est le nombre de variables. Remarquons qu'ici la constante de complexité est située en exposant. Nous verrons que, dans l'algorithme décrit, celle-ci est particulièrement élevée, et que quelque soit la structure géométrique de la variété étudiée, le pire cas (en terme de complexité) est systématiquement atteint. Ainsi, cet algorithme est inutile en pratique : il ne permet malheureusement pas de concrétiser l'apport en terme de complexité théorique en performances pratiques qui permettent de résoudre plus de problèmes que ceux que l'algorithme de décomposition cylindrique algébrique permet d'aborder.

La suite du chapitre porte sur les techniques permettant de rendre utile, en pratique, la méthode des points critiques. Dans le paragraphe 5.3, nous concentrons notre étude sur les méthodes permettant de garantir que l'application polynomiale choisie, dont on calcule les points critiques, atteint ses extrema sur chaque composante connexe de la variété étudiée. Celles-ci utilisent des applications polynomiales qui sont des carrés de fonction distance à un point choisi génériquement dans l'espace de travail. Le cas des variétés singulières et/ou non équi-dimensionnelles (induisant des chutes de rang dans la matrice jacobienne associée à l'ensemble des polynômes définissant la variété étudiée) est traîté en procédant à des appels récursifs de l'algorithme sur le lieu singulier de la variété étudiée puis, le lieu singulier du lieu singulier, et ainsi de suite. La dimension du lieu singulier considéré chutant à chaque étape, on ramène ainsi l'étude à la résolution de systèmes polynomiaux zéro-dimensionnels. Cet algorithme utilise la caractérisation algébrique des points critiques donnée par le lemme 4 et fait donc intensivement appel à des routines calculant des décompositions équi-dimensionnelles et radicales d'idéaux engendrés par des équations polynomiales. La sortie de tels algorithmes est généralement constituée de familles de bases de Gröbner dont la taille peut être exponentielle en la taille de l'entrée. Ainsi, les appels récursifs peuvent être coûteux. De plus, le calcul de points critiques de fonctions polynomiales étant des carrés de distance euclidienne à un point génériquement choisi est couteux devant des calculs de points critiques de fonction de projection qui sont linéaires. Ainsi, même si l'algorithme décrit dans ce paragraphe a permis des avancées pratiques substantielles, on concentre notre étude dans le paragraphe 5.4 sur l'usage de fonctions de projection.

Dans cette étude, on utilise intensivement les notions de projection dominante et de lieu de non-propreté introduites dans le chapitre précédent. Essentiellement, l'idée consiste à utiliser le fait que le lieu critique d'une fonction de projection dominante restreinte à une variété irréductible est de dimension inférieure à celle de la variété considérée (voir proposition 20). Ainsi, modulo le choix de bonnes projections, on garantit que nos calculs intermédiaires de lieux critiques permettent de se ramener à l'étude de variétés algébriques de dimension zéro. Il reste néanmoins à gérer les situations où certaines composantes connexes de la variété algébrique réelle étudiée ont une intersection vide avec les lieux critiques calculés. Dans ce cas, on montre que le calcul de pré-images d'au moins un point par composante connexe dans le complémentaire du lieu de non-propreté des projections considérées permet d'atteindre ces composantes connexes : on verra que les calculs sont menés de manière telle que ces pré-images sont de dimension zéro. Enfin, la présence de singularités, ou plus généralement, les chutes de rang dans les matrices jacobiennes sont gérées comme dans le paragraphe 5.3. En pratique, l'algorithme présenté dans le paragraphe 5.4 est bien plus performant que celui du paragraphe précédent : l'usage de fonctions de projections (qui sont linéaires) en lieu et place de fonctions distance (qui sont quadratiques) permet des gains d'efficacité substantiels. Ceci dit, cet algorithme effectue des calculs de lieux critiques de lieux critiques et ainsi de suite. Ces objets ont des degrés qui sont mal maîtrisés et contiennent génériquement des singularités. On préfère utiliser des fonctions de projection sur des droites pour en calculer les points critiques directement plutôt que d'effectuer une descente sur la dimension en calculant des lieux critiques de lieux critiques.

Ainsi, même si l'idée d'utiliser des fonctions de projection est validée expérimentalement, on cherche à améliorer l'usage qu'on en fait dans le paragraphe 5.5. Dans ce paragraphe, pour simplifier notre étude, on ne considère que des variétés lisses données par une famille de générateurs de l'idéal associé. Étant donnée une variété algébrique lisse $V \subset \mathbb{C}^n$, on montre que pour des choix génériques de projection sur des droites, toutes les composantes connexes de $V \cap \mathbb{R}^n$ se projettent en des intervalles fermés. On atteint donc ces composantes connexes en calculant les points critiques de la fonction de projection π considérée et en calculant l'intersection de V et de la pré-image par π d'un point arbitrairement choisi dans la droite sur laquelle on projette. On itère alors notre étude sur cette intersection dont le degré est le même que celui de V et dont la dimension est inférieure à celle de V. Cette stratégie est différemment mise en œuvre selon que V est équi-dimensionnelle ou non (on utilise alors soit le lemme 4 soit le lemme 5 pour caractériser les lieux critiques qu'on cherche à calculer). La notion de propreté d'une application polynomiale introduite dans le chapitre précédent est ici intensivement utilisée. En pratique, cet algorithme permet d'obtenir des résultats très largement inatteignables par ceux exposés dans les paragraphes précédents. Ce type d'algorithmes est à la base des implantations actuellement disponibles dans [128] pour le calcul d'au moins un point par composante connexe dans une variété algébrique réelle lisse. L'usage de bases de Gröbner permet de certifier que les choix de fonctions de projection sont "suffisamment génériques". Les estimations de complexité (en terme de nombre d'opérations), fondées sur les théorèmes bornant le coût de calculs de résolution géométriques, donnent des bornes simplement

exponentielles en le nombre de variables. Enfin, dans le cas où les équations de départ sont quadratiques, ces algorithmes sont polynomiaux en le nombre de variables et exponentiels en le nombre d'équations. L'analyse de la taille de la sortie de ces algorithmes a aussi permis d'obtenir de nouvelles bornes sur le nombre de composantes connexes d'une variété algébrique réelle. On dispose ainsi d'algorithmes très efficaces en pratique et dont on maîtrise la complexité pour le calcul d'au moins un point par composante connexe d'une variété algébrique réelle lisse. Il nous reste à améliorer les techniques développées pour les algorithmes des sections 5.3 et 5.4 pour gérer les cas où des chutes de rang dans les jacobiennes interviennent.

Dans le paragraphe 5.6, on considère une hypersurface $\mathcal{H} \subset \mathbb{C}^n$ définie par $f = 0$ (où f est un polynôme dans $\mathbb{Q}[X_1, \ldots, X_n]$) contenant une infinité de points singuliers et on développe une étude pour le calcul d'au moins un point par composante connexe de $\mathcal{H} \cap \mathbb{R}^n$. La stratégie qui consiste à étudier les images des composantes connexes de $\mathcal{H} \cap \mathbb{R}^n$ par des projections sur des droites génériques ayant fait ses preuves dans le cas lisse, on cherchera à l'adapter à ce contexte singulier. Le problème est que la caractérisation algébrique du lemme 4 ne permet pas de se ramener directement à l'étude de systèmes zéro-dimensionnels. On cherche dans ce paragraphe à éviter tant que faire ce peut à étudier directement le lieu singulier de $\mathcal{H}$ puis le lieu singulier du lieu singulier et ainsi de suite comme dans les paragraphes 5.3 et 5.4. En effet, ces lieux singuliers, dont on ne maîtrise pas le degré, sont souvent définis par des systèmes polynomiaux engendrant des idéaux non radicaux et non équi-dimensionnels qu'il est difficile décomposer d'une part et, d'autre part, ceci nous contraindrait à effectuer des calculs de points critiques de fonction polynomiale restreinte à des variétés algébriques qui nous sont données comme le lieu d'annulation de bases de Gröbner. Le nombre et le degré des polynômes dans ces bases pouvant être exponentiels en le nombre de variables, de tels calculs s'avèrent vite très difficiles à mettre en œuvre.

Une stratégie alternative consiste à déformer l'hypersurface $\mathcal{H}$ de manière à ramener notre étude à celle d'une hypersurface lisse. En effet, l'hypersurface définie par $f - \varepsilon = 0$ (où ε est un infinitésimal) est lisse. On montre qu'on calcule un point par composante de $\mathcal{H} \cap \mathbb{R}^n$ en appliquant l'algorithme du paragraphe 5.5 à l'hypersurface définie par $f - \varepsilon = 0$ et en calculant les limites des points obtenus lorsque ε tend vers 0. Le problème calculatoire réside dans le fait que la mise en œuvre directe de cette démarche ne permet pas d'obtenir des résultats pratiques satisfaisants : en effet, celle-ci oblige à effectuer les calculs dans $\mathbb{Q}(\varepsilon)$ alourdissant le coût de l'arithmétique exponentiellement en le nombre de variables. On montre alors comment éviter d'introduire explicitement cet infinitésimal et calculer *directement* les limites des points critiques qu'on cherche à calculer. L'algorithme obtenu permet d'avoir des performances pratiques bien supérieures aux stratégies procédant à des études récursives sur des lieux singuliers. De plus, on montre que la complexité de cette approche est polynomiale en la borne de Bézout et on montre que les sorties de cet algorithme sont de taille toujours strictement inférieure au pire cas attendu (c'est-à-dire des paramétrisations rationnelles encodant des ensembles algébriques de dimension zéro de degré égale à la borne de Bézout). Ceci est à corréler aux résultats présentés dans la section 5.2 où le pire cas est systématiquement atteint.

Le paragraphe 5.7 montre comment généraliser cette démarche au cas des variétés algébriques singulières (et/ou celles qui sont données par des systémes d'équations polynomiales engendrant des idéaux non radicaux). On aboutit à des algorithmes efficaces en pratique dont on sait borner la complexité par une quantité polynomiale en la borne de Bézout.

5.1 Sortie des algorithmes et élimination algébrique

Les algorithmes que nous étudions dans ce chapitre effectuent des calculs de points critiques de manière à ramener le calcul d'au moins un point par composante connexe à la *résolution* d'un (ou plusieurs) système(s) d'équations polynomiales zéro-dimensionnels c'est-à-dire admettant un nombre fini de solutions complexes. L'union des solutions de ces systèmes d'équations aura une intersection non vide avec chaque composante connexe de la variété algébrique réelle étudiée. Ces points seront représentés symboliquement de manière à pouvoir :

- obtenir des intervalles d'isolation de leurs coordonnées aussi précis que nécessaires ;
- et évaluer des polynômes multivariés en les coordonnées de ces points [7].

[7] On verra dans le chapitre suivant pourquoi il est important de pouvoir évaluer le signe d'un polynôme en un point algébrique réel.

Plusieurs représentations permettant de répondre à ce cahier des charges sont possibles. La plus générale est une représentation par ensemble triangulaire de polynômes (voir la série d'articles [10, 77, 87, 105, 9, 150, 151] et les articles de synthèse [71, 72]) déjà évoquée dans l'étape de remontée de l'algorithme de décomposition cylindrique algébrique (voir chapitre 3). Comme précédemment, on verra que pour résoudre les problèmes mentionnés ci-dessus, il nous faudra pouvoir manipuler des nombres algébriques réels. De plus, les ensembles triangulaires permettent de décomposer les variétés algébriques en composantes équi-dimensionnelles dont on peut calculer l'idéal associé. Ceci est utile dans la mesure où les caractérisations algébriques des points critiques donnés par les lemmes 4 et 5 supposent connues un système de générateurs de l'idéal associé à la variété algébrique considérée (et, pour le lemme 4, son équi-dimensionnalité).

On peut réduire le coût de l'isolation des coordonnées réelles (ou de l'évaluation du signe d'un polynôme en des points algébriques réels) en représentant les solutions d'un système d'équations polynomiales zéro-dimensionnel par une paramétrisation rationnelle des coordonnées des points du lieu-solution. Une telle représentation est introduite dans les travaux de Kronecker [81, 80] et constitue en un sens un cas particulier des ensembles triangulaires de polynômes.

Géométriquement, le procédé calculatoire revient à considèrer :

– une projection π sur une droite ;

– et l'image par π des solutions du système zéro-dimensionnel considéré.

Si la projection π est injective, on peut représenter les solutions du système zéro-dimensionnel sous la forme suivante :

$$\left\{\begin{array}{rcl} X_n & = & \frac{q_n(T)}{q_0(T)} \\ & \vdots & \\ X_1 & = & \frac{q_1(T)}{q_0(T)} \\ q(T) & = & 0 \end{array}\right.$$

où T est une nouvelle variable et les polynômes $q_0, q, q_1, \ldots, q_n$ sont univariés en T à coefficients rationnels. Les valeurs de T annulant q_0 sont les images des points du système zéro-dimensionnel considéré par la projection $\pi : (x_1, \ldots, x_n) \in \mathbb{C}^n \to u_1x_1 + \cdots + u_nx_n$ où on a choisi $(u_1, \ldots, u_n) \in \mathbb{Q}^n$ de manière à ce que la restriction de π en les points solutions du système considéré est injective.

Une fois qu'une telle représentation est calculée, isoler les coordonnées des solutions réelles (ou évaluer le signe d'un polynôme en les points réels encodés par une telle représentation) se ramène à isoler de manière suffisamment fine les racines réelles du polynôme q_0. Dans le cas où le corps de base sur lequel on travaille est le corps des rationnels $\mathbb{Q}$, on peut utiliser la méthode de Vincent [148] (plus connue sous le nom d'algorithme d'Uspensky [145]) pour lequel on trouve des variantes modernes efficaces (voir [126]). Lorsqu'on ne travaille pas sur un corps réel archimédien, le comptage des solutions réelles peut se faire au moyen des suites dites de Sturm-Habicht (voir [140, 66, 96, 98]).

Plusieurs méthodes permettent d'accéder à une telle représentation. Les premières ramènent la résolution d'un système zéro-dimensionnel engendrant un idéal I à des calculs d'algèbre linéaire dans l'algèbre-quotient $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I}$. En effet, si I est zéro-dimensionnel, cette algèbre-quotient se trouve être aussi un espace vectoriel de dimension finie. Pour ce faire, il est nécessaire de disposer d'une forme normale envoyant tous les polynômes $f \in \mathbb{Q}[X_1, \ldots, X_n]$ d'une même classe de $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I}$ sur un unique représentant. Une étape préalable consiste à calculer une représentation de l'algèbre-quotient $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I}$. Les bases de Gröbner permettent d'effectuer de tels calculs. La plus standard et, à ce jour, la plus efficace en général consiste à calculer une base de Gröbner de I pour un ordre monomial fixé, bien que d'autres options sont possibles pour cette étape (voir [144, 108]). Nous donnons ci-dessous les définitions et propriétés élémentaires des bases de Gröbner que nous exploiterons dans la suite. La seconde étape du calcul de paramétrisations rationnelles des solutions d'un système zéro-dimensionnel consiste en des calculs d'algèbre linéaire dans l'algèbre-quotient $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I}$ que nous décrivons très succinctement.

Nous verrons que le calcul de bases de Gröbner dans le cas des systèmes polynomiaux de dimension zéro se fait en une complexité simplement exponentielle en le nombre de variables et polynomiale en le maximum des degrés des polynômes donnés en entrée.

Une alternative à ces méthodes, connue sous le nom de *résolution géométrique* permet d'obtenir un procédé de résolution incrémental qui est polynomial en le maximum des degrés des variétés algébriques

définis par $f_1 = \cdots = f_i$ (pour $i = 1, \ldots, n$) si $f_1 = \cdots = f_s = 0$ (avec $s \geqslant n$) est le système zéro-dimensionnel à résoudre. Évidemment, dans le pire cas, ce degré est égale à la borne de Bézout, mais un tel résultat de complexité permet d'introduire une dépendance en des quantités géométriques (et non purement algébriques) dans les algorithmes d'élimination algébrique. Ce procédé s'appuie sur le codage des polynômes par des programmes d'évaluation (*straight-line program* en anglais)[8] et la seule implantation donnant des résultats pratiques intéressants code la sortie sur une base monomiale [92]. Ces algorithmes reposent sur les méthodes développées dans [60, 110, 59, 57]. L'implantation que nous évoquons ci-dessous est le paquetage `Kronecker` dû à G. Lecerf et se fonde sur les résultats exposés dans [61, 94, 93].

5.1.1 Représentations par ensembles triangulaires

On se donne un ordre sur les variables $X_1 < \ldots < X_n$. Étant donné un polynôme $f \in \mathbb{Q}[X_1, \ldots, X_n]$, on appelle *variable principale* de f la plus grande variable apparaissant dans f pour l'ordre monomial qu'on a fixé. Le *degré principal* de f est le degré de f en sa variable principale. L'*initial* d'un polynôme $f \in \mathbb{Q}[X_1, \ldots, X_n]$ est le coefficient dominant de ce polynôme lorsqu'il est vu comme univarié en sa variable principale. Le *séparant* d'un polynôme $f \in \mathbb{Q}[X_1, \ldots, X_n]$ est la dérivée partielle de f par rapport à sa variable principale.

Un ensemble triangulaire de polynômes est alors une famille finie T de polynômes dans $\mathbb{Q}[X_1, \ldots, X_n]$ telle que deux polynômes distincts de T ont des variables principales distinctes. L'objet géométrique associé à un tel ensemble triangulaire T de polynômes, qu'on appelle *quasi-variété* de T, est la *clôture de Zariski* de l'ensemble constructible, qu'on appelle *quasi-composante* de T, obtenu en considérant :

– le lieu d'annulation des polynômes de T
– duquel on retire les points annulant l'initial d'au moins un polynôme de T.

La structure algébrique associée à un ensemble triangulaire T est l'idéal qu'on appelle saturé de l'ensemble triangulaire T et qui est égale à

$$\mathrm{sat}(T) = \{f \in \mathbb{Q}[X_1, \ldots, X_n] \mid \exists k \in \mathbb{N}, \quad h^k f \in \langle T \rangle\}$$

où h est le produit des initiaux des polynômes de T. La variété algébrique associée au saturé d'un ensemble triangulaire est la quasi-variété de cet ensemble triangulaire.

Étant donné un ensemble triangulaire $T = \{t_{d+1}, \ldots, t_n\}$, on note T_{d+i} pour $i \in \{1, \ldots, n-d\}$ l'ensemble triangulaire de polynômes $\{t_{d+1}, \ldots, t_{d+i}\}$ et h_i le produit des initiaux de T_i. Un ensemble triangulaire T est dit *régulier* si et seulement si pour tout $i \in \{2, \ldots, n-d\}$, l'initial de t_{d+i} ne divise pas zéro dans l'algèbre-quotient $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{\mathrm{sat}(T_{i-1})}$.

Un ensemble triangulaire T est *séparable* si, pour $i \in \{d+1, \ldots, n\}$, le séparant s_i ne divise pas zéro dans $\mathbb{Q}[X_1, \ldots, X_n]/\mathrm{sat}(t_{d+1}, \ldots, t_i)$. Un ensemble triangulaire régulier et séparable T est dit *fortement normalisé* si pour $i \in \{d+1, \ldots, n\}$, h_i ne dépend que des variables transcendentes de T.

Les ensembles triangulaires réguliers et séparables jouissent d'une propriété intéressante pour ce qui nous concerne : leur quasi-variété et leur saturé sont respectivement des variétés algébriques et des idéaux équi-dimensionnels radicaux. Ainsi, décomposer l'idéal engendré par un système d'équations polynomiales en une famille de générateurs d'idéaux qui sont des saturés d'ensembles triangulaires réguliers et séparables permet de calculer les points critiques d'une application polynomiale restreinte à chacune des composantes équi-dimensionnelles de la variété étudiée (voir lemmes 4 et 5). Nous verrons plus loin comment exploiter cette propriété pour le calcul de points critiques d'applications polynomiales restreintes à des variétés algébriques non équi-dimensionnelles.

Les solutions d'un système zéro-dimensionnel sont données par l'union des solutions d'ensembles triangulaires réguliers de la forme

$$\begin{cases} t_n(X_1, \ldots, X_n) \\ \quad \vdots \\ t_2(X_1, X_2) \\ t_1(X_1) \end{cases}$$

[8] Le terme *programme d'évaluation* n'est pas tout à fait adapté : on entend ici par ce terme une suite d'instructions sans branchements ni boucles (on ne s'autorise que les opérations arithmétiques et l'affectation de variables). Bien que partiellement inapproprié, on continuera à employer ce terme dans la suite du document

Isoler les racines réelles de tels ensembles triangulaires se fait alors comme dans la phase de remontée de la décomposition cylindrique algébrique (voir chapitre 3) par la manipulation de nombres algébriques réels. Il en est de même pour l'évaluation du signe d'un polynôme en une solution d'un tel ensemble triangulaire.

5.1.2 Bases de Gröbner et calculs dans les algèbres-quotients

Les bases de Gröbner permettent de calculer modulo un idéal $I \subset \mathbb{Q}[X_1, \ldots, X_n]$, c'est-à-dire, d'envoyer tous les polynômes f d'une même classe de $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I}$ sur un seul et unique représentant (une fois que certaines précautions qu'on indique ci-dessous ont été prises).

Pour ce faire, il faut généraliser le procédé de division euclidienne du cadre univarié au cadre multivarié (qui permet de faire la même chose dans $\mathbb{Q}[X]$). Ce procédé est implicitement fondé sur le fait qu'on peut associer à tout polynôme un terme de tête (dans le contexte univarié, il s'agit du monôme de plus grand degré multiplié par son coefficient). On doit donc se donner un ordre monomial sur les monômes de $\mathbb{Q}[X_1, \ldots, X_n]$ qu'on identifie à des n-uplets de $\mathbb{N}^n$.

Définition 18. *Un ordre admissible sur les monômes (unitaires) de $\mathbb{Q}[X_1, \ldots, X_n]$ est une relation $\blacksquare > \blacksquare$ binaire sur $\mathbb{N}^n$ telle que :*

1. *$>$ est une relation d'ordre total sur $\mathbb{N}^n$,*
2. *si $\alpha > \beta$ et $\gamma \in \mathbb{N}^n$, alors $\alpha + \gamma > \beta + \gamma$,*
3. *pour l'ordre $>$, tout ensemble non vide admet un plus petit élément sur $\mathbb{N}^n$.*

Soit $\mathbf{X}^\alpha$ et $et\mathbf{X}^\beta$ avec $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ et $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$ deux monômes. Dans la pratique, on utilisera essentiellement :

- *l'ordre du degré lexicographique inverse* (DRL ou grevlex dans la littérature) : on dit que $\mathbf{X}^\alpha < \mathbf{X}^\beta$ si $\sum \beta_i < \sum \alpha_i$ ou, en cas d'égalité, si $\alpha_i < \beta_i$ pour le premier indice i tel que $\alpha_i \neq \beta_i$.
- *l'ordre lexicographique* : on dit que $\mathbf{X}^\alpha < \mathbf{X}^\beta$ si $\alpha_i > \beta_i$ pour le premier indice i tel que $\alpha_i \neq \beta_i$.

On utilisera aussi dans la suite des ordres d'élimination (voir [42]) qui combinent les ordres DRL et lexicographiques donnés ci-dessus.

Définition 19. *Soit $p = \sum_\alpha c_\alpha x^\alpha \in \mathbb{Q}[X_1, \ldots, X_n]$ et $>$ un ordre sur les monômes de $\mathbb{Q}[X_1, \ldots, X_n]$.*

1. *le multi-degré de p est :*
$$\text{multideg}(p) = \max\{\alpha \in \mathbb{N}^n \mid c_\alpha \neq 0\}$$
2. *le coefficient de plus haut degré de p est :*
$$\text{lc}(p) = c_{\text{multideg}(p)} \in \mathbb{Q}$$
3. *le monôme de plus haut degré de p est :*
$$\text{lm}(p) = x^{\text{multideg}(p)}$$
4. *le terme initial de p est :*
$$\text{in}(p) = \text{lc}(p)\text{lm}(p)$$

Dans la suite de cette section, on suppose fixé un ordre admissible sur les monômes de $\mathbb{Q}[X_1, \ldots, X_n]$.

Théorème 17. *Si $F = \{f_1, \ldots, f_s\}$ est une famille de polynômes de $\mathbb{Q}[X_1, \ldots, X_n]$, alors tout $f \in \mathbb{Q}[X_1, \ldots, X_n]$ peut s'écrire :*
$$f = a_1 f_1 + \ldots + a_s f_s + r$$
où $\forall i \in \{1, \ldots, s\}$, a_i et r sont des polynômes de $\mathbb{Q}[X_1, \ldots, X_n]$ tels qu'aucun des monômes de r ne soit divisible par l'un des $\text{in}(f_i)$.

On appellera *r une forme normale* de f modulo F. En fait, la preuve de ce théorème peut être établie en exhibant un algorithme calculant le reste d'un polynôme modulo une liste ordonnée. C'est l'algorithme de forme normale. La sortie de cet algorithme dépend de l'ordre dans lequel les polynômes interviennent dans l'algorithme de réduction. Elle n'est donc pas canonique. L'apport des bases de Gröbner consiste à rendre canonique cette opération une fois que l'ordre monomial est fixé.

Définition 20. *Étant donné un ordre monomial, une famille génératrice finie $G = (g_1, \ldots, g_s)$ d'éléments d'un idéal I de $\mathbb{Q}[X_1, \ldots, X_n]$ est une base de Gröbner si :*

$$\langle \mathrm{in}(g_1), \ldots, \mathrm{in}(g_s) \rangle = \langle \mathrm{in}(I) \rangle$$

La principale propriété des bases de Gröbner peut être résumée par :

Proposition 24. *Étant donné un ordre monomial, on pose $G = (g_1, \ldots, g_s)$ une base de Gröbner d'un idéal I dans $\mathbb{Q}[X_1, \ldots, X_n]$. Pour tout polynôme f de $\mathbb{Q}[X_1, \ldots, X_n]$, le reste de f modulo G (ou la forme normale de f modulo G) est déterminé de manière unique. En particulier, f est un élément de I si et seulement si son reste modulo G est nul.*

Le réduit d'un polynôme f par rapport à une base de Gröbner G est appelé forme normale de f modulo G.

Définition 21. *Une base de Gröbner réduite pour un idéal I de $\mathbb{Q}[X_1, \ldots, X_n]$ est une base de Gröbner pour I dont les polynômes sont constitués de monômes irréductibles modulo I.*

Le calcul de bases de Gröbner relève d'un procédé de réécriture, chaque polynôme appartenant au système de générateurs de l'idéal dont on cherche une base de Gröbner étant vu comme une règle de réécriture. On passe alors d'un système de générateurs à un autre (jusqu'à obtenir une base de Gröbner) en mettant en œuvre un mécanisme de complétion par adjonction de règles de réécritures (obtenues en forçant l'annulation des termes de tête de deux polynômes de la base courante).

On n'en dira pas plus, si ce n'est que le premier algorithme de calcul des bases de Gröbner est dû à Buchberger [32], que de nombreuses optimisations y ont été apportées jusqu'aux travaux de J.-C. Faugère [50, 51]. Ces derniers ont introduit des techniques d'algèbre linéaire rapide dans les calculs de bases de Gröbner et permettent d'éviter des calculs inutiles.

Dans le pire cas, les bases de Gröbner sont de taille doublement exponentielle en le nombre de variables (voir [102]). Il est important de noter que ce pire cas exhibé dans [102] est pathologique et ne se rencontre pas dans la pratique. Il est caractérisé par le fait que l'idéal engendré par le système d'équations donné en entrée n'est pas radical, et une décomposition primaire minimale de cet idéal contient un grand nombre de composantes primaires imergées.

Des résultats plus positifs montrent que dans le cas zéro-dimensionnel, le calcul de bases de Gröbner est de complexité simplement exponentielle en le nombre de variables ([83, 84, 67]). D'autres résultats [16] portent plus spécifiquement sur l'algorithme donné dans [51] et permettent d'obtenir des bornes de complexité simplement exponentielles en le nombre de variables sous certaines hypothèses de régularité (et pas uniquement dans le cas zéro-dimensionnel).

Dans le cas zéro-dimensionnel, les bases de Gröbner lexicographiques sont d'un intérêt plus particulier car en position Shape Lemma [24, 27, 55] elles permettent de compter le nombre de racines réelles. Ces bases de Gröbner peuvent être obtenues par l'algorithme de changement d'ordre FGLM [52].

En pratique[9], on est loin de constater un comportement doublement exponentiel. Les bases de Gröbner constituent un outil de résolution des systèmes d'équations polynomiales standard si bien que presque tous les systèmes de calcul formel permettent de les calculer plus ou moins efficacement. De plus, lorsqu'on utilise l'ordre DRL, les bases de Gröbner tirent avantageusement profit d'une éventuelle sur-détermination du système d'équations donnés en entrée (des explications partielles à ce constat empirique se trouvent dans [16]). Ce point est important dans la mesure où les systèmes polynomiaux engendrés par la caractérisation algébrique des points critiques donnés dans le lemme 4 sont sur-déterminés. Enfin, mentionnons qu'en combinant les techniques de calcul d'ensembles triangulaires avec des calculs de bases de Gröbner, on peut obtenir des décompositions équi-dimensionnelles et radicales d'idéaux telles que chaque composante équi-dimensionnelle soit encodée par une base de Gröbner engendrant son idéal associé.

Les systèmes de calcul formel réputés pour fournir les implantations les plus efficaces permettant le calcul de bases de Gröbner sont `Magma` [3] et `Singular` [7]. L'algorithme implanté est celui décrit dans [50]. Néanmoins, ils n'ont pas le niveau de performances du logiciel spécialisé `FGb` implanté en `C` par J.-C. Faugère.

[9] c'est-à-dire sur les systèmes polynomiaux intervenant dans de réelles applications, et à condition de disposer d'une implantation bien travaillée.

Des bases de Gröbner aux paramétrisations rationnelles. Voyons comment obtenir des paramétrisations rationnelles (plus précisément des Représentations Univariées Rationnelles, voir [121, 122]) à partir d'une base de Gröbner.

Si S est zéro-dimensionnel et $I = \langle S \rangle$, l'algèbre-quotient $A = \mathbb{Q}[X_1, \ldots, X_n]/I$ est un $\mathbb{Q}$-espace vectoriel dont la dimension est égale au nombre de solutions de S comptées avec multiplicités dans $\mathbb{C}^n$, qu'on note δ dans la suite. Voyons comment on réduit le calcul de paramétrisations rationnelles à des questions d'algèbre linéaire dans A. Pour simplifier, on suppose que I est radical.

On considère dans A les endomorphismes de multiplication M_f pour tout $f \in A$:

$$\begin{array}{rccc} M_f : & A & \longrightarrow & A \\ & p & \rightarrow & fp \end{array}$$

Évidemment, M_f est une application linéaire et pour tout couple de polynômes f, g, on a $M_f M_g = M_{fg}$.

Puisque M_f est une application linéaire, elle a un polynôme caractéristique $\chi_f \in \mathbb{Q}[T]$ si bien que $\chi_f(M_F) = 0$. Ainsi, $\chi_f(F) = 0$ dans A ce qui implique que $\chi_f(F)$ appartient à I. En d'autres termes, $\chi_f(F)$ s'annule en les racines de I.

Soit u un élément de A qui sépare les racines de I (pour tout couple de racines distinctes (x, y) de I, $u(x) \neq u(y)$) et χ_u le polynôme caractéristique de l'endomorphisme de multiplication par u dans A. Ainsi, la famille $1, u, \ldots, u^{\delta-1}$ forme une base de l'algèbre-quotient A en tant que $\mathbb{Q}$-espace vectoriel.

Il existe donc des polynômes univariés $G_1, \ldots, G_n$ tels que $X_i = G_i$ dans A (pour $i \in \{1, \ldots, n\}$). Ces polynômes constituent une paramétrisation possible des coordonnées des racines de I. Ce n'est pas la seule possible et comme indiqué dans [8, 122, 121], la plus pertinente consiste à considérer une fraction rationnelle $\frac{q_i}{q_0}$ où q_0 est la dérivée du polynôme minimal de l'endomorphisme de multiplication par u dans A.

Ceci dit, vérifier qu'un élément u de A est bien séparant (surtout dans le cas où I n'est pas radical), et accéder aux paramétrisations ne sont pas des opérations simples calculatoirement (les matrices manipulées sont de taille $\delta \times \delta$). Dans [121, 122], F. Rouillier donne une algorithmique efficace fondée sur :

- un calcul intelligent de la table de multiplication dans A fondés sur des calculs de formes normales ;
- des tests efficaces de choix d'élément séparant ;
- des formules de trace permettant d'obtenir les paramétrisations voulues.

Résultats de complexité. Soit S un système zéro-dimensionnel dans $\mathbb{Q}[X_1, \ldots, X_n]$, tel que l'idéal I est de degré δ. Dans [121, 122], F. Rouillier montre que le calcul d'une Représentation Univariée Rationnelle à partir de la table de multiplication de l'anneau-quotient $\mathbb{Q}[X_1, \ldots, X_n]/I$ peut se faire en $O(n\delta^2)$ opérations arithmétiques dans $\mathbb{Q}$. De plus, la table de multiplication peut se construire à partir d'une base de Gröbner en $O(\delta^4)$ opérations arithmétiques dans δ. En termes du nombre d'opérations arithmétiques, cet algorithme est polynomial en le nombre de racines complexes d'un système zéro-dimensionnel, une fois la base de Gröbner calculée.

Du point de vue pratique, le logiciel `RS` [120] implanté par F. Rouillier en `C` est le plus efficace pour calculer des représentations univariées rationnelles à partir d'une base de Gröbner. Il permet de résoudre efficacement des systèmes polynomiaux zéro-dimensionnels ayant un nombre de solutions complexes de l'ordre du millier. Interfacé avec `Maple` [4], il devrait bientôt y être intégré.

5.1.3 Résolution géométrique

Une alternative aux méthodes décrites ci-dessus a été dévelopée pour obtenir :

- dans le cas des systèmes zéro-dimensionnels une paramétrisation rationnelle de l'ensemble des solutions complexes ;
- dans le cas des systèmes de dimension positive, des paramétrisations rationnelles encodant des points génériques sur chaque composante équi-dimensionnelle de l'ensemble des complexes du système étudié.

L'entrée des algorithmes de calcul de résolution géométrique est un programme d'évaluation du système d'équations et d'inéquations polynomiales :

$$f_1 = \cdots = f_s = 0, \quad h \neq 0$$

où $(f_1, \ldots, f_s, h) \subset \mathbb{Q}[X_1, \ldots, X_n]$.

Dans les cas où $(f_1, \ldots, f_s, h)$ constitue une suite régulière réduite [10], la sortie de l'algorithme donné dans [61] est une paramétrisation rationnelle des solutions de la clôture de Zariski de l'ensemble constructible défini par le système donné en entrée. Cette paramétrisation rationnelle est écrite sur la base monomiale standard.

Si $(f_1, \ldots, f_s, h)$ n'est pas une suite régulière réduite, la sortie de l'algorithme donné dans [94] est un *ensemble* fini de paramétrisations rationnelles encodant des points génériques sur chaque composante équi-dimensionnelle de la clôture de Zariski de l'ensemble constructible défini par le système donné en entrée.

Le principe de l'algorithme consiste en un procédé itératif d'intersection et d'interpolation qui consiste à :

- calculer une résolution géométrique du système $f_1 = \cdots = f_i = 0, \ \ h \neq 0$
- calculer une courbe de remontée sur cette variété via un processus de remontée ■à la Hensel■;
- calculer l'intersection de cette courbe de remontée avec l'hypersurface définie par $f_{i+1} = 0$ et retirer de la résolution obtenue les points annulant h. On a ainsi obtenu une résolution géométrique de la clôture de Zariski de l'ensemble constructible défini par

$$f_1 = \cdots = f_{i+1} = 0, \quad h \neq 0.$$

Les algorithmes donnés dans [61, 94] sont probabilistes mais leur complexité est bien controllée. Dans la suite on note $M(x)$ le coût de la multiplication de deux polynômes univariés de degré x et on dira que $p \in \mathcal{O}_{\log}(x)$ si il existe une constante a telle que $p \in \mathcal{O}(x \log x^a)$. Enfin, on note $\mathcal{U}(a)$ la quantité $a \log^2(a) \log(\log(a))$.

Théorème 18. *[61] Soit $(f_1, \ldots, f_s, g)$ $s+1$ polynômes dans $\mathbb{Q}[X_1, \ldots, X_n]$ de degré borné par D, et $\mathcal{L}$ la complexité d'évaluation de $(f_1, \ldots, f_s, g)$. Supposons que $(g_1, \ldots, g_n)$ soit une suite régulière réduite dans l'ensemble $\{x \in \mathbb{C}^n \mid g \neq 0\}$.*

Il existe un algorithme probabiliste calculant une résolution géométrique de la clôture de Zariski de l'ensemble des solutions complexes du système $g_1 = \cdots = g_s = 0, \quad h \neq 0$ en

$$\mathcal{O}\left(n(n\mathcal{L} + n^3)\mathcal{U}(D.\delta)^2\right)$$

opérations arithmétiques dans $\mathbb{Q}$ où δ (qui est bornée par D^n) est le maximum des degrés des clôtures de Zariski des ensembles de solutions complexes des systèmes $f_1 = \cdots = f_i = 0, \quad h \neq 0$.

Dans le cas des systèmes polynomiaux ne formant pas une suite régulière réduite, le résultat de complexité conernant le calcul de résolutions géométriques

Théorème 19. *[94] Soit $f_1, \ldots, f_s$ et h des polynômes de degré borné par D dans $\mathbb{Q}[X_1, \ldots, X_n]$, représentés par un programme d'évaluation de longueur $\mathcal{L}$. Il existe un algorithme calculant une résolution géométrique de la clôture de Zariski de $V(g_1, \ldots, g_S) \setminus V(g)$ dont la complexité arithmétique est :*

$$\mathcal{O}_{\log}\left(Sn^4(n\mathcal{L} + n^4)M(D\mathfrak{d})\right)^3$$

où $\mathfrak{d}$ est le maximum des sommes des degrés algébriques des composantes irréductibles des clôtures de Zariski des ensembles constructibles définis par $f_1 = \cdots = f_i = 0, h \neq 0$ pour i dans $1, \ldots, s$.

Remarque. *Dans [94], G. Lecerf montre que la complexité binaire de l'algorithme qu'il y donne est*

$$\tau\mathcal{O}_{\log}\left(Sn^4(n\mathcal{L} + n^4)M(D\mathfrak{d})\right)^4$$

où τ borne la taille binaire des coefficients du système donné en entrée.

[10] Ceci signifie que si on note I_i l'idéal $\langle f_1, \ldots, f_i, Lh-1\rangle \cap \mathbb{Q}[X_1, \ldots, X_n]$ (où L est une nouvelle variable), f_{i+1} ne divise pas zéro dans $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I_i}$ (pour $i = 1, \ldots, n-1$) et les idéaux I_i sont radicaux (pour $i = 1, \ldots, n$)

Les algorithmes de calcul de résolution géométrique donnés dans [61, 94] sont plus récents et fondés sur des idées similaires à celles développées dans [60, 57, 59]. L'implantation du paquetage `Kronecker` dans le système de Calcul Formel Magma [3] dûe à G. Lecerf a un niveau de performance comparable à celui de la suite logicielle `Gb-RealSolving` développée en C++ par J.-C. Faugère et F. Rouillier mais est encore loin du niveau de performances de la suite `FGb-RS` qui lui a succédé (tout du moins sur le type de systèmes que nous avons été amenés à étudier).

Enfin, mentionnons que nous avons constaté que, en pratique, l'algorithme de résolution géométrique n'a pas en général un bon comportement sur les systèmes polynomiaux engendrés par la caractérisation algébrique de points critiques obtenus par le lemme 4. En effet, ces systèmes sont sur-déterminés. Ce qu'on constate en pratique c'est que, en général, le maximum des degrés δ_i apparraissant dans l'étude des variétés intermédiaires qui est faite dans le procédé de résolution incrémentale est supérieur au degré de la sortie. Cet algorithme a un bien meilleur comportement sur les systèmes issus de la caractérisation lagrangienne des points critiques (voir lemme 5).

Ceci dit, la complexité des algorithmes donnés dans [61, 94] s'exprime en fonction de certains degrés géométriques alors que, pour l'heure, la complexité des calculs de bases de Gröbner s'exprime en fonction de quantités purement algébriques. Dans la suite de ce chapitre, nous allons étudier divers algorithmes faisant intervenir des objets géométriques dont on va pouvoir évaluer finement le degré. Les résultats de complexité de [61, 94] permettent d'expliquer, partiellement, pourquoi, en pratique, on constate que telle stratégie est plus efficace que telle autre. Ce qui est remarquable, *mais n'est qu'un constat empirique sur le problème particulier qui nous intéresse*, c'est que toute amélioration obtenue par des estimations de complexité fondés sur les résultats de [61, 94] a une traduction concrète en terme de performances pratiques lorsqu'on utilise des bases de Gröbner. Ceci est donc un outil supplémentaire pour aiguiller la recherche de procédés géométriques permettant la calcul d'au moins un point par composante connexe bien qu'il ne puisse se subsitituer à une validation expérimentale des résultats obtenus.

Nous venons de décrire brièvement les outils d'élimination algébrique que nous utiliserons pour mettre en œuvre la méthode des points critiques. Dans la section suivante, nous montrons comment obtenir un algorithme calculant au moins un point par composante connexe dans un ensemble algébrique réel et relevant de la méthode des points critiques et dont la complexité est polynomiale en la borne de Bézout.

5.2 Obtenir une complexité polynomiale en la borne de Bézout

5.2.1 L'algorithme

Nous avons vu en introduction que le calcul d'au moins un point par composante connexe dans une hypersurface réelle $\mathcal{H} \cap \mathbb{R}^n$ compacte et lisse peut se faire simplement par le calcul de points critiques d'une projection choisie de manière telle que sa restriction à $\mathcal{H}$ admet un lieu critique qui soit zéro-dimensionnel (à condition qu'on sache résoudre un système d'équations polynomiales zéro-dimensionnels).

Ce paragraphe reprend l'algorithme décrit dans [18] qui met en œuvre ce principe et dont la complexité est polynomiale en la borne de Bézout. Celui-ci prend en entrée un système d'équations polynomiales dans $\mathbb{Q}[X_1, \ldots, X_n]$ définissant une variété algébrique $V \subset \mathbb{C}^n$ et retourne une famille finie de paramétrisations rationnelles encodant un ensemble algébrique zéro-dimensionnel inclus dans V et ayant une intersection non vide avec chaque composante connexe de $V \cap \mathbb{R}^n$. Cet algorithme procéde à diverses réductions pour ramener le calcul d'au moins un point par composante connexe dans $V \cap \mathbb{R}^n$ au cas d'une hypersurface lisse dont le lieu réel est compact. Cette réduction se fait en plusieurs étapes.

Tout d'abord, on passe du cas d'un système d'équations polynomiales $f_1 = \cdots = f_s = 0$ au cas d'une seule équation en considérant le polynôme $f = f_1^2 + \cdots + f_s^2$. L'hypersurface $\mathcal{H} \subset \mathbb{C}^n$ définie par $f = 0$ dans $\mathbb{C}^n$ a un lieu singulier qui contient la variété algébrique définie par $f_1 = \cdots = f_s = 0$ et est donc en général de dimension positive. De plus, l'ensemble algébrique réel $\mathcal{H} \cap \mathbb{R}^n$ n'a aucune raison d'être compact.

La réduction au cas d'une hypersurface lisse et compacte se fait en procédant à diverses déformations de l'hypersurface $\mathcal{H}$ pour finir par considérer une hypersurface $\mathcal{H}' \subset \mathbb{C}\langle\zeta, \Omega\rangle^{n+1}$ (où ζ et Ω sont des infinitésimaux) telle que :

- $\mathcal{H}'$ est une hypesurface lisse ;
- $\mathcal{H}' \cap \mathbb{R}\langle\zeta, \Omega\rangle^n$ est compacte ;

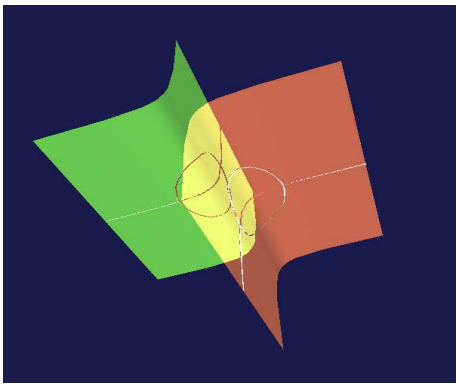

FIG. 17 –

- le lieu critique $\mathfrak{C}(\pi_1, \mathcal{H}')$ de la projection π_1 sur X_1 restreinte à $\mathcal{H}'$ est zéro-dimensionnel ;
- les limites (quand les infinitésimaux introduits tendent vers 0) des points obtenus comme projections de $\mathfrak{C}(\pi_1, \mathcal{H}')$ sur $X_1, \ldots, X_n$ ont une intersection non vide avec chaque composante connexe de $\mathcal{H} \cap \mathbb{R}^n$;
- si $F \in \mathbb{Q}\langle\zeta, \Omega\rangle[X_1, \ldots, X_n]$ est un polynôme square-free tel que $F = 0$ définit $\mathcal{H}'$ alors le systéme d'équations polynomiales ci-dessous qui définit $\mathfrak{C}(\pi_1, \mathcal{H}')$:

$$F = \frac{\partial F}{\partial X_2} = \cdots = \frac{\partial F}{\partial X_{n+1}} = 0$$

constitue une base de Gröbner pour l'ordre du degré lexicographique $X_1 < \cdots < X_n < X_{n+1}$.

Nous décrivons ci-dessous les techniques mises en œuvre pour procéder à une telle réduction.

Soit $f \in \mathbb{Q}[X_1, \ldots, X_n]$, on note $V(f) \subset C^n$ l'hypersurface définie par $f = 0$. Soit X_{n+1} une nouvelle variable, on pose

$$F_1 = f^2 + (X_1^2 + \cdots + X_{n+1}^2 - 1/\Omega^2)^2$$

où Ω est un infinitésimal.

Il est démontré dans [18] que l'hypersurface $V(F_1) \bigcap \mathbb{R}\langle 1/\Omega\rangle^{n+1}$ est contenue dans la boule ouverte de centre l'origine et de rayon $1/\Omega + 1$ et que l'extension de toute composante semi-algébriquement connexe de $V(f) \bigcap \mathbb{R}^n$ à $\mathbb{R}\langle\Omega\rangle^n$ contient la projection d'une composante de $V(F_1) \bigcap \mathbb{R}\langle\Omega\rangle^{n+1}$ sur $\mathbb{R}\langle\Omega\rangle^n$.

Ceci est illustré par les figures 17 et 18. On y considère une hyperbole dans un plan et le cylindre construit sur cet hyperbole dans l'espace. L'intersection de ce cylindre avec une sphère de rayon *suffisamment grand* définit une courbe

- dont chaque composante connexe est compacte d'une part ;
- et la donnée d'au moins un point dans celle-ci permet d'obtenir au moins un point par composante connexe de l'hyperbole en les projetant dans le plan d'autre part.

Le problème réside maintenant dans le fait que l'hypersurface définie par $F_1 = 0$ est singulière. On montre maintenant comment déformer F_1 pour obtenir à la fois une hypersurface $\mathcal{H}'$ lisse et que le lieu critique $\mathfrak{C}(\pi_1, \mathcal{H}')$ de la restriction de la projection π_1 sur X_1 à $\mathcal{H}'$ donnée par le lemme 4 constitue une base de Gröbner pour l'ordre du degré lexicographique $X_1 < \cdots < X_n < X_{n+1}$.

On note D le degré total de f et D_i (pour $i \in \{1, \ldots, n\}$) les degrés maximaux des monômes de f contenant la variable X_i et on suppose (quitte à renuméroter les variables apparaissant dans f) que $D_1 \geqslant \ldots \geqslant D_n$. On pose alors

$$F = (1 - \zeta)F_1 + \zeta(X_1^{2(D_1+1)} + \ldots + X_n^{2(D_n+1)} + X_{n+1}^6 - (n+1)(\Omega^{2(D+1)}))$$

où ζ est un infinitésimal positif. Il est démontré dans [18, 21] que :

1. L'ensemble $V(F) \bigcap R\langle\zeta\rangle^n$ est borné et lisse.

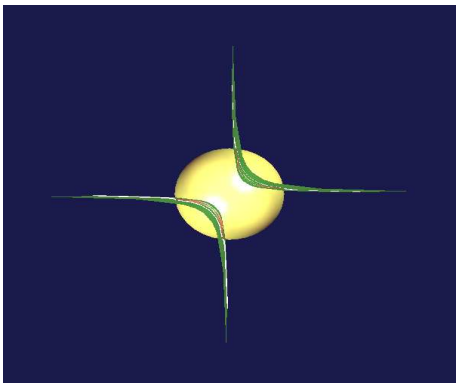

FIG. 18 –

2. Les polynômes
$$F, \frac{\partial F}{\partial X_2}, \ldots, \frac{\partial F}{\partial X_{n+1}}$$
forment une base de Gröbner pour l'ordre du degré lexicographique $X_1 > \ldots > X_n$: c'est pour garantir cette propriété que la déformation faite sur F_1 pour obtenir F fait intervenir des degrés élevés en les variables $X_1, \ldots, X_n$.
Si on note $\mathcal{H}' \subset \mathbb{C}\langle\zeta, \Omega\rangle$ l'hypersurface définie par $F = 0$ et par π_1 la projection sur X_1, le système ci-dessus définit bien le lieu critique $\mathfrak{C}(\pi_1, \mathcal{H}')$ de π_1 restreinte à $\mathcal{H}'$.
3. $\mathfrak{C}(\pi_1, \mathcal{H}')$ est un nombre fini de points dans $\mathbb{C}\langle\zeta, \Omega\rangle^n$.
4. Pour toute composante connexe C de $V(f) \bigcap \mathbb{R}^n$, il existe un point $x \in \mathfrak{C}(\pi_1, \mathcal{H}')$ tel que la limite du projeté de x sur $X_1, \ldots, X_n$ quand $, \zeta, \Omega$ tendent vers 0 appartienne à C.

Puisque le système
$$F, \frac{\partial F}{\partial X_2}, \ldots, \frac{\partial F}{\partial X_n}, \frac{\partial F}{\partial X_{n+1}}$$
est déjà une base de Gröbner pour l'ordre $X_1 < \cdots < X_{n+1}$, le calcul d'une paramétrisation de l'ensemble de ses solutions dans $\mathbb{C}\langle\zeta, \Omega\rangle^n$ se réduit à des opérations d'algèbre linéaire dans l'anneau des polynômes $\mathbb{Q}(\zeta, \Omega)[X_1, \ldots, X_{n+1}]$ quotienté par l'idéal engendré par le système ci-dessus. Ainsi, on obtient une description des points de $\mathcal{C}$ sous la forme :
$$\begin{cases} X_{n+1} &= \frac{q_{n+1}(T)}{q_0(T)} \\ X_n &= \frac{q_n(T)}{q_0(T)} \\ & \vdots \\ X_1 &= \frac{q_1(T)}{q_0(T)} \\ q(T) &= 0 \end{cases}$$

Ici les polynômes $q, q_0, q_1, \ldots, q_n, q_{n+1}$ sont des polynômes de $\mathbb{Q}(\zeta, \Omega)[T]$.

Obtenir une projection de ces points dans $X_1, \ldots, X_n$ est alors immédiat. Il reste à calculer les limites des points ainsi définis lorsque les infinitésimaux ζ et Ω tendent vers 0. Cette opération n'est pas immédiate et ne se limite pas à instantier ces ζ et Ω à 0 dans les polynômes $q, q_0, q_1, \ldots, q_n$, d'autant plus que lorsque ces infinitésimaux tendent vers 0, certaines solutions peuvent tendre vers l'infini. Une procédure permettant ce calcul est décrite dans [124]. Celle-ci est particulièrement coûteuse en pratique (son coût est polynomiale en la borne de Bézout). Des améliorations fondées sur des développements en séries de Puiseux sont proposées dans [127].

On peut maintenant donner une description complète d'un algorithme de calcul d'au moins un point par composante connexe dans une variété algébrique réelle. La complexité théorique de cet algorithme ainsi que son comportement en pratique sont discutés plus loin.

Algorithme : Calcul d'au moins un point par composante connexe d'une variété algébrique quelconque (Mise en œuvre de déformations – dû à Basu, Pollack et Roy)

- **Entrée :** Un système $S = (f_1, \ldots, f_s)$ d'équations polynomiales dans $\mathbb{Q}[X_1, \ldots, X_n]$.
- **Sortie :** Une liste de paramétrisations rationnelles représentant au moins un point par composante semi-algébriquement connexe de $V(S)$.

1. Poser $f := f_1^2 + \ldots + f_s^2$.
2. Introduire une nouvelle variable X_{n+1} et poser $F_1 := f + (X_1^2 + \ldots + X_n^2 + X_{n+1}^2 - 1/\Omega^2)^2$.
3. Poser $F := (1-\zeta)F + \zeta(X_1^{2(d_1+1)} + \ldots + X_n^{2(d_n+1)} + X_{n+1}^6 - (n+1)\Omega^{2(d+1)})$, où $d_1, \ldots, d_n, d_{n+1}$ sont les degrés totaux de F_1 en $X_1, \ldots, X_n, X_{n+1}$ tels que $d_1 \geqslant \ldots \geqslant d_{n+1}$.
4. Calculer les dérivées partielles $\frac{\partial F}{\partial X_1}, \ldots, \frac{\partial F}{\partial X_n}$.
5. Calculer une Représentation Univariée Rationnelle à coefficients dans $\mathbb{Q}(\Omega)\langle\zeta\rangle$ à partir de la base de Gröbner

$$[F, \frac{\partial F}{\partial X_1}, \ldots, \frac{\partial F}{\partial X_{n+1}}]$$

   associée à un élément bien séparant
6. Retourner les limites des points encodés par cette RUR lorsque ζ et Ω tendent vers 0.

5.2.2 Analyse de complexité et comportement en pratique

Soit D le maximum des degrés des polynômes $f_1, \ldots, f_s$ donné en entrée à l'algorithme ci-dessus. Le polynôme F_1 est de degré $2D$. Si on suppose que le degré total de chaque variable est D dans F_1, le polynôme F est alors de degré $4D$. La base de Gröbner nécessaire au calcul de Représentation Univariée Rationnelle est obtenue immédiatement, sans surcoût. Le degré de l'idéal engendré par cette base de Gröbner est alors *systématiquement* égale à $(4D)(4D-1)^n$. En appliquant les résultats de [121, 122], le calcul de Représentations Univariées Rationnelles se fait en $\mathcal{O}((4D)^{4(n+1)} + (n+1)(4D)^{2(n+1)})$ opérations arithmétiques dans $\mathbb{Q}(\zeta, \Omega)$. Dans le pire cas, le surcoût arithmétique de l'introduction de ζ et Ω est de l'ordre du degré de l'idéal. La complexité de cet algorithme est donc $\mathcal{O}((4D)^{6(n+1)} + (n+1)(4D)^{4(n+1)})$ opérations arithmétiques dans $\mathbb{Q}$. Il n'y a pas de surcoût à cette complexité induit par le calcul des limites (lorsque les infinitésimaux introduits tendent vers 0) des racines encodées par les paramétrisations.

Considérons maintenant l'hypersurface définie par le polynôme dans $\mathbb{Q}[X_1, \ldots, X_n]$ ci-dessous :

$$\sum_{i=1}^{n} (\prod_{j=1}^{D} (X_i - j))^2 = 0.$$

Ce polynôme est de degré $2D$ et le lieu réel de l'hypersurface qu'il définit est un ensemble de D^n points isolés. Ainsi, sur cet exemple, la taille de la sortie est en $\mathcal{O}(D)^n$, on peut donc considérer qu'un algorithme simplement exponentiel pour donner au moins un point par composante semi-algébriquement connexe est ■optimal■, si tant qu'on accepte ce qualificatif pour un algorithme dont la complexité est polynomiale en la taille de la sortie.

De manière à tester la taille des données intermédiaires apparaissant au cours d'un tel algorithme,

nous avons simulé celui-ci en `Maple` sur le système d'équations polynomiales suivant :

$$\begin{cases} x^2 + y^2 + z^2 - 1 = 0 \\ xyz - 1 = 0 \end{cases}$$

Notons que ce système d'équations est très simple et que l'algorithme de décomposition cylindrique algébrique parvient à le résoudre.

Après les manipulations effectuées par l'algorithme décrit dans le paragraphe précédent, nous obtenons directement une base de Gröbner qui permet de déduire facilement le degré de l'idéal qui lui est associé.

Dans le cas précis qui nous intéresse, on trouve que ce degré est 16128 ! Nous devons alors en calculer une Représentation Univariée Rationnelle. Il est évident que même sur les entiers, un tel calcul est trop couteux. Dans le cas présent, nous devons effectuer ces calculs dans $\mathbb{Q}\langle\Omega, \zeta\rangle$, ce qui complique le problème. Il n'est donc pas étonnant de constater que ce calcul ne passe pas. En posant l'hypothèse que pour une entrée de taille plus importante, le temps de calcul est plus important, il apparait clairement que cet algorithme ne pourra pas donner de bons résultats en pratique. Analysons les étapes bloquantes :

- sur l'exemple ci-dessus, le degré de l'idéal zéro-dimensionnel est un facteur bloquant. Soit D un entier qui borne le degré des polynômes du système d'entrée. Les degrés des polynômes P et Q calculés par l'algorithme sont alors bornés par $2D$. En bornant D_1 par D, on trouve que le degré de Q_1 est borné par $2D(2D + 1)$. Comme on a rajouté une variable, on trouve que le degré du système zéro-dimensionnel produit est **toujours** de l'ordre de $6(4D)^n$, ce qui donne sur notre exemple simple 20736. On constate que l'élévation au carré du pas 1 de l'algorithme ainsi que la déformation du pas 3 sont responsables de la taille de ces systèmes zéro-dimensionnels. Il est clair que la déformation du pas 3 de l'algorithme engendre une croissance de degré pour se ramener sans calcul à une base de Gröbner.
- Remarquons que même si on ne considère en entrée que des hypersurfaces, cette croissance de degrés intervient : le pas 2 de l'algorithme en est responsable. Or, cette déformation est rendue nécessaire par l'usage de la fonction de projection : on doit se ramener au cas d'une hypersurface compacte pour qu'elle atteigne ses valeurs critiques sur chacune des composantes semi-algébriquement connexes.
- Supposons que les méthodes de résolution des systèmes zéro-dimensionnels permettent de résoudre des problèmes dont la taille est de l'ordre de ce que nous avons obtenu. Notons qu'au pas 2 nous n'avons introduit qu'un seul infinitésimal. En revanche, il est clair que l'hypersurface obtenue contient une infinité de singularités. Ceci implique – en partie – l'introduction de l'infinitésimal dans le pas 3 de l'algorithme. Nous devrions alors travailler sur une arithmétique à deux infinitésimaux, dont les opérations élémentaires sont bien plus couteuses que sur les entiers.

Notons enfin que la taille des données intermédiaires est largement supérieure aux bornes données dans le chapitre 4 sur le nombre de points critiques restreinte à la variété définie par $f_1 = \ldots = f_s = 0$ (à supposer qu'il vérifie les hypothèses du lemme 5). En particulier, dans le cas quadratique, l'algorithme qu'on vient d'étudier n'est plus polynomial en le nombre de variables.

Pour parvenir à des algorithmes efficaces, on va :

- s'autoriser le calcul *explicite* de bases de Gröbner (ou l'usage de routines d'élimination algébrique) sans chercher à le contourner en procédant à des déformations. Par exemple, dans ce cas, le pas 3 de l'algorithme donné dans ce paragraphe peut être substitué par l'étude du polynôme $F := F_1 - \zeta$ qui définit une hypersurface lisse.
  Ceci présente l'avantage d'éviter la croissance de degré induit par ce pas d'une part et n'impose pas un degré systématiquement égale à la borne de Bézout, ce qui nous laisse une chance d'être efficace. De plus, notons que l'on garde un algorithme simplement exponentiel en le nombre de variables si les calculs de points critiques qu'on effectue induisent la résolution de systèmes zéro-dimensionnels.
- On n'est pas pour autant sorti d'affaire : rien n'indique que le système caractérisant les points critiques de la projection sur X_1 est zéro-dimensionnel. En revanche, si on sait prouver que pour un choix générique de projection [11] ceci est vérifié, on aura en pratique un bon algorithme (il n'en reste pas moins vrai qu'en théorie, éviter à coup sûr un Zariski fermé de degré δ dans $\mathbb{C}^n$ coûte δ^n opérations).
  On s'autorisera donc à faire dépendre nos algorithmes de choix génériques (lorsqu'on est capable de vérifier qu'ils sont bons), si tant est qu'en pratique un choix aléatoire s'avère correct.

[11] par générique, on entend ici que tout mauvais choix est inclus dans un fermé de Zariski

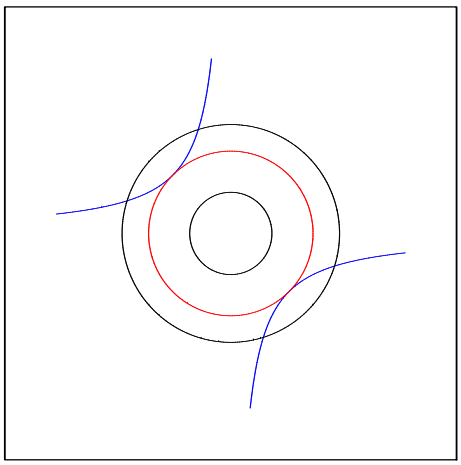

FIG. 19 – Points critiques de la fonction distance

- Pour éviter la croissance de degré induite par les pas 1 et 2 ainsi que l'introduction de singularités dans un problème qui initialement n'en avait pas, lorsque c'est possible, on évitera de :
  - se ramener au cas d'une hypersurface en considérant la somme des carrés des polynômes donnés en entrée ;
  - se ramener au cas compact en considérant l'intersection de la variété étudiée avec une hyperboule de rayon infiniment grand.
    Concernant ce dernier point, ceci implique de contourner l'hypothèse de compacité sous-jacente à toutes les présentations de la méthode des points critiques qu'on a faites jusqu'ici. Pour ce faire, on peut penser à utiliser des fonctions polynomiales qui associent à un point le carré de leur distance euclidienne à un autre point fixé.

5.3 Gestion récursive des chutes de rang dans les jacobiennes : Utilisation de fonctions distance à un point

Dans cette section, on contourne les problèmes de compacité en utilisant des calculs de points critiques d'une fonction associant à $4x \in \mathbb{C}^n$ le carré de sa distance euclidienne à un point $A \in \mathbb{Q}^n$. En effet, étant donnée une variété algébrique $V \cap \mathbb{C}^n$, et un point $A \in \mathbb{Q}^n$ il est évident que pour tout $r \in \mathbb{R}$ positif, $\varphi_A^{-1}(r) \cap V \cap \mathbb{R}^n$ est compact ce qui implique que la fonction φ_A est propre. Ainsi, grâce à la proposition 16, on sait que φ_A atteint ses extrema sur chaque composante connexe de $V \cap \mathbb{R}^n$. Cette "astuce" qui consiste à considérer une fonction distance au lieu d'une fonction de projection permet ainsi de contourner les problèmes liés à l'éventuelle non-compacité de $V \cap \mathbb{R}^n$.

Elle ne nous dit pas pour autant comment on peut ramener le calcul d'au moins un point par composante connexe dans $V \cap \mathbb{R}^n$ à la résolution de systèmes polynomiaux de dimension zéro. Deux problèmes doivent être traîtés :

- garantir le fait que le lieu critique de la restriction de φ_A à V est de dimension zéro lorsque V est lisse et équi-dimensionnelle et définie par un système de générateurs de l'idéal associé à V.
- gérer les éventuelles chutes de rang dans la matrice jacobienne associée à la famille de polynômes donnés en entrée et qui empêchent de caractériser le lieu critique de φ_A restreinte à la variété algébrique définie par le système donné en entrée.

Si $(f_1, \ldots, f_s)$ est une famille de polynômes dans $\mathbb{Q}[X_1, \ldots, X_n]$, on note $V(f_1, \ldots, f_s) \subset \mathbb{C}^n$ la variété algébrique définie par le système d'équations polynomiales :

$$f_1 = \ldots = f_s = 0$$

et $I = \langle f_1, \ldots, f_s \rangle$ l'idéal de $\mathbb{Q}[X_1, \ldots, X_n]$ engendré par cette famille de polynômes.

Étudions l'hypersurface définie par :

$$x^2 - y^2 z^2 + z^3 = 0$$

En choisissant le point $A = (1, 2, 3)$, et en appliquant le lemme 4, on obtient le système suivant :

$$\begin{cases} x^2 - y^2z^2 + z^3 = 0 \\ 2xy - 4x + 2yz^2x - 2yz^2 = 0 \\ -2yz^3 + 3yz^2 + 2y^3z - 4y^2z + 6z^2 = 0 \\ 2xz - 6x + 2y^2zx - 2y^2z - 3z^2x + 3z^2 = 0 \end{cases}$$

Ce système engendre un idéal de dimension 1 et de degré 1. Il contient l'ensemble des singularités de l'hypersurface :

$$\begin{cases} z = 0 \\ x = 0 \end{cases}$$

qui est de dimension strictement inférieure à celle de l'hypersurface. Par ailleurs, si on effectue une **décomposition équi-dimensionnelle de l'idéal** engendré par le système ci-dessus, on obtient en plus de l'ensemble des singularités l'ensemble zéro-dimensionnel de degré 15 suivant (décrit par une base de Gröbner lexicographique) :

```
[5398746452967737165 36*x-39839127175867630680*z^14+260049173095318667844*z^13_
-884921439347428617838*z^12+241439943785935603983*z^11-477189935892012519501 1*z^10_
+828348232997669903598 8*z^9-128727432633087200906 11*z^8+155057867732297876706 94*z^7_
-190231512612740652857 21*z^6+187831377104131807646 74*z^5-169860202089426392258 55*z^4_
+141312050284538749208 61*z^3-96334454318905163714 96*z^2+359278859613023062414 4*z-405065429115903549440,
107974929059354743307 2*y+388877953166856734616*z^14-239774056624577358342 0*z^13_
+789049928054229535769 4*z^12-213326745456412389166 13*z^11+406633699544901447192 45*z^10__
-710895613354483639091 84*z^9+108592493361350014231477*z^8-127906837049701883884902*z^7_
+162372795006716365235491*z^6-146027326440241785868030*z^5+145598671015416598891205*z^4_
-104163140703335157603823*z^3+780463042380827186421 72*z^2-211833873365449148816 80*z_
+222086046058895712457 6,
36*z^15-228*z^14+769*z^13-2108*z^12+4136*z^11-7323*z^10+11386*z^9-13908*z^8+17600*z^7_
-16778*z^6+16529*z^5-12732*z^4+9480*z^3-3639*z^2+852*z-80]
```

On voit sur cet exemple qu'en caractérisant les points critiques de la fonction distance à un point arbitrairement choisi, sur une variété algébrique définie par un ensemble fini de polynômes, on est ramené à l'étude d'une sous-variété de dimension inférieure (l'ensemble des singularités de la variété). C'est cette idée que l'on retrouve antérieurement dans [39] qu'on peut tenter de mettre en œuvre.

Notation. *Soit $S = \{f_1, \ldots, f_s\}$ un ensemble de polynômes dans $\mathbb{Q}[X_1, \ldots, X_n]$ tel que $V = V(S)$ est une variété de dimension d. Etant donné un point $A \in \mathbb{C}^n$, on définit l'ensemble algébrique suivant :*

$$\mathfrak{C}(V, A) = \{M \in V \mid \text{rang}(\mathbf{grad}_M(f_1), \ldots, \mathbf{grad}_M(f_s), \mathbf{AM} \leqslant n - d)\}$$

La construction et l'étude de $\mathfrak{C}(V, A)$ n'a d'intérêt que si :
- $\mathfrak{C}(V, A)$ intersecte chaque composante semi-algébriquement connexe de $V \bigcap \mathbb{R}^n$,
- $\mathfrak{C}(V, A)$ est strictement incluse dans V et en particulier qu'elle soit de dimension strictement inférieure à celle de V.

Sous ces conditions, il apparaît clairement que nous pourrons obtenir un algorithme calculant au moins un point par composante semi-algébriquement connexe de $V \bigcap \mathbb{R}^n$. Malheureusement, les conditions ci-dessus ne sont pas vraies en général, comme le montrent les exemples ci-dessous.

- **Exemple 1 :** Considérons la variété algébrique V définie par

$$f = (x^2 + y^2 - 1)^2 = 0$$

Il est aisé de s'apercevoir que quelque soit le point A choisi la variété algébrique définie par

$$f(M) = 0, \quad \mathbf{AM} // \mathbf{grad}_M(f)$$

est de dimension 1. En effet, l'ensemble des points qui vérifient :

$$f(M) = 0 \quad \mathbf{grad}_M(f) = \mathbf{0}$$

est égal à V. Notons que dans ce cas l'idéal $\langle P \rangle$ n'est pas radical.
Enfin, remarquons que l'ensemble des singularités de V est vide.

– **Exemple 2 :** Le cas des idéaux radicaux n'est pas exempt de difficultés lui aussi. Considérons la variété algébrique V définie par

$$\begin{cases} f_1 = (X_1^2 + X_2^2 - 1)(X_1 - 2) = 0 \\ f_2 = (X_1 - 2)X_3 = 0 \end{cases}$$

L'ensemble $V \bigcap R^3$ est la réunion du plan défini par l'équation $X_1 = 2$ et du cercle défini par les équations $X_1^2 + X_2^2 - 1 = 0$ et $X_3 = 0$. Il est facile de constater que chaque point du cercle est régulier et vérifie

$$\text{rang}\left(\begin{bmatrix} 3\,{X_1}^2 - 4\,X_1 + {X_2}^2 - 1 & 2\,X_2\,(X_1 - 2) & 0 \\ X_3 & 0 & X_1 - 2 \end{bmatrix}\right) = 2\,.$$

Ainsi, $\mathfrak{C}(V, A)$ n'intersecte pas chaque composante semi-algébriquement connexe de $V \bigcap \mathbb{R}^n$ puisqu'il ne peut contenir aucun point du cercle.

Dans l'exemple 2 ci-dessus, V est composée de composantes irréductibles de dimensions différentes. Les points critiques de la fonction distance qui ne se trouvent pas dans la composante principale de dimension d ne se trouveront donc pas dans $\mathfrak{C}(V, A)$ puisque ces tels points qui ne sont pas singuliers vérifient :

$$\text{rang}(\mathbf{grad}_M(f_1), \ldots, \mathbf{grad}_M(f_s), \mathbf{AM}) > n - d.$$

Par ailleurs, soit $M \in V$ tel que :

$$\dim(\mathbf{grad}_M(f_1), \ldots, \mathbf{grad}_M(f_s)) < n - d.$$

On a alors $M \in \mathfrak{C}(V, A)$. Ceci arrive en particulier lorsque M est un point singulier d'une composante irréductible de dimension d dans V.

Notation. *Soit V une variété algébrique de dimension d, $\{f_1, \ldots, f_s\}$ une famille de polynômes dans $\mathbb{Q}[X_1, \ldots, X_n]$ tel que $I(V) = \langle f_1, \ldots, f_s \rangle$. On note* $\text{Sing}(V)$ *la variété :*

$$\text{Sing}(V) = \{M \in V \mid \text{rang}(\mathbf{grad}_M(f_1), \ldots, \mathbf{grad}_M(f_s)) < n - d\}.$$

Théorème 20. *Soit V une variété algébrique équi-dimensionnelle de dimension d et $\{f_1, \ldots, f_s\} \subset \mathbb{Q}[X_1, \ldots, X_n]$ tel que $I(V) = \langle f_1, \ldots, f_s \rangle$.*

Il existe D un entier positif suffisamment grand, tel qu'il existe au moins un point A dans $\{1, \ldots, D\}^n$ vérifiant :

1. *$\mathfrak{C}(V, A)$ intersecte chaque composante semi-algébriquement connexe de $V \bigcap \mathbb{R}^n$,*
2. *$\mathfrak{C}(V, A) = \text{Sing}(V) \bigcup V_0$, où V_0 est un ensemble fini de points dans $\mathbb{C}^n$.*

De plus, $\dim(\mathfrak{C}(V, A)) < dim(V)$.

Remarque. *D'après la preuve du théorème 20 ci-dessus, un point A choisi au hasard est tel que* $\dim(\mathfrak{C}(V, A)) < \dim(V)$ *avec une probabilité un.*

Soit V une variété équi-dimensionnelle. Etant donnée une famille de générateurs de $I(V)$ on peut choisir un point A et calculer $\mathfrak{C}(V, A)$ tel que $\dim(\mathfrak{C}(V, A)) < \dim(V)$. D'après le théorème 20, une décomposition équi-dimensionnelle de $\mathfrak{C}(V, A)$ donne une composante zéro-dimensionnelle V_0 et plusieurs autres composantes équi-dimensionnelles de dimension positive. On peut alors appliquer le théorème 20 à chacune de ces composantes.

L'algorithme que nous proposons consiste à appliquer pas à pas le processus décrit ci-dessus en calculant à chaque étape des décompositions équi-dimensionnelles des variétés intermédiaires obtenues. A la fin, nous obtenons un ensemble de systèmes zéro-dimensionnels contenant au moins un point par composante semi-algébriquement connexe dans la variété $V \bigcap \mathbb{R}^n$.

Notation. *Pour $A \in \mathbb{C}^n$, $\mathcal{Q} = \{Q_1, \ldots, Q_s\} \subset \mathbb{Q}[X_1, \ldots, X_n]^s$, et $d \in \mathbb{N}$, $0 \leqslant d < n$, on définit $\Delta_{A,d}(\mathcal{Q})$ comme étant l'ensemble de tous les mineurs d'ordre $(n - d + 1, n - d + 1)$ de la matrice*

$$\left[\left[\frac{\partial Q_i}{\partial X_j}\right]_{(i=1,\ldots,n, j=1,\ldots,s)} | \mathbf{AM}\right]$$

D'après les résultats ci-dessus, les routines de base nécessaires pour l'implantation d'un tel algorithme qui calcule cet ensemble de systèmes zéro-dimensionnels sont les suivantes :

- **EquiDim** : prend en entrée un système d'équations polynomiales S et retourne une liste de systèmes de générateurs $\mathcal{P}_d, \ldots, \mathcal{P}_0$ engendrant des idéaux radicaux et équi-dimensionnels, tels que $V(S) = V(\mathcal{P}_d) \bigcup \ldots \bigcup V(\mathcal{P}_0)$.
- **Dim** : prend en entrée un système de générateurs d'un idéal et calcule la dimension de la variété associée,
- **Minors** : prend en entrée une famille finie de polynômes $\mathcal{Q}$, un entier d et un point A, et calcule $\Delta_{\mathcal{Q},d,A}(\mathcal{Q})$).

Nous obtenons l'algorithme ci-dessous.

Algorithme

- **Entrée :** Un système $S \subset \mathbb{Q}[X_1, \ldots, X_n]$ d'équations polynomiales.
- **Sortie :** Une liste de systèmes zéro-dimensionnels tel que l'ensemble de leurs solutions est inclus dans $V(S)$ et contient au moins un point par composante semi-algébriquement connexe de $V(S) \bigcap \mathbb{R}^n$.

1. list := EquiDim(S), result := [],
2. Choisir un point A dans K^n.
3. Tant que list $\neq \varnothing$ faire
   - S := first(list), poser $d := \mathrm{Dim}(S)$ et enlever S de list,
   - Si $d = 0$ alors result := result $\bigcup S$,
   - Sinon
     - (*) $Q = \mathrm{Minors}(S, d, A) \bigcup S$
     - $u = \mathrm{Dim}(Q)$
     - Si $u = d$ choisir un autre point A et aller au pas (*).
     - list := list $\bigcup$ EquiDim(Q)
4. Retourner result.

La première étape de l'algorithme précédent consiste à calculer des familles de générateurs de chaque composante équi-dimensionnelle du radical de l'idéal engendré par les polynômes donnés en entrée. On a vu qu'en pratique cette famille de générateurs est une base de Gröbner.

Soit $\mathcal{G} \subset \mathbb{Q}[X_1, \ldots, X_n]$ une telle base de Gröbner contenant s polynômes et engendrant un idéal équi-dimensionnel et radical de dimension d. D'aprés les résultats ci-dessus, le nombre de déterminants qui sont calculés par l'algorithme donné dans le paragraphe précédent est

$$\left(\begin{array}{c} s \\ n-d \end{array} \right) \left(\begin{array}{c} n \\ n-d+1 \end{array} \right).$$

Il est clair qu'un tel facteur combinatoire n'a que peu d'incidences dans le cas des hypersurfaces ($s = 1$ et $n - d = 1$), mais il devient limitant sur des problèmes significatifs, de co-dimension plus grande que 1. Surtout, le nombre de polynômes s dans $\mathcal{G}$ peut devenir suffisamment grand pour que le calcul de tous les mineurs de jacobienne devienne non négligeable en terme de temps de calcul. Les améliorations décrites ci-dessous ont donc pour but de faciliter la résolution de ces cas.

Dans le premier paragraphe de cette section, nous allons montrer comment, en donnant un peu plus de propriétés à $\mathcal{G}$, nous allons pouvoir en extraire une famille de $n - d$ polynômes représentant ■presque tous les points■ de $V(\mathcal{G})$ et permettant de ne calculer que d déterminants. Nous verrons en particulier que cette famille est un ensemble triangulaire de polynômes.

Dans le deuxième paragraphe de cette section, nous montrons comment les optimisations s'appliquent aux décompositions en idéaux premiers. Puis, nous montrons comment ces décompositions permettent :

- de réduire considérablement la taille de la sortie de nos algorithmes,

– d'éviter des calculs intuiles et donc de réduire les temps de calcul.

En effet en travaillant sur des composantes irréductibles, on évite l'étude des points qui appartiennent à l'intersection de deux de ces composantes.

L'apport des ensembles triangulaires. Soit $\mathcal{G} \subset \mathbb{Q}[X_1, \ldots, X_n]$ une **base de Gröbner lexicographique réduite** engendrant un idéal radical équi-dimensionnel de dimension d pour l'ordre $X_1 < \ldots < X_n$. Pour $p \in \mathbb{Q}[X_1, \ldots, X_n]$, on note $\mathrm{mvar}(p)$ (variable principale de p) la plus grande variable apparaissant dans p pour l'ordre $X_1 < \ldots < X_n$.

Soit $\mathcal{T} = (t_{d+1}, \ldots, t_n)$ un ensemble triangulaire extrait de $\mathcal{G}$ tel que :

– $\forall g \in \mathcal{G}$ il existe $i \in \{d+1, \ldots, n\}$ vérifiant
  – (i) $\mathrm{mvar}(t_i) = \mathrm{mvar}(g)$,
  – (ii) $\deg(t_i, \mathrm{mvar}(t_i)) \leqslant \deg(g, \mathrm{mvar}(t_i))$,
– $\forall i \in \{d+1, \ldots, n\}$ il n'existe pas de polynômes $g \in \mathcal{G}$ de même variable principale que t_i et de monôme dominant inférieur à celui de t_i pour l'ordre lexicographique.

Notons qu'un tel ensemble triangulaire est unique. On note **ExtractTriangular** une routine qui prend en entrée une base de Gröbner lexicographique réduite et qui retourne l'ensemble triangulaire extrait de la base d'entrée et vérifiant les propriétés ci-dessus.

Dans la suite, on suppose que la base de Gröbner lexicographique réduite $\mathcal{G}$ est telle que :

– l'ensemble triangulaire $\mathcal{T} \subset \mathcal{G}$ extrait de $\mathcal{G}$ par **ExtractTriangular** est **régulier** et **séparable**,
– $\mathrm{sat}(\mathcal{T}) = \langle \mathcal{G} \rangle$.

Notons que de telles suppositions impliquent que $\langle \mathcal{G} \rangle$ est équi-dimensionnel car il est saturé d'un ensemble triangulaire régulier, et que $\langle \mathcal{G} \rangle$ est un idéal radical car il est saturé d'ensemble triangulaire $\mathcal{T}$ séparable.

Soit $M = (x_1, \ldots, x_n)$, A un point de $\mathbb{Q}^n$, $d = \dim(V(\mathcal{G}))$, et considérons pour $j = 1, \ldots, d$ la liste des mineurs d'ordre $(n - d + 1)$ extraite de $\Delta_{A,d}(\mathcal{T})$:

$$\Gamma_A(\mathcal{T}) = \{\Gamma_A^{(j)}(\mathcal{T}) = det(\mathcal{M}_A^{(j)}), j = 1, \ldots, d\}$$

où

$$\mathcal{M}_A^{(j)} = \left[\begin{array}{c|c} \left[\frac{\partial t_i}{\partial X_j}\right]_{i=d+1,\ldots,n} & X_j - a_j \\ \hline \mathcal{U}_{\mathcal{T}} = \left[\frac{\partial t_i}{\partial X_k}\right]^{i=d+1,\ldots,n}_{k=d+1,\ldots,n} & \begin{array}{c} X_{d+1} - a_{d+1} \\ \vdots \\ X_n - a_n \end{array} \end{array}\right]$$

Sans nuire à la généralité, on peut supposer que $\mathrm{mvar}(t_i) = X_i$, ce qui rend les mineurs $\Gamma_A^{(j)}(\mathcal{T})$ faciles à calculer puisque $\mathcal{U}_{\mathcal{T}}$ est triangulaire supérieure. Nous allons montrer que nous pouvons substituer le calcul de $\Delta_{A,d}(\mathcal{G})$ par celui de $\Gamma_A(\mathcal{T})$ dans notre algorithme :

Proposition 25. *Soit $\mathcal{G}$ une base de Gröbner lexicographique réduite et $\mathcal{T}$ un ensemble triangulaire vérifiant les hypothèses ci-dessus. Soit $\mathcal{D}(V(\mathcal{G}), A) = V(\mathcal{G}) \bigcap V(\Gamma_A(\mathcal{T}))$, $d = \dim(\mathcal{G})$ et $\mathrm{Sep}(\mathcal{T}) = \prod_{i=d+1}^{n} \frac{\partial t_i}{X_i}$. Si A est un point de $\mathbb{Q}^n$ tel que $\dim(\mathfrak{C}(V(\mathcal{G}), A)) < \dim(V(\mathcal{G}))$ alors on a :*

– $\mathfrak{C}(V(\mathcal{G}), A) \subset \mathcal{D}(V(\mathcal{G}), A)$,
– $(\mathcal{D}(V(\mathcal{G}), A) \setminus V(\mathrm{Sep}(\mathcal{T}))) \subset V_0$,
– $\dim\left(\mathcal{D}(V(\mathcal{G}), A) \bigcap V(\mathrm{Sep}(\mathcal{T}))\right) < \dim(V(\mathcal{G}))$.

En particulier, $\dim(\mathcal{D}(V(\mathcal{G}), A)) < \dim(V(\mathcal{G}))$ *et $\mathcal{D}(V(\mathcal{G}), A)$ s'intersecte avec toute composante connexe de $V(\mathcal{G})$.*

Ainsi, dans les hypothèses où la proposition ci-dessus s'applique, seuls d déterminants doivent être calculés pour caractériser $\mathcal{D}(V(\mathcal{G}, A))$. L'algorithme induit requiert ainsi une routine ayant plus de propriétés qu'une décomposition équi-dimensionnelle. En effet, il n'est pas toujours possible d'extraire un ensemble triangulaire $\mathcal{T}$ régulier et séparable d'une base de Gröbner lexicographique réduite $\mathcal{G}$ telle que $\mathrm{sat}(\mathcal{T}) = \langle \mathcal{G} \rangle$. Pour s'en convaincre il suffit de considérer l'exemple $\langle x, yz \rangle$ pour l'ordre $x < y < z$.

On note **LexTriSetEquiDim** une routine qui prend en entrée un système d'équations polynomiales S et qui retourne un ensemble de bases de Gröbner lexicographiques réduites $\mathcal{G}_1, \ldots, \mathcal{G}_m$ telles que pour tout $i \in \{1, \ldots, m\}$:

– $\mathcal{T}_i :=$ ExtractTriangular$(\mathcal{G}_i)$ est un ensemble triangulaire régulier et séparable ;

– $\mathrm{sat}(\mathcal{T}_i) = \mathcal{G}_i$;
– $V(S) = V(\mathcal{G}_1) \bigcup \ldots \bigcup V(\mathcal{G}_m)$.

Remarque. *Une manière de concevoir une telle routine est d'implanter les algorithmes décrits dans [105, 9] et dont les sorties sont des ensembles triangulaires réguliers et séparables puis de calculer les saturés de ces ensembles triangulaires. Bien évidemment, ce n'est pas forcément la manière la plus judicieuse.*

Nous obtenons l'algorithme ci-dessous.

Algorithme : Calcul d'au moins un point par composante connexe d'une variété algébrique réelle quelconque (Utilisation de fonctions distances)

– **Entrée :** Un système $S \subset \mathbb{Q}[X_1, \ldots, X_n]$ d'équations polynomiales.
– **Sortie :** Une liste de systèmes zéro-dimensionnels tel que l'ensemble de leurs solutions est inclus dans $V(S)$ et contient au moins un point par composante semi-algébriquement connexe de $V(S) \bigcap \mathbb{R}^n$.

1. list := LexTriSetEquiDim(S), result := [],
2. Choisir un point A dans $\mathbb{Q}^n$.
3. Tant que list $\neq \varnothing$ faire
   – S := first(list), et enlever S de list, poser $d = \mathrm{Dim}(S)$,
   – Si $d = 0$ alors result := result $\bigcup S$,
   – Sinon
     – $\mathcal{T} = \mathrm{ExtractTriangular}(S)$.
     – (*) $Q = \Gamma_A(\mathcal{T}) \bigcup S$ et poser $u = \mathrm{Dim}(Q)$
     – Si $u = d$ choisir un autre point A et aller au pas (*).
     – list := list $\bigcup$ LexTriSetEquiDim(Q),
4. Retourner result.

Une fois les déterminants calculés, une étape d'élimination algébrique supplémentaire est nécessaire. Afin de rendre ces calculs plus faciles, on peut réduire modulo l'ensemble triangulaire les déterminants calculés à l'étape (*) de l'algorithme.

Notons $\mathrm{prem}(p, q, X)$ le pseudo-reste classique de deux polynômes p et q par rapport à la variable X. Si $p \in \mathbb{Q}[X_1, \ldots, X_n]$, sa forme réduite $\mathrm{prem}(p, \mathcal{T})$ peut être calculée par la procédure récursive suivante :
– si $\mathcal{T} = \varnothing$, alors $\mathrm{prem}(p, \mathcal{T}) = p$.
– sinon, si X_i est la plus grande variable apparaissant dans un polynôme $t \in \mathcal{T}$,

$$\mathrm{prem}(p, \mathcal{T}) = \mathrm{prem}(\mathrm{prem}(p, t, X_i), \mathcal{T} \setminus \{t\}).$$

En particulier, ceci implique qu'il existe des polynômes $q_{d+1}, \ldots q_n$ et des entiers positifs $i_{d+1}, \ldots, i_n$ tels que :

$$\mathrm{prem}(p, \mathcal{T}) = q_{d+1}t_{d+1} + \ldots + q_n t_n + h_{d+1}^{i_{d+1}} \ldots h_n^{i_n} p.$$

Ainsi, $V(\mathcal{G}) \bigcap V(\mathrm{prem}(p, \mathcal{T})) = V(\mathcal{G}) \bigcap (V(p) \cup V(h_{d+1} \ldots h_n))$. Par conséquent, on a :

$$\dim(V(\mathcal{G}) \bigcap V(p)) < \dim(V(\mathcal{G})) \Longrightarrow \dim(V(\mathcal{G}) \bigcap V(\mathrm{prem}(p, \mathcal{T})) < \dim(V(\mathcal{G})).$$

Implantations et performances pratiques. Les premières implantations de cet algorithme datent de [127]. Elles ont à l'époque permis de résoudre des problèmes inatteignables par la décomposition cylindrique algébrique ainsi que les variantes précédentes de la méthode des points critiques.

Les problèmes qu'on rencontre dans cet algorithme sont les suivants :

– l'état de l'art concernant les calculs de décomposition équi-dimensionnelle rend difficile les appels récursifs étudiant les lieux singuliers de lieux singuliers et ainsi de suite : en effet, ces lieux sont souvent définis par des systèmes polynomiaux non radicaux et non équi-dimensionnels qui sont des cas sur lesquels les bases de Gröbner ont un comportement moins bon.
– Même lorsque ces calculs sont accessibles, le fait de calculer des points critiques à partir de polynômes obtenus par une routine d'élimination algébrique rend difficile l'obtention de bonnes performances pratiques : en effet, ces polynômes sont souvent très denses comparativement à ceux donnés en entrée et de haut degré.
– Enfin, les calculs de points critiques d'applications polynomiales qui sont des carrés de distance euclidienne est plus délicat que ceux de fonctions de projection par exemple.

5.4 Gestion récursive des chutes de rang dans les jacobiennes : Utilisation de fonctions de projection

En effet, quelques expérimentations montrent qu'étant donné un système de générateurs de l'idéal associé à une variété algébrique $V \subset \mathbb{C}^n$, le calcul de points critiques d'une projection sur une droite restreinte à V est beaucoup moins couteux que le calcul de points critiques d'une fonction distance restreinte à la même variété algébrique V.

Notre objectif est donc maintenant de calculer au moins un point par composante connexe sur une variété algébrique réelle en n'effectuant que des calculs de points critiques de projections. Pour ce faire, on opère en construisant récursivement des sous-variétés dans la variété étudiée tout en assurant une chute de dimension à chaque étape de l'algorithme. Ce procédé est évidemment inspiré de celui expliqué dans le pararaphe précédent. La gestion des chutes de rang dans les jacobiennes se fait d'ailleurs de manière tout à fait similaire.

Soit $V \subset \mathbb{C}^n$ une variété algébrique de dimension d et $\Pi : V \to \mathbb{C}^d$ une projection dominante. Alors d'après le théorème sur la dimension des fibres [139, Ch. 1.6], Π a des fibres génériques de dimension 0. Dans ce cas, l'ensemble des points de $\mathbb{C}^d$ en lesquels Π n'est pas propre est une hypersurface [73] ; on notera P_Π un polynôme sans facteurs carrés définissant ce lieu de non-propreté. Le premier résultat ci-dessous montre comment P_Π peut être utilisé pour obtenir au moins un point par composante connexe de $V \cap \mathbb{R}^n$.

Théorème 21. *Soit $V \subset \mathbb{C}^n$ une variété algébrique* équi-dimensionnelle *de dimension d. Soit Π la projection*

$$\begin{array}{rccc} \Pi : & \mathbb{C}^n & \to & \mathbb{C}^d \\ & (x_1, \ldots, x_n) & \mapsto & (x_1, \ldots, x_d). \end{array}$$

Supposons que la restriction de Π à V est dominante et soit P_Π comme ci-dessus. Soit C une composante connexe de $V \cap \mathbb{R}^n$, telle que C ne contienne aucun point singulier de V, et aucun point critique de la restriction de Π à V.

Alors, il existe une composante connexe de l'ensemble semi-algébrique défini par $P_\Pi \neq 0$ qui est contenue dans $\Pi(C)$.

En conséquence, étant donnée une variété algébrique $V \subset \mathbb{C}^n$ et une projection Π satisfaisant les hypothèses du théorème 21, les composantes connexes de $V \cap \mathbb{R}^n$ peuvent être détectées en :
– calculant les lieux critiques et singuliers de la restriction de Π à V ;
– calculer au moins un point par composante connexe du semi-algébrique défini par $P_\Pi \neq 0$; et l'intersection de V avec les fibres de Π prises en ces points.

La mise en œuvre algorithmique de ce résultat est fondée sur des calculs d'ensembles triangulaires réguliers, séparables, fortement normalisés. Les résultats qui suivent montrent en effet qu'ils offent un cadre agréable dans notre contexte. Le point fondamental qui rend possible l'obtention d'un algorithme est prouvé dans [95] : si $(f_1, \ldots, f_s)$ est une famille de polynômes, il existe une famille d'ensembles triangulaires réguliers séparables fortement normalisés $\mathcal{T}_1, \ldots, \mathcal{T}_\ell$ telle qu'on a :

$$V(f_1, \ldots, f_s) = \cup_{i=1}^{\ell} \overline{W(\mathcal{T}_i)}.$$

Ainsi, on peut concentrer notre étude sur le cas des variétés donnés comme étant des clôtures de quasi-composantes associées à des ensembles triangulaires réguliers séparables fortement normalisés.

Le théorème ci-dessous est la traduction du théorème 21 dans ce contexte.

Théorème 22. *Soit $\mathcal{T} \subset \mathbb{Q}[X_1, \ldots, X_n]$ un ensemble triangulaire fortement normalisé dont on suppose que les variables transcendantes sont $X_1, \ldots, X_d$. Soit Π la projection*

$$\begin{array}{rccc} \Pi : & \mathbb{C}^n & \to & \mathbb{C}^d \\ & (x_1, \ldots, x_n) & \mapsto & (x_1, \ldots, x_d) \end{array}$$

s et h le produit de, respectivement, l'ensemble des séparants et des initiaux de $\mathcal{T}$. Soit $\overline{W(\mathcal{T})}$ la clôture de Zariski de $W(\mathcal{T})$ et C une composante connexe de $\overline{W(\mathcal{T})} \cap \mathbb{R}^n$. Si $C \cap V(s)$ est vide, alors il existe une composante connexe de l'ensemble semi-algébrique défini dans $\mathbb{R}^d$ par $h \neq 0$ qui est contenue dans $\Pi(C)$.

Ce théorème constitue la charpente de l'algorithme que nous présentons dans ce paragraphe. Étant donnée une famille de polynômes $f_1, \ldots, f_s$ dans $\mathbb{Q}[X_1, \ldots, X_n]$, on commence par calculer une décomposition en ensembles triangulaires fortement normalisés de la variété algébrique $V \subset \mathbb{C}^n$ définie par

$$f_1 = \cdots = f_s = 0.$$

Puis on applique le théorème 22 à chacun des ensembles triangulaires obtenus. Soit $\mathcal{T}$ un tel ensemble triangulaire. On reprend les notations du théorème 22. Les composantes connexes de la clôture de $W(\mathcal{T})$ sont atteintes

- soit en étudiant l'intersection de $\overline{W(\mathcal{T})}$ obtenue le produit des séparants de $\mathcal{T}$,
- soit en étudiant l'hypersurface définie par les initiaux de l'ensemble triangulaire considéré : pour cette dernière étude on doit calculer au moins un point par composante connexe dans le semi-algébrique défini par $h \neq 0$ dans $\mathbb{R}^d$.

Algorithme principal. On décrit maintenant l'algorithme obtenue à partir des résultats ci-dessus. Étant donnée un ensemble de polynômes $(f_1, \ldots, f_s) \subset \mathbb{Q}[X_1, \ldots, X_n]$, on commence par décomposer la variété algébrique définie par :

$$f_1 = \cdots = f_s = 0$$

où chaque composante obtenue est décrite comme étant des quasi-composantes d'ensembles triangulaires normalisés $(\mathcal{T}_1, \ldots, \mathcal{T}_\ell)$.

Pour chacun de ces ensembles triangulaires $\mathcal{T}$ on effectue les opérations suivantes :

- si $\mathcal{T}$ définit un ensemble fini de points, en calculer une paramétrisation rationnelle et retourner cette paramétrisation sinon ;
- trouver une projection dominante Π en identifiant les variables transcendentes de $\mathcal{T}$;
- calculer un ensemble de générateurs de $\overline{W(\mathcal{T})} \cap V(s)$, où s est le the produit des séparants de $\mathcal{T}$, et appeller récursivement l'algorithme à cette famille de polynômes ;
- calculer au moins un point par composante connexe de l'ensemble semi-algébrique défini par $h \neq 0$, où h est le produit des initiaux de $\mathcal{T}$, et appeler récursivement l'algorithme sur les fibres de Π prises au-dessus de ces points.

Remarquons qu'on peut obtenir au moins un point par composante connexe de l'ensemble semi-algébrique défini par $h \neq 0$ en calculant une décomposition cylindrique algébrique partielle [38].

Théorème 23. *L'algorithme ci-dessous s'arrête. Il retourne une famille de systèmes zéro-dimensionnels dont le lieu des solutions réelles a une intersection non vide avec chaque composante connexe de l'ensemble algébrique réel $V(f_1, \ldots, f_s) \cap \mathbb{R}^n$.*

La preuve d'arrêt de cet algorithme est une conséquence du résultat ci-dessous.

Lemme 6. *Soit $\mathcal{T} \subset \mathbb{Q}[X_1, \ldots, X_n]$ un ensemble triangulaire régulier séparable, Π la projection sur le sous-espace affine contenant les axes de coordonnées des variables transcendantes de $\mathcal{T}$ et y un point dans ce sous-espace. Alors la dimension de $\overline{W(\mathcal{T})} \cap \Pi^{-1}(y)$ est inférieure à celle de $\overline{W(\mathcal{T})}$.*

Lemme 7. *Soit $\mathcal{T} \subset \mathbb{Q}[X_1, \ldots, X_n]$ un ensemble triangulaire régulier séparable, Π la projection sur le sous-espace affine contenant les axes de coordonnées des variables transcendantes de $\mathcal{T}$ et s le produit des séparants des polynômes de $\mathcal{T}$. Alors la dimension de $\overline{W}(\mathcal{T}) \cap V(s)$ est inférieure à celle de $\overline{W(\mathcal{T})}$.*

Pour décrire notre algorithme, on suppose qu'on dispose des routines de calcul suivantes :

- `TriangularDecompose` : qui prend en entrée une famille de polynômes F dans $\mathbb{Q}[X_1, \ldots, X_n]$ définissant une variété algébrique $V \subset \mathbb{C}^n$ et retournent une famille de couples $\{(\mathcal{G}_i, \mathcal{T}_i) \mid i = 1, \ldots, p\}$ telle que :
  - pour tout $i = 1, \ldots, p$, $\mathcal{T}_i$ est un ensemble triangulaire régulier séparable et fortement normalisé ;
  - pour tout $i = 1, \ldots, p$, $\mathcal{G}_i$ est un ensemble fini de polynômes ;
  - V est la réunion des $V(\mathcal{G}_i)$ pour $i = 1, \ldots, p$;
  - pour tout $i = 1, \ldots, p$, $V(\mathcal{G}_i)$ est égale à la clôture de Zariski de $W(\mathcal{T}_i)$.

  En pratique les $\mathcal{G}_i$ sont bien évidemment des bases de Gröbner.
- `Parameterization` : qui prend en entrée un ensemble de polynômes engendrant un idéal zéro-dimensionnel et renvoie une paramétrisation rationnelle de l'ensemble de ses solutions.
- `Initials` et `Separants` : qui prennent en entrée un ensemble triangulaire régulier séparable et fortement normalisé et retournent respectivement le produit des initiaux et séparants de l'ensemble triangulaire donné en entrée.
- `Sampling` : qui prend en entrée un polynôme $h \in \mathbb{Q}[X_1, \ldots, X_n]$ et retourne une famille de paramétrisations rationnelles encodant au moins un point par composante connexe dans l'ensemble semi-algébrique défini par $h \neq 0$. Notons que l'algorithme de décomposition cylindrique algébrique décrit dans le chapitre 3 permet d'obtenir une implantation de cette routine.

Des résultats ci-dessus, on déduit l'algorithme suivant.

Algorithme : Calcul d'au moins un point par composante connexe d'une variété algébrique réelle quelconque (Utilisation de fonctions de projections)

- **Entrée :** Une famille $(f_1, \ldots, f_s) \subset \mathbb{Q}[X_1, \ldots, X_n]$ de polynômes définissant une variété algébrique $V \subset \mathbb{C}^n$.
- **Sortie :** Une famille de paramétrisations rationnelles encodant un nombre fini de points de V et ayant une intersection non vide avec chaque composante connexe de $V \cap \mathbb{R}^n$.

1. Poser $F =$ `TriangularDecompose`$([f_1, \ldots, f_s])$ et `sols` $:= []$
2. Pour tout C dans F faire
   (a) Si le premier élément $\mathcal{G}$ de C engendre un idéal de dimension zéro alors poser
   $$\texttt{sols} := \texttt{sols} \cup \texttt{Parameterization}(\mathcal{G})$$
   (b) sinon soit $\mathcal{T}$ le second élément de C et faire
      i. poser $s :=$ `Separants`$(\mathcal{T})$ et $h =$ `Initials`$(\mathcal{T})$
      ii. poser `points` $:=$ `Sampling`(h) et pour tout `point` dans `points` faire
      $$\texttt{sols} := \texttt{sols} \cup \texttt{Parameterization}(\mathcal{G} \cup \texttt{point})$$
      iii. Faire l'union de `sols` et des paramétrisations rationnelles retournées par l'appel récursif de l'algorithme avec comme entrée $\mathcal{G} \cup s$.
3. Retourner `sols`

Les premières implantations de cet algorithme ont rapidement remplacé dans [128] celles de l'algorithme donné dans le paragraphe précédent. En effet, l'impact en pratique du passage aux fonctions de projection est extrêmement rentable. Cet algorithme s'est aussi montré particulièrement efficace sur les exemples de grande co-dimension : en effet, dans ce cas, l'essentiel du calcul est concentré sur le calcul du premier appel à `TriangularDecompose` puisqu'à chaque appel récursif on a garanti que la dimension de l'objet traîté chute de un.

Ceci dit, il souffre des mêmes difficultés que le précédent : en effet, en travaillant récursivement sur des données obtenues comme le résultat d'un calcul d'élimination algébrique on atteint facilement les limites de ce qui est réalisable en machines. De plus, comme précédemment on ne sait pas borner correctement la taille des quantités apparaissant en cours de calculs : en effet, on est amené à calculer des représentations de lieux singuliers puis de lieux singuliers de lieux singuliers et ainsi de suite. On n'a donc pas moyen de donner en toute généralité une estimation de la complexité des données géométriques apparaissant en cours de calcul qui soit simplement exponentiel en le nombre de variables. C'est très insatisfaisant.

Plus grave encore, l'usage de la décomposition cylindrique algébrique pour implanter la routine `Sampling` fait parfois exploser le nombre de points retournés par l'algorithme. Ceci est évidemment le fait de la complexité doublement exponentielle de cet algorithme.

Enfin, le procédé de résolution géométrique lui-même est perfectible : en calculant des lieux critiques de lieux critiques et ainsi de suite, on peut montrer qu'on fait apparaître génériquement des singularités en cours d'algorithme d'une part et que d'autre part ce procédé récursif induit une croissance de degré qui n'est pas souhaitable.

Ainsi, même si l'usage de fonctions de projection a permis de gagner en efficacité, il est clair que celui qui en est fait dans l'algorithme présenté dans ce paragraphe peut être amélioré.

5.5 Le cas des variétés algébriques lisses

Dans un premier temps, on concentre notre étude dans les cas où la variété algébrique définie par le système d'équations donné en entrée est lisse et équi-dimensionnelle. On s'appuie alors sur la caractérisation des points critiques donnés dans le lemme 4. Le cas non-équi-dimensionnel est ensuite étudié en s'appuyant sur la caractérisation lagrangienne des points critiques du lemme 5.

5.5.1 Le cas équi-dimensionnel lisse

Notations. Soit $f_1, \ldots, f_s$ des polynômes de $\mathbb{Q}[X_1, \ldots, X_n]$, V le lieu complexe de leurs zéros communs et d la dimension de V. On suppose dans ce paragraphe que $f_1, \ldots, f_s$ définissent un idéal radical et que V est équi-dimensionnelle et lisse.

Pour i dans $\{1, \ldots, d\}$, on note π_i la projection canonique

$$\begin{array}{ccc} \mathbb{C}^n & \to & \mathbb{C}^i \\ (x_1, \ldots, x_n) & \mapsto & (x_1, \ldots, x_i). \end{array}$$

We denote by π_i its restriction to a map $\mathbb{R}^n \to \mathbb{R}^i$ et par J la matrice jacobienne associée à $f_1, \ldots, f_s$:

$$J = \begin{bmatrix} \frac{\partial f_1}{\partial X_n} & \cdots & \frac{\partial f_1}{\partial X_1} \\ \vdots & & \vdots \\ \frac{\partial f_s}{\partial X_n} & \cdots & \frac{\partial f_s}{\partial X_1} \end{bmatrix}.$$

On décrit maintenant les lieux critiques de $\pi_1, \ldots, \pi_d$ restreints à V à l'aide des mineurs de cette matrice (on est bien dans le cadre d'application du lemme 4).

Tout d'abord, pour $i = d + 1$, on définit Δ_{n-d} comme étant l'idéal $\langle f_1, \ldots, f_s \rangle$. Puis pour $i = 1, \ldots, d$, Δ_{n-i+1} est l'idéal engendré par $f_1, \ldots, f_s$ et tous les mineurs de taille $n-d$ dans J construits à partir des colonnes $1, \ldots, n-i$ (c'est-à-dire en utilisant les dérivées partielles par rapport aux variables $X_{i+1}, \ldots, X_n$). Remarquons que Δ_{n-i+1} est engendré par

$$S_i := \begin{pmatrix} s \\ n-d \end{pmatrix} \begin{pmatrix} n-i \\ n-d \end{pmatrix}$$

mineurs. La i-ème variété polaire $\mathfrak{C}(\pi_i, V)$ W_{n-i+1} est alors définie comme étant la variété algébrique associée à Δ_{n-i+1} ; en particulier, on pose $W_{n-d} = V$.

Puisque l'idéal $\langle f_1, \ldots, f_s \rangle$ est radical et que V est lisse et équi-dimensionnelle, on sais d'après le lemme 4 que W_{n-i+1} est en fait le lieu critique $\mathfrak{C}(\pi_i, V)$ de la restriction de π_i à V, pour $i \leqslant d$. Après changement générique linéaire de variables, on verra qu'on s'attend à ce que $\mathfrak{C}(\pi_i, V)$ (ou encore W_{n-i+1}) soit de co-dimension $n - i + 1$ pour tout i.

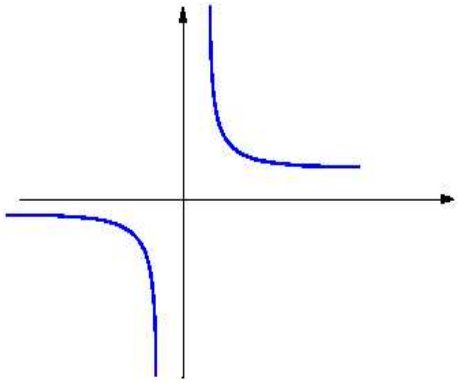

FIG. 20 –

Changements de variables. Pour $f \in \mathbb{Q}[X_1, \ldots, X_n]$ et $\mathbf{A} \in \mathrm{GL}_n(\mathbb{C})$, $f(\mathbf{AX})$ est le polynôme obtenu en appliquant le changement de variables induit par $\mathbf{A}$ sur f. Par souci de simplicité on écrira aussi $f^{\mathbf{A}} = f(\mathbf{AX})$.

Pour $i \in \{1, \ldots, d+1\}$, l'idéal $\Delta^{\mathbf{A}}_{n-i+1}$ est défini par les polynômes $f_1^{\mathbf{A}}, \ldots, f_s^{\mathbf{A}}$ et tous les mineurs de taille $n-d$ à partir des $n-i$ premières colonnes de leur matrice jacobienne. La variété polaire associée à cet idéal est notée $W^{\mathbf{A}}_{n-i+1}$ et est égale au lieu critique $\mathfrak{C}(\pi_i, V^{\mathbf{A}})$.

Résultats géométriques. Comme on l'a déjà évoqué précédemment, l'usage de fonctions de projection dans la méthode des points critiques est délicat dès lors qu'on ne dispose pas d'une hypothèse de compacité sur l'ensemble algébrique réel qu'on est en train d'étudier. Nous avions déjà illustré cet état de fait avec l'hyperbole. Dans le paragraphe suivant, nous avions montré comment en considérant des lieux de non-propreté on pouvait néanmoins obtenir des avancées. Ceci dit, comme nous l'avons expliqué à la fin du paragraphe précédent, au lieu de considérer une succession de lieux critiques

$$\mathfrak{C}(\pi_d, V), \ldots, \mathfrak{C}(\pi_i, V), \ldots, \mathfrak{C}(\pi_1, V)$$

nous considérions des lieux critiques de lieux critiques et ainsi de suite ce qui n'est pas satisfaisant.

Pour obtenir un algorithme résolument plus efficace, nous allons étudier les images des composantes connexes de $V \cap \mathbb{R}^n$ par les projections π_i (pour i allant de d à 1). Pour étudier ces images, nous aurons besoin d'assurer des propriétés de propreté.

Plus précisément, on va s'intéresser aux propriétés de propreté des projections π_i restreintes à la famille de variétés polaires que nous avons exhibé. De telles propriétés ne peuvent être systématiquement garanties : pour s'en convaincre il suffit de considérer la projection sur x restreinte à l'hyperbole définie par $xy - 1 = 0$. En revanche, si on fait un changement de variables on obtient des situations où :

- soit les deux composantes connexes de l'hyperbole se projettent sur l'axe des abscisses tout entier (voir figure 22) ;
- soit les deux composantes connexes de l'hyperbole se projettent sur deux intervalles fermés pour la topologie euclidienne (voir figure 21).

Ainsi, pour garantir que les diverses images par les projections π_i des composantes connexes de $V \cap \mathbb{R}^n$ sont fermées pour la topologie euclidienne, on va effectuer des changements de variable permettant d'assurer des propriété de propreté aux projections π_i restreintes à notre famille de variétés polaires.

On notera $\mathcal{P}(\mathbf{A})$ l'assertion suivante : *pour $i \in \{1, \ldots, d+1\}$, la restriction de π_{i-1} à $W^{\mathbf{A}}_{n-i+1}$ est propre.*

Proposition 26. *Soit C une composante connexe de $V \cap \mathbb{R}^n$. Pour i dans $1, \ldots, d$, la frontière de $\pi_i(C) \subset \mathbb{R}^i$ est incluse dans $\pi_i(W_{n-i+1} \cap C)$ si $\mathcal{P}(\mathbf{Id}_n)$ est satisfaite.*

Pour pouvoir appliquer le résultat ci-dessus, il nous faut garantir maintenant que pour un choix *générique* de changement de variable $\mathbf{A} \in GL_n(\mathbb{Q})$, l'assertion $\mathcal{P}(\mathbf{A})$ est satisfaite. C'est ce qu'affirme le résultat ci-dessous.

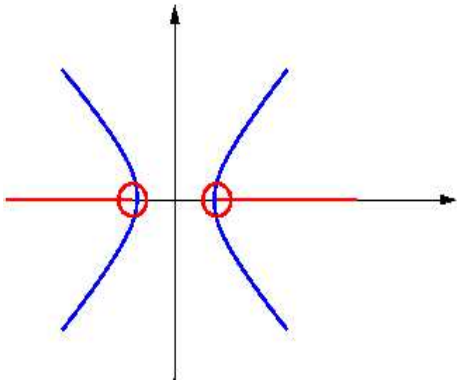

FIG. 21 –

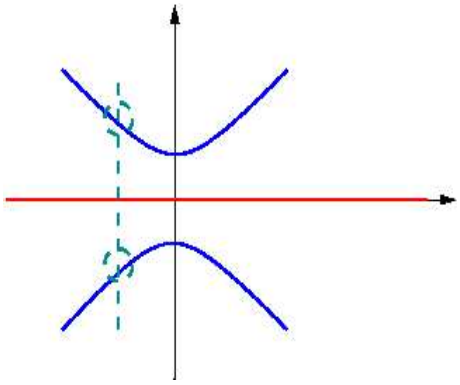

FIG. 22 –

Théorème 24. *Il existe un ouvert de Zariski non vide* Γ *dans* $\mathrm{GL}_n(\mathbb{C})$ *tel que pour* $\mathbf{A}$ *dans* Γ, $\mathcal{P}(\mathbf{A})$ *est satisfaite.*

Sous cette condition de généricité, le théorème ci-dessous permet de calculer au moins un point par composante connexe de $V \cap \mathbb{R}^n$. En effet, si la matrice $\mathbf{A}$ du Theorem 25 ci-dessous est dans $\mathrm{GL}_n(\mathbb{Q})$, alors les composantes connexes de $V^{\mathbf{A}} \cap \mathbb{R}^n$ sont en bijection triviale avec celles de $V \cap \mathbb{R}^n$.

Remarque. *La preuve du théorème 24 se trouve dans [132] et est faite dans un formalisme algébrique pour pouvoir faire une analyse de complexité sur la base des théorèmes 18 et 19. Ce résultat ne peut être assimilé à une application aveugle de la mise en position de Nœther. En effet, effectuer un changement de variable générique pour mettre en position de Nœther* W_{n-i} *modifie les variétés polaires* $W_{n-i+1}, \ldots, W_{n-d}$.

Nous pouvons maintenant donner le résultat géométrique principal sur lequel est fondé l'algorithme décrit dans ce paragraphe.

Théorème 25. *Soit* $\mathbf{A} \in \mathrm{GL}_n(\mathbb{R})$ *telle que* $\mathcal{P}(\mathbf{A})$ *est satisfaite. Soit* $p_d = (x_1, \ldots, x_d)$ *un point arbitrairement choisi dans* $\mathbb{R}^d$. *Pour* $j \in \{1, \ldots, d-1\}$, *on note* $p_j = (x_1, \ldots, x_j) \in \mathbb{R}^i$. *Pour* $j = 0$, *on pose par convention* $\pi_0^{-1}(p_0) = \mathbb{C}^n$.

Alors, les ensembles algébriques $W_{n-j}^{\mathbf{A}} \cap \pi_j^{-1}(p_j)$, *pour* $j \in \{0, \ldots, d\}$, *sont soit vides soit de dimension zéro. Leur réunion rencontre chaque composante connexe de* $V^{\mathbf{A}} \cap \mathbb{R}^n$.

Au final, l'algorithme que nous obtenons consiste à choisir aléatoirement une matrice $\mathbf{A} \in GL_n(\mathbb{Q})$ et à calculer des paramétrisations rationnelles des ensembles algébriques $W_{n-j}^{\mathbf{A}} \cap \pi_j^{-1}(p_j)$, pour $j \in \{0, \ldots, d\}$ qui sont soit vides soit de dimension zéro.

Dans la suite, on considère les routines suivantes :

- `Parameterization` : qui prend en entrée un ensemble de polynômes engendrant un idéal zéro-dimensionnel et renvoie une paramétrisation rationnelle de l'ensemble de ses solutions.
- `Dimension` : qui prend en entrée une famille de polynômes et retourne la dimension de l'idéal engendré par cette famille.
- `Minors` : qui prend en entrée une famille de polynômes F, la dimension d de l'idéal engendré par F et un polynôme p et retourne l'ensemble des mineurs obtenus par le lemme 4 pour caractériser les points critiques de l'application polynomiale $x \in \mathbb{C}^n \to p(x) \in \mathbb{C}$ restreinte à la variété algébrique définie par F.

pour décrire notre algorithme.

Algorithme : Calcul d'au moins un point par composante connexe d'une variété algébrique équi-dimensionnelle lisse donnée par un système engendrant un idéal radical

- **Entrée :** Une famille $(f_1, \ldots, f_s) \subset \mathbb{Q}[X_1, \ldots, X_n]$ de polynômes engendrant un idéal radical définissant une variété algébrique $V \subset \mathbb{C}^n$ lisse et équi-dimensionnelle.
- **Sortie :** Une famille de paramétrisations rationnelles encodant un nombre fini de points de V et ayant une intersection non vide avec chaque composante connexe de $V \cap \mathbb{R}^n$.

1. Choisir $\mathbf{A}$ aléatoirement dans $GL_n(\mathbb{Q})$ et poser $F := [f_1^{\mathbf{A}}, \ldots, f_s^{\mathbf{A}}]$
2. Poser $d :=$ `Dimension`(F)
3. Poser $\Delta :=$ `Minors`$([f_1^{\mathbf{A}}, \ldots, f_s^{\mathbf{A}}], d, X_1)$
4. Poser `sols` $:=$ `Parameterization`$(F \cup \Delta)$
5. Pour i allant de 2 à d faire
   (a) Poser $F := F \cup X_{i-1}$, $d := d-1$ et $\Delta :=$ `Minors`$(F, d-1, X_i)$
   (b) Poser `sols` $:=$ `Parameterization`$(F \cup \Delta)$
6. Retourner `sols` $\cup$ `Parameterization`$(F \cup X_d)$

Résultat de complexité. Dans le cas où la routine `ZeroDimSolve` consiste à utiliser l'algorithme de résolution géométrique donné par G. Lecerf et dont la complexité est donnée dans le théorème 18, on peut procéder à l'analyse de complexité de cet algorithme.

To state our complexity result, we need to define an important algebraic quantity associated to $f_1, \ldots, f_s$, denoted by δ. To this effect, we describe more precisely the systems defining the polar varieties.

Soit $\mathbf{A}$ une matrice de $\mathrm{GL}_n(\mathbb{C})$. Rappelons qu'on note S_i le nombre de mineurs nécessaires pour définir l'idéal $\Delta_{n-i+1}^{\mathbf{A}}$, $1 \leqslant i \leqslant d+1$. Pour $i = 1, \ldots, d+1$, on note $M_{i,1}^{\mathbf{A}}, \ldots, M_{i,S_i}^{\mathbf{A}}$ la suite ordonnée de ces mineurs. D'après la définition des idéaux $\Delta_{n-i+1}^{\mathbf{A}}$, on peut supposer que ces suites sont ordonnées de manière telle que $M_{i,1}^{\mathbf{A}}, \ldots, M_{i,S_i}^{\mathbf{A}}$ est un préfixe de $M_{j,1}^{\mathbf{A}}, \ldots, M_{j,S_j}^{\mathbf{A}}$ pour $i \geqslant j$. Ainsi, $M_{1,1}^{\mathbf{A}}, \ldots, M_{1,S_1}^{\mathbf{A}}$ est la plus longue de ces suites.

Considérons maintenant la suite

$$\mathcal{G}^{\mathbf{A}} = f_1^{\mathbf{A}}, \ldots, f_s^{\mathbf{A}}, M_{1,1}^{\mathbf{A}}, \ldots, M_{1,S_1}^{\mathbf{A}}.$$

Étant donnée une sous-suite préfixe G de la précédente $\mathcal{G}^{\mathbf{A}}$, on définit la quantité $\delta_G^{\mathbf{A}}$ comme étant la somme des degrés algébriques des composantes irréductibles de la variété définie par G. On définit $\delta^{\mathbf{A}}$ comme étant le maximum de tous les $\delta_G^{\mathbf{A}}$, et δ comme le maximum de tous les $\delta^{\mathbf{A}}$ pour $\mathbf{A}$ dans $\mathrm{GL}_n(\mathbb{Q})$ telle que $\mathcal{P}(\mathbf{A})$ est satisfaite.

Si $f_1, \ldots, f_s$ sont de degré bornés par D, alors δ is est borné par $n(D(n-d))^n$ [94, page 4]. Des expérimentations montrent que cette borne est atteinte si $s = n - d$ et tous les f_i sont effectivement de degré D et choisis génériquement parmi les polynômes en n variables de degré D.

On peut maintenant donner le résultat de complexité. On note $\mathcal{U}(x)$ le nombre d'opérations nécessaires à la multipliation de polynômes de degré x. La notation $f \in \mathcal{O}_{\log}(x)$ signifie $f \in \mathcal{O}(x \log(x)^a)$, pour une constante a.

Théorème 26. *Soit $f_1, \ldots, f_s$ des polynômes de degré borné par D dans $\mathbb{Q}[X_1, \ldots, X_n]$, donnés par un programme d'évaluation de longueur L. Supposons que $\langle f_1, \ldots, f_s \rangle$ est un idéal radical, et équi-dimensionnel et que la variété algébrique $V = V(f_1, \ldots, f_s) \subset \mathbb{C}^n$ est lisse et de dimension d.*

Il existe un algorithme probabiliste calculant une famille de résolutions géométriques dont la réunion des solutions réelles a une intersection non vide avec chaque composante connexe de $V \cap \mathbb{R}^n$. La complexité

de cet algorithme est en

$$\mathcal{O}_{\log}\left(Ln^{10}S_1(s+S_1)\mathcal{U}\left(D(n-d)\delta\right)^3\right)$$

opérations arithmétiques.

Remarquons qu'en un sens cette borne de complexité n'est pas très satisfaisante. En effet, d'après le théorème 15 dans le cas où $f_1, \ldots, f_s$ constitue une suite régulière, le nombre de points critiques de la projection sur un axe restreint à V est borné par

$$\binom{n}{n-s} D^s (D-1)^{n-s}$$

ce qui est bien inférieur aux bornes sur le degré données dans le théorème 26. Ceci provient du fait que l'algorithme de résolution géométrique de Lecerf étant incrémental, il est peu adapté aux systèmes sur-déterminés qui sont caractéristiques des caractérisations algébriques de lieux critiques fondés sur le lemme 4. Dans le paragraphe ci-après on montre comment généraliser cet algorithme au cas non équi-dimensionnel d'une part mais aussi obtenir des bornes de complexité qui soient dominées par la taille de la sortie dans le pire cas.

Utilisation des Bases de Gröbner et performances pratiques. Implanter cet algorithme en utilisant des bases de Gröbner a un intérêt certain dès qu'on prend quelques précautions. L'intérêt des bases de Gröbner ici provient évidemment d'une meilleure gestion de la sur-détermination qui est spécifique des systèmes algébriques que nous manipulons et qui définissent les points critiques qu'on cherche à calculer. Parmi les précautions à prendre, il faut veiller à :

- ne pas faire explicitement les changements de variable : en effet, dans notre algorithme faire un changement de variables génériques et choisir des projections génériques (dans le système de coordonnées initial) sont des opérations strictement équivalentes.
- l'usage des bases de Gröbner permet de certifier le choix des projections de manière à assurer les propriétés de propreté de nos projections associées à la famille de variétés polaires que nous considérons : en effet, celles-ci sont liées à la présence de zéro à l'infini dans des espaces projectifs ; les bases de Gröbner permettant le calcul de clôtures projectives, elles deviennent aussi dans ce cadre un outil de certification.

Les implantations de cet algorithme dans les cas lisses et équi-dimensionnels ont permis déjà de résoudre de nombreux problèmes qui étaient hors de portée des algorithmes qui ont déjà été exposés dans ce chapitre.

Voyons maintenant comment on peut généraliser cette approche au cas non équi-dimensionnel.

5.5.2 Le cas non équi-dimensionnel lisse

Comme précédemment, étant donné une variété algébrique $V \subset \mathbb{C}^n$ de dimension d, on note π_i (pour i dans $\{1, \ldots, d\}$) la projection canonique :

$$\begin{array}{rccc} \Pi_i : & \mathbb{C}^n & \longrightarrow & \mathbb{C}^i \\ & (x_1, \ldots, x_n) & \mapsto & (x_1, \ldots, x_i) \end{array}$$

et $W_{n-(i-1)}(V)$ le lieu critique de la restriction de π_i à V, c'est-à-dire **l'union des points critiques des restrictions de π_i à chaque composante équi-dimensionnelle de V**. On a évidemment :

$$W_n(V) \subset W_{n-1}(V) \subset \ldots \subset W_{n-d+1}(V) \subset W_{n-d}(V)$$

Une manière naïve d'utiliser les résultats du paragraphe précédent consiste à calculer une famille de générateurs des idéaux associés à chaque composante équi-dimensionnelle de V et à appliquer l'algorithme du paragraphe précédent à chacune de ces familles. En pratique, ces familles de générateurs seront des bases de Gröbner. On serait alors confronté aux mêmes problèmes que ceux rencontrés dans les algorithmes présentés dans les paragraphes 5.3 et 5.4 : le nombre de polynômes ainsi que leur degré et leur densité rend délicat le calcul des points critiques des projections considérées restreintes aux variétés définies par ces bases de Gröbner. Tant que faire se peut, il nous faut travailler avec les polynômes de départ et éviter d'avoir à travailler avec le résultat d'un calcul d'élimination algébrique. Pour ce faire, on a recours à la caractérisation lagrangienne des points critiques exhibées dans le lemme 5.

Lemme 8. *Soit $(f_1, \ldots, f_s)$ une famille de polynômes dans $\mathbb{Q}[X_1, \ldots, X_n]$. On suppose qu'elle engendre un idéal radical de dimension d et qu'elle définit une variété algébrique lisse $V \subset \mathbb{C}^n$. Étant donné un point $(p_1, \ldots, p_d)$ dans $\mathbb{Q}^d$, on considère le systéme d'équations polynomiales dans $\mathbb{Q}[\ell_1, \ldots, \ell_s, X_1, \ldots, X_n]$:*

$$\begin{cases} f_1 = \cdots = f_s = 0, \\ X_1 - p_1 = \cdots = X_i - p_i = 0 \\ \ell_1 \frac{\partial f_1}{\partial X_{i+1}} + \cdots + \ell_s \frac{\partial f_s}{\partial X_{i+1}} = 1 \\ \ell_1 \frac{\partial f_1}{\partial X_{i+2}} + \cdots + \ell_s \frac{\partial f_s}{\partial X_{i+2}} = 0 \\ \qquad\qquad \vdots \\ \ell_1 \frac{\partial f_1}{\partial X_n} + \cdots + \ell_s \frac{\partial f_s}{\partial X_n} = 0 \end{cases} \tag{2}$$

La projection de ses solutions complexes sur $X_1, \ldots, X_n$ est $\Pi_i^{-1}(p_1, \ldots, p_i) \cap W_{n-i}(V)$.

Lemme 9. *Soit $V \subset \mathbb{C}^n$ une variété algébrique lisse définie par s polynômes $f_1, \ldots, f_s$ de $\mathbb{Q}[X_1, \ldots, X_n]$ engendrant un idéal* radical. *Étant donnée $\mathbf{A} \in GL_n(\mathbb{Q})$, considérons $I_0^{\mathbf{A}} \subset \mathbb{Q}[\ell_1, \ldots, \ell_s, X_1, \ldots, X_n]$ l'idéal engendré par le système ci-dessous :*

$$\begin{cases} f_1^{\mathbf{A}} = \cdots = f_s^{\mathbf{A}} = 0 \\ \ell_1 \frac{\partial f_1^{\mathbf{A}}}{\partial X_1} + \cdots + \ell_s \frac{\partial f_s^{\mathbf{A}}}{\partial X_1} = 1 \\ \ell_1 \frac{\partial f_1^{\mathbf{A}}}{\partial X_2} + \cdots + \ell_s \frac{\partial f_s^{\mathbf{A}}}{\partial X_2} = 0 \\ \qquad\qquad \vdots \\ \ell_1 \frac{\partial f_1^{\mathbf{A}}}{\partial X_n} + \cdots + \ell_s \frac{\partial f_s^{\mathbf{A}}}{\partial X_n} = 0 \end{cases}$$

Il existe un fermé de Zariski $\mathcal{H} \subsetneq GL_n(\mathbb{C})$ tel que si $\mathbf{A} \notin \mathcal{H}$, $I_0^{\mathbf{A}}$ est radical et l'idéal d'élimination $I_0^{\mathbf{A}} \cap \mathbb{Q}[X_1, \ldots, X_n]$ est zéro-dimensionnel *ou égale à $\langle 1 \rangle$.*

On suppose de plus que $f_1, \ldots, f_s$ est une suite régulière. Alors, il existe un fermé de Zariski $\mathcal{H}' \subsetneq GL_n(\mathbb{C})$ tel que si $\mathbf{A} \notin \mathcal{H}'$, l'idéal $I_0^{\mathbf{A}}$ est radical et est soit zéro-dimensionnel *ou égale à $\langle 1 \rangle$.*

Étant donnée une famille de polynômes $(f_1, \ldots, f_s) \subset \mathbb{Q}[X_1, \ldots, X_n]$, d la dimension de l'idéal $\langle f_1, \ldots, f_s \rangle$, $\mathbf{A} \in GL_n(\mathbb{Q})$, et $p = (p_1, \ldots, p_d)$ un point de $\mathbb{Q}^d$ on note $I_i^{\mathbf{A},p}$ (pour $i \in \{1, \ldots, d-1\}$) l'idéal de $\mathbb{Q}[X_1, \ldots, X_n, \ell_1, \ldots, \ell_k]$ engendré par :

$$\begin{cases} f_1^{\mathbf{A}} = \cdots = f_s^{\mathbf{A}} = 0, \\ X_1 - p_1 = 0, \ldots, X_i - p_i = 0 \\ \ell_1 \frac{\partial f_1^{\mathbf{A}}}{\partial X_{i+1}} + \cdots + \ell_1 \frac{\partial f_s^{\mathbf{A}}}{\partial X_{i+1}} = 1 \\ \ell_1 \frac{\partial f_1^{\mathbf{A}}}{\partial X_{i+2}} + \cdots + \ell_1 \frac{\partial f_s^{\mathbf{A}}}{\partial X_{i+2}} = 0 \\ \qquad \vdots \\ \ell_1 \frac{\partial f_1^{\mathbf{A}}}{\partial X_n} + \cdots + \ell_1 \frac{\partial f_s^{\mathbf{A}}}{\partial X_n} = 0 \end{cases}$$

et $I_d^{\mathbf{A},p}$ l'idéal de $\mathbb{Q}[X_1, \ldots, X_n, \ell_1, \ldots, \ell_k]$ engendré par $f_1^{\mathbf{A}} = \cdots = f_s^{\mathbf{A}} = X_1 - p_1 = \cdots = X_d - p_d = 0$. Enfin on note $I_0^{\mathbf{A},p}$ l'idéal engendré par :

$$\begin{cases} f_1^{\mathbf{A}} = \cdots = f_s^{\mathbf{A}} = 0, \\ \ell_1 \frac{\partial f_1^{\mathbf{A}}}{\partial X_1} + \cdots + \ell_1 \frac{\partial f_s^{\mathbf{A}}}{\partial X_1} = 1 \\ \ell_1 \frac{\partial f_1^{\mathbf{A}}}{\partial X_2} + \cdots + \ell_1 \frac{\partial f_s^{\mathbf{A}}}{\partial X_2} = 0 \\ \qquad \vdots \\ \ell_1 \frac{\partial f_1^{\mathbf{A}}}{\partial X_n} + \cdots + \ell_1 \frac{\partial f_s^{\mathbf{A}}}{\partial X_n} = 0 \end{cases}$$

C'est le résultat ci-dessous qui nous permet de généraliser l'algorithme du paragraphe précédent au cas non équi-dimensionnel.

Théorème 27. *Soit $(f_1, \ldots, f_s) \subset \mathbb{Q}[X_1, \ldots, X_n]$ une famille de polynômes qui engendre un idéal radical et définit une variété algébrique lisse de dimension d. Il existe un fermé de Zariski $\mathcal{H} \subsetneq GL_n(\mathbb{Q})$ et une hypersurface $\mathcal{P} \subsetneq \mathbb{C}^d$ tels que si $\mathbf{A} \notin \mathcal{H}$ et $p \in \mathbb{Q}^d \setminus \mathcal{P}$,*

- *les idéaux $I_i^{\mathbf{A},p}$ (pour tout $i \in \{0, \ldots, d\}$) sont radicaux ;*
- *les idéaux $I_i^{\mathbf{A},p} \cap \mathbb{Q}[X_1, \ldots, X_n]$ (pour tout $i \in \{0, \ldots, d\}$) sont soit zéro-dimensionnels soit égaux à $\langle 1 \rangle$;*
- *l'ensemble de leurs racines réelles a une intersection non vide avec chaque composante équi-dimensionnelle de $V \cap \mathbb{R}^n$.*

D'après le résultat ci-dessus, après un choix générique de $\mathbf{A} \in GL_n(\mathbb{Q})$, les idéaux d'élimination $I_i^{\mathbf{A}} \cap \mathbb{Q}[X_1, \ldots, X_n]$ sont soit zéro-dimensionnels soit égaux à $\langle 1 \rangle$ et permettent d'obtenir au moins un point par composante connexe de $V \cap \mathbb{R}^n$.

Remarquons que le résultat ci-dessus permet d'obtenir des bornes sur le nombre de composantes connexes d'une variété algébrique réelle lisse en appliquant les résultats du paragraphe 4.4 du chapitre 4 et qui sont meilleures que celles qui sont obtenues classiquement (voir [21]) ou en bornant à l'aide du théorème de Bézout les sorties des algorithmes présentés dans les paragraphes précédents.

Théorème 28. *Soit $(f_1, \ldots, f_s) \subset \mathbb{Q}[X_1, \ldots, X_n]$ (avec $s \leqslant n-1$) une famille de polynômes engendrant un idéal radical et définissant une variété algébrique lisse $V \subset \mathbb{C}^n$ de dimension d. On note $D_1, \ldots, D_s$ les degrés respectifs de $f_1, \ldots, f_s$ et D le maximum de $D_1, \ldots, D_s$. Le nombre de composantes connexes de $V \cap \mathbb{R}^n$ est borné par :*

$$D_1 \cdots D_s \sum_{i=0}^{d} (D-1)^{n-s-i} \binom{n-i}{n-i-s}$$

De plus, si $(f_1, \ldots, f_s)$ est une suite régulière, le nombre de composantes connexes de $V \cap \mathbb{R}^n$ est borné par :

$$D_1 \cdots D_s \sum_{i=0}^{n-s} (D-1)^{n-s-i} \binom{n-1-i}{n-i-s}$$

Enfin, remarquons que dans le cas où $D \leqslant 2$, la sortie de notre algorithme est polynomiale en le nombre de variables et exponentielle en le nombre d'équations.

L'algorithme. Soit $p = (p_1, \ldots, p_d)$ un point de $\mathbb{Q}^d$. L'algorithme fondé sur le théorème 27 consiste à choisir *aléatoirement* une matrice $\mathbf{A} \in GL_n(\mathbb{Q})$ et

- à résoudre les systèmes polynomiaux engendrant les idéaux $I_i^{\mathbf{A}}$ (pour $i = 1, \ldots, d-1$) :

$$\begin{cases} f_1^{\mathbf{A}} = \cdots = f_s^{\mathbf{A}} = 0, \\ X_1 - p_1 = 0, \cdots, X_i - p_i = 0 \\ \ell_1 \frac{\partial f_1^{\mathbf{A}}}{\partial X_{i+1}} + \cdots + \ell_1 \frac{\partial f_s^{\mathbf{A}}}{\partial X_{i+1}} = 1 \\ \ell_1 \frac{\partial f_1^{\mathbf{A}}}{\partial X_{i+2}} + \cdots + \ell_1 \frac{\partial f_s^{\mathbf{A}}}{\partial X_{i+2}} = 0 \\ \qquad \vdots \\ \ell_1 \frac{\partial f_1^{\mathbf{A}}}{\partial X_n} + \cdots + \ell_1 \frac{\partial f_s^{\mathbf{A}}}{\partial X_n} = 0 \end{cases}$$

- résoudre le système

$$\begin{cases} f_1^{\mathbf{A}} = \cdots = f_s^{\mathbf{A}} = 0, \\ \ell_1 \frac{\partial f_1^{\mathbf{A}}}{\partial X_1} + \cdots + \ell_s \frac{\partial f_s^{\mathbf{A}}}{\partial X_1} = 1 \\ \ell_1 \frac{\partial f_1^{\mathbf{A}}}{\partial X_2} + \cdots + \ell_s \frac{\partial f_s^{\mathbf{A}}}{\partial X_2} = 0 \\ \qquad \vdots \\ \ell_1 \frac{\partial f_1^{\mathbf{A}}}{\partial X_n} + \cdots + \ell_s \frac{\partial f_s^{\mathbf{A}}}{\partial X_n} = 0 \end{cases}$$

  engendrant l'idéal $I_0^{\mathbf{A}}$;
- et enfin résoudre le système ci-dessous $f_1^{\mathbf{A}} = \cdots = f_s^{\mathbf{A}} = X_1 - p_1 = \cdots = X_d - p_d = 0$ engendrant l'idéal $I_d^{\mathbf{A}}$.

Remarquons qu'ici les systèmes polynomiaux qu'on cherche à résoudre engendrent des idéaux $I_i^{\mathbf{A}} \subset \mathbb{Q}[X_1, \ldots, X_n, \ell_1, \ldots, \ell_s]$ de *dimension positive* dont les intersections avec $\mathbb{Q}[X_1, \ldots, X_n]$ sont de dimension zéro ou triviale. Évidemment, ce qu'on cherche à calculer est l'intersection $I_i^{\mathbf{A}} \cap \mathbb{Q}[X_1, \ldots, X_n]$.

En théorie, ceci se fait aisément à l'aide des bases de Gröbner si on utilise un ordre monomial d'élimination $[\ell_1, \ldots, \ell_s] > [X_1, \ldots, X_n]$. Une fois ce calcul effectué, le calcul de paramétrisations rationnelles des solutions des idéaux zéro-dimensionnels obtenus se fait classiquement.

Pour ce qui est de l'usage de la résolution géométrique, il est suffisant de calculer des paramétrisations rationnelles de points génériques obtenus dans chaque composante équi-dimensionnelle C_p de dimension p du lieu-solution de $I_i^{\mathbf{A}}$ (ces points sont obtenus en intersectant C_p avec p formes linéaires génériques de $\mathbb{Q}[X_1, \ldots, X_n, \ell_1, \ldots, \ell_k]$. Ceci est équivalent à :

- effectuer un changement linéaire de variables générique $\mathbf{B} \subset GL_{n+s}(\mathbb{Q})$ envoyant le vecteur de coordonnées $[X_1, \ldots, X_n, \ell_1, \ldots, \ell_s]$ sur un nouveau vecteur de coordonnées $[v_1, \ldots, v_{n+s}]$
- calculer une paramétrisation rationnelle $(q, q_0, q_1, \ldots, q_{n+s})$ de l'intersection de chaque composante équi-dimensionnelle C_p de dimension p de l'ensemble des solutions complexes de $I_i^{\mathbf{A}}$ et du sous-espace linéaire défini par $v_1 = \cdots = v_p = 0$
- calculer une paramétrisation rationnelle de l'ensemble des solutions de $I_i^{\mathbf{A}} \cap \mathbb{Q}[X_1, \ldots, X_n]$ en multipliant $\mathbf{B}^{-1}$ par l vecteur $(q_1/q_0, \ldots, q_{n+s}/q_0)$ et en retournant les n premières coordonnée sur vecteur obtenu.

Une fois ce calcul effectué, on obtient des paramétrisations rationnelles d'au moins un point par composante connexe de $V \cap \mathbb{R}^n$ exprimées dans le systèmes de coordonnées induit par le changement de variables associé à $\mathbf{A}$. Obtenir des paramétrisations rationnelles dans le système de coordonnées initial se fait alors simplement en multipliant par $\mathbf{A}^{-1}$ les paramétrisations précédemment calculées.

Pour décrire l'algorithme que nous avons obtenus, nous considérons donc les routines ci-dessous :

- `Lagrange` : qui prend en entrée une famille de polynômes F et un polynôme p et retourne le système de Lagrange caractérisant les points critiques de l'application $x \in \mathbb{C}^n \to p(x) \in \mathbb{C}$ restreinte à la variété algébrique définie par F, conformément au lemme 5 ;
- `EliminateSolve` : qui prend en entrée une famille de polynômes F dans $\mathbb{Q}[\mathbf{X}, \mathbf{L}]$ et une liste de variables $\mathbf{L}$ et retourne un système de générateurs de l'idéal $\langle F \rangle \cap \mathbb{Q}[\mathbf{X}]$.

Algorithme : Calcul d'au moins un point par composante connexe d'une variété algébrique lisse donnée par un système engendrant un idéal radical

- **Entrée :** Une famille $(f_1, \ldots, f_s) \subset \mathbb{Q}[X_1, \ldots, X_n]$ de polynômes engendrant un idéal radical définissant une variété algébrique $V \subset \mathbb{C}^n$ lisse.
- **Sortie :** Une famille de paramétrisations rationnelles encodant un nombre fini de points de V et ayant une intersection non vide avec chaque composante connexe de $V \cap \mathbb{R}^n$.

1. Choisir $\mathbf{A}$ aléatoirement dans $GL_n(\mathbb{Q})$ et poser $F := [f_1^{\mathbf{A}}, \ldots, f_s^{\mathbf{A}}]$
2. Poser $d :=$ `Dimension`(F)
3. Poser $\Delta :=$ `Lagrange`$([f_1^{\mathbf{A}}, \ldots, f_s^{\mathbf{A}}], X_1)$ et affecter à $\mathbf{L} := [\ell_1, \ldots, \ell_s]$ (les variables introduites par `Lagrange`.
4. Poser `sols` := `Parameterization`(`EliminateSolve`$(\Delta, \mathbf{L})$)
5. Pour i allant de 2 à d faire
   (a) Poser $F := F \cup X_{i-1}$, $d := d - 1$ et
   $$\Delta :=$$ `Lagrange`(F, X_i)
   et affecter à $\mathbf{L} := [\ell_1, \ldots, \ell_{s+i-1}]$ (les variables introduites par `Lagrange`.
   (b) Poser
   `sols` := `Parameterization`(`EliminateSolve`$(\Delta, \mathbf{L})$)
6. Retourner `sols` $\cup$ `Parameterization`$(F \cup X_d)$

La complexité de cet algorithme dépend évidemment de la complexité de la routine d'élimination algébrique utilisée pour obtenir `EliminateSolve`.

Penchons-nous tout d'abord sur l'usage des bases de Gröbner. Tout d'abord les astuces permettant d'éviter les changements explicites de variables décrites dans le paragraphe précédent doivent être utilisées. Comme on manipule des idéaux de dimension positive, sans informations algébriques supplémentaires sur les systèmes engendrant $I_i^{\mathbf{A}}$ (telle que la régularité ou la semi-régularité, voir [16]), la régularité de Hilbert [23] ne peut pas être bornée de manière satisfaisante. Ainsi, en l'état actuel des connaissances sur le sujet, on ne peut pas donner de bornes meilleures que celles qui sont doublement exponentielles en le nombre de variables [102] pour estimer la complexité de notre algorithme quand on l'implante en utilisant des bases de Gröbner. Ceci dit, il faut plus voir les commentaires ci-dessus comme le constat d'un non-résultat que comme un résultat. Les expérimentations pratiques que nous avons effectuées montrent clairement que les bases de Gröbner n'ont pas un comportement doublement exponentiel en le nombre de variables sur les systèmes de Lagrange que nous avons eu à considérer. En pratique, il est en général encore préférable d'utiliser les bases de Gröbner pour résoudre ce type de systèmes algébriques. Ceci dit, les meilleures performances pratiques sont obtenues en imposant (par localisation) des conditions de rang sur la matrice jacobienne associée à la famille de polynômes donnée en entrée après avoir effectué une décomposition équi-dimensionnelle. Ainsi, si G est une base de Gröbner d'une composante équi-dimensionnelle de dimension p de l'idéal $I_i^{\mathbf{A}}$, on utilise la caractérisation des points critiques qu'on cherche à calculer du lemme 5 en faisant comme si la famille $(f_1, \ldots, f_s)$ engendrait $\langle G \rangle$ de manière à obtenir une famille de mineurs de jacobienne $\mathcal{D}$. Puis, il suffit de calculer une base de Gröbner de $\langle G \rangle + \langle \mathcal{D} \rangle$. C'est cette stratégie qui est, en l'état actuel des connaissances et des implantations, la plus efficace. Elle permet de résoudre des problèmes très largement non atteignables par les méthodes précédemment décrites.

Les résultats de complexité sur les calculs de résolution géométrique permettent en revanche de donner une estimation de complexité de l'algorithme décrit dans ce paragraphe qui soit intéressante.

Dans la suite, on note $g_1^{\mathbf{A}}$ le polynôme $\ell_1 \frac{\partial f_1^{\mathbf{A}}}{\partial X_1} + \cdots + \ell_s \frac{\partial f_s^{\mathbf{A}}}{\partial X_1} - 1$ et on note g_i le polynôme $\ell_1 \frac{\partial f_1^{\mathbf{A}}}{\partial X_i} + \cdots + \ell_s \frac{\partial f_s^{\mathbf{A}}}{\partial X_i}$ (pour $i = 2, \ldots, n$).

D'après le théorème 27 et le corollaire 3, le maximum des degrés algébriques des composantes irréductibles des variétés i8ntermédiaires définies par $f_1^{\mathbf{A}}, \ldots, f_i^{\mathbf{A}}$ (pour $1 \leqslant i \leqslant s$) et $f_1^{\mathbf{A}}, \ldots, f_s^{\mathbf{A}}, g_1^{\mathbf{A}}, \ldots, g_i^{\mathbf{A}}$ (pour $1 \leqslant i \leqslant n$) est borné par $D^s(D-1)^{n-s}\binom{n}{n-s}$.

Le système définissant $I_0^{\mathbf{A}}$ a $n+s$ variables et contient $n+s$ polynômes.

De plus, étant donné un programme d'évaluation de longueur $\mathcal{L}$ du système $(f_1, \ldots, f_s)$, on obtient un programme d'évaluation du système définissant $I_0^{\mathbf{A}}$ de longueur $\mathcal{O}((\mathcal{L} + n^2))$ en utilisant les résultats de [22].

Cette discussion permet d'énoncer le résultat ci-dessous :

Théorème 29. *Soit $(f_1, \ldots, f_s)$ une famille de polynômes de $\mathbb{Q}[X_1, \ldots, X_n]$ engendrant un idéal radical et définissant une variété algébrique lisse $V \subset \mathbb{C}^n$. On note D le maximum des degrés de f_i (pour $i = 1, \ldots, s$) et L la longueur d'un programme d'évaluation du système $(f_1, \ldots, f_s)$. Il existe un algorithme probabiliste calculant au moins un point par composante connexe de $V \cap \mathbb{R}^n$ en :*

$$\mathcal{O}_{\log}\left((n+s)^5((n+s)(L+n^2)+(n+s)^3)M(D\mathfrak{d})^3\right)$$

opérations dans $\mathbb{Q}$ où $\mathfrak{d}$ bornée par $D^s(D-1)^{n-s}\binom{n}{n-s}$.

Remarque. *Remarquons que lorsque $(f_1, \ldots, f_s)$ est une suite régulière, $\mathfrak{d}$ est borné par*

$$D^s(D-1)^{n-s}\binom{n-1}{n-s}.$$

De plus, dans le cas où $D \leqslant 2$, on obtient un algorithme de complexité polynomiale en le nombre de variables et exponentiel en le nombre d'équations sans modifications partiaculières. On trouve déjà de tels algorithmes dans [63, 64] mais ils souffrent des mêmes défauts que celui exposé dans le paragraphe 5.2 de ce chapitre et ont des constantes de complexité bien plus élevées que celles que nous obtenons.

Nous disposons maintenant d'algorithmes efficaces pour calculer au moins un point par composante connexe dans une variété algébrique réelle donnée par une famille de polynômes engendrant un idéal radical et définissant une variété algébrique lisse. Il nous faut maintenant nous pencher sur les cas où des chutes de rang apparaissent dans les matrices jacobiennes associées aux polynômes donnés en entrée. Nous avons déjà étudié ces cas dans les paragraphes 5.3 et 5.4 et expliqué les limites des algorithmes qui y sont décrits. Les avancées obtenues dans le cas des variétés non équi-dimensionnelles sont fondées sur la volonté d'éviter au maximum d'avoir à relancer récursivement nos algorithmes sur des sorties de routines d'élimination algébrique. C'est cette volonté qu'on poursuit dans les cas où des chutes de rang apparaissent dans les jacobiennes en revisitant les stratégies de déformation infinitésimale avec un souci d'efficacité pratique.

5.6 Le cas des hypersurfaces singulières

Ce paragraphe est consacré à l'élaboration d'un algorithme efficace de calcul d'au moins un point par composante connexe dans une variété algébrique définie par une équation $f = 0$ (avec $f \in \mathbb{Q}[X_1, \ldots, X_n]$) dans le cas où l'hypersurface $\mathcal{H} \subset \mathbb{C}^n$ définie par $f = 0$ contient une infinité de points singuliers. Pour ce faire, on ramène le problème au calcul de limites de points critiques d'une application polynomiale restreinte à l'hypersurface définie par $f - \varepsilon = 0$ (lorsque ε tend vers 0). En effet, cette dernière est lisse et donc on peut appliquer les caractérisations algébriques des lemmes 4 et 5. La difficulté réside dans le fait que pour obtenir un algorithme efficace en pratique, on doit éviter d'effectuer nos calculs dans $\mathbb{Q}(\varepsilon)$ ou sur $\mathbb{Q}\langle\varepsilon\rangle$ ce qu'implique l'introduction *explicite* de cet infinitésimal.

5.6.1 Calcul de limites de points critiques

Soit f un polynôme dans $\mathbb{Q}[X_1, \ldots, X_n]$ de degré borné par D. Pour $t \in \mathbb{Q}$, on note $\mathcal{H}_t \subset \mathbb{C}^n$ l'hypersurface définie par $f - t = 0$.

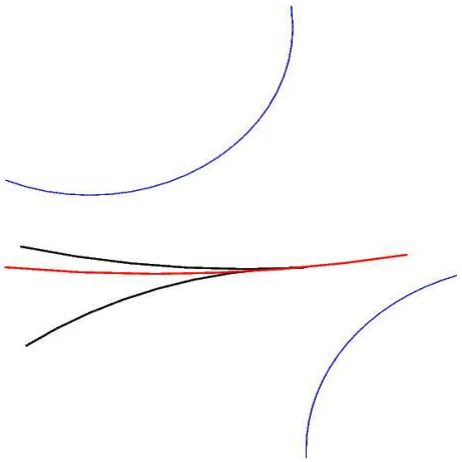

FIG. 23 – Limites de points critiques

Soit $\varphi : x \in \mathbb{C}^n \to \varphi(x) \in \mathbb{C}$ une application polynomiale. Pour $t \in \mathbb{Q}$, on note $\mathfrak{C}(\varphi, \mathcal{H}_t)$ le lieu critique de la restriction de φ à $\mathcal{H}_t$. Le résultat suivant caractérise les limites bornées de $\mathfrak{C}(\varphi, \mathcal{H}_t)$ quand t tend vers 0.

Théorème 30. *Soit L une nouvelle variable, et $I \subset \mathbb{Q}[L, X_1, \ldots, X_n]$ l'idéal engendré par la famille de polynômes :*

$$L.\frac{\partial f}{\partial X_1} - \frac{\partial \varphi}{\partial X_1}, \ldots, L.\frac{\partial f}{\partial X_n} - \frac{\partial \varphi}{\partial X_n}$$

Supposons que I soit de dimension 1, et que $\mathfrak{C}(\varphi, \mathcal{H}_0)$ soit de dimension au plus zéro.

Alors, l'ensemble des limites bornées de $\mathfrak{C}(\varphi, \mathcal{H}_t)$ quand t tend vers 0 est contenu dans la variété algébrique associée à l'idéal

$$I_0 = \langle f \rangle + (I \cap \mathbb{Q}[X_1, \ldots, X_n]) \subset \mathbb{Q}[X_1, \ldots, X_n]$$

et I_0 est de dimension 0 au plus. .

Remarque. *Le résultat ci-dessus n'est vraiment utile que si $\mathcal{H}_0$ n'est pas lisse puisque, dans ce cas, l'ensemble des limites bornées de $\mathfrak{C}(\varphi, \mathcal{H}_t)$ quand $t \to 0$ peut contenir strictement $\mathfrak{C}(\varphi, \mathcal{H}_0)$.*

La figure 23 illustre bien le phénomène sous-jacent au théorème 30. On y a tracé le *cusp* ainsi que la courbe définie par I et sa projection sur (X, Y) (ici φ est la projection sur la droite horizontale vivant dans le plan où le *cusp* est défini). Les points de $\mathfrak{C}(\varphi, \mathcal{H}_t)$ vérifient :

$$f - t = 0, L\mathbf{grad}(f) = \mathbf{grad}(\varphi)$$

Lorsque ces points tendent vers le point singulier du *cusp*, L tend vers l'infini.

Remarque. *Chaque hypothèse du théorème 30 est importante, en particulier celle qui impose à $\mathfrak{C}(\varphi, \mathcal{H}_0)$ d'être au plus de dimension zéro. En effet, si on considère l'hypersurface définie par $xy = 0$, et que φ est la projection sur x, le théorème tombe en défaut (pour tout $t \neq 0$, $\mathfrak{C}(\varphi, \mathcal{H}_t) = \varnothing$).*

Le corollaire ci-dessous montre qu'on contrôle bien le degré des objets géométriques introduits par le théorème 30.

Corollaire 4. *Soit D un entier qui borne le degré de f et celui de φ. En utilisant les notations introduites ci-dessus, le degré de $\sqrt{I}$ est borné par $n(D-1)^{n-1}$ et le degré de $\sqrt{I_0}$ est borné par $n.D.(D-1)^{n-1}$.*

Algorithme utilisant des bases de Gröbner. Des résultats classiques sur les bases de Gröbner (voir [42, Chapitre 9]) montrent comment mettre en œuvre facilement le résultat ci-dessus. Il s'agit finalement d'éliminer la variable L dans l'idéal I en utilisant, par exemple, un ordre par bloc DRL avec $[L] > [X_1, \ldots, X_n]$ puis d'ajouter à la base de Gröbner obtenue le polynôme f.

Algorithme utilisant la résolution géométrique. L'algorithme de de calcul de résolutions géométriques (voir [94]) ne permet pas *a priori* de calculer des idéaux d'élimination. Néanmoins, il est possible de calculer la clôture de Zariski de l'ensemble constructible défini par un système d'équations et d'inéquations polynomiales. Remarquons que l'idéal

$$I = \langle L.\frac{\partial f}{\partial X_1} - \frac{\partial \varphi}{\partial X_1}, \ldots, L.\frac{\partial f}{\partial X_n} - \frac{\partial \varphi}{\partial X_n}\rangle \cap \mathbb{Q}[X_1, \ldots, X_n]$$

contient l'idéal J engendré par l'ensemble Δ de tous les mineurs $(2,2)$ de la matrice jacobienne associée à $\mathrm{Jac}(f, \varphi)$. Soit $\mathcal{P}$ un idéal premier associé à $\sqrt{J}$ qui ne soit pas associé à $\sqrt{I}$ et y un point *générique* dans la variété algébrique associée à $\mathcal{P}$. Remarquons que si il existe $i \in \{1, \ldots, n\}$ tel que $\frac{\partial f}{\partial X_i}(y) \neq 0$, alors y appartient à la courbe associée à $I \cap \mathbb{Q}[X_1, \ldots, X_n]$ ce qui n'est pas possible d'après nos hypothèses.

Ainsi, pour calculer une résolution géométrique de la variété algébrique associée à $I \cap \mathbb{Q}[X_1, \ldots, X_n]$ il est suffisant de saturer J par une somme aléatoire des dérivées partielles de f

$$b_1\frac{\partial f}{\partial X_1} + \cdots + b_n\frac{\partial f}{\partial X_n}.$$

Ce4ci peut se faire en donnant en entrée à l'algorithme de résolution géométrique le système :

$$\Delta, \quad b_1\frac{\partial f}{\partial X_1} + \cdots + b_n\frac{\partial f}{\partial X_n} \neq 0$$

où les b_i sont choisis aléatoirement dans $\mathbb{Q}$.

Une autre stratégie consiste à calculer pour $i = 1, \ldots, n$ des résolutions gémétriques des systèmes

$$\Delta, \quad \frac{\partial f}{\partial X_i} \neq 0$$

5.6.2 Algorithmes

On étudie maintenant les diverses manières d'utiliser les résultats ci-dessus pour obtenir des algorithmes permettant de calculer au moins un point par composante connexe dans un ensemble algébrique réel défini par une équation polynomiale $f = 0$ (avec $f \in \mathbb{Q}[X_1, \ldots, X_n]$) dans le cas où l'hypersurface $\mathcal{H}_0 \subset \mathbb{C}^n$ définie par $f = 0$ est singulière.

La stratégie consiste à utiliser le théorème 30 et la méthode des points critiques mise en œuvre soit en considérant une fonction "distance à un point" (comme dans [124, 11, 14]) soit des fonctions de projection (comme dans [133, 132, 12]).

Utilisation des fonctions distance. Étant donné un point $A = (a_1, \ldots, a_n)$ dans $\mathbb{Q}^n$, soit φ_A l'application polynomiale qui envoie $y \in \mathbb{C}^n$ sur le carré de la fonction distance au point A :

$$\begin{array}{rccc} \varphi_A : & \mathbb{C}^n & \to & \mathbb{C} \\ & (x_1, \ldots, x_n) & \to & (x_1 - a_1)^2 + \cdots + (x_n - a_n)^2 \end{array}$$

Le théorème ci-dessous montre qu'en calculant les limites de points critiques de la fonction distance à un point A choisi génériquement dans $\mathbb{C}^n$ comme suggéré par le théorème 30, on obtient au moins un point par composante connexe dans $\mathcal{H}_0 \cap \mathbb{R}^n$.

Théorème 31. *Il existe un fermé de Zariski $\mathcal{A} \subsetneq \mathbb{C}^n$ tel que pour $A = (a_1, \ldots, a_n) \in \mathbb{Q}^n \setminus \mathcal{A}$ la variété algébrique associée à l'idéal*

$$\langle f\rangle + \left(\langle L.\frac{\partial f}{\partial X_1} - (X_1 - a_1), \ldots, L.\frac{\partial f}{\partial X_n} - (X_n - a_n)\rangle \cap \mathbb{Q}[X_1, \ldots, X_n]\right)$$

(où L est une nouvelle variable) est de dimension au plus zéro et a une intersection non vide avec chaque composante connexe de l'ensemble algébrique réel $\mathcal{H}_0 \cap \mathbb{R}^n$.

La preuve de ce résultat est fondée sur les deux lemmes ci-dessous qui ont leur intérêt propre. Le premier est déjà montré dans [124] et montre que le calcul des limites bornées des points critiques de la fonction distance au point A restreinte à $\mathcal{H}_t$ quand t tend vers 0 permet d'obtenir au moins un point par composante connexe dans $\mathcal{H}_0 \cap \mathbb{R}^n$.

Lemme 10. *[124] Soit A un point de $\mathbb{Q}^n$ et φ_A une application polynomiale qui associe à $x \in \mathbb{C}^n$ le carré de la fonction distance à A. Chaque composante connexe de $\mathcal{H}_0$ contient au moins un point qui est une limite bornée de $\mathfrak{C}(\varphi_A, \mathcal{H}_t)$ quand t tend vers* 0.

Le lemme suivant montre que si le point A est choisi suffisamment génériquement, les hypothèses du théorème 30 sont satisfaites.

Lemme 11. *Il existe un fermé de Zariski $\mathcal{A} \subsetneq \mathbb{C}^n$ tel que pour $A = (a_1, \ldots, a_n) \in \mathbb{Q}^n \setminus \mathcal{A}$, l'idéal I_A engendré par :*

$$L.\frac{\partial f}{\partial X_1} - (X_1 - a_1), \ldots, L.\frac{\partial f}{\partial X_n} - (X_n - a_n)$$

est équi-dimensionnel, de dimension 1*, et $\mathfrak{C}(\varphi_A, \mathcal{H}_0)$ est de dimension au plus* 0.

D'après le théorème 31, on peut déduire un algorithme calculant au moins un point par composante connexe dans $\mathcal{H}_0 \cap \mathbb{R}^n$ en utilisant soit des bases de Gröbner soit des calculs de résolutions géométriques. Un tel algorithme est basé sur le calcul des limites de points critiques la restriction de φ_A à $\mathcal{H}_t$ quand t tend vers 0.

Dans le paragraphe suivant, on montre comment obtenir un autre algorithme calculant toujours au moins un point par composante connexe dans $\mathcal{H}_0 \cap \mathbb{R}^n$ en adaptant les résultats de [132] à notre contexte. Au lieu d'applcations polynomiales quadratiques, on utilise ici des fonctions de projection qui sont linéaires.

Algorithme : Cas hypersurface singulière (Utilisation de fonctions distances)

- **Entrée :** Un polynôme $f \in \mathbb{Q}[X_1 \ldots, X_n]$ définissant une hypersurface singulière $\mathcal{H} \subset \mathbb{C}^n$.
- **Sortie :** Une famille de paramétrisations rationnelles dont les solutions sont incluses dans $\mathcal{H}$ et ayant une intersection non vide avec chaque composante connexe de $\mathcal{H} \cap \mathbb{R}^n$.

1. Choisir un point A aléatoirement.
2. Vérifier que $\mathfrak{C}(\varphi_A, \mathcal{H}_0)$ est de dimension au plus 0.
3. Calculer une représentation de l'ensemble des solutions de $\langle L\frac{\partial f}{\partial X_1} - \frac{\partial \varphi_A}{\partial X_1}, \ldots, L\frac{\partial f}{\partial X_n} - \frac{\partial \varphi_A}{\partial X_n}\rangle \cap \mathbb{Q}[X_1, \ldots, X_n]$.
4. Intersecter avec $< f\rangle$ et retourner une paramétrisation rationnelle de l'ensemble des solutions calculées.

Pour les mêmes raisons pratiques que celles évoquées précédemment, on cherche maintenant à décliner cette démarche en utilisant des fonctions de projection de manière analogue à celle développée dans le paragraphe 5.5.

Utilisation de fonctions de projection. Comme précédemment, étant donnée une matrice $\mathbf{A}$ dans $GL_n(\mathbb{Q})$, on note $f^{\mathbf{A}}$ le polynôme $f(\mathbf{A}.X)$ et $\mathcal{H}_t^{\mathbf{A}} \subset \mathbb{C}^n$ l'hypersurface définie par $f^{\mathbf{A}} - t = 0$ (pour $t \in \mathbb{Q}$). On considère les projections canoniques :

$$\begin{array}{rccc} \Pi_i : & \mathbb{C}^n & \to & \mathbb{C}^i \\ & (x_1, \ldots, x_n) & \to & (x_1, \ldots, x_i) \end{array}$$

Étant donné un point arbitrairement choisi $(p_1, \ldots, p_{n-1})$ dans $\mathbb{Q}^{n-1}$ et une matrice $\mathbf{A} \in GL_n(\mathbb{Q})$, soit $I_i^{\mathbf{A}}$ (pour $i = 1, \ldots, n-2$) l'idéal :

$$\left(\langle L.\frac{\partial f^{\mathbf{A}}}{\partial X_{i+1}} - 1, \frac{\partial f^{\mathbf{A}}}{\partial X_{i+2}}, \ldots, \frac{\partial f^{\mathbf{A}}}{\partial X_n}, X_1 - p_1, \ldots, X_i - p_i\rangle \cap \mathbb{Q}[X_1, \ldots, X_n]\right)$$

soit $I_{n-1}^{\mathbf{A}}$ l'idéal $\langle X_1 - p_1, \ldots, X_n - p_n\rangle$ et soit $I_0^{\mathbf{A}}$ l'idéal :

$$\left(\langle L.\frac{\partial f^{\mathbf{A}}}{\partial X_1} - 1, \frac{\partial f^{\mathbf{A}}}{\partial X_2}, \ldots, \frac{\partial f^{\mathbf{A}}}{\partial X_n}\rangle \cap \mathbb{Q}[X_1, \ldots, X_n]\right)$$

Le théorème ci-dessous montre comment obtenir au moins un point par composante connexe dans $\mathcal{H}_0 \cap \mathbb{R}^n$ en ayant une démarche géométrique analogue à celle développée dans le paragraphe 5.5 de ce chapitre (c'est-à-dire fondée sur des calculs de points critiques de fonctions de projection choisies génériquement).

Théorème 32. *Soit $(p_1, \ldots, p_{n-1})$ un point arbitrairement choisi dans $\mathbb{Q}^{n-1}$. Il existe un sous-ensemble Zariski-fermé $\mathcal{A} \subsetneq GL_n(\mathbb{C})$ tel que pour $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$, l'union des variétés algébriques associées aux idéaux $\langle f^{\mathbf{A}}\rangle + I_i^{\mathbf{A}}$ (pour $i = 0, \ldots, n-1$) est au plus de dimension zéro et a une intersection non vide avec chaque composante connexe de l'ensemble algébrique réel $\mathcal{H}_0^{\mathbf{A}} \cap \mathbb{R}^n$.*

La preuve de ce résultat se fonde sur les lemmes suivants.

Lemme 12. *Soit C une composante connexe de $\mathcal{H}_0 \cap \mathbb{R}^n$ et supposons que $\Pi_1(C)$ est fermé (pour la topologie euclidienne). Supposons de plus qu'il existe $t_0 \in]0, +\infty[$ tel que pour tout $t \in]0, t_0[$ et toute composante connexe C_t de $(\mathcal{H}_t \cup \mathcal{H}_{-t}) \cap \mathbb{R}^n$, $\Pi_1(C_t)$ soit fermé. Alors :*
- *soit pour un choix arbitraire de $p_1 \in \mathbb{Q}$, C a une intersection non vide avec l'hyperplan défini par $X_1 - p_1 = 0$*
- *soit C contient une limite de $\mathfrak{C}(\Pi_1, \mathcal{H}_t)$ quand t tend vers 0.*

Le lemme suivant généralise le précédent. Étant donné un point $(p_1, \ldots, p_{n-1}) \in \mathbb{Q}^{n-1}$, pour $i \in \{1, \ldots, n-1\}$ on note $H_i \subset \mathbb{C}^n$ l'intersection de l'hyperplan défini par $X_1 - p_1 = \cdots = X_i - p_i = 0$.

Lemme 13. *Soit C une composante connexe de $\mathcal{H}_0 \cap \mathbb{R}^n$. Supposons que pour tout $i \in \{1, \ldots, n-1\}$ la projection $\Pi_i(C)$ soit fermée et que pour toute composante connexe C' de $(\mathcal{H}_0 \cap H_i) \cap \mathbb{R}^n$, $\Pi_{i+1}(C')$ soit aussi fermée. Supposons aussi qu'il existe $t_0 \in]0, +\infty[$ tel que pour tout $t \in]0, t_0[$, et toute composante connexe C_t de $(\mathcal{H}_t \cup \mathcal{H}_{-t}) \cap \mathbb{R}^n$ et tout $i \in \{1, \ldots, n-1\}$ la projection $\Pi_i(C_t)$ soit fermée et que pour toute composante connexe C'_t de $(\mathcal{H}_t \cup \mathcal{H}_{-t}) \cap H_i) \cap \mathbb{R}^n$, $\Pi_{i+1}(C'_t)$ soit fermé.*

Alors :
- *soit C contient une limite de $\mathfrak{C}(\Pi_1, \mathcal{H}_t)$ quand t tend vers 0 ;*
- *soit il existe $i \in \{1, \ldots, n-2\}$ tel que $C \cap H_i$ contient une limite de $\mathfrak{C}(\Pi_{i+1}, \mathcal{H}_t \cap H_i)$ ou de $\mathcal{H}_t \cap H_{n-1}$ quand t tend vers 0.*

Comme dans le paragraphe précédent, on identifie maintenant un changement linéaire de variables à la matrice associée $\mathbf{A} \in GL_n(\mathbb{Q})$ et, étant donné une variété algébrique $V \subset \mathbb{C}^n$ on note $V^{\mathbf{A}}$ la variété algébrique obtenue après action de $\mathbf{A}$. Dans la suite, on note $\mathrm{Sing}(V)$ le lieu singulier de V.

Lemme 14. *Soit $V \subset \mathbb{C}^n$ une variété algébrique. Il existe un sous-ensemble Zariski-fermé $\mathcal{A} \subsetneq GL_n(\mathbb{C})$ tel que pour tout $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$, étant donnée une composante connexe $C^{\mathbf{A}}$ de $V^{\mathbf{A}}$ pour tout $i \in \{1, \ldots, n-1\}$, $\Pi_i(C^{\mathbf{A}})$ est fermé.*

Lemme 15. *Il existe un sous-ensemble Zariski-fermé $\mathcal{A} \subsetneq GL_n(\mathbb{C})$ et $t_0 \in \mathbb{R}$ tel que pour tout $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$ et tout $t \in]0, t_0[\cap \mathbb{Q}$, chaque composante connexe de $\mathcal{H}_t \cap \mathbb{R}^n$ a une image fermée (pour la topologie euclidienne) par la projection Π_1.*

Remarque. *D'après le paragraphe 5.6.1 et le théorème 32, on en déduit un algorithme (utilisant soit des bases de Gröbner soit des calculs de résolutions géométriques) pour le calcul d'au moins un point par composante connexe dans l'ensemble algébrique réel $\mathcal{H}_0 \cap \mathbb{R}^n$.*

Étant donné $(p_1, \ldots, p_{n-1}) \in \mathbb{Q}^{n-1}$, on note f_i (pour $i = 1, \ldots, n-1$) le polynôme f où les indéterminées $X_1, \ldots, X_i$ sont substituées par $p_1, \ldots, p_i$. On remarque alors que l'utilisation de la résolution géométrique peut être simplifié puisqu'il devaient suffisant de donner en entrée à l'algorithme donné dans [61] le système d'équations et d'inéquations polynomiales :

$$f_i^{\mathbf{A}} = \frac{\partial f_i^{\mathbf{A}}}{\partial X_{i+2}} = \cdots = \frac{\partial f_i^{\mathbf{A}}}{\partial X_n} = 0, \quad \frac{\partial f_i^{\mathbf{A}}}{\partial X_{i+1}} \neq 0$$

(pour $i = 1, \ldots, n-2$*) et* $f^{\mathbf{A}} = \frac{\partial f^{\mathbf{A}}}{\partial X_2} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_n} = 0, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_1} \neq 0$ *et d'isoler les racines réelles du polynôme univarié* $f^{\mathbf{A}}_{n-1}$.

Enfin, notons qu'une stratégie alternative peut être d'introduire un infinitesimal ε*, de calculer une paramétrisation rationnelle pour des solutions des systèmes :*

$$f_i^{\mathbf{A}} - \varepsilon = \frac{\partial f_i^{\mathbf{A}}}{\partial X_{i+2}} = \cdots = \frac{\partial f_i^{\mathbf{A}}}{\partial X_n} = 0, \quad \frac{\partial f_i^{\mathbf{A}}}{\partial X_{i+1}} \neq 0$$

(pour $i = 1, \ldots, n-2$*) et*

$$f^{\mathbf{A}} - \varepsilon = \frac{\partial f^{\mathbf{A}}}{\partial X_2} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_n} = 0, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_1} \neq 0$$

de calculer les limites des ensembles de solutions ainsi définies quand ε *tend vers* 0*, et d'isoler les solutions réelles du polynôme* $f^{\mathbf{A}}_{n-1} = 0$*. Dans la section suivante on montre que c'est la première stratégie qui est la plus efficace en pratique comme en théorie.*

Algorithme : Cas hypersurface singulière (Utilisation de fonctions de projections)

- **Entrée :** Un polynôme $f \in \mathbb{Q}[X_1 \ldots, X_n]$ définissant une hypersurface singulière $\mathcal{H} \subset \mathbb{C}^n$.
- **Sortie :** Une famille de paramétrisations rationnelles dont les solutions sont incluses dans $\mathcal{H}$ et ayant une intersection non vide avec chaque composante connexe de $\mathcal{H} \cap \mathbb{R}^n$.

1. Choisir aléatoirement $\mathbf{A} \in GL_n(\mathbb{Q})$ et soit `sols` une liste vide.
2. Calculer une représentation de l'ensemble des solutions de $\langle L\frac{\partial f^{\mathbf{A}}}{\partial X_i} - 1, \frac{\partial f^{\mathbf{A}}}{\partial X_{i+1}}, \ldots, \frac{\partial f^{\mathbf{A}}}{\partial X_n}\rangle \cap \mathbb{Q}[X_1, \ldots, X_n]$
3. Calculer une paramétrisation rationnelle de l'intersection de $\mathcal{H}$ et de la courbe dont la représentation a été calculée précédemment.
4. Ajouter cette paramétrisation à `sols`.
5. Pour i allant de 2 à n faire
   - Calculer une représentation de l'ensemble des solutions de $\langle X_1, \ldots, X_{i-1}, L\frac{\partial f^{\mathbf{A}}}{\partial X_i} - 1, \frac{\partial f^{\mathbf{A}}}{\partial X_{i+1}}, \ldots, \frac{\partial f^{\mathbf{A}}}{\partial X_n}\rangle \cap \mathbb{Q}[X_1, \ldots, X_n]$
   - Calculer une paramétrisation rationnelle de l'intersection de $\mathcal{H}$ et de la courbe dont la représentation a été calculée précédemment.
   - Ajouter cette paramétrisation à `sols`.
6. Ajouter à `sols` une paramétrisation rationnelle de l'ensemble des solutions de $\langle f, X_1, \ldots, X_n\rangle$.
7. Retourner `sols`.

Implantation et performances pratiques. L'usage des bases de Gröbner, en usant des mêmes précautions que celles décrites dans le paragraphe 5.5 pour :

- éviter les changements de variable explicites ;
- et vérifier que les projections choisies sont suffisamment génériques (toujours via des calculs de clôture projective pour garantir les hypothèses de propreté, en particulier on a montré qu'il est suffisant que celles-ci soient vérifiées pour une hypersurface définie par $f^{\mathbf{A}} - e = 0$ où e est un rationnel qui n'est pas une valeur critique de l'application $x \in \mathbb{C}^n \to f(x) \in \mathbb{C}$)

permet d'obtenir une implantation déterministe et particulièrement efficace en pratique de cet algorithme. Celle-ci a permis de résoudre des problèmes que les techniques de gestion récursive des chutes de rang dans les jacobienne sont incapables de traîter (voir paragraphes 5.3 et 5.4).

En particulier, les nouvelles fonctionnalités implantées par J.-C. Faugère dans le logiciel `FGb` [49] pour le calcul d'idéaux d'élimination ainsi que le calcul du radical d'un idéal zéro-dimensionnel permet des gains d'efficacité substantiels.

Du point de vue de la complexité, on peut montrer à l'aide des résultats de [83, 84], que si on suppose que les premiers choix de projection génériques sont les bons, on a un algorithme dont la complexité est polynomiale en D^n où D borne le degré du polynôme définissant l'hypersurface qu'on étudie et n est le nombre de variables.

On peut néanmoins affiner ce résultat de complexité en étudiant l'usage des résolutions géométriques dans ce contexte, ce qui est l'objet de la suite de ce paragraphe.

5.6.3 Estimations de complexité

On ne donne ici que les estimations de complexité concernant l'algorithme de calcul d'au moins un point par composante connexe d'un ensemble algébrique réel défini par une seule équation fondé sur le théorème 32 : ce choix s'explique par le fait que les bornes obtenues sont meilleures que celles obtenues à partir du théorème 31.

Les descriptions données ci-dessus des algorithmes fondés sur les théorèmes 31 et 32 ne dépendent d'aucune procédure d'élimination algébrique. D'après le paragraphe 5.6.1, on peut utiliser soit des calculs de base de Gröbner soit des calculs de résolution géométrique pour obtenir des implantations mettant en œuvre *en pratique* les descriptions données ci-dessus.

Ainsi la complexité des algorithmes de ce paragraphe dépend de la complexité des procédures d'élimination algébrique utilisées. D'après le théorème 32, calculer au moins un point par composante connexe dans $\mathcal{H}_0 \cap \mathbb{R}^n$ se réduit à choisir aléatoirement un changement de variables $\mathbf{A} \in GL_n(\mathbb{Q})$, d'ísoler les solutions réelles de $\mathcal{H}_0^{\mathbf{A}} \cap V(X_1, \ldots, X_n)$ et calculer les limites des points critiques

$$\mathfrak{C}(\Pi_1, \mathcal{H}_t^{\mathbf{A}}), \mathfrak{C}(\Pi_2, \mathcal{H}_t^{\mathbf{A}}) \cap V(X_1), \ldots, \mathfrak{C}(\Pi_{n-1}, \mathcal{H}_t^{\mathbf{A}}) \cap V(X_1, \ldots, X_{n-2})$$

quand t tend vers 0. On décrit ci-dessous une procédure fondée sur le calcul de résolution géométrique pour calculer les limites de points critiques de la restriction à $\mathcal{H}_t$ d'une projection sur une droite, lorsque t tend vers 0.

Algorithme Cas hypersurface singulière (Utilisation de résolutions géométrique – Présentation détaillée)

- **Entrée :** Un polynôme $f \in \mathbb{Q}[X_1 \ldots, X_n]$ définissant une hypersurface singulière $\mathcal{H} \subset \mathbb{C}^n$.
- **Sortie :** Une famille de paramétrisations rationnelles dont les solutions sont incluses dans $\mathcal{H}$ et ayant une intersection non vide avec chaque composante connexe de $\mathcal{H} \cap \mathbb{R}^n$.

1. Calculer une résolution géometrique G encodant un point générique dans la clôture de Zariski de la courbe définie par :
$$\frac{\partial f^{\mathbf{A}}}{\partial X_2} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_n} = 0, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_1} \neq 0$$
2. Obtenir l'image de G modulo un nombre premier choisi aléatoirement, calculer l'intersection avec $f^{\mathbf{A}} = 0$, enlever les points obtenus en lesquels $\frac{\partial f^{\mathbf{A}}}{\partial X_1}$ s'annule, et remonter les entiers en utilisant le système de remontée :
$$f^{\mathbf{A}} = \frac{\partial f^{\mathbf{A}}}{\partial X_2} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_n} = 0, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_1} \neq 0$$
On obtient ainsi les limites régulières de $\mathfrak{C}(\Pi_1, \mathcal{H}_t^{\mathbf{A}})$ quand t tend vers 0.
3. Alors calculer l'intersection de la courbe encodée par G avec les hypersurfaces définies par $\frac{\partial f^{\mathbf{A}}}{\partial X_1} = 0$ et $f^{\mathbf{A}} = 0$ modulo des nombres premiers et retrouver le résultat final en faisant des remontées chinoises et de la reconstruction rationnelle.

On estime maintenant la complexité de chaque étape de l'algorithme décrit ci-dessus. Soit $\mathcal{L}$ la longueur du programme d'évaluation encodant le système :
$$f^{\mathbf{A}} = \frac{\partial f^{\mathbf{A}}}{\partial X_2} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_n} = 0, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_1} \neq 0$$
et n le nombre de variables. La première étape est effectuée en $\mathcal{O}(n^2(\mathcal{L}+n^2)(\mathcal{U}(D\delta)^2 + h\mathcal{U}(\delta))$ opérations binaires, où h est la taille binaire maximale des coefficients de G et δ est le degré maximal de la clôture des ensembles algébriques :
$$f^{\mathbf{A}} = \frac{\partial f^{\mathbf{A}}}{\partial X_2} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_i} = 0, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_1} \neq 0$$
pour $i = 2, \ldots, n$. Remarquons que δ est bornée par $(D-1)^{n-1}$.

La seconde étape a un coût qui est en $\mathcal{O}(n(\mathcal{L}+n^2)\mathcal{U}(D\delta)(h_{\text{reg}}+\mathcal{U}(D\delta))$ opérations binaires où h_{reg} est le maximum des tailles binaires des coefficients de la résolution géométrique encodant les limites régulières des points critiques (voir la section sur la remontée des entiers et l'intersection avec une hypersurface des courbes de remontée dans [61]). Enfin, chaque calcul de la troisième étape a une complexité en $\mathcal{O}(n(\mathcal{L}+n^2)h_{\text{sing}}\mathcal{U}(D\delta))$ (voir la section sur l'intersection d'une courbe de remontée avec une hypersurface dans [61]). Le nombre de tels calculs est h_{sing}, où h_{sing} est la taille binaire maximale des coefficients apparaissant dans la résolution géométrique encodant les limites singulières des points critiques. Ainsi, on déduit de cette discussion le résultat de complexité ci-dessous.

Théorème 33. *Soit f un polynôme dans $\mathbb{Q}[X_1, \ldots, X_n]$ de degré borné par D, dont la complexité d'évaluation est bornée par $\mathcal{L}$ et $\mathcal{H} \subset \mathbb{C}^n$ l'hypersurface définie par $f = 0$. L'algorithme ci-dessus calcule au moins un point par composante connexe de $\mathcal{H} \cap \mathbb{R}^n$ en une complexité binaire*
$$\mathcal{O}\left(n^2(n\mathcal{L}+n^2)\left((1+h_{\text{sing}})\mathcal{U}(D.\delta)^2 + h_{\text{reg}}\mathcal{U}(\delta)\right)\right.$$

où δ est le degré maximal des variétés algébriques étudiées durant le processus de résolution incrémental et est borné par $D.(D-1)^{n-1}$.

Remarque. *Soit $\mathfrak{d}$ la somme des degrés des composantes équi-dimensionnelles du lieu singulier de $\mathcal{H}_0$ ayant une dimension strictement positive. On peut raffiner l'estimation de degré $D(D-1)^{n-1}$ données ci-dessus pour borner δ en remarquant que le degré de la courbe définie comme étant la clôture de Zariski de l'ensemble des solutions du système :*

$$\frac{\partial f^{\mathbf{A}}}{\partial X_2} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_n} = 0, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_1} \neq 0$$

est borné par $(D-1)^{n-1} - \mathfrak{d}$. Ainsi, alors que dans le cas lisse la borne $D(D-1)^{n-1}$ peut être atteinte, ceci n'est pas possible dans les cas où $\mathcal{H}_0$ a un lieu singulier de dimension positive.

En prenant en compte la discussion ci-dessus et en effectuant une analyse précise des degrés apparaissant dans les algorithmes relevant du théorème 32, on obtient le résultat suivant.

Théorème 34. *Soit $H_1, \ldots, H_{n-2}$ des hyperplans génériques de $\mathbb{Q}^n$. Le nombre de composantes connexes de $\mathcal{H}_0 \cap \mathbb{R}^n$ est borné par*

$$D(1 + (D-1) + \cdots + (D-1)^{n-1} - (\mathfrak{d}_0 + \cdots + \mathfrak{d}_{n-2})),$$

où $\mathfrak{d}_i$ (resp. $\mathfrak{d}_0$) est la somme des degrés des composantes equi-dimensionnelles de dimension positive du lieu singulier de $\mathcal{H}_0 \cap (\cap_{j=1}^{i} H_i)$ (resp. $\mathcal{H}_0$).

Il nous reste maintenant à étudier comment généraliser les résultats de ce paragraphe au cas des systèmes polynomiaux. C'est l'objectif du paragraphe suivant.

5.7 Le cas des systèmes polynomiaux définissant une variété algébrique singulière

On considère donc un système d'équations polynomiales

$$f_1 = \cdots = f_s = 0$$

où $f_i \in \mathbb{Q}[X_1, \ldots, X_n]$ pour $i \in \{1, \ldots, s\}$ définissant une variété algébrique $V \subset \mathbb{C}^n$. Ici, on ne suppose pas que l'idéal $\langle f_1, \ldots, f_s \rangle$ soit radical ni que la variété V soit lisse. On ne peut donc pas utiliser les caractérisations algébriques des lemmes 4 et 5 pour caractériser les points critiques d'applications polynomiales restreintes à V. On va néanmoins montrer comment ramener le calcul d'au moins un point par composante connexe de la variété algébrique réelle $V \cap \mathbb{R}^n$ au calcul de limites de points critiques d'applications polynomiales restreintes à des variétés algébriques obtenues par déformation infinitésimale du système

$$f_1 = \cdots = f_s = 0.$$

5.7.1 Résultats préliminaires

Soit donc $\varphi : y \in \mathbb{C}^n \to \varphi(y) \in \mathbb{C}$ une application polynomiale avec $\varphi \in \mathbb{Q}[X_1, \ldots, X_n]$. On note $\mathfrak{C}(\varphi, V)$ l'ensemble des points critiques de φ restreinte au lieu régulier de chaque composante équidimensionnelle de V. On suppose que

- $\mathfrak{C}(\varphi, V)$ est de dimension au plus zéro ;
- pour toute composante connexe C de $V \cap \mathbb{R}^n$, $\varphi(C)$ est un intervalle de $\mathbb{R}$ fermé (pour la topologie euclidienne).

Cette dernière hypothèse implique que :

- soit $\varphi(C) = \mathbb{R}$ auquel cas pour tout $x \in \mathbb{R}$, C a une intersection non vide avec $\varphi^{-1}(x)$ pour tout $x \in \mathbb{R}$;
- soit $\varphi(C) \neq \mathbb{R}$ auquel cas pour x dans la frontière de $\varphi(C)$, C a une intersection non vide avec $\varphi^{-1}(x)$.

C'est évidemment le dernier cas qui rend les choses compliquées. On va chercher à déformer le système $f_1 = \cdots = f_s = 0$ pour définir une suite de points critiques dépendant d'un infinitésimal dont les limites contiennent les points dont les images par φ contiennent l'ensemble des frontières des $\varphi(C)$ pour les composantes connexes C de $V \cap \mathbb{R}^n$.

Soit donc C une composante connexe de $V \cap \mathbb{R}^n$ telle que $\varphi(C) \neq \mathbb{R}$ et $y \in C$ tel que $\varphi(y)$ est dans la frontière de $\varphi(C)$. Sans nuire à la généralité, on suppose que dans toute boule $B(y,r) \subset \mathbb{R}^n$ centrée en y de rayon $r > 0$, il existe $y' \in B(y,r)$ tel que :

$$f_1(y') > 0, \ldots, f_s(y') > 0$$

On en déduit aisément le résultat suivant :

Lemme 16. *Sous les hypothèses et notations ci-dessus, il existe une composante connexe C' de l'ensemble semi-algébrique défini par :*

$$f_1 > 0, \ldots, f_s > 0$$

tel que y appartienne à l'adhérence de C'.

Ce lemme ne permet malheureusement pas encore de caractériser y de manière suffisamment précise pour qu'il puisse être calculé en tant que solution d'un système d'équations polynomiales de dimension zéro. Ceci dit, y appartenant à la clôture d'une composante connexe de l'ensemble semi-algébrique défini par

$$f_1 > 0, \ldots, f_s > 0$$

on est logiquement tenté de vouloir le calculer en tant que limite d'une suite de points vivant dans ce semi-algébrique, cette suite de points devant être une suite de points critiques. Pour ce faire, on va exhiber des variétés algébriques réelles dont certaines composantes connexes sont incluses dans les composantes connexes du semi-algébrique $\mathcal{S}$.

Soit C' une composante connexe de $\mathcal{S}$. Plus précisément, pour tout couple de points (y_1, y_2) dans C' et un chemin quelconque γ dans C' reliant y_1 et y_2, les polynômes $f_1, \ldots, f_s$ ont des minima positifs sur γ. Ainsi, l'extension de γ à $\mathbb{R}\langle\varepsilon\rangle^n$ est entièrement contenue dans une composante connexe du semi-algébrique $S \subset \mathbb{R}\langle\varepsilon\rangle^n$ défini par

$$f_1 - a_1\varepsilon \geqslant 0, \cdots, f_s - a_s\varepsilon \geqslant 0$$

et, il existe une composante connexe C'' de S contenant C'.

L'application de [21, proposition 13.1, chapitre 13] donne l'existence d'un sous-ensemble $\{i_1, \ldots, i_k\} \subset \{1, \ldots, s\}$ et d'une composante connexe de l'ensemble algébrique réel défini par

$$f_{i_1} - a_{i_1}\varepsilon = \cdots = f_s - a_{i_k}\varepsilon = 0.$$

incluse dans C'. Ceci est résumé par le résultat suivant.

Théorème 35. *Soit $C' \subset \mathbb{R}^n$ une composante connexe de l'ensemble semi-algébrique défini par :*

$$f_1 > 0, \ldots, f_s > 0,$$

ε un infinitésimal et $a = (a_1, \ldots, a_s) \in \mathbb{Q}^s \setminus \{0\}$. Pour $\mathcal{I} = \{i_1, \ldots, i_k\} \subset \{1, \ldots, s\}$, on note $V^{\mathcal{I}}_{\varepsilon,a} \subset \mathbb{C}\langle\varepsilon\rangle^n$ la variété algébrique définie par

$$f_{i_1} - a_{i_1}\varepsilon = \cdots = f_{i_k} - a_{i_k}\varepsilon = 0.$$

Alors, il existe $\mathcal{I} = \{i_1, \ldots, i_k\} \subset \{1, \ldots, s\}$ et une composante connexe $C^{\mathcal{I}}_{\varepsilon,a}$ de $V^{\mathcal{I}}_{\varepsilon,a} \cap \mathbb{R}\langle\varepsilon\rangle$ tels que $C^{\mathcal{I}}_{\varepsilon,a}$ est incluse dans l'extension de C' dans $\mathbb{R}\langle\varepsilon\rangle^n$.

De plus, il existe un fermé de Zariski $\mathcal{A} \subset \mathbb{C}^n$ tel que pour tout $a \in \mathbb{Q}^n \setminus \mathcal{A}$, $V^{\mathcal{I}}_{\varepsilon,a}$ est lisse, et l'idéal engendré par $f_{i_1} - a_{i_1}\varepsilon, \ldots, f_{i_k} - a_{i_k}\varepsilon = 0$ est soit radical équi-dimensionnel de dimension $n - k$ soit égale à $\langle 1 \rangle$.

La dernière assertion est une conséquence directe du théorème de Sard lorsqu'on considère l'application polynomiale :

$$\begin{array}{ccc} \mathbb{C}^n & \longrightarrow & \mathbb{C}^k \\ y & \to & (f_{i_1}(y), \ldots, f_{i_k}(y)) \end{array}$$

Cette dernière assertion est importante car elle implique que pour un choix générique de $a = (a_1, \ldots, a_s)$ on peut utiliser les caractérisations algébriques de points critiques donnés dans les lemmes 4 et 5.

Ceci est heureux car c'est l'étude des points critiques de φ restreinte aux variétés algébriques $V^{\mathcal{I}}_{\varepsilon,a}$ qui permet de définir des suites points critiques convergents vers y.

Plus précisément, si on considère un sous-ensemble maximal (pour l'inclusion) $\mathcal{I} = \{i_1, \ldots, i_k\} \subset \{1, \ldots, s\}$ tel qu'il existe $y_\varepsilon \in V^{\mathcal{I}}_{\varepsilon,a} \cap \mathbb{R}\langle\varepsilon\rangle^n$ dans l'extension de $B(y, r)$ à $\mathbb{R}\langle\varepsilon\rangle^n$ pour tout $r > 0$, alors il existe des points $\mathfrak{C}(\varphi, V^{\mathcal{I}}_{\varepsilon,a})$ convergents vers y lorsque ε tend vers 0.

Théorème 36. *Soit $\varphi : y \in \mathbb{C}^n \to \varphi(y) \in \mathbb{C}$ une application polynomiale avec $\varphi \in \mathbb{Q}[X_1, \ldots, X_n]$ et $V \subset \mathbb{C}^n$ une variété algébrique définie par :*

$$f_1 = \cdots = f_s = 0$$

où $f_i \in \mathbb{Q}[X_1, \ldots, X_n]$ pour $i \in \{1, \ldots, s\}$. On fait les hypothèses suivantes :
- *le lieu critique $\mathfrak{C}(\varphi, V)$ de la restriction de φ à V est de dimension au plus zéro ;*
- *toute composante connexe C de $V \cap \mathbb{R}^n$ a une image fermée par φ (pour la topologie euclidienne) ;*
- *soit C une composante connexe de $V \cap \mathbb{R}^n$ telle que $\varphi(C) \neq \mathbb{R}$ et $y \in C$ un point tel que $\varphi(y)$ appartient à la frontière de $\varphi(C)$;*
- *pour tout $r > 0$, il existe y' dans la boule $B(y, r)$ de centre y de rayon r tel que :*

$$f_1(y') > 0, \ldots, f_s(y') > 0$$

Alors, il existe $\{i_1, \ldots, i_k\} \subset \{1, \ldots, s\}$ et $\mathcal{A} \subsetneq \mathbb{C}^s$ tel que, si $a = (a_1, \ldots, a_s) \in \mathbb{Q}^s \setminus \mathcal{A}$ et si on note $V^{\mathcal{I}}_{\varepsilon,a} \subset \mathbb{C}\langle\varepsilon\rangle^n$ la variété algébrique définie par :

$$f_{i_1} - a_{i_1}\varepsilon = \cdots = f_{i_k} - a_{i_k}\varepsilon$$

- *l'idéal engendré par $f_{i_1} - a_{i_1}\varepsilon, \ldots, f_{i_k} - a_{i_k}\varepsilon$ est soit radical équi-dimensionnel de dimension $n - k$ soit égale à $\langle 1\rangle$;*
- *$V^{\mathcal{I}}_{\varepsilon,a}$ est lisse ;*
- *il existe $y_\varepsilon \in \mathfrak{C}(\varphi, V^{\mathcal{I}}_{\varepsilon,a})$ qui tend vers y quand ε tend vers 0.*

Le résultat ci-dessus permet donc de caractériser y comme une limite de points critiques de φ restreinte à une variété algébrique $V^{\mathcal{I}}_{\varepsilon,a}$ (les propriétés de régularité sur le système définissant $V^{\mathcal{I}}_{\varepsilon,a}$ permettant d'utiliser les lemmes 4 et 5) mais son application directe nécessite d'introduire *explicitement* un infinitésimal et donc d'effectuer les calculs soit dans $\mathbb{Q}(\varepsilon)$ soit dans $\mathbb{Q}\langle\varepsilon\rangle$ ce qui en pratique ne donne pas des résultats satisfaisants. On montre dans la suite de ce paragraphe comment obtenir les limites des points critiques qu'on cherche à calculer en s'inspirant des techniques mises en œuvre dans le paragraphe 5.6.

5.7.2 Calcul des limites de points critiques.

Pour simplifier les notations, on suppose qu'on cherche à calculer les limites (lorsque ε tend vers 0) des points critiques de φ restreinte à la variété algébrique $V_{\varepsilon,a} \subset \mathbb{C}\langle\varepsilon\rangle^n$ définie par :

$$f_1 - a_1\varepsilon = \cdots = f_s - a_s\varepsilon = 0$$

où $s \leqslant n$ et $a = (a_1, \ldots, a_s) \in \mathbb{Q}^n$ est choisi de manière telle que :
- l'idéal $\langle f_1 - a_1\varepsilon, \ldots, f_s - a_s\varepsilon\rangle$ est radical et équi-dimensionnel ;
- si l'idéal $\langle f_1 - a_1\varepsilon, \ldots, f_s - a_s\varepsilon\rangle$ est différent de $\langle 1\rangle$ alors il est de dimension $n - s$;
- $V_{\varepsilon,a}$ est lisse.

On suppose maintenant que l'idéal $\langle f_1 - a_1\varepsilon, \ldots, f_s - a_s\varepsilon\rangle$ est différent de $\langle 1\rangle$.

D'après les hypothèses ci-dessus, on peut utiliser les caractérisations algébriques des lemmes 4 et 5 pour calculer une représentation de $\mathfrak{C}(\varphi, V_{\varepsilon,a})$. Soit $\mathcal{M}(\varphi)$ l'ensemble des mineurs $(n - s + 1, n - s + 1)$ de la matrice jacobienne associée à la famille de polynômes

$$f_1, \ldots, f_s, \varphi.$$

Remarquons que les polynômes de $\mathcal{M}(\varphi)$ ne dépendent pas de ε.

Enfin, on note $V_a \subset \mathbb{C}^{n+1}$ la clôture de Zariski de l'ensemble des points annulant les polynômes :

$$f_1 - a_1 T, \ldots, f_s - a_s T$$

(où T est une nouvelle variable) pour lesquels la matrice jacobienne associée à $f_1, \ldots, f_s$ est de rang $n-s$. Si on note Π l'application polynomiale qui envoie $x = (x_1, \ldots, x_n, t) \in \mathbb{C}^{n+1}$ sur $(\varphi(x_1, \ldots, x_n), t)$, remarquons que calculer les limites de $\mathfrak{C}(\varphi, V_{\varepsilon,a})$ lorsque ε tend vers 0 revient à calculer la projection sur $X_1, \ldots, X_n$ de $\mathfrak{C}(\Pi, V_a) \cap \{y \in \mathbb{C}^{n+1} \mid T = 0\}$.

Ceci est équivalent à considérer la variété $\mathfrak{V}_a \subset \mathbb{C}^n$ définie comme étant la clôture de Zariski de l'ensemble des points vérifiant :

$$\frac{f_1}{a_2} - \frac{f_2}{a_1} = \cdots = \frac{f_1}{a_s} - \frac{f_s}{a_1} = 0, \quad \text{et} \quad \forall m \in \mathcal{M}(\varphi), \quad m = 0$$

tels que la rang de la jacobienne associée à $f_1, \ldots, f_s$ est $n-s$ et à calculer l'intersection de $\mathfrak{V}_a$ avec l'ensemble des points annulant $f_1, \ldots, f_s$.

Proposition 27. *Soit $V \subset \mathbb{C}^n$ la variété algébrique définie par :*

$$f_1 = \cdots = f_s = 0$$

et $\mathfrak{V}_a \subset \mathbb{C}^n$ la variété algébrique définie comme étant la clôture de Zariski de l'ensemble des points vérifiant

$$\frac{f_1}{a_2} - \frac{f_2}{a_1} = \cdots = \frac{f_1}{a_s} - \frac{f_s}{a_1} = 0, \quad \textit{et} \quad \forall m \in \mathcal{M}(\varphi), \quad m = 0.$$

tels que la rang de la jacobienne associée à $f_1, \ldots, f_s$ est $n-s$.

Alors, si $\mathfrak{C}(\varphi, V)$ est de dimension au plus 0, $\mathfrak{V}_a \cap V$ contient l'ensemble des limites de $\mathfrak{C}(\varphi, \mathcal{V}_{\varepsilon,a})$ lorsque ε tend vers 0.

De plus, si $\mathfrak{V}_a$ est de dimension au plus 1, alors $\mathfrak{V}_a \cap V$ est de dimension au plus 0.

Remarque. *Le résultat ci-dessus est fondé sur la caractérisation des points critiques donnée par le lemme 4. On peut énoncer un résultat similaire fondé sur la caractérisation algébrique donnée par le lemme 5 en considérant les points annulant le système :*

$$\begin{cases} \ell_1 \frac{\partial f_1}{\partial X_1} + \cdots + \ell_s \frac{\partial f_s}{\partial X_1} \\ \qquad\qquad \vdots \\ \ell_1 \frac{\partial f_1}{\partial X_n} + \cdots + \ell_s \frac{\partial f_s}{\partial X_n} \\ \frac{f_1}{a_2} - \frac{f_2}{a_1} = \cdots = \frac{f_1}{a_s} - \frac{f_s}{a_1} = 0 \end{cases}$$

pour lesquels le rang de la jacobienne associée à $f_1, \ldots, f_s$ est $n-s$ et en en considérant la projection sur $X_1, \ldots, X_n$.

Voyons maintenant comment utiliser le résultat ci-dessus pour calculer les limites de $\mathfrak{C}(\varphi, \mathcal{V}_{\varepsilon,a})$ lorsque ε tend vers 0. La difficulté provient du fait que l'on n'a pas directement une famille de générateurs de l'idéal associé à $\mathfrak{V}_a$, c'est-à-dire l'ensemble des polynômes s'annulant sur $\mathfrak{V}_a$.

Calculs des limites en utilisant des bases de Gröbner. Étant donné le système d'équations polynomiales

$$\frac{f_1}{a_2} - \frac{f_2}{a_1} = \cdots = \frac{f_1}{a_s} - \frac{f_s}{a_1} = 0, \quad \text{et} \quad \forall m \in \mathcal{M}(\varphi), \quad m = 0.$$

plusieurs alternatives sont possibles pour accéder à une famille de générateurs de $\mathfrak{V}_a$:

1. soit on calcule une décomposition équi-dimensionnelle de l'idéal engendré par ce système et on n'en garde que les composantes de dimension au plus 1 ;
2. soit on sature cet idéal par une somme aléatoire des mineurs $(n-s-1, n-s-1)$ de la matrice jacobienne associée à $f_1, \ldots, f_s$;

3. soit on sature cet idéal par un des mineurs $(n-s-1, n-s-1)$ de la matrice jacobienne J associée à $f_1, \ldots, f_s$, puis on ajoute ce mineur à notre système d'équations en saturant l'idéal engendré par ce nouveau système par un autre mineur $(n-s-1, n-s-1)$ de J et ainsi de suite jusqu'à obtenir $\langle 1 \rangle$ ou que l'ensemble des solutions du nouvel idéal qu'on vient de calculer est inclus dans les précédents.

En pratique, c'est la solution 3 qui est la plus pertinente en l'état actuel des implantations. La solution 2 est coûteuse et probabiliste. Hors l'intérêt des bases de Gröbner ici est de pouvoir obtenir des algorithmes déterministes. La solution 1 est elle aussi coûteuse en l'état actuel des implantations.

Une fois ce calcul effectué, il suffit d'ajouter les équations $f_1, \ldots, f_s$ aux systèmes de générateurs obtenus et de calculer à nouveau une base de Gröbner. Finalement, ces calculs sont les analogues de ceux présentés dans le paragraphe 5.6.

Remarque. *On pourrait aussi décrire ces calculs sur la base de la caractérisation algébrique fondée sur le lemme 5 qui est évoquée plus haut. Les bases de Gröbner tirant profit de la sur-détermination des systèmes décrits ci-dessus, il est préférable de mener les calculs comme on les a décrit.*

Calculs des limites en utilisant la résolution géométrique. L'algorithme de résolution géométrique permet de tenir compte directement d'inéquations. Ainsi, pour calculer une représentations de $\mathfrak{V}_a$ il est suffisant de considérer le système d'équations et d'inéquations

$$\frac{f_1}{a_2} - \frac{f_2}{a_1} = \cdots = \frac{f_1}{a_s} - \frac{f_s}{a_1} = 0, \quad \text{et} \quad \forall m \in \mathcal{M}(\varphi), \quad m = 0, \quad \sum_{\mathfrak{m} \in \mathfrak{M}} b(\mathfrak{m})\mathfrak{m} \neq 0.$$

où $\mathfrak{M}$ est l'ensemble des mineurs $(n-s-1, n-s-1)$ de la matrice jacobienne associée à $f_1, \ldots, f_s$ et les $b(\mathfrak{m})$ sont des rationnels choisis aléatoirement.

On obtient alors des paramétrisations rationnelles de points génériques dans $\mathfrak{V}_a$. À l'instar des techniques utilisées dans le paragraphe 5.6 et fondées sur [136] on peut calculer une représentation paramétrée de $\mathfrak{V}_a$ lorsqu'elle est de dimension 1. Une fois ce calcul effectué, on intersecte la courbe obtenue avec f_1. Ici encore, les calculs sont analogues à ceux du paragraphe 5.6.

Remarque. *Contrairement aux calculs utilisant les bases de Gröbner, on a intérêt dans le contexte des résolutions géométriques à utiliser la caractérisation lagrangienne des points critiques donnée dans le lemme 5 et évoquée plus haut.*

5.7.3 Application aux fonctions de projection.

Voyons maintenant comment utiliser les résultats exposés ci-dessus pour calculer au moins un point par composante connexe dans l'ensemble algébrique réel $V \cap \mathbb{R}^n$ en n'effectuant que des calculs de limites de points critiques de projections. Le problème réside dans le fait de garantir que les images des composantes connexes de $V \cap \mathbb{R}^n$ par les projections considérées sont bien des fermés (pour la topologie euclidienne). Comme dans les paragraphes 5.5 et 5.6, ceci est assuré génériquement, à changement linéaire de variables près.

Étant donnée une matrice $\mathbf{A} \in GL_n(\mathbb{Q})$, $a = (a_1, \ldots, a_s) \in \mathbb{Q}^n$ et $\mathcal{I} = \{i_1, \ldots, i_k\} \subset \{1, \ldots, s\}$ on note $V_{\varepsilon,a}^{\mathcal{I},\mathbf{A}} \subset \mathbb{C}\langle\varepsilon\rangle^n$ la variété algébrique définie par :

$$f_{i_1}^{\mathbf{A}} - a_{i_1}\varepsilon = \cdots = f_{i_k}^{\mathbf{A}} - a_{i_k}\varepsilon = 0$$

On considére aussi les projections canoniques

$$\begin{array}{rccc} \pi_i : & \mathbb{C}^n & \longrightarrow & \mathbb{C}^i \\ & (x_1, \ldots, x_n) & \to & (x_1, \ldots, x_i) \end{array}$$

Enfin, soit $\mathcal{M}_{\mathcal{I}}^{\mathbf{A}}(\pi_i)$ est l'ensemble des mineurs de la matrice jacobienne associée à la famille de polynômes $(f_1, \ldots, f_s, X_1, \ldots, X_i)$. On note $\mathfrak{V}_{a,i}^{\mathcal{I},\mathbf{A}} \subset \mathbb{C}^n$ la variété algébrique définie comme étant la clôture de Zariski de l'ensemble des points vérifiant :

$$\frac{f_{i_1}^{\mathbf{A}}}{a_{i_2}} - \frac{f_{i_2}^{\mathbf{A}}}{a_{i_1}} = \cdots = \frac{f_{i_1}^{\mathbf{A}}}{a_{i_k}} - \frac{f_{i_k}^{\mathbf{A}}}{a_{i_1}} = 0, \quad \forall m \in \mathcal{M}_{\mathcal{I}}^{\mathbf{A}}(\pi_i), \quad m = 0$$

et pour lesquels la jacobienne associée à $f_{i_1}, \ldots, f_{i_k}$ est de rang $n-k$.

Pour terminer, pour $i = 1, \ldots, n$, on note $H_i \subset \mathbb{C}^n$ le sous-espace affine défini par $X_1 = \cdots = X_i = 0$. Par convention, $H_0 = \mathbb{C}^n$.

Le résultat ci-dessous montre comment obtenir au moins un point par composante connexe de $V \cap \mathbb{R}^n$ en effectuant des calculs de limites de points critiques de fonctions de projection. La technique employée mixe les méthodes mises en œuvre dans les paragraphes 5.5 et 5.6.

Théorème 37. *Il existe un fermé de Zariski $\mathfrak{A} \subsetneq GL_n(\mathbb{C})$ et un fermé de Zariski $\mathcal{A} \subsetneq \mathbb{C}^n$ tels que pour tout $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathfrak{A}$ et tout $a = (a_1, \ldots, a_s) \in \mathbb{Q}^n \setminus \mathcal{A}$, on a pour tout $\mathcal{I} \subset \{1, \ldots, s\}$ et $i = \{1, \ldots, n\}$:*

- *les variétés algébriques $\mathfrak{V}_{a,i}^{\mathcal{I},\mathbf{A}} \cap H_{i-1}$ sont de dimension au plus 1 ;*
- *les variétés algébriques $\mathfrak{V}_{a,i}^{\mathcal{I},\mathbf{A}} \cap H_{i-1} \cap V$ sont de dimension au plus 0 et contiennent les limites de $\mathfrak{C}(\pi_i, \mathcal{V}_{\varepsilon,a}^{\mathcal{I},\mathbf{A}}) \cap H_i$ lorsque ε tend vers 0.*

De plus, l'union des ensembles algébriques

$$\bigcup_{\mathcal{I} \subset \{1,\ldots,s\}} \left(\cup_{i=0}^{n-1} \mathfrak{C}(\pi_i, \mathfrak{V}_{\varepsilon,a}^{\mathcal{I},\mathbf{A}}) \cap H_i\right)$$

est de dimension au plus zéro et a une intersection non vide avec chaque composante connexe de $V \cap \mathbb{R}^n$.

Ce résultat se fonde sur le lemme 14 du paragraphe 5.6 et les lemmes ci-dessous, assurant que pour un choix générique de $\mathbf{A}$, les projections des composantes connexes des ensembles algébriques réels considérés (y compris ceux obtenus par déformation du système initial) sont des fermés pour la topologie euclidienne.

Le résultat suivant se montre de manière similaire à celui du lemme 12.

Lemme 17. *Soit $\mathbf{A} \in GL_n(\mathbb{Q})$, $a \in \mathbb{Q}^s$ et $C^{\mathbf{A}}$ une composante connexe de $V^{\mathbf{A}} \cap \mathbb{R}^n$ et supposons que $\Pi_1(C^{\mathbf{A}})$ est fermé (pour la topologie euclidienne). Supposons de plus que pour tout $\mathcal{I} \subset \{1, \ldots, s\}$, il existe $t_0 \in]0, +\infty[$ tel que pour tout $t \in]0, t_0[$ et toute composante connexe $C_t^{\mathbf{A}}$ de $(\mathcal{V}_{t,a}^{\mathcal{I},\mathbf{A}} \cup \mathcal{V}_{-t,a}^{\mathcal{I},\mathbf{A}}) \cap \mathbb{R}^n$, $\Pi_1(C_t)$ soit fermé. Alors :*

- *soit pour un choix arbitraire de $p_1 \in \mathbb{Q}$, $C^{\mathbf{A}}$ a une intersection non vide avec l'hyperplan défini par $X_1 - p_1 = 0$*
- *soit $C^{\mathbf{A}}$ contient une limite de $\mathfrak{C}(\Pi_1, \mathcal{V}_{t,a}^{\mathcal{I},\mathbf{A}})$ quand t tend vers 0.*

Le lemme suivant généralise le précédent. Les techniques de preuve sont similaires à celles des résultats du paragraphe 5.6. Étant donné un point $(p_1, \ldots, p_{n-1}) \in \mathbb{Q}^{n-1}$, pour $i \in \{1, \ldots, n-1\}$ on note $H_i \subset \mathbb{C}^n$ l'intersection de l'hyperplan défini par $X_1 - p_1 = \cdots = X_i - p_i = 0$.

Lemme 18. *Soit $\mathbf{A} \in GL_n(\mathbb{Q})$, $a \in \mathbb{Q}^s$ et $C^{\mathbf{A}}$ une composante connexe de $V^{\mathbf{A}} \cap \mathbb{R}^n$. Supposons que pour tout $i \in \{1, \ldots, n-1\}$ la projection $\Pi_i(C^{\mathbf{A}})$ soit fermée et que pour toute composante connexe $C'^{,\mathbf{A}}$ de $(V \cap H_i) \cap \mathbb{R}^n$, $\Pi_{i+1}(C'^{,\mathbf{A}})$ soit aussi fermée.*

Supposons aussi qu'il existe $t_0 \in]0, +\infty[$ tel que pour tout $t \in]0, t_0[$, et toute composante connexe $C_t^{\mathbf{A}}$ de $(\mathcal{V}_{t,a}^{\mathcal{I},\mathbf{A}} \cup \mathcal{V}_{t,a}^{\mathcal{I},\mathbf{A}} \cap \mathbb{R}^n$ et tout $i \in \{1, \ldots, n-1\}$ la projection $\Pi_i(C_t^{\mathbf{A}})$ soit fermée et que pour toute composante connexe $C_t'^{,\mathbf{A}}$ de $\left(\mathcal{V}_{t,a}^{\mathcal{I},\mathbf{A}} \cup \mathcal{V}_{t,a}^{\mathcal{I},\mathbf{A}} \cap H_i\right) \cap \mathbb{R}^n$, $\Pi_{i+1}(C_t')$ soit fermé.

Alors, il existe $\mathcal{I}$ tel que :

- *soit C contient une limite de $\mathfrak{C}(\Pi_1, \mathcal{V}_{t,a}^{\mathcal{I},\mathbf{A}})$ quand t tend vers 0 ;*
- *soit il existe $i \in \{1, \ldots, n-2\}$ tel que $C \cap H_i$ contient une limite de $\mathfrak{C}(\Pi_{i+1}, \mathcal{V}_{t,a}^{\mathcal{I},\mathbf{A}} \cap H_i)$ ou de $\mathcal{V}_{t,a}^{\mathcal{I},\mathbf{A}} \cap H_{n-1}$ quand t tend vers 0.*

Lemme 19. *Il existe des sous-ensembles Zariski-fermés $\mathfrak{A} \subsetneq GL_n(\mathbb{C})$ et $\mathcal{A} \subsetneq \mathbb{C}^n$ et $t_0 \in \mathbb{R}$ tels que pour tout $\mathcal{I} \subset \{1, \ldots, s\}$, tout $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathfrak{A}$, tout $a \in \mathbb{Q}^s \setminus \mathcal{A}$ et tout $t \in]0, t_0[\cap \mathbb{Q}$, chaque composante connexe de $\mathcal{V}_{t,a}^{\mathcal{I},\mathbf{A}} \cap \mathbb{R}^n$ a une image fermée (pour la topologie euclidienne) par la projection Π_1.*

On déduit du théorème 37, l'algorithme ci-dessous.

Algorithme : Calcul d'au moins un point par composante connexe d'une variété algébrique réelle quelconque

- **Entrée :** Une famille $(f_1, \ldots, f_s) \subset \mathbb{Q}[X_1, \ldots, X_n]$ de polynômes définissant une variété algébrique $V \subset \mathbb{C}^n$.
- **Sortie :** Une famille de paramétrisations rationnelles encodant un nombre fini de points de V et ayant une intersection non vide avec chaque composante connexe de $V \cap \mathbb{R}^n$.

1. Choisir aléatoirement $\mathbf{A} \in GL_n(\mathbb{Q})$ et $a \in \mathbb{Q}^s$.
2. Poser `sols` := []
3. Pour tout $\mathcal{I} \subset \{1, \ldots, s\}$ de cardinalité inférieure ou égale à n faire
   (a) Pour $i = 0, \ldots, n$, calculer une paramétrisation rationnelle des limites de $\mathfrak{C}(\Pi_1, \mathfrak{V}_{\varepsilon,a}^{\mathcal{I},\mathbf{A}} \cap H_i)$ quand $\varepsilon \to 0$ comme indiqué ci-dessus où H_i est défini par $X_1 = \cdots = X_i = 0$.
   (b) Calculer une paramétrisation rationnelle de ces limites qui annulent $f_1^{\mathbf{A}}, \ldots, f_s^{\mathbf{A}}$.
   (c) Faire l'union de `sols` et de cette paramétrisation rationnelle.
4. Retourner `sols`.

Implantation et résultats pratiques. Des implantations préliminaires de cet algorithme ont été faites en utilisant des calculs de bases de Gröbner. Le procédé de certification du choix des fonctions de projection est similaire à celui utilisé pour certifier les implantations de l'algorithme décrit dans le paragraphe 5.6.

Mentionnons que :

- le facteur combinatoire (induit par le nombre de systèmes à étudier) n'est pas si terrible qu'il n'y paraît : grâce au choix générique des a_i celui-ci est limité à 2^{n-1} (si $s < n$) grâce au théorème 35, de plus des branches de calcul peuvent être détectées comme étant inutiles et donc élagées.
- l'apport pratique de cet algorithme est important devant les techniques fondées sur des études récursives de lieux singuliers lorsque ceux-ci sont difficiles à décomposer et/ou de grande dimension.

Ceci dit, il subsiste des cas où cette approche n'est pas ou peu rentable comparativement à des études récursives sur des lieux singuliers notamment lorsque ceux-ci sont de faible dimension. Il s'agit donc d'une alternative complémentaire aux approches récursives précédemment.

Complexité. L'étude des ensembles semi-algébriques définis par :

$$f_1^{\mathbf{A}} \ \sigma\ _1 0, \ldots, f_s^{\mathbf{A}} \sigma_s 0$$

avec $\sigma_i \in \{>, <\}$ pour $i \in \{1, \ldots, s\}$ se ramène à l'étude des ensembles algébriques définis par

$$f_{i_1}^{\mathbf{A}} \pm a_1 \varepsilon = \cdots = f_{i_k}^{\mathbf{A}} \pm a_{i_k} \varepsilon = 0$$

pour $\{i_1, \ldots, i_k\} \subset \{1, \ldots, s\}$ avec $k \leqslant n$ puisque d'après le théorème 35 la variété algébrique définie par le système ci-dessus est soit vide soit dimension $n - k$.

Si $s > n$, on pose $S = \sum_{i=1}^{n} \binom{s}{i} 2^{i-1}$, sinon on pose $S = \sum_{i=1}^{s} \binom{s}{i} 2^{i-1}$. Ainsi, il y a S tels systèmes à considérer. Pour chacun de ces systèmes, on doit calculer :

- les limites des points critiques de π_1 restreinte à $V_{\varepsilon,a}^{\mathbf{A},\mathcal{I}}$ (où $a = (a_1, \ldots, a_s)$ et $\mathcal{I} = \{i_1, \ldots, i_k\}$) ;
- puis instantier X_1 à une valeur arbitraire, 0 par exemple, et recommencer itérativement sur le nouveau système obtenu.

Dans la suite, on note $\mathcal{L}$ la longueur d'un programme d'évaluation encodant le système $f_1, \ldots, f_s$.

On note aussi δ le maximum des degrés algébriques apparaissant quand on considère incrémentalement les systèmes polynômiaux définissant les variétés $\mathfrak{V}_a^{\mathcal{I},\mathbf{A}}$. Si on utilise une version de la proposition 27 (voir la remarque qui lui succède) fondée sur la caractérisation lagrangienne des points critiques du lemme 5 ainsi que les résultats du paragraphe 4.4, on trouve que δ est borné par $D^s(D-1)^{n-s}\binom{n}{s}$ si $s < n$ ou par D^n si $s > n$.

On déduit de cette discussion le résultat suivant :

Théorème 38. *Soit V une variété algébrique définie par*

$$f_1 = \cdots = f_s = 0$$

où les f_i sont des polynômes de $\mathbb{Q}[X_1, \ldots, X_n]$ de degré borné par D. On note $\mathcal{L}$ la longueur d'un programme d'évaluation du système $(f_1, \ldots, f_s)$. Il existe un algorithme probabiliste calculant au moins un point par composante connexe de $V \cap \mathbb{R}^n$ en

$$\mathcal{O}(S(n+s)^5((n+s)(\mathcal{L}+n^2)+(n+s)^3)M(D\mathfrak{d})^3)$$

opérations arithmétiques dans $\mathbb{Q}$ (où δ est défini comme ci-dessus et est borné par $D^n(D-1)^{n-s}\binom{n}{s}$ si $s < n$ et D^n sinon).

Notons que de manière similaire aux améliorations obtenues sur les quantités bornant δ en fin de paragraphe 5.6, on peut améliorer les bornes données ci-dessus portant sur δ.

5.8 Notes bibliographiques et commentaires

Les représentations triangulaires apparaissent sous différents formalismes [152, 76, 88, 87] dans un cadre algébrique ainsi que dans un cadre algébro-différentiel [119, 118]. Des études spécifiques tant théoriques que pratiques sont menées dans [105] et [9] selon qu'on cherche une décomposition au sens de Lazard (une description complète des variétés en quasi-composantes d'ensembles triangulaires) ou au sens de Kalkbrener (une décomposition des variétés clôtures de quasi-composantes). Une description unifiée des objets relatifs à ces décompositions apparaît dans [10] (voir aussi [71, 72]). La complexité du calcul d'ensembles triangulaires est encore mal connue. Quelques résultats se trouvent dans [54] et des avancées importantes ont été obtenues dans [135, 43].

Du point de vue des implantations, plusieurs tentatives ont été faites mais relativement peu sont disponibles. Mentionnons néanmoins les implantations de M. Moreno Maza dans le système de calcul formel `Axiom` [2] qui y est intégré depuis sa version 2.2. Ces implantations incluent des approches développées initialement dans [76] et [88]. À la même époque, P. Aubry a développé des versions, toujours en `Axiom` et partageant les routines de base de celles de M. Moreno Maza des approches développées dans [76]. Des versions ont été développées, toujours par M. Moreno Maza en `Aldor` [1] (successeur d'`Axiom`), ainsi que par F. Lemaire, M. Moreno Maza et les doctorants de ce dernier dans la bibliothèque `Maple` [4] `RegularChains`. Enfin, D. Wang a développé sa propre bibliothèque `Maple CharSets` [149]. À notre connaissance, ces bibliothèques, développées dans des langages de haut niveau, n'ont pas le niveau de performances des meilleures implantations de calcul de bases de Gröbner.

La littérature sur les bases de Gröbner est extrêmement dense. Initialement, le premier algorithme permettant de les calculer est dû à Bucherberger [32, 33]. De multiples améliorations ont été proposées, notamment via l'utilisation de calculs modulaires, de la fonction de Hilbert, d'algorithmes de changement d'ordre [142, 143, 52]. Dans [23], les auteurs montrent que sous certaines hypothèses de généricité, l'ordre le plus économique en terme de temps de calcul est l'ordre DRL. L'exposé qui est fait du sujet dans [42] (voir aussi [26]) constitue sans nul doute une excellente introduction au sujet. Algorithmiquement, les avancées majeures récentes sont dûes à J.-C. Faugère [50, 51]. Les résultats de [50] permettent d'importer des techniques d'algèbre linéaire rapide dans les calculs de bases de Gröbner. Les résultats de [51] permettent d'éviter des calculs se réduisant à 0 lorsque c'est possible. Ces algorithmes ont permis des avancées pratiques très importantes et ouvrent la voie à des analyses de complexité extrêmement fines (voir [16]) portant sur [51]. D'autres analyses de complexité portant essentiellement sur le cas zéro-dimensionnel se trouvent dans [83, 84, 56, 84, 67]. L'idée de réduire le calcul de bases de Gröbner à des questions d'algèbre linéaire se trouve déjà dans [86]. De manière plus générale, l'idée de résoudre des systèmes algébriques via des calculs d'algèbre linéaire est exploitée dès les travaux de Macaulay [99, 100, 101].

Le calcul de bases de Gröbner est maintenant une fonctionnalité qui apparaît dans presque tous les systèmes de Calcul Formel. Les niveaux d'efficacité sont très disparates. Les systèmes `Magma` [3] et `Singular` [7] sont réputés pour être les systèmes ayant les implantations de calculs de bases de Gröbner les plus performantes. Celles-ci sont basées sur [50]. Ceci dit, c'est le logiciel spécialisé `FGb` [49], implanté en `C` et utilisable via son interface avec `Maple` [4] qui offre un niveau de performances et une richesse de fonctionnalités qui permet d'avoir des implantations très efficace des algorithmes décrits dans ce chapitre. Le logiciel `FGb` sera prochainement intégré à `Maple`.

L'idée de représenter les solutions d'un système zéro-dimensionnel par des paramétrisations rationnelles (faisant intervenir des éléments primitifs) est sous-jacente aux travaux de Kronecker [81]. On la retrouve aussi dans [100, 147, 109]. Celle-ci est algorithmiquement exploitée dans [37, 78, 55, 35, 114, 84, 8, 58]. Le calcul de paramétrisations rationnelles à partir d'une représentation d'algébre-quotient est développé dans [121, 122]. Des études complémentaires sont menées dans [31, 123]. À notre connaissance, cet algorithme, dont la sortie est appelée *Représentation Univariée Rationnelle* donne des implantations [120] dont les performances pratiques sont les plus efficaces pour le calcul de ce type d'objets. Les résolutions géométriques (variantes de paramétrisations rationnelles qui diffèrent des représentations univariées eationnelles dans le cas d'idéaux non radicaux) sont développés dans [60, 110, 57, 59] pour aboutir aux travaux de G. Lecerf [61, 94, 93] qui ont permis l'obtention d'une implantation [92].

Le calcul de telles représentations est encore peu diffusé dans les systèmes de Calcul Formel même s'ils offrent tous les fonctionnalités de base pour implanter "facilement" l'algorithme décrit dans [122]. Des implantations existent notamment dans `Singular` [7] et `Axiom` [2]. Leurs performances pratiques sont très loin d'être exploitables par les algorithmes décrits dans ce chapitre. Seul le logiciel `RS` [120], implanté en `C` par F. Rouillier offre un niveau de performances satisfaisant.

L'implantation du paquetage `Kronecker` [92] dans `Magma` [3] valide expérimentalement les résultats de complexité obtenus sur les méthodes de résolution géométrique et a des performances pratiques intéressantes eu égard au caractère récent de cette implantation et le langage dans lequel elle est faite. Elle n'atteint tout de même pas le niveau de performances des logiciels `FGb/RS`.

Les travaux de Grigoriev et Vorobjov (voir [65]) sont le point de départ des algorithmes permettant de donner au moins un point par composante connexe d'un ensemble semi-algébrique (et donc a fortiori d'un ensemble algébrique réel), qui sont

- polynomiaux en le nombre et le degré des polynômes et simplement exponentiels en le nombre de variables
- et relèvent tous de la méthode des points critiques dont on a vu diverses variantes.

La contribution de Grigoriev et Vorobjov a ensuite amélioré par Heintz, Roy et Solerno [69, 70], puis par Renegar [114] et enfin une série de papiers de Basu, Pollack et Roy [17, 18, 19], ces derniers allant jusqu'à donner un algorithme permettant l'élimination des quantificateurs dont la complexité est doublement exponentielle en *le nombre d'alternance de quantificateurs* (et non pas doublement exponentiel en le nombre de variables).

La stratégie globale proposée (voir [18]) pour calculer au moins un point par composante connexe dans un ensemble semi-algébrique est basée sur la construction de routines réduisant le problème de départ à un problème plus facile :

- a) Trouver au moins un point par composante semi-algébriquement connexe dans un ensemble semi-algébrique.
- b) Trouver au moins un point par composante semi-algébriquement connexe dans un ensemble algébrique réel défini par un système d'équations.
- c) Trouver au moins un point par composante semi-algébriquement connexe dans un ensemble algébrique réel défini par une seule équation.
- d) Trouver au moins un point par composante semi-algébriquement connexe dans un ensemble algébrique algébrique réel défini par un système d'équations ayant un nombre fini de solutions complexes.
- e) Compter et isoler les racines d'un polynôme univarié.

Par exemple, le problème b) peut être réduit au problème c) en étudiant la somme des carrés des polynômes intervenant dans le système que l'on veut étudier. Aussi le problème d) est réduit au problème e) en calculant une Représentation Univariée Rationnelle (voir [121, 122] et en étudiant le premier polynôme de la sortie.

Néanmoins, aucune de ces contributions ne permettait d'obtenir des implantations efficaces en comparaison des résultats obtenus par les meilleurs implantations de l'algorithme de décomposition cylindrique algébrique.

En reprenant une idée évoquée par Seidenberg dans [138], on trouve une première approche fondée sur le calcul de points critiques du carré de la distance euclidienne à un point dans [124]. La complexité de cette approche est simplement exponentielle en le nombre de variables modulo le fait que le premier choix du point par rapport auquel les distances euclidiennes sont considérées est le bon. Cette hypothèse n'est aucunement restrictive en pratique puisqu'elle est vérifiée pour un choix aléatoire de ce point. Le cas singulier est géré en effectuant explicitement une déformation infinitésimale.

Dans [11], on trouve l'algorithme décrit dans le paragraphe 5.3. Diverses améliorations sont fournies dans [127]. L'usage de fonctions polynomiales qui sont des carrés de distance euclidienne est repris dans le contexte de résolution géométrique et dans le cas lisse et équi-dimensionnelle en considérant la notion de *variété polaire généralisée* dans [14, 15]. Ces derniers articles sont précédés de [13, 12] où les auteurs considèrent des fonctions de projection mais se restreignent au cas compact et lisse.

L'usage des fonctions de projection comme indiqué dans le paragraphe 5.4 est dû à [133]. Les avancées exhibées dans le paragraphe 5.5 se trouvent dans [132, 134].

La gestion efficace des singularités donnée dans le paragraphe 5.6 est dûe à [130].

Du point de vue des implantations, l'algorithme décrit dans [11] est implanté dans le système de calcul formel `Mathematica` [5]. Les résultats pratiques de cette implantation sont globalement comparables à ceux obtenus avec l'implantation de l'algorithme de décomposition cylindrique algébrique disponible dans le même système, mais pas meilleurs. Ceci est essentiellement dû au fait que les routines d'élimination algébrique implantées dans `Mathematica` [5] sont très loin du niveau d'efficacité de celles disponibles dans `Singular` [7], `Magma` [3] et encore plus loin de celles de `FGb`. Les implantations disponibles dans [128] sont fondées sur des variantes des algorithmes décrits dans les paragraphes 5.5, 5.6 et 5.7 de ce chapitre et utilisent les logiciels `FGb` et `RS` pour les calculs de bases de Gröbner et de Représentations Univariées Rationnelles. La conjonction de l'efficacité de ces routines d'élimination et des méthodes géométriques sous-jacentes à ces algorithmes permet d'obtenir des performances pratiques très largement supérieures à celles de l'algorithme de décomposition cylindrique algébrique. Afin de se donner une idée de l'efficacité qu'on peut attendre des implantations les plus abouties de tels algorithmes, on calcule au moins un point par composante connexe dans l'hypersurface définie par le polynôme donné dans le paragraphe 1.2 du chapitre 1 en moins de 10 sec. sur un Pentium Centrino 1.86 GHz avec 2048 KB de Cache et 1 Gb de RAM alors que la phase de projection de l'algorithme de décomposition cylindrique algébrique sature la mémoire du même ordinateur au bout de 24 heures de calcul.

6 Tests du vide et calcul d'au moins un point par composante connexe d'un ensemble semi-algébrique

Dans ce chapitre, on aborde le problème du test du vide et du calcul d'au moins un point par composante connexe d'un ensemble semi-algébrique défini par un système d'équations et d'inégalités polynomiales

$$f_1 = \cdots = f_s = 0, \quad g_1 > 0, \ldots, g_k > 0$$

où les f_i et les g_i sont des polynômes de $\mathbb{Q}[X_1, \ldots, X_n]$ de degré borné par D.

Ces questions sont ramenées au calcul d'au moins un point par composante connexe dans des variétés algébriques réelles obtenues par déformation infinitésimale du système donné en entrée.

La figure 24 illustre bien le procédé. Supposons que l'ensemble semi-algébrique dont on cherche au moins un point par composante connexe est constituée des points de la sphère et du tore sur la figure (qui sont définis par les égalités du système) situés à gauche du plan vertical qui y est tracé. Les composantes connexes de ce semi-algébriques sont au nombre de deux et constituées de la sphère d'une part et d'une partie du tore d'autre part.

Si on calcule au moins un point par composante connexe dans l'ensemble des points annulant les égalités données en entrée, on trouvera forcément un point sur cette sphère mais on n'est pas sûr de calculer au moins un point sur le tore qui appartienne à notre ensemble semi-algébrique. Pour ce faire, on considère l'intersection de la sphère et du tore avec l'ensemble des points annulant une "petite" déformation du polynôme définissant notre plan. On obtient deux cercles sur le tore. En calculer au moins un point par composante connexe achève l'obtention d'au moins un point par composante connexe dans le semi-algébrique qui nous intéresse. Remarquons que si on déforme trop ce polynôme on risque de "râter" la deuxième composante connexe de ce semi-algébrique. Un moyen simple de ne "pas trop déformer" est évidemment de considérer des déformations infinitésimales.

Dans la suite de ce chapitre, on verra comment généraliser ce procédé qui est inspiré de la géométrie algorithmique (voir [30]).

Du point de vue calculatoire, il est important de pouvoir évaluer le signe d'un polynôme en les solutions d'un système zéro-dimensionnel (pour distinguer les solutions de ce système qui appartiennent à l'ensemble semi-algébrique qu'on étudie). D'autre part, la tâche de base à effectuer dans les algorithmes présentés dans ce chapitre est de calculer au moins un point par composante connexe dans une variété algébrique réelle. On a vu dans le chapitre précédent qu'il est préférable de se ramener à des situations où la variété qu'on étudie est lisse et qu'elle est définie par un système d'équations polynomiales engendrant un idéal radical. Lorsque c'est possible, il faudra donc qu'on veille à obtenir de telles situations.

Enfin, on a aussi vu dans le chapitre précédent que l'introduction explicite d'infinitésimaux est difficile à concilier avec l'usage efficace d'algorithmes d'élimination algébrique. On est ici dans un contexte légèrement différent : alors que dans le chapitre précédent, on introduisait des infinitésimaux pour les faire tendre vers 0, ici on introduit des infinitésimaux pour finalement les spécialiser en une valeur *suffisamment petite*. Par *suffisamment petite*, on entendra qu'il faut spécialiser ε dans un intervalle $]0, e[$ tel que la restriction d'une certaine application polynomiale φ à une variété algébrique V réalise une fibration localement triviale sur $\varphi^{-1}(]0, e[) \cap V$. On voit apparaître ici l'utilité de la notion de *valeur critique généralisée* introduite dans le chapitre 4 dont nous faisons ici un usage intensif. Ainsi, avant d'aborder explicitement le problème du calcul d'au moins un point par composante connexe dans un ensemble semi-algébrique, nous concentrons notre étude sur le calcul de valeurs critiques généralisées d'applications polynomiales.

Dans le premier paragraphe, étant donné un polynôme $f \in \mathbb{Q}[X_1, \ldots, X_n]$, on montre comment calculer un polynôme univarié non nul dont l'ensemble des racines contient l'ensemble des valeurs critiques généralisées $K(f)$ de l'application polynomiale $x \in \mathbb{C}^n \to f(x) \in \mathbb{C}$, c'est-à-dire

$$\{c \in \mathbb{C} \mid \exists (x_\ell)_{\ell \in \mathbb{N}}, \quad f(x_\ell) \to c, \ \ ||x_\ell||.||d_{x_\ell} f|| \to 0, \quad \text{quand} \quad \ell \to \infty\}$$

(voir définition 16, chapitre 4). Une fois qu'on a obtenu un polynôme univarié dont les racines contiennent les valeurs critiques généralisées de f, on peut les isoler et choisir un rationnel $e \in \mathbb{Q}$ compris entre 0 et la plus petite valeur critique généralisée positive de f. Les propriétés topologiques de $K(f)$ (voir chapitre 4) impliquent alors que si l'ensemble semi-algébrique défini par $f > 0$ n'est pas $\mathbb{R}^n$ (auquel cas en donner

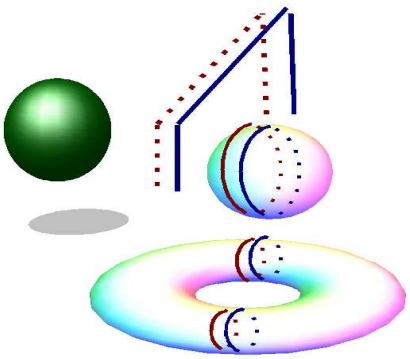

FIG. 24 –

au moins un point par composante connexe n'est pas très difficile), chacune de ses composantes connexes contient une composante connexe de l'ensemble algébrique réel défini par $f - e = 0$. On a donc réduit le problème du calcul d'au moins un point par composante connexe du semi-algébrique défini par $f > 0$ à :

- un pré-calcul de valeurs critiques généralisées de l'application $x \in \mathbb{C}^n \to f(x) \in \mathbb{C}$;
- le calcul d'au moins un point par composante connexe de l'ensemble algébrique réel défini par $f - e = 0$ où $e \in \mathbb{Q}$ est compris entre 0 et le plus petit réel positif de $F(f)$.

Remarquons que puisque l'ensemble des valeurs critiques de f est inclus dans $K(f)$, l'ensemble algébrique défini par $f - e = 0$ est lisse.

La stratégie concernant les ensembles semi-algébriques définis par des systèmes plus généraux

$$f_1 = \cdots = f_s = 0, \quad g_1 > 0, \ldots, g_k > 0$$

est identique mais soumise à quelques contraintes. Historiquement, la résolution de ces systèmes est réduite au calcul d'au moins un point par composante connexe des ensembles algébriques réels définis par :

$$f_1 = \cdots = f_s = 0, \quad g_{i_1} - \varepsilon = \cdots = g_{i_\ell} - \varepsilon = 0$$

(où $\{i_1, \ldots, i_\ell\} \subset \{1, \ldots, s\}$ et ε est un infinitésimal).

On est logiquement tenté ici de considérer ε comme une variable et de calculer les valeurs critiques généralisées de la projection sur cette variable restreinte à la variété qu'on vient de définir. Malheureusemen, on ne sait effectuer ces calculs que dans les cas où la variété considérée est lisse et équi-dimensionnelle et définie par un système de générateurs de son idéal associé (voir paragraphe 4.3 du chapitre 4). On retrouvera donc ce type d'hypothèse dans la suite. De plus, le seul calcul de valeurs critiques généralisées décrit ci-dessus n'est pas suffisant pour trouver une bonne spécialisation pour ε. Il faudra en plus calculer des intersections de courbes de points critiques avec des hypersurfaces pour y parvenir.

Les algorithmes que nous obtenons permettent de résoudre des problèmes inaccessibles par l'algorithme de décomposition cylindrique algébrique (lorsque les hypothèses d'application de nos algorithmes sont vérifiées). Leur complexité est simplement exponentielle en le nombre de variables, polynomiale en le degré des polynômes donnés en entrée et polynomiale en un facteur combinatoire qu'on explicitera.

6.1 Calcul de valeurs critiques généralisées : Le cas des applications de $\mathbb{C}^n$ dans $\mathbb{C}$

Ce paragraphe est consacré à l'élaboration d'un algorithme de calcul des valeurs critiques généralisées d'une application $x \in \mathbb{C}^n \to f(x) \in \mathbb{C}$ où f est un polynôme de $\mathbb{Q}[X_1, \ldots, X_n]$. Rappelons que les valeurs critiques généralisées $K(f)$ d'une telle application appartiennent à l'ensemble

$$\{c \in \mathbb{C} \mid \exists (x_\ell)_{\ell \in \mathbb{N}}, \quad f(x_\ell) \to c, \ \ ||x_\ell||.||d_{x_\ell} f|| \to 0, \quad \text{quand} \quad \ell \to \infty\}$$

(voir définition 16, chapitre 4).

Notons que la traduction d'une telle définition en une formule du premier ordre avec quantificateurs mise en conjonction avec le théorème de Tarski-Seidenberg (voir théorème 2 chapitre 2) et le lemme de sélection des courbes (voir lemme 1) implique qu'on peut réécrire la définition ci-dessus sous la forme suivante : $c \in \mathbb{C}$ *est une valeur critique généralisée de* f *si et seulement si il existe une courbe* $\gamma : [0,1[\to \mathbb{C}^n$ *telle que* $f(\gamma(t))$ *tend vers* c *et* $||\gamma(t)||.||d_{\gamma(t)}f||$ *tend vers* 0 *quand* t *tend vers* 1. Dans la suite, on va chercher à calculer une telle courbe (il s'agira en fait d'une courbe de points critiques) et à caractériser les valeurs critiques asymptotiques comme le lieu de non-propreté d'une certaine projection restreinte à cette courbe.

Pour cela, nous avons besoin de quelques résultats préliminaires.

Lemme 20. *Pour tout* $\mathbf{A} \in GL_n(\mathbb{Q})$, $K(f)$ *et* $K(f^{\mathbf{A}})$ *sont égaux, et il en est de même pour* $K_0(f)$ *(resp.* $K_\infty(f)$*) et* $K_0(f^{\mathbf{A}})$ *(resp.* $K_\infty(f^{\mathbf{A}})$*).*

De plus, si c *est une valeur critique (resp. une valeur critique asymptotique) de* f*, alors pour tout* $e \in \mathbb{Q}$, $c - e$ *est une valeur critique (resp. une valeur critique asymptotique) de* $f + e$.

Comme on peut caractériser les valeurs critiques à l'aide d'une formule du premier ordre avec quantificateurs dont les atomes sont des inégalités et des égalités polynomiales, le théorème de Tarski-Seidenberg ainsi que le lemme de sélection des courbes permettent d'obtenir facilement le lemme suivant.

Lemme 21. *Soit* f *un polynôme de* $\mathbb{Q}[X_1, \ldots, X_n]$. *Considerons* $c \in \mathbb{C}$ *et* $(z_\ell)_{\ell \in \mathbb{N}} \subset \mathbb{C}^n$ *une suite de points telle que :*

- $f(z_\ell)$ *tend vers* c *quand* ℓ *tend vers* ∞ *;*
- $||z_\ell||$ *tend vers* ∞ *quand* ℓ *tend vers* ∞ *;*
- $||z_\ell||.||d_{z_\ell}f||$ *tend vers* 0 *quand* ℓ *tend vers* ∞.

On note $\mathbf{X}$ *le vecteur* $X_1, \ldots, X_n$. *Il existe un ensemble Zariski-fermé* $\mathcal{A} \subsetneq GL_n(\mathbb{C})$ *tel que pour tout* $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$, $||\mathbf{AX}(z_\ell)||$ *tend vers* ∞ *quand* ℓ *tend vers* ∞.

6.1.1 Résultats géométriques

Soit f un polynôme de $\mathbb{Q}[X_1, \ldots, X_n]$, et $\mathcal{H} \subset \mathbb{C}^{n+1}$ l'hypersurface definie par $f - T = 0$ (où T est une nouvelle variable). Étant donné $x = (x_1, \ldots, x_n) \in \mathbb{C}^n$, on note $F_i : \mathbb{C}^n \to \mathbb{C}^{n+1}$ l'application polynomiale envoyant x sur :

$$\left((\partial f/\partial X_i)(x), (X_1 \partial f/\partial X_i)(x), \ldots, (X_n \partial f/\partial X_i)(x)\right)$$

et $\widetilde{F}_i : \mathbb{C}^n \to \mathbb{C}^{in+i+1}$ l'application polynomiale envoyant x sur :

$$\left(F_1(x), F_2(x), \ldots, F_i(x), f(x)\right).$$

On considère dans la suite l'application polynomiale $\varphi : \mathbb{C}^n \to \mathbb{C}^{n^2+n+1}$ envoyant $x = (x_1, \ldots, x_n)$ sur

$$(F_1(x), \ldots, F_n(x), f(x))$$

qui coincide avec $\widetilde{F}_n$. Pour toute application polynomiale ψ, on note Γ_ψ l'image de ψ et $\overline{\Gamma}_\psi$ sa clôture de Zariski. Pour $(i,j) \in \{1, \ldots, n\}^2$, on introduit les nouvelles variables a_i, et $a_{i,j}$ telles que $\overline{\Gamma}_\varphi$ est définie comme la variété algébrique associée à l'idéal :

$$\left\langle f - T, (\partial f/\partial X_i - a_i)_{i \in \{1,\ldots,n\}}, (X_i.\partial f/\partial X_j - a_{i,j})_{(i,j) \in \{1,\ldots,n\}^2} \right\rangle$$

intersecté avec l'anneau des polynômes $\mathbb{Q}[T, a_1, \ldots, a_n, a_{1,1}, \ldots, a_{n,n}]$.
Soit $L_i \subset \mathbb{C}^{in+i+1}$ l'axe de coordonnée de T, c'est-à-dire la droite définie par :

$$a_1 = \cdots = a_i = a_{1,1} = \cdots = a_{n,1} = \cdots = a_{1,i} = \cdots = a_{n,i} = 0.$$

La droite L_n est notée L dans la suite.

Dans [82, 74] Kurdyka et ses collaborateurs montrent que $\overline{\Gamma}_\varphi \cap L$ est égale à l'ensemble des valeurs critiques généralisées de f. L'ensemble des *valeurs critiques asymptotiques* de f, qu'on note $K_\infty(f)$, est caractérisé comme étant l'intersection du lieu de non-propreté de φ avec L.

6.1.2 Caractérisation géométrique des valeurs critiques généralisées sous des hypothèses de propreté

Dans la suite, pour $i = n, \ldots, 2$, on considère les projections :

$$\begin{array}{rccc} \Pi_i : & \mathbb{C}^{n+1} & \to & \mathbb{C}^i \\ & (x_1, \ldots, x_n, t) & \mapsto & (x_{n-i+2}, \ldots, x_n, t) \end{array}$$

Pour $i = 1, \ldots, n-1$, soit $W_{n-i} \subset \mathbb{C}^{n+1}$ la clôture de Zariski de l'ensemble constructible défini par :

$$f - T = \frac{\partial f}{\partial X_1} = \cdots = \frac{\partial f}{\partial X_i} = 0, \quad \frac{\partial f}{\partial X_{i+1}} \neq 0.$$

On notera aussi $\mathcal{H}$ par W_n.

On considèrera dans la suite des applications polynomiales entre des variétés algébriques complexes ou réelles. La notion de propreté relatives à ces applications sera alors relative aux topologies induites par les les topologies métriques de $\mathbb{C}$ ou $\mathbb{R}$.

Étant donné $\mathbf{A} \in GL_n(\mathbb{Q})$ et $j \in \{2, \ldots, n\}$, on dira que la propriété $\mathcal{P}_j(\mathbf{A})$ est satisfaite si et seulement si pour tout $i \in \{j, \ldots, n\}$, la restriction de l'application Π_i à $W_i^{\mathbf{A}}$ est propre et la restriction de l'application Π_{i+1} à W_i est birationnelle sur son image.

On supposera dans la suite de ce paragraphe qu'il existe un ensemble Zariski fermé $\mathcal{A} \subsetneq GL_n(\mathbb{Q})$ tel que pour tout $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$ et $j \in \{2, \ldots, n\}$, the propriété $\mathcal{P}_j(\mathbf{A})$ est satisfaite.

Remarque. *Remarquons que d'après le théorème de Bertini-Sard theorem [139], si $\mathcal{P}(\mathbf{A})$ est vraie, alors la restriction de Π_i à W_i est une application finie et alors $W_i^{\mathbf{A}}$ a pour dimension i.*

On prouve ci-dessous que si $\mathcal{P}_2(\mathbf{A})$ est satisfaite, étant donné $c \in K_\infty(f)$, il existe une suite de points $(z_\ell)_{\ell \in \mathbb{N}}$ dans $W_1^{\mathbf{A}}$ tel que :
- $f(z_\ell)$ tend vers c quand ℓ tend vers ∞
- $||z_\ell||$ tend vers ∞ quand ℓ tend vers ∞
- $||z_\ell||.||d_{z_\ell} f||$ tend vers 0 quand ℓ tend vers ∞

si bien que l'existence d'une valeur critique asymptotique peut se lire sur W_1 qui est de dimension 1.

Proposition 28. *Considérons $c \in K_\infty(f)$. Il existe un fermé de Zariski $\mathcal{A} \subsetneq GL_n(\mathbb{C})$ tel que pour tout $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$, il existe une suite de points $(z_\ell)_{\ell \in \mathbb{N}}$ telle que :*
- *pour tout $\ell \in \mathbb{N}$, $z_\ell \in W_{n-1}^{\mathbf{A}}$;*
- *$f^{\mathbf{A}}(z_\ell) \to c$ quand $\ell \to \infty$;*
- *$||z_\ell||$ tend vers ∞ quand ℓ tend vers ∞ ;*
- *$||z_\ell||.||d_{z_\ell} f^{\mathbf{A}}|| \to 0$ quand $\ell \to \infty$.*

Le résultat suivant montre que sous des hypothèses portant sur la propreté des projections Π_i et la dimension des variétés polaires, les valeurs critiques généralisées peuvent être caractérisées en étudiant la variété polaire W_1 qui est une courbe.

Proposition 29. *Considérons $c \in K_\infty(f)$. Il existe un fermé de Zariski $\mathcal{A} \subsetneq GL_n(\mathbb{C})$ tel que pour tout $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$, il existe une suite de points $(z_\ell)_{\ell \in \mathbb{N}}$ telle que :*
- *pour tout $\ell \in \mathbb{N}$, $z_\ell \in W_1^{\mathbf{A}}$;*
- *$f^{\mathbf{A}}(z_\ell) \to c$ quand $\ell \to \infty$;*
- *$||z_\ell||$ tend vers ∞ quand ℓ tend vers ∞ ;*
- *$||z_\ell||.||d_{z_\ell} f^{\mathbf{A}}|| \to 0$ quand $\ell \to \infty$.*

6.1.3 Garantir les hypothèses de propreté

On montre maintenant qu'il existe un fermé de Zariski $\mathcal{A} \in GL_n(\mathbb{C})$ tel que pour tout $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$, la propriété $\mathcal{P}_1(\mathbf{A})$ est satisfaite, ce qui est résumé dans la proposition suivante.

Proposition 30. *Il existe un fermé de Zariski $\mathcal{A} \subsetneq GL_n(\mathbb{C})$ tel que pour tout $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$ et pour tout $j \in \{1, \ldots, n-1\}$:*
- *la restriction de Π_j à W_j est propre.*

– *la restriction de Π_{j+1} à W_j est birationnelle sur son image.*

Dans [132], les auteurs montrent qu'étant donnée une hypersurface $\mathcal{H} \subset \mathbb{C}^{n+1}$, il existe un fermé de Zariski $\mathcal{A} \subsetneq GL_{n+1}(\mathbb{C})$ tel que pour $j \in \{1, \ldots, n-1\}$ et pour tout $\mathbf{A} \in GL_{n+1}(\mathbb{Q}) \setminus \mathcal{A}$, la restriction de Π_j à $W_j^{\mathbf{A}}$ est propre et satisfait une propriété de normalization de Nœther.

Ce résultat ne peut pas être utilisé tel quel puisqu'ici on considère une hypersurface définie par $f - T = 0$ et qu'on n'autorise que des changements de variables sur $X_1, \ldots, X_n$. Néanmoins, le procédé d'intersection incrémentale donné dans [60, 59, 57], qui est utilisé dans la preuve des résultats de [132] permet de montrer que :

Proposition 31. *Pour $i = 1, \ldots, n$, on note $\Delta_i^{\mathbf{A}}$ les idéaux associés à la clôture de Zariski de l'ensemble constructible défini par :*

$$\frac{\partial f^{\mathbf{A}}}{\partial X_1} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_i} = 0, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_{i+1}} \neq 0$$

Il existe un fermé de Zariski $\mathcal{A} \subsetneq GL_n(\mathbb{C})$ tel que :

- *pour tout $i \in \{1, \ldots, n\}$ et pour tout premier $P_i^{\mathbf{A}}$ associé à $\Delta_i^{\mathbf{A}}$, l'extension $\mathbb{C}[\mathbf{X}_{\geqslant i+1}] \to \mathbb{C}[\mathbf{X}]/P_i^{\mathbf{A}}$ est entière (où on note $\mathbf{X}_{\geqslant i+1}$ l'ensemble des variables $X_{i+1}, \ldots, X_n$ et $\mathbf{X}$ l'ensemble des variables $X_1, \ldots, X_n$).*
- *pour tout $i \in \{2, \ldots, n-1\}$, la restriction de la projection $\pi_i : (x_1, \ldots, x_n) \to (x_i, \ldots, x_n) \in \mathbb{C}^{n-i+1}$ à la variété algébrique définie par $\Delta_i^{\mathbf{A}}$ est birationnelle sur son image.*

On peut alors utiliser la preuve de [132, Proposition 3, Section 2.5], qui est fondée sur [73, Lemma 3.10] (permettant de relier la propreté de π_i au fait que les extensions définies ci-dessus sont entières) pour obtenir le résultat suivant :

Lemme 22. *On note π_{i+1} la projection $(x_1, \ldots, x_n) \in \mathbb{C}^n \to (x_{i+1}, \ldots, x_n) \in \mathbb{C}^{n-i}$. Il existe un fermé de Zariski $\mathcal{A} \subsetneq GL_n(\mathbb{C})$ tel que pour tout $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$ et pour tout $i \in \{1, \ldots, n\}$, la restriction de π_{i+1} à la variété algébrique définie par $\Delta_i^{\mathbf{A}}$ est propre.*

La preuve du fait que si la restriction de π_i à la variété algébrique définie par $\Delta_i^{\mathbf{A}}$ est propre, alors la restriction de Π_i à $W_i^{\mathbf{A}}$ est propre se fait de manière classique en utilisant des arguments de nature topologique.

Le fait que la restriction de Π_i à $W_i^{\mathbf{A}}$ est birationnelle provient du fait que la restriction de π_i à $\Delta_i^{\mathbf{A}}$ l'est aussi.

On dispose maintenant de tous les outils nécessaires pour énoncer un résultat de nature géométrique qui permet de caractériser l'ensemble des *valeurs critiques généralisées* de f.

6.1.4 Résultat géométrique principal

La combinaison des propositions 29, et 30 ainsi que le lemme 21 mènent alors au résultat suivant.

Théorème 39. *Il existe un fermé de Zariski $\mathcal{A} \subsetneq GL_n(\mathbb{C})$ tel que pour tout $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$ l'ensemble $K_\infty(f)$ des valeurs critiques asymptotiques de f est contenu dans l'ensemble de non-propreté de la restriction de la projection $\pi_T : (x_1, \ldots, x_n, t) \to t$ à la clôture de Zariski de l'ensemble constructible défini par :*

$$f^{\mathbf{A}} - T = \frac{\partial f^{\mathbf{A}}}{\partial X_2} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_n} = 0, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_1} \neq 0.$$

Remarque. *Remarquons que le résultat ci-dessus ne fait qu'affirmer que $K_\infty(f)$ est contenu dans le lieu de non-propreté de la restriction de la projection $\Pi : (x_1, \ldots, x_n, t) \in \mathbb{C}^{n+1} \to t \in \mathbb{C}$ à W_1. Cet ensemble est de dimension 0 d'après [73]. Néanmoins, cette inclusion peut être stricte comme l'illustre l'exemple ci-dessous.*

Exemple. *Dans [133], les auteurs utilisent [73, Lemma 3.10] pour calculer le lieu de non-propreté de la restriction d'une projection à une variété algébrique. En notant $I^{\mathbf{A}}$ l'idéal associé à $W_1^{\mathbf{A}}$, cet algorithme s'instantie dans notre cas particulier à calculer à calculer le polynôme caractéristique de la multiplication par X_1 dans $\mathbb{Q}(T)[X_1, \ldots, X_n]/I^{\mathbf{A}}$. Le lieu de non-propreté de la projection sur T est alors la réunion des lieux d'annulation des dénominateurs de ce polynôme caractéristique vu comme un polynôme univarié en X_1.*

Considérons donc le polynôme suivant

$$f = X_1 + X_1^2 X_2 + X_1^4 X_2 X_3$$

En effectuant le changement de variables ci-dessous

$$\begin{array}{rcl} X_1 & \leftarrow & X_1 + X_2 + X_3 \\ X_2 & \leftarrow & X_1 + 2X_2 + 3X_3 \\ X_3 & \leftarrow & X_1 + 4X_2 + 9X_3 \end{array}$$

on trouve que le lieu de non-propreté de la projection sur T est le lieu d'annulation de polynôme univarié ci-dessous

$$256\,T^2\,(20\,T + 1)$$

En effectuant le changement de variables ci-dessous

$$\begin{array}{rcl} X_1 & \leftarrow & 10213\,X_1 + 41543\,X_2 + 51532\,X_3 \\ X_2 & \leftarrow & X_1 + 44904\,X_2 + 10334\,X_3 \\ X_3 & \leftarrow & X_1 + 58200\,X_2 + 1597\,X_3 \end{array}$$

on trouve que le lieu de non-propreté de la projection sur T est le lieu d'annulation du polynôme univarié ci-dessous

$$T^2\,(898540\,T + 117941)\,.$$

Ainsi, $K_\infty(f)$ est le lieu d'annulation du pgcd des ces polynômes univariés et est donc $\{0\}$.

6.1.5 L'algorithme et sa complexité

Étant donné un polynôme $f \in \mathbb{Q}[X_1, \ldots, X_n]$, on nomtre maintenant comment calculer l'ensemble des valeurs critiques généralisées $K(f)$ de l'application polynomiale $x \in \mathbb{C}^n \to f(x) \in \mathbb{C}$.

Comme les algorithmes présentés dans le chapitre précédent, nos algorithmes dépendent ici de procédures d'élimination algébrique. Ainsi, on utilisera soit des bases de Gröbner soit la résolution géométrique.

Nous décrivons ci-dessous des algorithmes permettant les calculs de $K_0(f)$ et de $K_\infty(f)$ fondés soit sur des calculs de bases de Gröbner soit sur des calculs de résolution géométrique. L'utilisation des bases de Gröbner permet d'obtenir un algorithme déterministe dont les performances en pratique sont satisfaisantes. L'usage de l'algorithme de résolution géom'etrique permet d'obtenir un algorithme probabiliste dont la complexité est bien maîtrisée.

Calcul de $K_0(f)$. La première étape d'un algorithme permettant de calculer $K(f)$ est le calcul de l'ensemble des valeurs critiques $K_0(f)$ de f. Celles-ci sont représentées comme les racines d'un polynôme univarié. En notant I l'idéal

$$\langle f - T, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n} \rangle.$$

le théorème de Sard assure qu'il existe un polynôme non identiquement nul $P \in \mathbb{Q}[T]$ tel que : $\langle P \rangle = I \cap \mathbb{Q}[T]$ et, par définition que l'ensemble des racines de P est $K_0(f)$.

Les bases de Gröbner permettent de tels calculs sur les idéaux d'élimination.

Algorithme calculant $K_0(f)$ via des calculs de bases de Gröbner

- **Entrée :** un polynôme f dans $\mathbb{Q}[X_1, \ldots, X_n]$.
- **Sortie :** un polynôme univarié $P \in \mathbb{Q}[T]$ such that its zero-set is $K_0(f)$.
- Calculer une base de Gröbner G pour un ordre d'élimination $[X_1, \ldots, X_n] > [T]$ de l'idéal engendré par :

$$\langle f - T, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n} \rangle.$$

- Retourner l'élément de G appartenant à $\mathbb{Q}[T]$.

Remarquons maintenant que $\sharp K_0(f) \leqslant (D-1)^n$ puisque $K_0(f)$ est défini comme l'ensemble des valeurs prises par un polynôme sur chaque composante primaire isolée d'un idéal engendré par n polynômes de degré au plus $D-1$. On pourrait ainsi espérer obtenir un algorithme calculant une représentation de $K_0(f)$ en une complexité $(D-1)^{\mathcal{O}(n)}$. Ce but peut être atteint en substituant les calculs de bases de Gröbner par des calculs de résolutions géométriques. La première étape est le calcul de paramétrisations rationnelles de points génériques sur chaque composante équi-dimensionnelle de la variété algébrique définie par :

$$\frac{\partial f}{\partial X_1} = \cdots = \frac{\partial f}{\partial X_n} = 0.$$

Une fois que celles-ci sont obtenues, on peut obtenir les valeurs prises par f en ces points qui sont encodées par un polynôme univarié.

Algorithme probabiliste calculant $K_0(f)$ via des calculs de résolution géométrique

- **Entrée :** un polynôme f dans $\mathbb{Q}[X_1, \ldots, X_n]$.
- **Sortie :** un polynôme univarié $P \in \mathbb{Q}[T]$ such that its zero-set is $K_0(f)$.
- Soit G l'ensemble des paramétrisations rationnelles retournées par l'algorithme de résolution géométrique sur une entrée donnée par $\frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n}$.
- Pour chaque élément $g = (q, q_0, q_1, \ldots, q_n)$ de G, substituer dans $f - T$ les variables X_i par $\frac{q_i}{q_0}$ pour $i = 1, \ldots, n$. Mettre le résultat au même dénominateur et calculer le résultant du polynôme obtenu et de q par rapport à T.
- Retourner le produit des polynômes obtenus.

La complexité de l'algorithme ci-dessus est bornée par le coût duu calcul des paramétrisations rationnelles de points génériques sur les composantes équi-dimensionnelles de la variété algébrique définie par :

$$\frac{\partial f}{\partial X_1} = \cdots = \frac{\partial f}{\partial X_n} = 0$$

Calcul de $K_\infty(f)$. Il reste à montrer comment calculer $K_\infty(f)$. D'après la Remarque 6.1.4 et l'exemple 6.1.4, ceci peut se faire via des calculs d'algèbre linéaire dans l'algèbre-quotient $\mathbb{Q}(T)[X_1, \ldots, X_n]/I^{\mathbf{A}}$ où $I^{\mathbf{A}}$ est l'idéal associé à $W_1^{\mathbf{A}}$.

Algorithme déterministe. Pour obtenir un algorithme déterministe, on doit pouvoir vérifier que le changement de variables aléatoirement choisi vérifie les proriétés requises pour pouvoir appliquer le théorème 39. Remarquons tout d'abord que les mauvais choix de matrices $\mathbf{A}$ sont contenus dans un sous-ensemble strict et fermé (pour la topologie de Zariski) de $GL_n(\mathbb{C})$. Étant donné $f \in \mathbb{Q}[X_1, \ldots, X_n]$, on note $\deg(f, [X_1, \ldots, X_i])$ le degré de f quand il est vu comme un polynôme dans l'anneau des polynômes $\mathbb{Q}(X_{i+2}, \ldots, X_n)[X_1, \ldots, X_i]$ et on note φ_i l'application qui envoie $f \in \mathbb{Q}[X_1, \ldots, X_n]$ sur $X_0^{\deg(f,[X_1,\ldots,X_{i+1}])} f(\frac{X_1}{X_0}, \ldots, \frac{X_{i+1}}{X_0}, X_{i+2}, \ldots, X_n)$.

D'après [133, 89], la propreté de la restriction de Π_i à la clôture de Zariski de l'ensemble constructible défini par :

$$f^{\mathbf{A}} - T = \frac{\partial f^{\mathbf{A}}}{\partial X_1} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_i}, \quad \frac{f^{\mathbf{A}}}{\partial X_{i+1}} \neq 0$$

peut être testée en calculant l'intersection de la clôture projective de $W_{n-i}^{\mathbf{A}}$ dans $\mathbb{P}^{i+1}(\mathbb{C}) \times \mathbb{C}^{n-i}$ avec l'hyperplan à l'infini. Ceci peut être fait par des calculs de bases de Gröbner (voir [42]). Un test préliminaire consiste à appliquer φ_i au système définissant W_{n-i}, en y instantiant X_0 à 1 et à vérifier qu'en substituant X_k par 1 (pour $k = 1, \ldots, i-1$), le système obtenu engendre $\langle 1 \rangle$. En utilisant des calculs de bases de Gröbner, de tels calculs s'effectuent en pratique très rapidement. Des calculs modulo des nombres premiers peuvent aussi être effectués pour des choix de matrices $\mathbf{A} \in GL_n(\mathbb{Q})$ creuses.

Dans la suite on note `SetOfNonProperness` une routine prenant en entrée un système d'équations et d'inéquations polynomiales et un ensemble de variables et retourne une représentation du lieu de non-propreté de la projection sur les variables données en entrée restreinte à la clôture de Zariski de l'ensemble contructible défini par le système donné en entrée. On trouve la description d'une telle procédure dans [133, 89].

Algorithme calculant $K_\infty(f)$ via des calculs de bases de Gröbner

- **Entrée :** un polynôme f dans $\mathbb{Q}[X_1, \ldots, X_n]$.
- **Sortie :** un polynôme univarié $P \in \mathbb{Q}[T]$ tel que l'ensemble de ses racines contient $K_\infty(f)$.
- Choisir aléatoirement $\mathbf{A} \in GL_n(\mathbb{Q})$ et vérfier que ce choix est suffisamment générique. Recommencer tant que ce n'est pas le cas.
- Retourner `SetOfNonProperness`$([f^{\mathbf{A}} - T = \frac{\partial f^{\mathbf{A}}}{\partial X_1} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_{n-1}} = 0, \frac{\partial f^{\mathbf{A}}}{\partial X_n} \neq 0], \{T\})$

Algorithme probabiliste. Comme dans le cas du calcul de $K_0(f)$, les bases de Gröbner ne permettent pas d'obtenir des résultats de complexité satisfaisants, c'est-à-dire même si le premier choix de $\mathbf{A}$ est correct. L'utilisation des calculs de résolution géométrique permet en revanche d'atteindre cet objectif. Il faudra néanmoins utiliser des extensions des résultats [136] au cas des systèmes à paramètres.

Plus précisément, dans le système d'équations et d'inégalités polynomiales

$$f^{\mathbf{A}} - T = \frac{\partial f^{\mathbf{A}}}{\partial X_1} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_{n-1}} = 0, \frac{\partial f^{\mathbf{A}}}{\partial X_n} \neq 0$$

T est considéré comme un paramètre. D'après [12], si le choix de $\mathbf{A}$ est suffisamment générique, il engendre un idéal radical de dimension 0 dans $\mathbb{Q}(T)[X_1, \ldots, X_n]$. La sortie est une résolution géométrique

$$\begin{cases} X_n & = & \frac{q_n(X_1,T)}{q_0(X_1,T)} \\ & \vdots & \\ X_2 & = & \frac{q_2(X_1,T)}{q_0(X_1,T)} \\ q(X_1,T) & = & 0 \end{cases}$$

L'ensemble de non-propreté de la restriction de la projection sur T à la clôture de Zariski de l'ensemble constructible défini par le système donné en entrée est contenu dans le lieu d'annulation du plus petit commun multiple des dénominateurs des coefficients de q.

Algorithme probabiliste calculant $K_\infty(f)$ via des calculs de résolution géométrique
– **Entrée :** un polynôme f dans $\mathbb{Q}[X_1, \ldots, X_n]$. – **Sortie :** un polynôme univarié $P \in \mathbb{Q}[T]$ tel que l'ensemble de ses racines contient $K_\infty(f)$. – Considérer T comme un paramètre dans le système $f^{\mathbf{A}} - T = \frac{\partial f^{\mathbf{A}}}{\partial X_1} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_{n-1}} = 0, \frac{\partial f^{\mathbf{A}}}{\partial X_n} \neq 0$ et calculer une résolution géométrique. – Remonter le paramètre. – Retourner le plus petit commun multiple des dénominateurs des coefficients du polynôme éliminant q.

Estimations de complexité. D'après le théorème 19 (voir aussi [94]), les versions probabilistes des algorithmes calculant des représentations de $K_0(f)$ et $K_\infty(f)$ permettent d'effectuer une analyse de complexité pertinente. En effet, en utilisant des versions fortes du théorème de Bézout (voir [53]), la somme des degrés des composantes primaires isolées de l'idéal engendré par :

$$\frac{\partial f}{X_1} = \cdots = \frac{\partial f}{X_n} = 0$$

est bornée par $(D-1)^n$ (où D est le degré de f). Ainsi, le polynôme retourné par l'algorithme probabiliste calculant une représentation de $K_0(f)$ a un degré borné par $(D-1)^n$.

On s'intéresse maintenant au calcul de $K_\infty(f)$. L'algorithme probabiliste donné ci-dessus calcule un polynôme univarié encodant le lieu de non-propreté de la restriction d'une projection à la clôture de Zariski du lieu solution du système :

$$f^{\mathbf{A}} - T = \frac{\partial f^{\mathbf{A}}}{\partial X_1} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_{n-1}}, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_n} \neq 0$$

qui a un degré borné par $(D-1)^{n-1}$ puisque, d'après le thèeorème de Bézout, la clôture de Zariski du lieu de solutions complexes du système

$$f^{\mathbf{A}} - T = \frac{\partial f^{\mathbf{A}}}{\partial X_1} = \cdots = \frac{\partial f^{\mathbf{A}}}{\partial X_{n-1}}, \quad \frac{\partial f^{\mathbf{A}}}{\partial X_n} \neq 0$$

a un degré au plus $(D-1)^{n-1}$. D'après [136], la remontée du paramètre T s'effectue en une complexité qui est log-linéaire en la complexité d'évaluation du système polynomial ci-dessus et quadratique en le degré de la courbe étudiée.

En bornant la complexité d'évaluation de f par D^n, la discussion mène au résultat de complexité suivant.

Théorème 40. *L'algorithme probabiliste donné ci-dessus et calculant une représentation de $K_0(f)$ effectue au plus $\mathcal{O}(n^7 D^{4n})$ opérations arithmetiques dans $\mathbb{Q}$.*

L'algorithme probabiliste donné ci-dessus et calculant une représentation de $K_\infty(f)$ effectue au plus most $\mathcal{O}(n^7 D^{4n})$ opérations arithmetiques dans $\mathbb{Q}$.

Remarque. *D'après la remarque 5.1.3, la complexité binaire des versions probabilistes des algorithmes donnés ci-dessus est $\mathcal{O}(\tau n^7 D^{5n})$ où τ borne la taille binaire des coefficients de f.*

6.2 Calcul de valeurs critiques généralisées : le cas des applications polynomiales restreintes à une variété algébrique

Étant donnée une variété algébrique lisse et équi-dimensionnelle $V \subset \mathbb{C}^n$ définie par un système d'équations polynomiales

$$f_1 = \cdots = f_s = 0$$

(avec $f_i \in \mathbb{Q}[X_1, \ldots, X_n]$ pour $i \in \{1, \ldots, s\}$) engendrant un idéal radical, on considère maintenant une application polynomiale $\varphi : x \in V \to \varphi(x) \in \mathbb{C}$ (avec $\varphi \in \mathbb{Q}[X_1, \ldots, X_n]$). Notre objectif ici est d'exhiber un algorithme calculant l'ensemble des valeurs critiques généralisées de φ, c'est-à-dire (voir définition 17 du chapitre 4) l'ensemble des points $c \in \mathbb{C}$ pour lesquels il existe une suite de points $(x_\ell)_{\ell \in \mathbb{N}} \subset V$ et $C \in \mathcal{C}$ tels que :

- $\varphi(x_\ell)$ tend vers y quand ℓ tend vers ∞ ;
- pour tout $M \in \mathcal{M}^C$, $M(x_\ell)$ tend vers 0 quand ℓ tend vers ∞ ;
- pour tout $M \in \mathcal{M}^C$, les produits $(X_1.M)(x_\ell), \ldots, (X_n.M)(x_\ell)$ tendent vers 0 quand ℓ tend vers ∞ ;

où on utilise les notation suivantes :

- La matrice jacobienne associée à $(f_1, \ldots, f_s, \varphi_1, \ldots, \varphi_k)$ est notée $\mathrm{Jac}(F, \varphi)$;
- Étant donné un sous-ensemble $\mathcal{I} = \{i_1, \ldots, i_{n-d}\} \subset \{1, \ldots, s\}$ de cardinalité $n - d$ et un sous-ensemble $\mathcal{J} = \{j_1, \ldots, j_{n-d+1}\} \subset \{1, \ldots, n\}$ de cardinalité $n-d+1$, on note $M_{\mathcal{I},\mathcal{J}} \in \mathbb{Q}[X_1, \ldots, X_n]$ le mineur de $\mathrm{Jac}(F, \varphi)$ de taille $n - d + 1$ construit en prenant les rangées $i_1, \ldots, i_{n-d}, s+1$, et les colonnes $j_1, \ldots, j_{n-d+1}$ de $\mathrm{Jac}(F, \varphi)$;
- Étant donnés de tels sous-ensembles $\mathcal{I}$ et $\mathcal{J}$ comme ci-dessus et $i \in \mathcal{I}$ et $j \in \mathcal{J}$ on note $M_{\mathcal{I}\setminus\{i\},\mathcal{J}\setminus\{j\}}$ le mineur de $\mathrm{Jac}(F, \varphi)$ suivant la même contruction que précédemment. Si ce mineur est non nul on note $M^{i,j}_{\mathcal{I},\mathcal{J}}$ la fraction rationnelle $M_{\mathcal{I},\mathcal{J}}/M_{\mathcal{I}\setminus\{i\},\mathcal{J}\setminus\{j\}}$, sinon on pose $M^{i,j}_{\mathcal{I},\mathcal{J}} = 0$.
- on note alors $C = \{(i_1, j_1) \in \mathcal{I}_1 \times \mathcal{J}_1, \ldots, (i_N, j_N) \in \mathcal{I}_N \times \mathcal{J}_N\}$ un ensemble de couples tels que pour $\alpha = 1, \ldots, N$, le dénominateur de la fraction rationnelle $M^{i_\alpha,j_\alpha}_{\mathcal{I}_\alpha,\mathcal{J}_\alpha}$ n'est pas un diviseur de zéro dans $\mathbb{Q}[X_1, \ldots, X_n]/\langle f_1, \ldots, f_s\rangle$, et on note $\mathcal{C}$ l'ensemble de tels couples C.
- Étant donné $C = \{(i_\alpha, j_\alpha) \in \mathcal{I}_\alpha \times \mathcal{J}_\alpha \mid \alpha = 1, \ldots, N\} \in \mathcal{C}$, on note $\mathcal{M}^C$ l'ensemble des fractions rationnelles $M^{i_\alpha,j_\alpha}_{I_\alpha,J_\alpha}$ pour $\alpha = 1, \ldots, N$.

On va procéder comme dans le paragraphe précédent, c'est-à-dire en exhibant une courbe de points critiques telle que l'ensemble des valeurs critiques asymptotiques de φ est inclus dans le lieu de non-propreté d'une certaine projection restreinte à cette courbe.

Pour cela, on considère les projections :

$$\begin{array}{rccc} \Pi_i : & \mathbb{C}^{n+1} & \to & \mathbb{C}^i \\ & (x_1, \ldots, x_n, t) & \mapsto & (x_{n-i+2}, \ldots, x_n, t) \end{array}$$

Étant donnée $\mathbf{A} \in GL_n(\mathbb{Q})$ et T une nouvelle variable, on note $V^{\mathbf{A}}_\varphi$ la variété algébrique définie par :

$$f^{\mathbf{A}}_1 = \cdots = f^{\mathbf{A}}_s = \varphi - T = 0.$$

Il alors est clair que calculer les valeurs critiques généralisées de φ est équivalent à calculer les valeurs critiques généralisées de la restriction de la projection $\pi_T : (x_1, \ldots, x_n, t) \to t$ à V^T_φ.

L'ensemble des valeurs critiques généralisées de φ étant l'union des valeurs critiques et des valeurs critiques asymptotiques de φ, on concentre notre étude sur le calcul des valeurs critiques asymptotiques de φ. Les valeurs critiques de φ sont aisément obtenues comme étant les images des points critiques de la restriction de π_T à V par π_T. Dans la suite on note $\mathfrak{C}_0$ la pré-image de ces valeurs critiques par π_T dans $\mathbb{C}^{n+1}$.

Enfin, on note $\mathfrak{C}(\Pi_i, V^{\mathbf{A}}_\varphi)$ le lieu critique de Π_i restreinte à $V^{\mathbf{A}}_\varphi \setminus \mathfrak{C}_0$. Enfin, pour $\mathbf{A} \in GL_n(\mathbb{Q})$ et $j \in \{2, \ldots, n\}$, on dira que la propriété $\mathcal{P}_j(\mathbf{A})$ est satisfaite si pour tout $i \in \{\}$, la restriction de Π_i à $\mathfrak{C}(\Pi_i, V^{\mathbf{A}}_\varphi)$ est propre et la restriction de Π_{i+1} à $\mathfrak{C}(\Pi_i, V^{\mathbf{A}}_\varphi)$ est bi-rationnelle.

Dans ce contexte, les résultats du paragraphe 6.1.2 sont complètement transposables. Il en est naturellement de même de la proposition 30, si bien qu'on peut comme dans le paragraphe précédent caractériser les valeurs critiques asymptotiques de φ comme appartenant au lieu de non-propreté d'une courbe critique dans $V^{\mathbf{A}}_\varphi$, ceci étant conditionné par un choix suffisamment générique de $\mathbf{A}$ dans $GL_n(\mathbb{Q})$. On énonce donc directement la caractérisation algébrique des valeurs critiques asymptotiques de φ que nous obtenons.

Théorème 41. *Il existe un fermé de Zariski $\mathcal{A} \subsetneq GL_n(\mathbb{C})$ tel que pour tout $\mathbf{A} \in GL_n(\mathbb{Q}) \setminus \mathcal{A}$ l'ensemble $K_\infty(f)$ des valeurs critiques asymptotiques de φ restreinte à V est contenu dans l'ensemble de non-propreté de la restriction de la projection $\pi_T : (x_1, \ldots, x_n, t) \to t$ à la clôture de Zariski de l'ensemble constructible $\mathfrak{C}(\Pi_2, V_\varphi^{\mathbf{A}}) \setminus K_0$.*

L'algorithme de calcul des valeurs critiques asymptotiques de φ consiste donc à choisir suffisamment génériquement $\mathbf{A} \in GL_n(\mathbb{Q})$ et à calculer $\mathfrak{C}(\Pi_2, V_\varphi^{\mathbf{A}})$.

Ainsi, on obtient l'algorithme ci-dessous.

Algorithme : Calcul des valeurs critiques généralisées d'une application polynomiale restreinte à une variété algébrique lisse et équi-dimensionnelle

- **Entrée :** Un système d'équations polynomiales $f_1 = \cdots = f_s = 0$ dans $\mathbb{Q}[X_1, \ldots, X_n]$ engendrant un idéal radical équi-dimensionnel dont la variété algébrique associée V est lisse, et un polynôme $\varphi \in \mathbb{Q}[X_1, \ldots, X_n]$.
- **Sortie :** Un polynôme univarié non nul dont l'ensemble des racines contient l'ensemble des valeurs critiques généralisées de l'application polynomiale $x \in \mathbb{C}^n \to \varphi(x)$ restreinte à V.

1. Choisir aléatoirement $\mathbf{A} \in GL_n(\mathbb{Q})$.
2. Calculer une représentation de la courbe $\mathfrak{C}(\Pi_2, V_\varphi^{\mathbf{A}})$.
3. Calculer un polynôme univarié représentant le lieu de non-propreté de la restriction de π_T à $\mathfrak{C}(\Pi_2, V_\varphi^{\mathbf{A}})$.
4. Calculer un polynôme reprśentant les valeurs critiques de π_T restreinte à $V_\varphi^{\mathbf{A}}$.
5. Retourner le produit des polynômes précédemment calculés.

Si on choisit d'utiliser comme procédure d'émination algébrique les algorithmes de calcul de résolution géométrique, on obtient sans peine une estimation de la complexité de l'algorithme ci-dessus.

Théorème 42. *Soit $V \subset \mathbb{C}^n$ une variété algébrique lisse définie par*

$$f_1 = \cdots = f_s = 0$$

où les polynômes f_i (pour $i = 1, \ldots, s$) appartiennent à $\mathbb{Q}[X_1, \ldots, X_n]$, sont de degré borné par D et engendrent un idéal radical et équi-dimensionnel de dimension d.

Soit $\varphi \in \mathbb{Q}[X_1, \ldots, X_n]$ de degré lui aussi borné par D et $\mathcal{L}$ la longueur d'un programme d'évaluation de $(f_1, \ldots, f_s, \varphi)$.

L'algorithme ci-dessus calcule l'ensemble des valeurs critiques généralisées de $x \in V \to \varphi(x)$ en

$$\mathcal{O}(n^7 (n-d)^{4d} D^{4n})$$

opérations arithmétiques dans $\mathbb{Q}$.

Notons que dans la complexité ci-dessus, le facteur $(n-d)^{4d}$ provient du fait qu'on n'accède pas aux valeurs critiques asymptotiques via une formulation lagrangienne mais en annulant des mineurs de matrice jacobienne. Comme on a ramené le calcul de ces valeurs critiques asymptotiques au calcul du lieu de non-propreté d'une projection restreinte à une courbe de points critiques et comme cette courbe de points critiques peut être définie comme la projection de l'ensemble des solutions d'un système *"à la Lagrange"*, on pourrait écrire une estimation de complexité plus fine. Ceci dit, on a vu que les caractérisations lagrangiennes de points critiques permettent de lever une hypothèse d'équi-dimensionnalité (voir paragraphe 5.5 du chapitre précédent). L'usage de ce type de formulation pour lever l'hypothèse

d'équi-dimensionnalité au calcul de valeurs critiques asymptotiques présente dans ce chapitre est le sujet d'études actuelles qui devraient donc exhiber des complexités meilleures que celle qui est donnée ci-dessus.

Enfin, comme dans le paragraphe précédent, on peut obtenir des versions certifiées de cet algorithme en utilisant des calculs de bases de Gröbner. Les implantations qui en résultent ont des performances pratiques satisfaisantes même si pour des raisons qu'on ne détaillera pas ici, des améliorations peuvent être attendues.

6.3 Application au calcul d'un point par composante connexe dans un ensemble semi-algébrique défini par une inégalité

Dans ce paragraphe, on montre comment utiliser l'algorithme de calcul de valeurs critiques généralisées donné dans le paragraphe 6.1 de ce chapitre pour calculer au moins un point par composante connexe d'un ensemble semi-algébrique défini par une seule inégalité ou une seule inéquation.

Le procédé est fondé sur les propriétés topologiques des valeurs critiques généralisées (voir théorème 11 du chapitre 4). En effet, il existe un réel suffisamment petit $e_0 \in]0, +\infty[$ tel que chaque composante connexe de $\mathcal{S}$ contient une composante connexe du lieu réel de l'hypersurface définie par $f - e_0 = 0$ et qu'il en est de même pour tout réel e compris entre 0 et e_0 (voir [21, chapitre 13]). On peut ainsi réduire la recherche d'un point par composante connexe dans $\mathcal{S}$ à la recherche d'un point par composante connexe dans le lieu réel d'une hypersurface si on sait déterminer e_0. Or, le fait que pour tout $e \in \mathbb{R}$ compris entre 0 et la plus petite valeur critique généralisée positive de l'application $\widetilde{f} : x \in \mathbb{R}^n \to f(x)$, les lieux réels des hypersurfaces définies par $f - e = 0$ sont difféomorphes implique qu'il suffit de calculer les valeurs critiques généralisées de $\widetilde{f}$ pour obtenir e_0.

Le résultat ci-dessous se prouve donc en utilisant des techniques classiques de géométrie algébrique réelle.

Théorème 43. *Soit f un polynôme de $\mathbb{Q}[X_1, \ldots, X_n]$ et $\mathcal{S} \subsetneq \mathbb{R}^n$ l'ensemble semi-algébrique défini par $f > 0$. Soit $e \in \mathbb{Q}$ tel que $0 < e < \min(|r|, r \in K(f) \cap \mathbb{R})$.*

Considérons l'hypersurface $\mathcal{H}_e$ définie par $f - e = 0$. Alors, pour chaque composante connexe S de $\mathcal{S}$, il existe une composante connexe C de $\mathcal{H}_e \cap \mathbb{R}^n$ telle que $C \subset S$.

Remarque. *D'après le théorème 43, décider du vide de l'ensemble semi-algébrique défini par $f > 0$ se réduit à décider du vide du lieu réel d'une hypersurface.*

En substituant f par $-f$ on peut évidemment écrire un résultat similaire si l'ensemble semi-algébrique est défini par $f < 0$ ou encore par $f \neq 0$.

L'Algorithme. L'algorithme qu'on décrit ci-dessous s'appuie sur le théorème 43. Étant donné un polynôme f de $\mathbb{Q}[X_1, \ldots, X_n]$ de degré D, cet algorithme calcule au moins un point par composante connexe de l'ensemble semi-algébrique défini par $f > 0$. Supposons tout d'abord que $\mathcal{S} = \mathbb{R}^n$. Dans ce cas, la donnée de n'importe quel point de $\mathbb{R}^n$ convient.

Si $\mathcal{S} \neq \mathbb{R}^n$, la première étape consiste à calculer l'ensemble des valeurs critiques généralisées de l'application polynomiale $f : x \in \mathbb{C}^n \to f(x) \in \mathbb{C}$. En utilisant la version probabiliste de l'algorithme décrit dans le paragraphe 6.1.5 de ce chapitre, ceci peut se faire en $\mathcal{O}(n^7 D^{4n})$ opérations arithmétiques dans $\mathbb{Q}$.

On a vu dans le paragraphe 6.1.5 que le degré des polynômes dont l'ensemble des racines contient ces valeurs critiques généralisées est borné par $\mathcal{O}(D^n)$. Ainsi, isoler les racines réelles de ces polynômes se fait en $\mathcal{O}(D^{3n})$ opérations arithmétiques dans $\mathbb{Q}$ (voir [126]). Choisir un rationnel positif e compris entre 0 et la plus petite valeur critique généralisée réelle positive est immédiat.

Une fois ce travail effectué, il reste à calculer au moins un point par composante connexe de l'ensemble algébrique réel défini par $f - e = 0$. Puisque l'ensemble des valeurs critiques généralisées de f contient l'ensemble des valeurs critiques de f, l'hypersurface définie par $f - e = 0$ est lisse. On peut donc utiliser les algorithmes donnés dans le paragraphe 5.5 du chapitre 5. La complexité des algorithmes probabilistes donnés dans ce paragraphe est $\mathcal{O}(n^7 D^{3n})$ opérations arithmétiques dans $\mathbb{Q}$.

Pour distinguer les cas $\mathcal{S} = \mathbb{R}^n$ et $\mathcal{S} \neq \mathbb{R}^n$, il faudra ajouter aux paramétrisations rationnelles qu'on vient de calculer un point $p \in \mathbb{Q}^n$ choisi aléatoirement (si $f(p) > 0$ bien sûr).

Ainsi, si on se donne les routines :

– `GeneralizedCriticalValues` : qui prend en entrée un polynôme $f \in \mathbb{Q}[X_1, \ldots, X_n]$ et retourne un polynôme non nul dont l'ensemble des racines contient l'ensemble des valeurs critiques généralisées de l'application $x \in \mathbb{C}^n \to f(x) \in \mathbb{C}$;
– `Isolate` : qui prend en entrée un polynôme univarié et isole les racines réelles de ce polynôme ;
– `Sampling` : qui prend en entrée un polynôme $f \in \mathbb{Q}[X_1, \ldots, X_n]$ et calcule au moins un point par composante connexe de la variété algébrique réelle définie par $f = 0$.

on obtient l'algorithme suivant :

Algorithme : Calcul d'au moins un point par composante connexe d'un semi-algébrique défini par une inégalité

– **Entrée :** Un polynôme $f \in \mathbb{Q}[X_1, \ldots, X_n]$
– **Sortie :** Une famille de paramétrisations rationnelles encodant un nombre fini de points et ayant une intersection non vide avec chaque composante connexe de l'ensemble semi-algébrique défini par $f > 0$.

1. Poser $P :=$ `GeneralizedCriticalValues`(f).
2. Tant P est divisible par sa variable (qu'on note T) poser $P := P/T$
3. Poser `intervalles` := `Isolate`(P).
4. Si 0 appartient à l'un des intervalles d'isolation, revenir au pas précédent en augmentant la précision.
5. Si non choisir $e \in \mathbb{Q}$ positif et plus petit que la plus petite valeur critique généralisée positive encodée par P.
6. Poser `sols` := `Sampling`$(f - e)$.
7. Choisir aléatoirement $p \in \mathbb{Q}^d$ et si $f(p) > 0$ retourner l'union de `sols` et p.

La discussion ci-dessus donne le résultat de complexité suivant :

Théorème 44. *Soit f un polynôme de $\mathbb{Q}[X_1, \ldots, X_n]$ de degré D et $\mathcal{S}$ l'ensemble semi-algébrique défini par $f > 0$. Les versions probabilistes de l'algorithme donné ci-dessus calculent au moins un point par composante connexe de $\mathcal{S}$ en effectuant $\mathcal{O}(n^7 D^{4n})$ opérations arithmétiques dans $\mathbb{Q}$.*

Implantations et performances pratiques. L'usage des bases de Gröbner a permis de donner des algorithmes déterministes de calculs de valeurs critiques généralisées et de calcul d'au moins un point par composante connexe dans une hypersurface lisse (voir paragraphes 5.5 et 6.1). Les performances pratiques des implantations qui en résultent sont significativement meilleures que celles des meilleurs implantations de l'algorithme de décomposition cylindrique algébrique si le polynôme donné en entrée est *irréductible*.

Dans le cas contraire, la décomposition cylindrique algébrique tire profit des factorisations des polynômes apparaissant dans la phase de projection. Ceci induit des simplifications et des chutes de degré qui n'apparaissent pas si on fait un usage aveugle de l'algorithme qu'on vient de décrire. Ceci dit, dans le cas où f n'est pas irréductible, donner au moins un point par composante connexe du semi-algébrique défini par $f > 0$ est équivalent à donner au moins un point par composante connexe de semi-algébriques définis par des systèmes d'inégalités obtenus à partir des facteurs de f. Ceci est traité dans le paragraphe suivant.

Avant d'aborder ce paragraphe, nous étudions une application importante (car apparaissant dans diverses applications, voir par exemple [48]) des algorithmes calculant au moins un point par composante connexe d'un semi-algébrique défini par une inégalité (ou une inéquation) : il s'agit de la détermination de l'égalité entre dimension complexe et dimension réelle de l'ensemble des solutions d'une équation

polynomiale $f = 0$. Ceci revient à déterminer l'existence de points réels *réguliers* dans une hypersurface complexe.

Application : détermination de l'existence de points réels réguliers dans une hypersurface On s'intéresse au problème suivant : étant donné un polynôme $f \in \mathbb{Q}[X_1, \ldots, X_n]$ de degré D, décider si l'hypersurface $\mathcal{H}$ definie par $f = 0$ contient des points réels réguliers. Ce problème consiste à décider si la dimension réelle de $\mathcal{H} \cap \mathbb{R}^n$ est égale à la dimension complexe de $\mathcal{H}$. De tels problèmes apparaissent dans de nombreuses applications (en particulier en géométrie algorithmique ou en démonstration automatique de théorème géométrique automatique) étudiant des situations géometriques génériques.

Comme on l'a mentionné dans le chapitre 3, ces questions peuvent être résolues en utilisant l'algorithme de décomposition cylindrique algébrique mais la complexité de cette méthode est doublement exponentielle en le nombre de variables. En pratique, ces méthodes sont limitées aux situations ne faisant pas intervenir plus de 4 variables.

Un tel problème peut aussi être traîté en calculant le *radical réel* de l'idéal $\langle f \rangle \subset \mathbb{Q}[X_1, \ldots, X_n]$ (qui est l'idéal radical de $\mathbb{Q}[X_1, \ldots, X_n]$ dont la variété algébrique associée est la plus petite – pour l'ordre induit par l'inclusion – contenant $\mathcal{H} \cap \mathbb{R}^n$). La dimension du radical réel est alors la dimension réelle de $\mathcal{H} \cap \mathbb{R}^n$. Un tel idéal peut être calculé en utilisant les algorithmes donnés dans [25, 39]. Ces algorithmes font des études récursives de lieux singuliers imbriqués les uns dans les autres à l'instar des algorithmes donnés dans les paragraphes 5.3 et 5.4 du chapitre précédent. À notre connaissance, borner les degrés des lieux singuliers étudiés dans ces algorithmes conduit aussi à des quantités doublement exponentielle en le nombre de variables.

La dimension réelle de $\mathcal{H}$ peut être calculée en utilisant l'algorithme donné dans [21, Chapter 14]. La complexité de cet algorithme est $D^{\mathcal{O}(n^2)}$. Malheureursement, il utilise des méthodes de réduction similaire à celles vues dans le paragraphe 5.2 du chapitre précédent, si bien que la constante de complexité apparaissant ici en exposant est particulièrement élevée.

Toutes les méthodes mentionnées ci-dessus calculent exactement la dimension réelle de $\mathcal{H} \cap \mathbb{R}^n$ ce qui est une spécification de sortie plus forte que le problème qu'on cherche à résoudre. Dans le cas où f est sans facteurs carrés, le problème qu'on cherche à résoudre peut être traité en décidant si au moins un des ensembles semi-algébriques $\mathcal{S}_i \subset \mathbb{R}^n$ défini par $f = 0, \frac{\partial f}{\partial X_i} \neq 0$ (pour $i = 1, \ldots, n$) est non vide. Dans le paragraphe suivant on se dotera d'algorithmes permettant de décider du vide de tels ensembles semi-algébriques. Mais il faut noter ici que cette méthode fait dépendre la résolution du problème d'un facteur combinatoire qu'on voudrait pouvoir éviter. De plus, on verra que l'étude de chacun de ces ensembles semi-algébriques se réduit à l'étude de 2 ensembles algébriques réels.

Le résultat donné ci-dessous montre comment réduire le problème de déterminer l'existence de points réels réguliers dans une hypersurface définie par $f = 0$ au problème de décider si il existe un couple de points $(x, x') \in \mathbb{R}^n \times \mathbb{R}^n$ tels que $f(x) > 0$ et $f(x') < 0$. Les versions probabilistes de cet algorithme ont une complexité en $\mathcal{O}(n^7 D^{4n})$ opérations arithmétiques dans $\mathbb{Q}$.

Théorème 45. *Soit f un polynôme sans facteurs carrés dans $\mathbb{Q}[X_1, \ldots, X_n]$ et $\mathcal{H} \subset \mathbb{C}^n$ l'hypersurface définie par $f = 0$. Il existe des points réels réguliers dans $\mathcal{H}$ si et seulement si il existe $(x, x') \in \mathbb{R}^n \times \mathbb{R}^n$ tels que $f(x) > 0$ et $f(x') < 0$.*

L'Algorithme. L'algorithme qu'on obtient est évidemment fondé sur le théorème 45. Son entrée est un polynôme f de $\mathbb{Q}[X_1, \ldots, X_n]$ de degré D. On commence par calculer la partie square-free de f (qu'on continue de noter f ci-dessous).

Il nous faut alors déterminer le signe de f sur un point rationnel de $\mathbb{Q}^n$ choisi aléatoirement en lequel f ne s'annule pas.

Si f est évaluée négativement sur ce point, il faut alors décider du vide de l'ensemble semi-algébrique défini par $f > 0$ (sinon on doit évidemment décider du vide du semi-algébrique défini par $f < 0$). En utilisant l'algorithme probabiliste donné ci-dessus qui se base sur des calculs de valeurs critiques généralisées, ceci se fait en $\mathcal{O}(n^7 D^{4n})$ opérations arithmétiques dans $\mathbb{Q}$.

Ainsi, si on se dote de la routine suivante :

– `SamplingIneq` : qui prend en entrée un polynôme $f \in \mathbb{Q}[X_1, \ldots, X_n]$ et retourne une famille de paramétrisations rationnelles dont l'ensemble des solutions réelles a une intersection non vide avec chaque composante connexe du semi-algébrique défini par $f > 0$;

– `Real` : qui prend en entrée une paramétrisation rationnelle et retourne des approximations des racines réelles encodées par les paramétrisations données en entrée.

on obtient l'algorithme ci-dessous.

Algorithme : Décision de l'existence de points réels réguliers dans une hypersurface

– **Entrée :** Un polynôme $f \in \mathbb{Q}[X_1, \ldots, X_n]$
– **Sortie :** `true` si il existe des points réels réguliers dans l'hypersurface $\mathcal{H} \subset \mathbb{C}^n$ définie par $f = 0$, `false` sinon.

1. Choisir $p \in \mathbb{Q}^n$ aléatoirement.
2. Tant que $f(p) = 0$ retourner à l'étape précédente.
3. Si $f(p) < 0$ alors poser `Param`=`SamplingIneq`(f) et si $\cup_{\mathtt{P} \in \mathtt{Param}}$`Real`(`P`) est non vide retourner `true` sinon retourner `false`
4. Si $f(p) > 0$ alors poser `Param`=`SamplingIneq`(-f) et si $\cup_{\mathtt{P} \in \mathtt{Param}}$`Real`(`P`) est non vide retourner `true` sinon retourner `false`

En pratique, cet algorithme tire pleinement profit de l'efficacité de l'algorithme de calcul d'au moins un point par composante connexe d'un ensemble semi-algébrique défini par une inéaglité et qu'on a donné précédemment. Il a notamment permis de résoudre l'un des problèmes posés pour l'étude du diagramme de Voronoi de trois droites de l'espace (voir [48]).

6.4 Application au calcul d'un point par composante connexe dans un ensemble semi-algébrique sous des hypothèses de régularité

6.4.1 Préliminaires

On considère maintenant un ensemble semi-algébrique $\mathcal{S} \subset \mathbb{R}^n$ défini par le système :

$$f_1 = \cdots = f_s = 0, \quad g_1 > 0, \ldots, g_k > 0$$

où $(f_1, \ldots, f_s, g_1, \ldots, g_k)$ est une famille de polynômes de $\mathbb{Q}[X_1, \ldots, X_n]$ telle que :
– l'idéal engendré par $\langle f_1, \ldots, f_s \rangle$ est un idéal radical et équi-dimensionnel de dimension d ;
– la variété algébrique $V \subset \mathbb{C}^n$ définie par le système

$$f_1 = \cdots = f_s = 0$$

est lisse.

Dans [21], on trouve le résultat ci-dessous qui permet de réduire le calcul d'au moins un point par composante connexe de $\mathcal{S}$ au calcul d'au moins un point par composante connexe de varétés algébriques réelles définies par des systèmes d'équations polynomiales dans $\mathbb{Q}\langle\varepsilon\rangle[X_1, \ldots, X_n]$.

Proposition 32. *[21] En reprenant les notations ci-dessus, soit C une composante connexe de $\mathcal{S}$. Il existe une famille $\{i_1, \ldots, i_\ell\} \subset \{1, \ldots, k\}$ telle que la variété algébrique réelle définie par*

$$f_1 = \cdots = f_s = 0, \quad g_{i_1} - \varepsilon = \cdots = g_{i_\ell} - \varepsilon = 0$$

(où ε est un infinitésimal) ait une composante connexe incluse dans l'extension de C à $\mathbb{R}\langle\varepsilon\rangle^n$.

L'usage du résultat ci-dessus pose plusieurs problèmes :
– tout d'abord, comme on l'a vu dans le chapitre précédent, l'introduction d'un infinitésimal alourdit considérablement le coût de l'arithmétique : en effet, il faut alors mener les calculs dans $\mathbb{Q}(\varepsilon)$ ou $\mathbb{Q}\langle\varepsilon\rangle$;

– de plus, on n'a aucune garantie sur le fait que les variétés algébriques définies par les systèmes mentionnés ci-dessus soient lisses et que ces systèmes engendrent des idéaux équi-dimensionnels, or ce sont des cas auxquels on voudrait pouvoir se ramener car, comme on l'a vu dans le chapitre précédent, ils sont plus faciles à appréhender.

On préfère donc utiliser un résultat similaire au théorème 35 du chapitre précédent.

Théorème 46. *Soit $C \subset \mathbb{R}^n$ une composante connexe de l'ensemble semi-algébrique $\mathcal{S} \subset \mathbb{R}^n$ défini par :*

$$f_1 = \cdots = f_s = 0, \quad g_1 > 0, \ldots, g_k > 0$$

ε un infinitésimal et $a = (a_1, \ldots, a_s) \in \mathbb{Q}^s \setminus \{0\}$. Pour $\mathcal{I} = \{i_1, \ldots, i_\ell\} \subset \{1, \ldots, k\}$, on note $V^{\mathcal{I}}_{\varepsilon,a} \subset \mathbb{C}\langle\varepsilon\rangle^n$ la variété algébrique définie par

$$f_1 = \cdots = f_s = 0, \quad g_{i_1} - a_{i_1}\varepsilon = \cdots = g_{i_\ell} - a_{i_\ell}\varepsilon = 0.$$

et on suppose que $\langle f_1, \ldots, f_s\rangle$ est radical et équi-dimensionnel de dimension d et que la variété algébrique qui lui est associée est lisse.

Alors, il existe $\mathcal{I} = \{i_1, \ldots, i_\ell\} \subset \{1, \ldots, k\}$ et une composante connexe $C^{\mathcal{I}}_{\varepsilon,a}$ de $V^{\mathcal{I}}_{\varepsilon,a} \cap \mathbb{R}\langle\varepsilon\rangle^n$ tels que $C^{\mathcal{I}}_{\varepsilon,a}$ est incluse dans l'extension de C dans $\mathbb{R}\langle\varepsilon\rangle^n$.

De plus, il existe un fermé de Zariski $\mathcal{A} \subset \mathbb{C}^n$ tel que pour tout $a \in \mathbb{Q}^n \setminus \mathcal{A}$, $V^{\mathcal{I}}_{\varepsilon,a}$ est lisse, et l'idéal engendré par $f_1, \ldots, f_s, g_{i_1} - a_{i_1}\varepsilon, \ldots, g_{i_k} - a_{i_\ell}\varepsilon$ est soit radical équi-dimensionnel de dimension $n - d - \ell$ soit égale à $\langle 1\rangle$.

L'avantage de ce résultat est double :

– si d est la dimension de la variété algébrique définie par $f_1 = \cdots = f_s = 0$, il réduit le calcul d'au moins un point par composante connexe de $\mathcal{S}$ à l'étude de $\sum_{i=0}^{\min(d,k)} \binom{k}{i}$ systèmes d'équations polynomiales ;

– il permet l'usage des algorithmes efficaces de calcul d'au moins un point par composante connexe de variétés algébriques réelles *lisses*, ce qui est un cas plus facile à appréhender.

6.4.2 L'algorithme

Il nous faut néanmoins éviter d'introduire *explicitement* l'infinitésimal mentionné dans le résultat ci-dessus.

Pour cela, considérons-le comme une variable ainsi que la projection $\pi_\varepsilon : (x_1, \ldots, x_n, \varepsilon) \in \mathbb{C}^{n+1} \to \varepsilon$. D'après le théorème 46, il existe $\mathcal{I} \subset \{1, \ldots, k\}$ et $e_0 \in \mathbb{R}$ positif tel que pour tout $e \in]0, e_0[$, la variété algébrique réelle $V^{\mathcal{I}}_{e,a} \cap \mathbb{R}^n$ a une composante connexe incluse dans $\mathcal{S}$.

Dans ce cas, choisir e_0 suffisamment petit implique de :

– s'assurer que les composantes connexes de $V^{\mathcal{I}}_{e,a} \cap \mathbb{R}^n$ évoluent continument dans $]0, e_0[$ en fonction de e, pour cela il est suffisant d'assurer que π_ε réalise une fibration localement triviale sur $\pi_\varepsilon^{-1}(]0, e_0[) \cap V^{\mathcal{I}}_{e,a}$;

– s'assurer que si pour tout $e \in]0, \alpha[$ tel que $V^{\mathcal{I}}_{e,a} \cap \mathbb{R}^n$ contienne une composante connexe incluse dans $\mathcal{S}$ (c'est-à-dire telle que les polynômes g_j pour $j \in \{1, \ldots, s\}$ sont positifs en chaque point de cette composante), il en est de même pour toutes les variétés $V^{\mathcal{I}}_{e',a}$ pour tout $e' \in [\alpha, e_0[$.

Le premier point peut aisément être assuré dès lors qu'on dispose d'un algorithme efficace de valeurs critiques généralisées. C'est essentiellement l'apport du paragraphe 6.2 de ce chapitre. Une fois ce calcul effectué, il suffit d'isoler la plus petite racine réelle positive du polynôme définissant ces valeurs critiques généralisées et de choisir un rationnel e_1 compris entre 0 et la borne inférieure de cet intervalle d'isolation pour avoir un intervalle candidat $]0, e_1[$.

Le second point ne pose pas problème lui non plus. En effet, on peut démontrer que si il existe un intervalle $]0, e'[\subset]0, e_1[$ tel que pour tout $e \in]0, e'[$ il existe une composante connexe C_e de $V \cap \mathbb{R}^n$ incluse dans $\mathcal{S}$ et qu'il existe $e \geqslant e'$ tel que C_e contienne un point annulant g_j (pour au moins un $j \in \{1, \ldots, k\} \setminus \mathcal{I}$), alors il existe e'' tel que la variété algébrique réelle définie par :

$$f_1 = \cdots = f_s = 0, \quad \frac{g_{i_1}}{a_{i_1}} = \cdots = \frac{g_{i_\ell}}{a_{i_\ell}} = \frac{g_j}{a_j} = e''$$

contienne au moins une composante connexe incluse dans $\mathcal{S}$. Celle-ci sera donc détectée par l'étude de la variété algébrique réelle $V^{\mathcal{I}\cup\{j\}}_{\varepsilon,a}$.

L'intervalle candidat $]0, e_1[$ est donc le bon.

Ainsi, pour tout $\mathcal{I} \subset \{1, \ldots, k\}$, on calcule les valeurs critiques généralisées des restrictions de π_ε à $V^{\mathcal{I}}_{\varepsilon,a}$, on ramène notre étude à celles de variétés algébriques réelles définies par des systèmes d'équations polynomiales à coefficients dans $\mathbb{Q}$. Ces variétés étant lisses et équi-dimensionnelles et les idéaux engendrés par les systèmes les définissant étant radicaux, on peut utiliser sans aucun problème les algorithmes du paragraphe 6.2 du chapitre précédent.

Si on se dote des routines suivantes :

- `GeneralizedCriticalValues` : qui prend en entrée un système d'équations polynomiales et une variable X et retourne un polynôme univarié non nul dont l'ensemble des racines réelles contient l'ensemble des valeurs critiques généralisées de la projection sur X restreinte à la variété algébrique réelle définie par le système donné en entrée.
- `Sampling` : qui prend en entrée un système d'équations polynomiales et retourne une famille de paramétrisations rationnelles encodant au moins un point par composante connexe de la variété algébrique réelle définie par le système donné en entrée.
- `TestSign` : qui prend en entrée une paramétrisation rationnelle $\mathcal{P}$ et une liste L de polynômes et retourne une liste d'approximations numériques des points réels encodés par $\mathcal{P}$ en lesquels chaque polynôme de la liste L est positif.

on obtient l'algorithme ci-dessous.

Algorithme : Calcul d'au moins un point par composante connexe d'un semi-algébrique sous des hypothèses de régularité (Cas d'un système d'équations et d'inégalités polynomiales)

- **Entrée :** Un système d'équations et d'inégalités polynomiales $f_1 = \cdots = f_s = 0,\ g_1 > 0, \ldots, g_k > 0$ dans $\mathbb{Q}[X_1, \ldots, X_n]$ telle que $\langle f_1, \ldots, f_s \rangle$ engendre un idéal radical et équi-dimensionnel dont la variété algébrique associée est lisse.
- **Sortie :** Une famille de paramétrisations rationnelles encodant au moins un point par composante connexe de l'ensemble semi-algébrique défini par le système donné en entrée.

1. Choisir aléatoirement $\mathbf{A} \in GL_n(\mathbb{Q})$ et $a \in \mathbb{Q}^k$ et poser `sols` := [].
2. Pour tout $\mathcal{I} \subset \{1, \ldots, k\}$ faire
   (a) Construire le système F définissant $V^{\mathcal{I},\mathbf{A}}_{\varepsilon,a}$ où ε est vu comme une variable
   (b) Poser $P :=$ `GeneralizedCriticalValues`(F, ε)
   (c) Choisir $e \in \mathbb{Q}$ positif et plus petit que la plus petite valeur critique généralisée encodée par P.
   (d) Instantier ε à e dans F et affecter le résultat obtenu à F_e.
   (e) Poser `points` := `TestSign`(`Sampling`$(F_e), \{g_j, j \in \{1, \ldots, s\} \setminus \mathcal{I}$
   (f) Poser `sols` := `sols` $\cup$ `points`.
3. Retourner `sols`

Remarque. *Le cas où la variété algébrique $V \subset \mathbb{C}^n$ définie par*

$$f_1 = \cdots = f_s = 0$$

n'est pas équi-dimensionnelle ne pose pas de difficulté théorique. En effet, on peut toujours calculer une famille de bases de Gröbner engendrant des idéaux dont les variétés associées sont les composantes équi-

dimensionnelles de V. Il est alors possible d'utiliser l'algorithme précédent sur chacune des composantes équi-dimensionnelles.

Les problèmes pratiques posés par cette approche peuvent vite devenir inextricables. On souhaiterait pouvoir utiliser des techniques similaires à celles utilisées dans le paragraphe 5.5 du chapitre précédent pour gérer le passage au contexte non-équi-dimensionnel. Ceci ne peut être fait que si on dispose d'une caractérisation lagrangienne des valeurs critiques généralisées d'une application polynomiale restreinte à une variété algébrique non équi-dimensionnelle. Obtenir une telle caractérisation est l'objet d'un travail en cours.

6.4.3 Complexité et performances pratiques

On peut maintenant donner la complexité des versions probabilistes de l'algorithme décrit ci-dessus lorsque la routine d'élimination algébrique utilisée est l'algorithme de résolution géométrique. L'entrée de l'algorithme est un système d'équations et d'inégalités polynomiales

$$f_1 = \cdots = f_s = 0, \quad g_1 > 0, \ldots, g_k > 0$$

et on notera $\mathcal{L}$ la longueur d'un programme d'évaluation de la famille $(f_1, \ldots, f_s, g_1, \ldots, g_k)$.

Si d est la dimension de la variété algébrique $V \subset \mathbb{C}^n$ définie par :

$$f_1 = \cdots = f_s = 0$$

on peut (grâce au théorème 46) borner le nombre de variétés algébriques V (où $\mathcal{I} \subset \{1, \ldots, k\}$) à étudier par $\sum_{\ell=0}^{\min(d,k)} \binom{k}{\ell}$.

Pour chacune variété agébrique V, on doit :

- calculer les valeurs critiques généralisées de la projection sur ε restreinte à V, la complexité de cette étape est donnée par le théorème 42 ;
- choisir un rationnel compris entre 0 et la plus petite de ces valeurs, la complexité de cette étape n'influe pas sur la complexité globale de l'algorithme ;
- calculer au moins un point par composante de $V_{e,a}^{\mathcal{I}} \cap \mathbb{R}^n$, la complexité de cette étape est donnée par le théorème 29.
- déterminer le signe des g_j (pour $j \in \{1, \ldots, k\} \backslash \mathcal{I}$) en les points réels encodés par les paramètrisations rationnelles fournies par l'étape précédente, la complexité de cette étape n'influe pas sur la compexité globale de l'algorithme.

Cette discussion permet donc d'énoncer le résultat ci-dessous.

Théorème 47. *Soit $\mathcal{S} \subset \mathbb{R}^n$ un ensemble semi-algébrique défini par*

$$f_1 = \cdots = f_s = 0, \quad g_1 > 0, \ldots, g_k > 0$$

où $(f_1, \ldots, f_s, g_1, \ldots, g_k)$ sont des polynômes de $\mathbb{Q}[X_1, \ldots, X_n]$ de degré borné par D. Soit $\mathcal{L}$ la longueur d'un programme d'évaluation de $(f_1, \ldots, f_s, g_1, \ldots, g_k)$.

Si la variété algébrique définie par $f_1 = \cdots = f_s = 0$ est lisse et que l'idéal $\langle f_1, \ldots, f_s \rangle$ est radical et équi-dimensionnel de dimension d, l'algorithme ci-dessus calcule au moins un point par composante connexe de $\mathcal{S}$ en

$$\mathcal{O}(n^7 (n-d)^{4d} D^{4n})$$

opérations arithmétiques dans $\mathbb{Q}$.

Implantations et performances pratiques. De premières implantations de cet algorithme utilisant les bases de Gröbner comme routine d'élimination algébrique ont été effectuées. Bien évidemment, l'usage des bases de Gröbner permet d'obtenir des versions déterministes de l'algorithme qu'on vient de décrire.

Cet algorithme tirant profit de l'efficacité des algorithmes donnés dans le chapitre précédent sur les problèmes de plus de 4 variables, cette première implantation a d'ores et déjà permis de résoudre des applications inaccessibles à l'algorithme de décomposition cylindrique algébrique. Ceci dit, il apparaît que diverses stratégies peuvent être employées (dans l'ordre d'étude des familles $\mathcal{I}$) et donnent des résultats pratiques sensiblement différents : sur certains problèmes certaines sont plutôt lentes devant d'autres et le rapport d'inverse sur d'autres probèmes. Il reste encore un certain nombre de choses à comprendre et/ou un travail d'implantation à effectuer avant d'arriver à des résultats pratiques satisfaisants.

6.5 Notes bibliographiques et commentaires

Le calcul d'au moins un point par composante connexe d'un ensemble semi-algébrique défini par un système d'équations et d'inégalités polynomiales par déformation pour ensuite appliquer les méthodes de points critiques apparaît sous différentes formes dans [65, 69, 70, 114, 17, 18, 19]. Ces algorithmes n'ont en général aucune restriction sur l'entrée contrairement à celui du paragraphe 6.4 de ce chapitre. Ils souffrent néanmoins de constantes de complexité situées en exposant particulièrement élevées et sont inutilisables en pratique.

Les valeurs critiques généralisées sont initialement introduites dans [82, 74, 75]. Ces travaux fournissent les premiers algorithmes permettant leur calcul via des idéaux d'élimination (l'un de ces algorithmes est évoqué dans le paragraphe 6.1). La taille des données intermédiaires est particulièrement élevée devant la taille de la sortie, si bien que ces algorithmes sont très peu efficaces.

L'idée d'utiliser des propriétés de propreté pour ramener le calcul de valeurs critiques asymptotiques d'une application polynomiale pour ramener leur calcul à celui du lieu de non-propreté d'une projection restreinte à une courbe critique apparaît initialement dans [129] et est développée dans [131]. On y trouve les algorithmes et estimations de complexité donnés dans le paragraphe 6.1. L'algorithme de calcul d'au moins un point par composante connexe d'un ensemble semi-algébrique défini par une seule inégalité ou une seule inéquation du paragraphe 6.3, ainsi que son application à la détermination de l'existence de points réels réguliers dans un ensemble algébrique défini par une seule équation apparaissent aussi dans [131].

Ce chapitre n'aborde pas le calcul d'au moins un point par composante connexe d'un ensemble semi-algébrique défini par un système d'équations et d'inégalités (non strictes) polynomiales

$$f_1 = \cdots = f_s = 0, g_1 \geqslant 0, \ldots, g_k \geqslant 0$$

Ce problème se ramène en fait directement à l'étude des variétés algébriques réelles définies par

$$f_1 = \cdots = f_s = g_{i_1} = \cdots = g_{i_\ell} = 0$$

pour tout $\mathcal{I} = \{i_1, \ldots, i_\ell\} \subset \{1, \ldots, s\}$ (voir [21, Chapitre 13]). Une étude de ce problème et son application à un problème de reconnaissance de forme figurent aussi dans [91].

Enfin, le calcul de valeurs critiques généralisées d'une application polynomiale restreinte à une variété algébrique lisse peut être utilisé pour éviter les choix de projection générique (et/ou vérifier que les choix de projection sont suffisamment génériques) dans les algorithmes du paragraphe 5.5 du chapitre précédent. En effet, ces algorithmes sont fondés sur le fait que les composantes connexes des variétés choisies ont une image fermée (pour la topologie euclidienne) par les projections choisies. Si ce n'est pas le cas, les extrêmités de ces intervalles sont fatalement des valeurs critiques asymptotiques (puisque dans ce cas, on ne peut pas avoir fibration localement triviale autour ces extrêmités). Un calcul de valeur critique asymptotique permet de récupérer ces valeurs et il suffit alors de considérer des fibres au-dessus de rationnels choisis entre chacune des valeurs critiques asymptotiques calculées.

Références

[1] ALDOR. http ://www.aldor.org/.

[2] Axiom. http ://wiki.axiom-developer.org/FrontPage.

[3] MAGMA. http ://magma.maths.usyd.edu.au/.

[4] Maple. http ://www.maplesoft.org/.

[5] Mathematica. http ://www.wolfram.com/.

[6] Reduce. http ://www.uni-koeln.de/REDUCE/.

[7] Singular. http ://www.singular.uni-kl.de/.

[8] M. E. Alonso, E. Becker, M.-F. Roy, and T. Wörmann. Zeroes, multiplicities and idempotents for zerodimensional systems. In *Proceedings MEGA'94*, volume 142 of *Progress in Mathematics*, pages 1–15. Birkhäuser, 1996.

[9] P. Aubry. *Ensembles triangulaires de polynômes et résolution de systèmes algébriques*. PhD thesis, Université Paris 6, 1999.

[10] P. Aubry, D. Lazard, and M. Moreno Maza. On the theories of triangular sets. *Journal of Symbolic Computation, Special Issue on Polynomial Elimination*, 28 :105–124, 1999.

[11] P. Aubry, F. Rouillier, and M. Safey El Din. Real solving for positive dimensional systems. *Journal of Symbolic Computation*, 34(6) :543–560, 2002.

[12] B. Bank, M. Giusti, J. Heintz, and G.-M. Mbakop. Polar varieties and efficient real equation solving : the hypersurface case. *Journal of Complexity*, 13(1) :5–27, 1997.

[13] B. Bank, M. Giusti, J. Heintz, and G.-M. Mbakop. Polar varieties and efficient real elimination. *Mathematische Zeitschrift*, 238(1) :115–144, 2001.

[14] B. Bank, M. Giusti, J. Heintz, and L.-M. Pardo. Generalized polar varieties and efficient real elimination procedure. *Kybernetika*, 40(5) :519–550, 2004.

[15] B. Bank, M. Giusti, J. Heintz, and L.-M. Pardo. Generalized polar varieties : Geometry and algorithms. *to appear in Journal of complexity*, 2005.

[16] M. Bardet, J.-C. Faugère, and B. Salvy. Asymptotic behaviour of the index of regularity of semi-regular quadratic polynomial systems. In *Proceedings of the8th MEGA (Effective Methods in Algebraic Geometry)*, 2005.

[17] S. Basu. *Algorithms in semi-algebraic geometry*. PhD thesis, New-York University, 1996.

[18] S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *Journal of ACM*, 43(6) :1002–1045, 1996.

[19] S. Basu, R. Pollack, and M.-F. Roy. A new algorithm to find a point in every cell defined by a family of polynomials. In *Quantifier elimination and cylindrical algebraic decomposition*. Springer-Verlag, 1998.

[20] S. Basu, R. Pollack, and M-F Roy. Computing roadmaps of semi-algebraic sets on a variety. *Journal of the AMS*, 3(1) :55–82, 1999.

[21] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry*. Springer-Verlag, 2003.

[22] W. Baur and V. Strassen. The complexity of partial derivatives. *Theoret. Comput. Science*, 22 :317–330, 1982.

[23] D. Bayer and M. Stillman. On the complexity of computing syzygies. *Journal of Symbolic Computation*, 6 :135–147, 1988.

[24] E. Becker, M. G. Marinari, T Mora, and C. Traverso. The shape of the Shape Lemma. In *Proceedings of ISSAC'94*, pages 129–133. ACM Press, 1994.

[25] E. Becker and R. Neuhaus. Computation of real radicals for polynomial ideals. In *Computational Algebraic Geometry*, volume 109 of *Progress in Mathematics*, pages 1–20, 1993.

[26] E. Becker and V. Weipsfenning. *Grœbner bases : a computational approach to commutative algebra*. Graduate Texts in Mathematics : readings in Mathematics. Springer-Verlag, 1993.

[27] E. Becker and T. Wörmann. Radical computations of zero-dimensional ideals and real root counting. *Mathematics and Computers in Simulation*, 1994.

[28] R. Benedetti and J.-J. Risler. *Real algebraic and semi-algebraic sets*. Hermann, 1990.

[29] J. Bochnak, M. Coste, and M.-F. Roy. *Real algebraic Geometry*. Ergebnisse der Mathematik und ihrer Grenzgebite. Springer-Verlag, 1998.

[30] J.D. Boissonnat and M. Yvinnec. *Algorithmic geometry*. Cambridge University Press, 1998.

[31] A. Bostan, B. Salvy, and E. Schost. Fast algorithms for zero-dimensional polynomial systems using duality. *Applicable Algebra in Engineering, Communication and Computing*, 14(4) :239–272, 2003.

[32] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, University of Innsbruck, 1965.

[33] B. Buchberger. Gröbner bases : An algoritmic method in polynomial ideal theory. In *Multidimensional System Theory*, pages 374–383. Reidel, Dordrecht, 1985.

[34] J. Canny. *The complexity of robot motion planning*. MIT Press, 1987.

[35] J. Canny. Some algebraic and geometric problems in pspace. In *Proceedings STOC*, pages 460–467, 1988.

[36] J. Canny. Computing roadmaps in general semi-algebraic sets. *The Computer Journal*, 1993.

[37] A.L. Chistov and D.Y. Grigoriev. Polynomial factoring of multivariate polynomials over a global field. Technical report, LOMI pre-print, Steklov Institute, 1982.

[38] G. E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. *Lecture notes in computer science*, 33 :515–532, 1975.

[39] P. Conti and C. Traverso. Algorithms for the real radical. Unpublished manuscript.

[40] S. Corvez and F. Rouillier. Using computer algebra tools to classify serial manipulators. In F. Winkler, editor, *Automated Deduction in Geometry*, volume 2930 of *Lecture Notes in Artificial Intelligence*, pages 31–43. Springer, 2003.

[41] M. Coste. Introduction à la géométrie semi-algébrique. Polycopié, Institut de Recherche Mathématique de Rennes.

[42] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties and algorithms : an introduction to computational algebraic geometry and commutative algebra*. Springer-Verlag, 1992.

[43] X. Dahan and E. Schost. Sharp estimates for triangular sets. In *Proceedings of ISSAC'04*. ACM Press, 2004.

[44] J. Della Dora, C. Dicrescenzo, and D. Duval. About a new method method for computing in algebraic number fields. In *Proceedings of EUROCAL 85*, volume 204 of *Lecture Notes of Computer Science*, pages 289–290. Springer-Verlag, 1985.

[45] L. Dupont, D. Lazard, S. Lazard, and S. Petitjean. Near-optimal parameterization of the intersection of quadrics : I. The generic algorithm. Technical Report 5667, INRIA, September 2005.

[46] L. Dupont, D. Lazard, S. Lazard, and S. Petitjean. Near-optimal parameterization of the intersection of quadrics : II. A classification of pencils. Technical Report 5668, INRIA, September 2005.

[47] J. El Omri and P. Wenger. Changing posture for cuspidal robot manipulators. In *Proceeding of the 1996 IEEE Int. Conf on Robotics and Automation*, pages 3173–3178, 1996.

[48] H. Everett, D. Lazard, S. Lazard, and Safey El Din M. The Voronoi diagram of three lines in $\mathbf{R}^3$. In *submitted to Symposium on Computational Geometry*, 2007.

[49] J.-C. Faugère. Gb/FGb. available at `http ://fgbrs.lip6.fr`.

[50] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F4).-. *Journal of Pure and Applied Algebra*, 139(1–3) :61–88, 1999.

[51] J.-C. Faugère. A new efficient algorithm for computing Gröbner without reduction to zero (F5). In *Proceedings of ISSAC 2002*, pages 75 – 83. ACM Press, 2002.

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

[53] W. Fulton. *Intersection theory*, volume 2 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, second edition, 1998.

[54] G. Gallo and B. Mishra. Efficient algorithms and bounds for wu-ritt characteristic sets. In *Proceedings MEGA'90*. Birkhaüser, 1990.

[55] P. Gianni and T. Mora. Algebraic solution of systems of polynomial equations using gröbner bases. In *Proceedings of AAECC*, volume 356 of *Lecture Notes in Computer Science*, pages 247–257. 247-257, 1989.

[56] M. Giusti. Complexity of standard bases in projective dimension zero. In *Proceedings of EUROCAL 87*, volume 378 of *Lecture Notes in Computer Science*, pages 333–335, 1989.

[57] M. Giusti, K. Hägele, J. Heintz, J.-E Morais, J.-L. Montaña, and L.-M. Pardo. Lower bounds for Diophantine approximation. In *Proceedings of MEGA'96*, number 117, 118 in Journal of Pure and Applied Algebra, pages 277–317, 1997.

[58] M. Giusti and J. Heintz. La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial. In *Computational Algebraic Geometry and Commutative Algebra*, volume XXXIV of *Symposia Matematica*, pages 216–256. Cambridge University Press, 1993.

[59] M. Giusti, J. Heintz, J.-E. Morais, J. Morgenstern, and L.-M. Pardo. Straight-line programs in geometric elimination theory. *Journal of Pure and Applied Algebra*, 124 :101–146, 1998.

[60] M. Giusti, J. Heintz, J.-E. Morais, and L.-M. Pardo. When polynomial equation systems can be solved fast ? In *Proceedings of AAECC-11*, volume 948 of *LNCS*, pages 205–231. Springer, 1995.

[61] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. *Journal of Complexity*, 17(1) :154–211, 2001.

[62] L. Gonzalez-Vega. Applying quantifier elimination to the Birkhoff interpolation problem. *Journal of Symbolic Computation*, 1996.

[63] D. Grigoriev and D. De Klerk, E. Pasechnik. Finding optimum subject to few quadratic constraints in polynomial time. In *Proceedings of MEGA'2003*, 2003.

[64] D. Grigoriev and D. Pasechnik. Polynomial time computing over quadratic maps i. sampling in real algebraic sets. *Computational complexity*, 14 :20–52, 2005.

[65] D. Grigoriev and N. Vorobjov. Solving systems of polynomials inequalities in subexponential time. *Journal of Symbolic Computation*, 5 :37–64, 1988.

[66] W. Habicht. Eine Verallgemeinrung des Sturmschen Wurzelzählverfahrens. *Comm. Math. Helvetici*, 21 :99–116, 1948.

[67] A. Hashemi and D. Lazard. Complexity of zero-dimensional gröbner bases. *Submitted to Journal of Symbolic Computation.*, 2006.

[68] J. Heintz, G. Jerónimo, J. Sabia, J. San Martin, and P. Solerno. Intersection theory and deformation algorithm. the multi-homogeneous case. Manuscript, 2002.

[69] J. Heintz, M.-F. Roy, and P. Solernò. On the complexity of semi-algebraic sets. In *Proceedings IFIP'89 San Francisco, North-Holland*, 1989.

[70] J. Heintz, M.-F. Roy, and P. Solernò. On the theoretical and practical complexity of the existential theory of the reals. *The Computer Journal*, 36(5) :427–431, 1993.

[71] E. Hubert. Notes on triangular sets and triangulation-decomposition algorithms. I. Polynomial systems. In *Symbolic and numerical scientific computation (Hagenberg, 2001)*, volume 2630 of *Lecture Notes in Comput. Sci.*, pages 1–39. Springer, Berlin, 2003.

[72] E. Hubert. Notes on triangular sets and triangulation-decomposition algorithms. II. Differential systems. In *Symbolic and numerical scientific computation (Hagenberg, 2001)*, volume 2630 of *Lecture Notes in Comput. Sci.*, pages 40–87. Springer, Berlin, 2003.

[73] Z. Jelonek. Testing sets for properness of polynomial mappings. *Mathematische Annalen*, 315(1) :1–35, 1999.

[74] Z. Jelonek and K. Kurdyka. On asymptotic critical values of a complex polynomial. *J. Reine Angew. Math.*, 565 :1–11, 2003.

[75] Z. Jelonek and K. Kurdyka. Quantitative generalized Bertini-Sard theorem for smooth affine varieties. *Discrete Comput. Geom.*, 34(4) :659–678, 2005.

[76] M. Kalkbrener. *Three contributions to elimination theory.* PhD thesis, Kepler University, 1991.

[77] M. Kalkbrener. *Three contributions to elimination theory.* PhD thesis, Kepler University, Linz, 1991.

[78] H. Kobayashi, S. Moritsugu, and R. W. Hogan. On solving systems of algebraic equations. In *Proceedings of ISSAC 99*, volume 358 of *Lecture Notes in Computer Science*, pages 139–149. Springer-Verlag, 1988.

[79] V. Koltun and M. Sharir. Three dimensional euclidean voronoi diagrams of lines with a fixed *SIAM J. Comput.*, 32(3) :616–642, 2003.

[80] L. Kronecker. Zur Theorie der Elimination einer Variabeln aus zwei algebraischen Gleichung. *Monatsberichte der Kǿniglich Preussischen Akademie der Wissenschaften*, pages 535–600, 1881.

[81] L. Kronecker. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. *Journal für die Reine une Angewandte Mathematik*, 92 :1–122, 1882.

[82] K. Kurdyka, P. Orro, and S. Simon. Semialgebraic sard theorem for generalized critical value. *Journal of differential geometry*, 56(1) :67–92, 2000.

[83] Y. N. Lakshmann. A single exponential bound of the complexity of computing Gröbner bases of zero-dimensional ideals. In C. Traverso T. Mora, editor, *Proc. Effective Methods in Algebraic Geometry, MEGA'90*, volume 94 of *Progress in Mathematics*, pages 227–234. Birkhaüser, 1991.

[84] Y.N. Lakshmann and D. Lazard. On the complexity of zero-dimensional algebraic systems. In *Effective methods in algebraic geometry*, volume 94 of *Progress in Mathematics*, pages 217–225. Birkhaüser, 1991.

[85] J.-B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM Journal on Optimization*, 11(3) :796–817, 2001.

[86] D. Lazard. Gaussian elimination and resolution of systems of algebraic equations. volume 162 of *Lecture Notes in Computer Science*, pages 146–157. Springer-Verlag, 1983.

[87] D. Lazard. A new method for solving algebraic systems of positive dimension. *Disc. Appl. Math.*, 33 :147–160, 1991.

[88] D. Lazard. Solving zero-dimensional algebraic systems. *Journal of Symbolic Computation*, 13 :117–133, 1992.

[89] D. Lazard and F. Rouillier. Solving parametric polynomial systems. *to appear in Journal of Symbolic Computation*, 2007.

[90] D. Lazard and F. Rouillier. Solving parametric polynomial systems. *Journal of Symbolic Computation*, to appear.

[91] C. Le Guernic, F. Rouillier, and M. Safey El Din. On the practical computation of one point in each connected component of a semi-algebraic set defined by a polynomial system of equations and non-strict inequalities. In L. Gonzalez-Vega and T. Recio, editors, *Proceedings of EACA'04 Conference*, 2004.

[92] G. Lecerf. `Kronecker` magma package for solving polynomial systems by means of geometric resolutions. available at `http ://www.math.uvsq.fr/ lecerf/software/`.

[93] G. Lecerf. *Une alternative aux méthodes de réécriture pour la résolution des systèmes algébriques.* PhD thesis, École polytechnique, 2001.

[94] G. Lecerf. Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers. *Journal of Complexity*, 19(4) :564–596, 2003.

[95] F. Lemaire. *Contribution à l'algorithmique en algèbre différentielle.* PhD thesis, Université des Sciences et Technologies de Lille, 2002.

[96] T. Lickteig and M-F Roy. Cauchy index computation. *Calcolo*, 33, 1996.

[97] H. Lombardi, M.-F. Roy, and M. Safey El Din. New structure theorems for subresultants. *Journal of symbolic computation*, 29(4) :663–690, 2000.

[98] R. Loos. Generalized polynomial remainder sequence. In R. Loos B. Buchberger, G.-E. Collins, editor, *Computer Algebra, Symbolic and Algebraic Computation*. Springer-Verlag, 1988.

[99] F.S. Macaulay. On some formulas in elimination. In *Proc. London Math. Soc.*, volume 3, 1902.

[100] F.S. Macaulay. *The Algebraic Theory of Modular Systems*. Cambridge University Press, 1916.

[101] F.S. Macaulay. Some properties of enumeration in the theory of modular systems. In *Proc. London Math. Soc.*, volume 26, 1927.

[102] E. Mayr and A. Meyer. The complexity of the word problem for commutative semi-groups and polynomial ideals. *Advance in Mathematics*, 46(127) :305–329, 1982.

[103] S. Mc Callum. *An improved projection operator for Cylindrical Algebraic Decomposition*. PhD thesis, University of Wisconsin-Madison, 1984.

[104] M. Mezzarobba and M. Safey El Din. Computing roadmaps in smooth real algebraic sets. In J.-G. Dumas, editor, *Proceedings of Transgressive Computing 2006*, pages 327–338, 2006. isbn : 84-689-8381-0.

[105] M. Moreno Maza. *Calculs de pgcd au-dessus des tours d'extensions simples et résolution des systèmes d'équations algébriques*. PhD thesis, Université Paris 6, 1997.

[106] A. Mosig. *Efficient algorithms for shape and pattern matching*. PhD thesis, Bonn University, to appear, 2004.

[107] A. Mosig and M. Clausen. Approximately matching polygonal curves with respect to the fréchet distance. *submitted to Computational Geometry – Theory and Applications*, 2004.

[108] B. Mourrain and P. Trébuchet. Generalized normal forms and polynomial system solving. In M. Krauers, editor, *International Symposium on Symbolic and Algebraic Computation*, pages 253–260. ACM Press, 2005.

[109] R. Narasimham. *Introduction to the theory of analytic spaces*. Springer-Verlag, 1966.

[110] L.M. Pardo. How lower and upper complexity bounds meet in elimination theory. In *Proceedings of AAECC*, volume 948 of *Lecture Notes in Computer Science*, pages 33–69. Springer-Verlag, 1995.

[111] P. A. Parillo. Semi-definite relaxations for semi-algebraic problems., 2001.

[112] G. Rémond. Élimination multihomogène. In *Introduction to algebraic independence theory*, volume 1752 of *Lecture Notes in Math.*, pages 53–81. Springer, Berlin, 2001.

[113] G. Rémond. Géométrie diophantienne multiprojective. In *Introduction to algebraic independence theory*, volume 1752 of *Lecture Notes in Math.*, pages 95–131. Springer, Berlin, 2001.

[114] J. Renegar. On the computational complexity and geometry of the first order theory of the reals. *Journal of Symbolic Computation*, 13(3) :255–352, 1992.

[115] B. Reznick. Some concrete aspects of hilbert's 17-th problem, 1999. Preprint available at `http ://www.math.uiuc.edu/Reports/reznick/98-002.html`.

[116] R. Rioboo. *Quelques aspects du calcul exact avec les nombres réels*. PhD thesis, University Pierre et Marie Curie (Paris 6), 1992.

[117] R. Rioboo. Towards faster real algebraic numbers. In *Proceedings of ISSAC 2002*, pages 221–228. ACM Press, 2002.

[118] J.F. Ritt. Differential equations from an algebraic standpoint. 1932.

[119] J.F. Ritt. *Differential Algebra*. Dover Publications, 1966.

[120] F. Rouillier. RS, RealSolving. available at `http ://fgbrs.lip6.fr`.

[121] F. Rouillier. *Algorithmes efficaces pour l'étude des zéros réels des systèmes polynomiaux*. PhD thesis, Université de Rennes I, 1996.

[122] F. Rouillier. Solving zero-dimensional systems through the Rational Univariate Representation. *AAECC Journal*, 9(5) :433–461, 1999.

[123] F. Rouillier. On solving zero-dimensional systems with rational coefficients. *submitted to Journal of Symbolic Computation*, 2005.

[124] F. Rouillier, M.-F. Roy, and M. Safey El Din. Finding at least one point in each connected component of a real algebraic set defined by a single equation. *Journal of Complexity*, 16 :716–750, 2000.

[125] F. Rouillier, M. Safey El Din, and É. Schost. Solving the birkhoff interpolation problem via the critical point method : an experimental study. In *Proceedings of ADG'2000*, 2000.

[126] F. Rouillier and P. Zimmermann. Efficient isolation of polynomial real roots. *Journal of Computational and Applied Mathematics*, 162(1) :33–50, 2003.

[127] M. Safey El Din. *Résolution réelle des systèmes polynomiaux de dimension positive*. PhD thesis, Université Paris 6, January 2001.

[128] M. Safey El Din. RAGLib (Real Algebraic Geometry Library), Maple package. available at `http ://www-calfor.lip6.fr/~safey/RAGLib`, 2003.

[129] M. Safey El Din. Generalized critical values and solving polynomial inequalities. In *Proceedings of ICPSS, Extended abstract*. Paris 6 University, 2004.

[130] M. Safey El Din. Finding sampling points on real hypersurfaces in easier in singular situations. In *MEGA (Effective Methods in Algebraic Geometry) Electronic proceedings*, 2005.

[131] M. Safey El Din. Generalized critical values and testing sign conditions on a polynomial. In D. Wang and Z. Zheng, editors, *Proceedings of International Conference on Mathematical Aspects of Computer and Information Sciences*, pages 61–84, 2006.

[132] M. Safey El Din and É. Schost. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. In *Proceedings of the 2003 international symposium on Symbolic and algebraic computation*, pages 224–231. ACM Press, 2003.

[133] M. Safey El Din and É. Schost. Properness defects of projections and computation of one point in each connected component of a real algebraic set. *Journal of Discrete and Computational Geometry*, 2004.

[134] M. Safey El Din and P. Trébuchet. Strong bi-homogeneous Bézout theorem and its use in effective real algebraic geometry. *in preparation*, 2005.

[135] E. Schost. Degree bounds and lifting techniques for triangular sets. In *Proceedings of ISSAC'02*, pages 238–245. ACM Press, 2002.

[136] É. Schost. Computing parametric geometric resolutions. *Journal of Applicable Algebra in Engineering, Communication and Computing 13(5) : 349 - 393, 2003*, 13(5) :349–393, 2003.

[137] C. Segre. Studio sulle quadriche in uno spazio lineare ad un numero qualunque di dimensioni. *Mem. della R. Acc. delle Scienze di Torino*, 36(2) :3–86, 1883.

[138] A. Seidenberg. A new decision method for elementary algebra. *Annals of Mathematics*, 60 :365–374, 1954.

[139] I. Shafarevich. *Basic Algebraic Geometry 1*. Springer Verlag, 1977.

[140] C. Sturm. Mémoire sur la résolution des équations numériques. *Inst. France Sc. Math. Phys.*, 6, 1835.

[141] A. Tarski. *A decision method for elementary algebra and geometry*. University of California Press, 1951.

[142] C. Traverso. Gröbner trace algorithms. In *Proceedings of ISSAC'88*, volume 358 of *Lecture Notes in Computer Science*, pages 125–138. Springer-Verlag, 1988.

[143] C. Traverso. Hilbert functions and the Buchberger algorithm. *Journal of Symbolic Computation*, 22 :355–376, 1996.

[144] P. Trébuchet. Generalized normal forms for positive dimensional ideals. In *Proceedings of the1st International Conference on Polynomial System Solving*, 2004.

[145] J. Uspensky. *Theory of equations*. Mc Graw-Hill, 1948.

[146] B.-L. van der Waerden. On hilbert's function, series of composition of ideals and a generalization of a theorem of bezout. In *Proc. Roy. Acad. Amsterdam*, volume 31, pages 749–770, 1929.

[147] B.L. Van der Waerden. *Moderne Algebra I.* 1930.

[148] M. Vincent. Sur la résolution des équations numériques. *Journal de Mathématiques pures et appliquées*, pages 341–372, 1836.

[149] D. Wang. CharSets, a Maple library devoted to triangular decomposition. downloadable at `http ://www-spiral.lip6.fr/~wang`.

[150] D. Wang. An elimination method for polynomial systems. *J. Symb. Comp.*, 16 :83–114, 1993.

[151] D. Wang. *Elimination Methods*. Springer Verlag, 2001.

[152] W.T. Wu. On zeros of algebraic equations – an application of Ritt principle. *Kexue Tongbao*, 31 :1–5, 1986.