UPMC
PARIS UNIVERSITAS

THÈSE DE DOCTORAT DE L'UNIVERSITÉ PIERRE ET MARIE CURIE

Spécialités
informatique et mathématiques

(École doctorale d'informatique, télécommunications et électronique)

Présentée par

M. Guillaume Moroz

pour obtenir le titre de

DOCTEUR de l'UNIVERSITÉ PIERRE ET MARIE CURIE

Sujet de thèse :

Sur la décomposition réelle et algébrique des systèmes dépendant de paramètres

soutenue le 9 décembre 2008

devant le jury composé de :

Directeur de thèse :	M. Fabrice ROUILLIER	-	INRIA
Rapporteurs :	M. Hoon HONG	-	North Carolina State University
	M. Kazuhiro YOKOYAMA	-	Rikkyo University
Examinateurs :	Mme Marie-Françoise Roy	-	Université de Rennes 1
	M. Daniel Lazard	-	Université Pierre et Marie Curie
	M. Damien Chablat	-	IRCCyN
	M. Philippe WENGER	-	IRCCyN

Table des matières

Résumé

Cette thèse traite des systèmes paramétrés. Ils modélisent de nombreuses applications apparaissant dans divers domaines, comme la robotique ou la calibration. Soit S un système d'équations et d'inéquations polynomiales dépendant de paramètres. Nous abordons le problème de décrire l'ensemble des ouverts connexes U de l'espace des paramètres tels que S restreint à U admet un nombre constant de solutions réelles.

En robotique, notre avons pu détecter les positions cuspidales, importantes pour la planification de trajectoire des robots parallèles 3-RPR dans le plan. En calibration photographique, nous avons pu décrire le nombre de solutions physiquement réalisables du problème Perspective-3- Points.

D'un point de vue théorique, nous analysons le problème du calcul de la variété discriminante d'un système paramétré. Sous certaines hypothèses,nous montrons que le calcul de la variété discriminante peut se réduire à un calcul de projection. En particulier, nous présentons un algorithme polynomial en espace pour la calculer.

Dans le cas des systèmes d'équations polynomiales quelconques, nous in- troduisons les décompositions régulières, où chaque composante est représentée par une suite régulière en dehors d'une hypersurface. Notre algorithme est basé sur la saturation d'idéal et possède de bonnes performances en pratique. Cette représentation permet en outre, dans le cadre des systèmes paramétrés, de diminuer la combinatoire liée au calcul de lieux critiques pour la discrimination des paramètres. Par ailleurs, nous déduisons de ces travaux un nouvel algorithme pour le calcul du radical d'un idéal.

Summary

This thesis deals with parametric systems. They appear is many applications, such as robotics or camera calibration. Let S be a parametric system of polynomial equations and inequalities. We study the problem of describing the open connected sets U of the parameters' space such that S restricted to U has a constant number of real solutions.

In robotics, we describe the cuspidal configurations of planar parallel robots, important for path planing. In camera calibration, we detect explicitly the number of solutions to the Perspective-3-Points problem physically achievable.

From a theoretical point of view, we analyse the problem of computing the discriminant variety of a parametric system. Under some assumptions, we show that a discriminant variety computation can be reduced to a projection computation. In particular, we present a polynomial space algorithm to compute it.

In the case of a general polynomial system, we introduce the regular decompositions, where each component is represented by a sequence of polynomials regular outside a hypersurface. To compute such decompositions, our algorithm uses mainly the saturation of polynomial ideals and seems efficient in practice. In the case of parametric systems, this representation allows us to decrease a combinatorial factors that appears in the computation of the discriminant variety. Beside, we deduce from this work a new algorithm to compute the radical of a polynomial ideal.

Remerciements

En premier lieu, je tiens à exprimer toute ma gratitude envers Fabrice Rouillier qui m'a fait découvrir le calcul formel, et a encadré ma thèse. Son enthousiasme, ses idées et sa rigueur ont été un moteur essentiel dans mon travail.

Je tiens aussi à remercier Daniel Lazard, qui a toujours pris le temps de répondre aux nombreuses questions que je lui ai soumises. Chacune de ses réponses a été autant d'exposés passionnants. Je le remercie aussi d'avoir accepté de faire partie de mon jury de thèse.

Je remercie chaleureusement Hoon Hong et Kazuhiro Yokoyama qui m'ont fait l'honneur d'accepter de rapporter ma thèse et de venir assister à la soutenance. Je remercie aussi Marie-Françoise Roy, Damien Chablat et Philippe Wenger d'avoir accepté de faire partie de mon jury, ainsi que de l'intérêt qu'ils ont porté à mon travail.

Je remercie Amir Hashemi, avec qui j'ai eu de nombreuses discussions très enrichissantes. Je suis aussi reconnaissant envers Mohab Safey El Din pour son enthousiasme sans limite et les nombreuses idées qu'il a partagé avec moi. Je remercie Jean-Charles Faugère pour ses remarques pertinentes et au contact de qui j'ai beaucoup appris. Merci aussi à Guénael Renault, à Valérie Ménissier-Morain et à Cyriaque M'Baka qui m'ont soutenu tout au long de ma thèse.

J'ai aussi bien évidemment une pensée particulière pour ceux que j'ai côtoyé au LIP6, dont Philippe Aubry, Olivier Bodini, Emmanuel Chailloux, Ludovic Perret, Michèle Soria, Philippe Trébuchet, Dongming Wang et Annick Valibouze. Merci aussi à mes camarades de thèse Carine Pivoteau, Sajjad Rahmany, Alexis Darrasse, Xiao Rong, Sylvain Lachartre, Ye Liang, Niu Wei, Ting Zhao.

Je tiens aussi à remercier les personnes qui se sont montré disponibles et avec qui j'ai eu l'occasion d'avoir des discussions très enrichissantes, notamment Grégoire Lecerf, Eric Schost, Laurent Busé et Marc Chardin. Je remercie aussi Hirokazu Anai et Jürgen Gerhard qui m'ont respectivement invité à venir travailler avec eux.

Je veux aussi remercier tous mes amis qui m'ont permis de prendre du recul dans les moments difficiles, dans le désordre : Martial, Bei, Tristan, Béa, Borg, Fédérico, Céline, Xin, Frédéric, Nicolas, Julien, François-Régis, Amir, Clémence, Jean-Charles, Marina, Hadrien, Maïliss, Mathieu, Linda, Alyssia, Aurélia, Frédéric, Dorothé, Julien, et tout ceux que je pourrais avoir oublié.

Je remercie aussi mes parents, mon frère et toute ma famille qui m'ont sans cesse soutenu et encouragé.

Enfin, je remercie tout particulièrement ma femme Frieda, pour son soutien, pour son aide et pour son amour, même dans les moments les plus difficiles.

Chapitre 1

Introduction

La résolution des systèmes polynomiaux dépendant de paramètres est un enjeu important pour le calcul scientifique. La robotique [27, 145], la cartographie [144, 47], la biologie [10, 106], la théorie du contrôle [3], l'optimisation [45] sont autant de domaines où ces types de systèmes apparaissent naturellement.

Cette thèse porte sur l'étude et la conception d'algorithmes efficaces pour la résolution certifiée de systèmes paramétrés, ainsi que sur l'application de ces méthodes à des problèmes ouverts en robotique et calibration ainsi qu'à quelques challenges plus académiques.

Enjeux et motivations

Problématique

On considère un système paramétré S de la forme :

$$(E)\begin{cases} f_1(\mathbf{T},\mathbf{X}) = 0 \\ \vdots \\ f_m(\mathbf{T},\mathbf{X}) = 0 \end{cases} \quad \text{et} \quad (I)\begin{cases} g_1(\mathbf{T},\mathbf{X}) \gneq 0 \\ \vdots \\ g_r(\mathbf{T},\mathbf{X}) \gneq 0 \end{cases}$$

où $f_1,\dots,f_m,g_1,\dots,g_r$ sont des polynômes de $\mathbb{Q}[t_1,\dots,t_s][x_1,\dots,x_n]$ (les symboles $\gneq$ peuvent être remplacés par $>$ ou $\neq$).

Les variables $\mathbf{T}$ sont les s paramètres du système et $\mathbf{X}$ sont les n inconnues. De plus on se place essentiellement dans le cas où S admet génériquement un nombre fini de solutions. Plus précisément, pour presque tout point p de l'espace des paramètres $\mathbb{C}^s$ ou $\mathbb{R}^s$, le système S spécialisé en p admet un nombre fini de solutions complexes.

Un problème récurent dans les applications est la classification des solutions de tels systèmes en fonction du nombre de ses solutions réelles.

Plus précisément, étant donné le système S et un entier k, on veut le plus souvent déterminer l'ensemble des valeurs des paramètres pour lesquels S admet exactement k solutions. Par exemple, on veut pouvoir décider si S admet exactement une solution pour certaines valeurs des paramètres, ou encore connaître les valeurs des paramètres pour lesquels S n'admet pas de solutions.

Dans notre cadre, nous considérons en priorité les valeurs génériques ou réalisables des paramètres. Le principal problème auquel nous nous intéressons dans cette thèse est le suivant :

Poblème 1. *Soient S un système paramétré génériquement zéro-dimensionnel et k un entier.*

Existe-t-il un ensemble ouvert de valeurs de paramètres pour lesquels S admet exactement k solutions ?

□

Nous traitons donc dans cette thèse principalement des systèmes génériquement zéro-dimensionnels. Notamment, nous ne considérons pas le cas des systèmes qui n'admettent génériquement aucune solution, ni celui des systèmes qui admettent génériquement un nombre infini de solutions complexes.

Dans le premier cas, la classification des valeurs génériques des paramètres est trivial. L'enjeu consiste alors à considérer le comportement des solutions au-dessus d'une variété algébrique de mesure nulle, ce qui correspond à un type de problème plus éloigné de ceux étudiés dans le cadre de cette thèse.

Dans le deuxième cas, où le système admet génériquement un nombre infini de solutions complexes, la classification des paramètres en fonction du nombre de solutions réelles nécessite la résolution de problèmes de nature complètement différente de ceux abordés ici. Notamment, on doit par exemple déterminer si la dimension réelle est égale à la dimension complexe du système considéré. Nous présentons quelques pistes pour aborder ces problèmes en conclusion.

Efficacité théorique et pratique

Pour la résolution des systèmes polynomiaux, les bornes de complexité asymptotique théorique des algorithmes considérés ne sont pas toujours un indicateur fidèle de leur comportement en pratique.

Ces différences sont encore plus importantes lorsqu'on considère des systèmes polynomiaux dont les coefficients dépendent de paramètres. Considérons par exemple le problème de l'élimination d'une variable y dans un système de deux polynômes bivariés p et q de $K[x, y]$. Le problème consiste à trouver un polynôme non trivial de $K[x]$ s'annulant sur toutes les racines communes à p et q. Dans le cas où les coefficients de p et q sont rationnels, les méthodes utilisant l'évaluation et l'interpolation polynomiale pourront s'avérer très efficaces en pratique, tandis que les méthodes basées sur le résultant direct de p et q par rapport à y pourront s'avérer plus efficaces dans le cas où K est un corps de fractions polynomiales en plusieurs variables.

Dans nos analyses d'algorithmes, plutôt que de donner directement des bornes de complexité, nous nous attachons à réduire les problèmes considérés à des problèmes classiques comme l'élimination de variables ou la saturation d'un idéal par un polynôme (qui peut elle même se calculer par l'élimination d'une variable). Ceci permet d'utiliser différentes fonctions de l'état de l'art selon que l'on désire borner finement la complexité théorique ou obtenir une implantation rapide.

Algorithmes, applications, implantations et complexité

Chaque algorithme conçu au cours de cette thèse l'a été dans le but de résoudre des problèmes applicatifs considérés comme ouverts dans l'état de l'art, de garantir une complexité asymptotique raisonnable dans le pire des cas, et a été systématiquement implanté et diffusé.

La conception des algorithmes a ainsi été guidée non seulement par des considérations théoriques, mais aussi par des objectifs pratiques qui, bien que non quantifiables, fournissent des informations supplémentaires qui ne sont pas toujours prises en compte dans les modèles théoriques asymptotiques.

A titre d'exemple simple illustrant ce propos, on pourra remarquer que dans le cadre de l'analyse asymptotique, un algorithme en $\mathcal{O}\left(n^{\log_2(3)}\right)$[1] est considéré comme moins efficace qu'un algorithme en $\mathcal{O}\left(n \log_2(n) \log_2(\log_2(n))\right)$. Cependant, d'un point de vue plus pratique, un calcul rapide permet de vérifier que tant que $3 < n < 200$, on a $n^{\log_2(3)} \leq n \log_2(n) \log_2(\log_2(n))$. Ainsi, si l'on veut multiplier deux entiers de tailles inférieurs à 200 mots machines, l'étude théorique asymptotique ne suffit pas pour décider si l'on doit plutôt utiliser l'algorithme de Karatsuba ou l'algorithme de Shönhage et Strassen (voir [131, chapitre 3] ou [78, chapitre 4] pour plus de précisions sur ces algorithmes).

L'implantation systématique des algorithmes au cours de leur conception a permis ainsi de prendre en considération certaines observations pratiques qui n'apparaissent pas nécessairement dans les études asymptotiques.

Variété discriminante

La notion mathématique fondamentale que nous utiliserons pour résoudre le problème de classification de paramètres est celle de *variété discriminante* introduite dans [87].

Une variété discriminante est un fermé de Zariski $\mathcal{D}_S$ de l'espace des paramètres. Pour toute composante connexe $\mathcal{U}$ du sous-espace de paramètres $\mathbb{R}^s \setminus \mathcal{D}_S$ (resp. $\mathbb{C}^s \setminus \mathcal{D}_S$), la projection sur l'espace des paramètres constitue un revêtement analytique de $\mathcal{U}$ par les solutions de S. En particulier, au-dessus de $\mathcal{U}$, S admet un nombre constant de racines réelles (resp. complexes).

La plus petite variété discriminante d'un système paramétré est appelée *variété discriminante minimale*. Cette variété est intrinsèque au système considéré, et est incontournable si l'on veut classifier les paramètres en fonction du nombre de solutions de S. Par ailleurs, cette variété est définie de manière théorique, indépendamment de tout algorithme. Cela nous fournit ainsi un cadre bien défini qui facilite la conception et l'optimisation des algorithmes la calculant.

Tout au long de cette thèse, nous utiliserons les notations suivantes.

Notations 1. *Soit S un système de n équations polynomiales $f_1 = 0, \ldots, f_m = 0$ et r inéquations polynomiales $g_1 \neq 0, \ldots, g_r \neq 0$, tel que les polynômes de S appartiennent à $\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]$.*

On suppose en outre que le système considéré est génériquement 0-dimensionnel, c'est à dire que pour presque tout p de l'espace des paramètres, le système S spécialisé en p est

[1] $\log_2(3) \simeq 1.585$

0-*dimensionnel.*

Les notations suivantes sont associées au système S :

- $\mathbb{C}^s$ *(resp.* $\mathbb{R}^s$*) désigne l'espace complexe (resp. réel) des paramètres*
- $\mathbb{C}^s \times \mathbb{C}^n$ *(resp.* $\mathbb{R}^s \times \mathbb{R}^n$*) est l'espace total des solutions complexes (resp. réelles)*
- I_S *est l'idéal* $\langle f_1, \ldots, f_k \rangle : \prod_{i=1}^{r} g_i^{\infty}$
- $\mathcal{C}_S$ *est l'ensemble constructible des zéros du système S dans* $\mathbb{C}^s \times \mathbb{C}^n$*, défini comme les zéros communs de* $f_1, \ldots, f_k$ *privés des zéros de chacun des polynômes* $g_1, \ldots, g_r$*.*
- π_S *est la projection canonique de* $\mathcal{C}_S$ *sur l'ensemble des valeurs des paramètres* $\mathbb{C}^s$*.*

□

On définit précisément la *variété discriminante* comme suit :

Définition 1. *(Variété discriminante) Soit S un système paramétré. En utilisant les notations 1, on dit que $V \subset \mathbb{C}^s$, une variété algébrique de l'espace des paramètres, est une variété discriminante si et seulement si π_S restreinte à $\pi_S^{-1}(\mathbb{C}^s \setminus V)$ définit un revêtement analytique fini de $\pi_S^{-1}(\mathbb{C}^s \setminus V)$ sur $\mathbb{C}^s \setminus V$.*

□

Un système dépendant de paramètres admet plusieurs variété discriminantes. Cependant, on s'intéressera plus particulièrement à la plus petite d'entre elles, appelée *variété discriminante minimale.*

Définition 2. *(Variété discriminante minimale)*
Soit S un système paramétré. On appelle variété discriminante minimale *et on note $\mathcal{D}_S$ l'intersection de toute les variétés discriminantes de S.*

□

Le travail de D.Lazard et F.Rouillier ([87]) montre que l'on peut décomposer la variété discriminante minimale $\mathcal{D}_S$ d'un système paramétré en quatre composantes constructibles, appelées $\mathcal{O}_{inf}$, $\mathcal{O}_{ineq}$, $\mathcal{O}_{crit}$ et $\mathcal{O}_{sd}$.

Définition 3. *(Composantes d'une variété discriminante) Soit S un système paramétré génériquement 0-dimensionnel. On définit les quatre variété $\mathcal{O}_{ineq}(S), \mathcal{O}_{inf}(S), \mathcal{O}_{crit}(S), \mathcal{O}_{sd}(S) \subset \mathbb{C}^s$.*

- $\mathcal{O}_{ineq}(S)$ *est la projection par π_S de l'intersection de $\mathcal{C}_S$ avec l'hypersurface définie par $g_1 \cdots g_r = 0$*
- $\mathcal{O}_{inf}(S)$ *est l'ensemble des valeurs de paramètres $p \in \mathbb{C}^s$ telles que pour tout voisinage $\mathcal{U}$ de p, $\pi_S^{-1}(\mathcal{U})$ n'est pas borné*
- $\mathcal{O}_{crit}(S)$ *est la projection des points singuliers de $\mathcal{C}_S$ et des points critiques de π_S*
- $\mathcal{O}_{sd}(S)$ *est la projection des composantes de $\mathcal{C}_S$ de dimension inférieure à s*

On notera par la suite $V_{ineq}(S), V_{inf}(S), V_{crit}(S), V_{sd}(S)$ les clôtures respectives de $\mathcal{O}_{ineq}(S), \mathcal{O}_{inf}(S), \mathcal{O}_{crit}(S), \mathcal{O}_{sd}(S)$

□

La propriété suivante montre que l'union des clôtures de ces composantes définit aussi la variété discriminante minimale, permettant ainsi de la décomposer d'un point de vue plus algébrique.

Propriété 1. *([87]) Soit S un système paramétré génériquement 0-dimensionnel. Alors sa variété discriminante minimale est :*

$$\mathcal{D}_S = V_{ineq}(S) \cup V_{inf}(S) \cup V_{crit}(S) \cup V_{sd}(S) = \mathcal{O}_{ineq}(S) \cup \mathcal{O}_{inf}(S) \cup \mathcal{O}_{crit}(S) \cup \mathcal{O}_{sd}(S)$$

□

D'un point de vue algorithmique, ces quatre composantes peuvent se calculer au moyen de méthodes très différentes les unes des autres.

V_{inf} et V_{ineq}. D'abord, sans aucune condition particulière imposée sur le système considéré, les auteurs de [87] montrent que l'on peut calculer $V_{inf}(S)$ et $V_{ineq}(S)$ au moyen des bases de Gröbner pour un produit d'ordres du degré.

V_{sd}. La composante $V_{sd}(S)$ étant la projection de composantes de dimensions strictement inférieures à s, on peut l'obtenir en utilisant un algorithme de décomposition équidimensionnel des solutions de S, puis en éliminant les inconnues des composantes voulues. On verra notamment en partie II que l'on peut se contenter d'une décomposition équidimensionnelle partielle séparant uniquement les composantes de dimension maximale des composantes de petites dimensions.

Dans le cas où le nombre d'équations de S est égal au nombre d'inconnues n, la variété $V_{sd}(S)$ est vide. Cela évite le calcul de décomposition que l'on doit faire en toute généralité pour exhiber les composantes de dimensions inférieure à s.

V_{crit}. Lorsque le système S considéré est génériquement radical, et ne contient pas de composantes immergés, on peut calculer la composante $V_{crit}(S)$ en utilisant le critère jacobien. Présenté notamment dans [35, chapitre 16.5], ce critère permet de calculer exactement $V_{crit}(S)$ au moyen de méthodes d'élimination de variables dans un certain idéal jacobien. Dans le cas général, $V_{crit}(S)$ s'obtient en appliquant le critère jacobien sur la composante dite *principale* des solutions de S que l'on peut définir avec la proposition suivante.

Proposition 1. *Soit S un système paramétré . On note $P_1, \ldots, P_k$ les idéaux premiers associés à I_S, et I_S^e l'idéal engendré par I_S dans $\mathbb{Q}(t_1, \ldots, t_s)[x_1, \ldots, x_n]$. Soient V_1, V_2 les variétés définis par :*

- *L'union des variétés irréductibles associés à $\overline{\mathcal{C}_S}$:*

$$V_1 := \bigcup_{P_i \cap \mathbb{Q}[t_1,\ldots,t_s]=\{0\}} \mathcal{V}(P_i)$$

- *La variété définie par l'idéal I_S^e contracté dans $\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]$:*

$$V_2 := \mathcal{V}(I_S^e \cap \mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n])$$

Alors, les deux variétés définies ci-dessus sont égales et l'idéal radical de la variété correspondante est appelée composante principale *de S, et notée I_p.* □

Systèmes bien posés

Les considérations algorithmiques nous induisent à définir une catégorie de systèmes paramétrés pour lesquels le calcul de la variété discriminante est a priori plus simple.

Définition 4. *(Système bien posé)*
Soit S un système dépendant de paramètres. En utilisant les notations 1, on dit que S est bien posé *si et seulement si le nombre d'équations de S égale le nombre de variables $x_1, \ldots, x_n$ et l'idéal engendré par I_S dans $\mathbb{Q}(t_1, \ldots, t_s)[x_1, \ldots, x_n]$ est :*
- *Zéro-dimensionel*
- *Radical*

□

Comme nous le verrons dans les chapitres 4,5, cette situation est courante dans les systèmes modélisant des applications de robotique ou de calibration par exemple. En effet les systèmes dépendant de paramètres sont souvent conçus afin que des algorithmes de Newton puissent calculer les solutions pour une spécification générique des paramètres. De telles conditions conduisent naturellement à la conception de systèmes vérifiant toutes les hypothèses d'un système bien posé.

La variété discriminante minimale d'un système S bien posé est alors composée des trois composantes $V_{ineq}(S) \cup V_{inf}(S) \cup V_{crit}(S)$. Dans [87], les auteurs montrent comment calculer ces variétés au moyen de bases de Gröbner. D'un point de vue de la complexité, au vue de l'état de l'art, cette approche ne nous permet pas d'exhiber des bornes fines sur la complexité du calcul de la variété discriminante. Nous verrons dans le chapitre 3 une amélioration significative de la borne sur le degré et la complexité du calcul de la variété discriminante minimale d'un système bien posé.

Systèmes surdéterminés

Dans le cas plus général, on peut d'abord considérer le cas des systèmes S dits *surdéterminés* : ces systèmes sont génériquement radicaux, mais peuvent posséder un nombre d'équations m supérieur au nombre d'inconnues s.

Dans ce cas, les composantes $V_{inf}(S)$ et $V_{ineq}(S)$ peuvent se calculer au moyen des bases de Gröbner par bloc, comme dans le cas des systèmes bien posés.

La composante $V_{sd}(S)$ est projection des composantes de petite dimension. Cette composante est vide dans le cas des systèmes bien posé, mais pas dans le cas général. Pour la calculer, nous devons séparer la composante principal des composantes de petites dimensions.

Lorsque S est génériquement radical, le critère jacobien permet de calculer une variété contenant $V_{crit}(S)$ (voir [35]). On doit alors considérer un idéal jacobien engendré par $m + \binom{m}{s}$ polynômes. Dans certains cas, le calcul de cet idéal peut être une étape bloquante du calcul de la variété discriminante. Par ailleurs, lorsque l'idéal n'est pas génériquement radical, nous devons alors calculer le radical de sa composante principal.

Un algorithme adapté semble alors nécessaire pour calculer d'une part la composante principale I_p ainsi que les composantes de petites dimensions du système considéré pour en calculer sa variété discriminante.

Les *décompositions régulières* introduites dans la deuxième partie permettent d'une part de calculer une décomposition équidimensionnelle des solutions de S pour le calcul de $V_{sd}(S)$, et d'autre part de supprimer le facteur combinatoire $m + \binom{m}{s}$ apparaissant lors du calcul de l'idéal jacobien.

Lorsque le système considéré S n'est pas génériquement radical, on ne peut plus appliquer directement le critère jacobien pour le calcul de $V_{crit}(S)$. Il existe dans ce cas diverses méthodes pour calculer le radical. On verra dans la deuxième partie une nouvelle méthode basée sur les décompositions régulières et les travaux de [36] pour calculer le radical des composantes qui nous intéresse.

Enfin, nous verrons que notre algorithme général de décomposition régulière peut être modifié pour calculer plus efficacement la séparation entre les composantes de dimension maximale et celles de plus petites dimensions.

État de l'art

Dans la littérature, on trouve différente méthodes permettant de traiter le problème général de classification des paramètres en fonction du nombre de solutions réelles d'un système. Il est difficile de comparer ces algorithmes entre eux dans la mesure ou la spécification des objets calculés n'est pas la même.

Cependant on notera que pour le problème de classification considéré dans cette thèse, et fréquent dans les applications, le calcul d'une variété discriminante minimale ou large est implicite dans toutes les méthodes considérées.

Décomposition Cylindrique Algébrique

La Décomposition Cylindrique Algébrique a été introduite par Collins ([26]). Étant donné un ensemble de polynômes $f_1, \ldots, f_m$ de $\mathbb{Q}[x_1, \ldots, x_n]$, l'algorithme de Décomposition Cylindrique Algébrique produit une partition de l'espace en cellules homéomorphes à $]0,1[^k$, $0 \leq k \leq n$, telles que le vecteur de signes de $f_1, \ldots, f_m$ est constant sur chacune de ces cellules.

Si l'on ne s'intéresse, comme dans notre problème, au cas générique uniquement, Hong et Collins ont introduit dans [66] la Décomposition Cylindrique Algébrique partielle où l'on ne calcule que les cellules homéomorphes à $]0,1[^n$ ([66]). Une autre amélioration pertinente pour notre problème est la prise en compte de contraintes de type double égalité polynomiale pour la construction de la DCA ([11]).

Dans le pire cas, l'algorithme original ainsi que ces différentes variantes possèdent une complexité au moins doublement exponentielle en le nombre de variable. Appliqué à notre problème, en notant d le degré maximal des polynômes de S, le calcul d'une DCA coûterait au plus :

$$d^{\mathcal{O}\left((n+s)2^{n+s}\right)}$$

opérations arithmétiques.

Souffrant d'une grande complexité théorique asymptotique, ces algorithmes sont cependant implanté dans de nombreux systèmes de calculs formels et restent une référence pour la

résolution de problème paramétré, avec des performances pratiques raisonnables sur certaines classes de problèmes.

Élimination des quantificateurs

En toute généralité, le problème de classification peut être vu comme un problème d'élimination de quantificateurs. La fonction général d'élimination des quantificateurs peut s'énoncer ainsi dans les réels.

Théorème 1. *(Élimination des quantificateurs)*
Soient $X_1, \ldots, X_k, Y_1, \ldots, Y_l$ des variables. On note $\mathbf{X}_{[1]}, \cdots, \mathbf{X}_{[\omega]}$ une partition de l'ensemble des variables $X_1, \ldots, X_k$ où chaque $X_{[i]}$ constitue un bloc de variables. Alors si φ est une formule de la forme :

$$\varphi(Y_1, \ldots, Y_l) = Q_1 \mathbf{X}_{[1]} \cdots Q_\omega \mathbf{X}_{[\omega]} \bigvee_j \left(\bigwedge_i (P_{i,j}(X_1, \ldots, X_k, Y_1, \ldots, Y_l) s_{i,j} 0) \right)$$

où $Q_i \in \{\exists, \forall\}$ et $s_{i,j} \in \{<, >, =\}$
Alors il existe une formule sans quantificateur φ' :

$$\varphi(Y_1, \ldots, Y_l) = \bigvee_j \left(\bigwedge_i (P'_{i,j}(X_1, \ldots, X_k, Y_1, \ldots, Y_l) s_{i,j} 0) \right)$$

telle que $\varphi' \Leftrightarrow \varphi$. □

Un algorithme explicite permettant d'éliminer les quantificateurs peut se trouver dans le livre de Basu, Pollack et Roy [5]. Cette algorithme utilise notamment l'élimination de variables dans un idéal [28, chapitre 3].

Dans le cadre du problème qui nous intéresse, l'utilisation de l'élimination des quantificateurs conduira notamment au calcul d'une variété discriminante large du système considéré.

Si l'on veut appliquer cette méthode directement au problème général de classification des paramètres que l'on considère, il est difficile de trouver une formule faisant intervenir moins de deux blocs alternés de quantificateurs.

On verra cependant que après avoir réduit le problème du calcul de la variété discriminante à un problème d'élimination de variables, nous pourrons utiliser avantageusement les bornes de complexités proposés dans [5].

Vecteurs de multiplicité

Grigoriev et Vorobjov ont introduit dans [59] un algorithme de calcul des vecteurs de multiplicité. Plus précisément, étant donné un système zéro-dimensionnel, le vecteur de multiplicité associé au système est l'ensemble des solutions associées à leur multiplicité.

En considérant un système S d'équations polynomiales paramétrées, sans inégalité, Grigoriev et Vorobjov exhibent un algorithme produisant une partition de l'espace des paramètres en ensembles semi-algébriques $\mathcal{C}$ tels que :

– soit S admet un nombre infini de solutions pour tout point de $\mathcal{C}$
– soit S admet un vecteur de multiplicité constant pour tout point de $\mathcal{C}$

En ne conservant que les vecteurs de multiplicités correspondant aux cellules ouvertes de l'espace des paramètres, on peut alors répondre au problème de classification des paramètres dans le cas où le problème ne contient pas d'inégalité. La complexité en temps d'un calcul basé sur cette méthode est alors majoré par :

$$d^{\mathcal{O}(n^2 s)}$$

Lieu dégénéré d'une paramétrisation

Dans [129], Schost étudie la représentation sous forme d'ensemble triangulaire des solutions d'un système zéro-dimensionnel S à coefficients dans un corps de fraction comme $\mathbb{Q}(t_1, \ldots, t_s)$ par exemple. Soient $\mathbf{T}_1, \ldots, \mathbf{T}_k$ des ensembles triangulaires de $\mathbb{Q}(t_1, \ldots, t_s)[x_1, \ldots, x_n]$ dont l'union des zéros forment les zéros de S.

Dans ce cadre, [129] introduit le lieu dégénéré, dont la notion se rapproche le plus de la notion de variété discriminante. Le lieu dégénéré est une hypersurface algébrique $\mathcal{V}(\Delta) \subset \mathbb{C}^s$ telle que pour tout $(t_1^0, \ldots, t_s^0) \in \mathbb{C}^s \setminus \mathcal{V}(\Delta)$, chaque $\mathbf{T}_i$ peut-être spécialisé en $(t_1^0, \ldots, t_s^0)$ (i.e. les dénominateurs des coefficients de $\mathbf{T}_i$ ne s'annulent pas en $(t_1^0, \ldots, t_s^0)$), et l'ensemble de polynômes obtenus génèrent alors un idéal radical.

On peut vérifier que le polynôme Δ défini une variété discriminante large de S. Et le degré de Δ est borné dans [129] par :

$$3nD^2 + n^2 D$$

où D est le degré de S majoré par d^n dans le pire des cas.

La borne que nous présentons dans cette thèse pour majorer spécifiquement le degré de la variété discriminante minimale d'un système bien posé est plus fine que si nous avions utilisé directement la borne du lieu dégénéré.

Valeurs critiques généralisées

La notion de valeurs critiques généralisées est présentée dans [114, 81, 69, 71]. Cette notion a notamment été utilisée par Safey El Din dans [125, 126, 127] pour le calcul efficace d'un point par composante connexe d'un ensemble semi-algébrique.

Soient $f := (f_1, \ldots, f_s)$ un vecteur de polynômes de $\mathbb{Q}[x_1, \ldots, x_n]$ et $\mathcal{X}$ une variété algébrique lisse. Les valeurs critiques généralisées du vecteur de fonctions polynomiales $f : \mathcal{X} \to \mathbb{C}^s$ sont l'union des valeurs critiques classiques et des valeurs critiques asymptotiques de f (voir [69, 71] par exemple pour les définitions précises de ces notions).

Dans le cas où les zéros $\mathcal{X}$ du système paramétré S forment une variété lisse, la variété discriminante minimale coïncide alors avec les valeurs critiques généralisés de la fonction de projection trivial de $\mathcal{X}$ sur l'espace des paramètres. On peut remarquer que la notion de valeur critique généralisée est plus générale que la notion de variété discriminante minimale dans le sens où elle caractérise l'invariance topologique d'un système paramétré génériquement de

dimension positive, et moins générale dans le sens où elle ne traite pas les variétés singulières ou semi-algébrique.

On peut notamment remarquer que dans les cas où les deux notions coïncident, la borne obtenue dans [71] sur le degré des valeurs critiques généralisées est identique à celle prouvée dans ce chapitre sur le degré de la variété discriminante minimale. La borne que nous obtenons reste de plus valable pour la variété discriminante minimale d'un système bien posé dont les zéros possèdent des singularités.

Discriminant

On peut enfin citer la notion de discriminant d'un polynôme en une variable, basée sur le résultant, introduit par Sylvester dans le prolongement des travaux de Bézout [19, 109, 136, 137] dont on peut trouver une version moderne dans [25]. Notamment, cette notion donne un critère sur les coefficients d'un polynôme univarié pour qu'il admette des racines multiples.

Une extension de ces méthodes au cas creux se trouve dans le livre [49], sous le nom de $\mathcal{A}$-discriminants. Cette théorie permet d'obtenir des formules plus faciles à manipuler en supposant que les coefficients du polynôme considéré ne s'annulent pas, notamment dans le cas où le polynôme considéré est creux. Cette notion peut aussi se généraliser au cas de systèmes polynomiaux multivariés (voir [32] par exemple).

A la différence de la notion de variété discriminante minimale, cette notion fondamentalement basé sur le calcul de résultants, est développée d'abord pour le cas où les coefficients des polynômes considérés sont des variables indépendantes, et ne traite que les systèmes d'équations.

Organisation

L'étude algorithmique du problème de classification des solutions d'un système paramétré nous a conduit à distinguer une catégorie de systèmes pour lequel le problème se résout plus simplement. Ces systèmes, dits *bien posé* , sont en outre les plus fréquents dans les applications.

Dans une première partie, nous présentons une étude théorique du degré et du calcul de la variété discriminante dans le cas des systèmes bien posé. Nous avons aussi implanté le calcul de la variété discriminante pour ces systèmes. Cela nous a fournit un outil important pour la résolution d'un problème de calibration d'appareil photo, ainsi que d'un problème issu de la théorie de polynômes creux, présentés dans les chapitres 4 et 5.

Dans une deuxième partie, nous étudions les systèmes paramétrés plus généraux, possédant notamment plus d'équations que de variables. Nous présentons dans ce cas un algorithme permettant de décomposer un tel système en composantes équidimensionnelles, où chaque composante est représentée par un ensemble d'équations et d'inéquations, tel que le nombre d'équations égale le nombre de variables. Ce pré-traitement nous permet dans la plupart des cas de transformer un système surdéterminé en système bien posé. Nous verrons notamment au chapitre 9 une application de cette méthode sur un système surdéterminé issu d'un problème ouvert de robotique.

Systèmes bien posés

Chapitre 3 : Variété discriminante et complexité. Dans le cadre des systèmes bien posés, nous exhibons pour la première fois des bornes fines sur la complexité du calcul et le degré de la variété discriminante minimale. Nous présentons en particulier un algorithme de réduction du calcul de la variété discriminante à celui de la projection d'une variété algébrique.

Les méthodes de projection ont beaucoup été étudiées, notamment au cours des vingt dernières années. Notre réduction à la fonction de projection nous permet ainsi de déduire les résultats suivants. Si d est une borne supérieure du degré des polynômes de S, alors, sa variété discriminante minimale est de degré au plus :

$$D := (n+r)d^{(n+1)}$$

et elle se calcule en au plus :

$$(n+r)^{\mathcal{O}(s)}d^{\mathcal{O}(sn)}$$

opérations arithmétiques.

Ce travail a été l'objet de la publication [102].

Chapitre 4 : Application à la cartographie. Considérons trois points de référence A, B, C dans l'espace réelle à trois dimension, et un point de contrôle P. Le problème original, appelé *Perspective three Point*, consiste à retrouver la position de P en fonction des angles $\widehat{APB}, \widehat{BPC}, \widehat{CPA}$, et des longueurs AB, BC, AC.

Cependant, si on connaît les valeurs des paramètres $\widehat{APB}, \widehat{BPC}, \widehat{CPA}, AB, BC, AC$, on ne peut pas toujours déterminer la position du point P de manière unique.

Soit S le système d'équations paramétrés dont les solutions sont la position de P. Nous avons pu pour la première fois résoudre le problème 1 correspondant à ce système. Notamment nous avons exhibé 5 points dans l'espace des paramètres autour desquels le système admet respectivement $0, 2, 4, 6, 8$ solutions.

Ce travail a été l'objet de la publication [41].

Chapitre 5 : Application à l'étude de systèmes algébriques creux. La théorie des polynômes creux fait le lien entre le nombre de monômes d'un système d'équations 0-dimensionnel et le nombre de ses solutions. Dans ce cadre, Haas [60] puis Dickenstein et al. [32] ont présenté une famille de systèmes paramétrés creux :

$$H_{(a,b,k)} := \begin{cases} x^{2k} + ay^k - y = 0 \\ y^{2k} + bx^k - x = 0 \\ a \neq 0, b \neq 0, x > 0, y > 0 \end{cases}$$

dont la classification des paramètres a, b en fonction du nombre de solution s'avère particulièrement difficile. En utilisant des méthodes ad hoc basées sur des méthodes de points critiques ([24]) couplées avec la théorie des $\mathcal{A}$-discriminants ([49, 32]), ils arrivent pour $k = 3$ à exhiber un ouvert $\mathcal{U}_3$ de l'espace des paramètres où le système $H_{(a_0,b_0,k)}$ admet exactement 5 solutions pour tout $(a_0, b_0) \in \mathcal{U}$.

Après un travail sur la modélisation des systèmes de Haas, nous avons réussi à exhiber un ouvert $\mathcal{U}_k$ jusqu'à $k = 9$, et nous avons pu calculer la variété discriminante minimale de ces systèmes pour $k \leq 13$.

Ce travail a été publié dans [104].

Systèmes surdéterminés

Chapitre 7 : Décomposition régulière. Ce chapitre introduit les *décompositions régulières*. C'est une forme de décomposition équidimensionnelle d'un idéal I où chaque composantes est représentée par le couple (S, F) où S est une suite régulière de polynômes, et F un ensemble de polynômes. Un tel couple est alors appelé *ensemble régulier*. On distingue deux types de décompositions :

- la *décomposition régulière stricte* : étant donné un idéal I, sa décomposition régulière stricte D est un ensemble de couples (S, F), représentant chacun la variété constructible $\mathcal{C}(S, F) = \mathcal{V}(S) \setminus \mathcal{V}(\prod_{f \in F} f)$. et vérifiant :

$$\mathcal{V}(I) = \bigcup_{(S,F) \in D} \mathcal{C}(S, F)$$

  En outre, on impose que les intersections deux à deux des ensembles constructibles $\mathcal{C}(S_1, F_1)$ et $\mathcal{C}(S_2, F_2)$ pour $(S_1, F_1), (S_2, F_2) \in D$ soient vides.
- la *décomposition régulière minimale* : étant donné un idéal I, sa décomposition régulière minimale D est un ensemble de couples (S, F),représentant cette fois chacun la variété algébrique $\mathcal{Z}(S, F) = \overline{\mathcal{V}(S) \setminus \mathcal{V}(\prod_{f \in F} f)}$. et vérifiant :

$$\mathcal{V}(I) = \bigcup_{(S,F) \in D} \mathcal{Z}(S, F)$$

  En outre, on impose que les composantes irréductibles de chacune des variétés $\mathcal{Z}(S_0, F_0)$ pour $(S_0, F_0) \in D$ ne soit incluses dans aucunes des variétés $\mathcal{Z}(S, F)$ pour $(S, F) \in D, (S, F) \neq (S_0, F_0)$.

Alors que la plupart des travaux calculant une décomposition équidimensionnelle s'appuient sur l'élimination de variables ([140, 85, 73, 50, 20, 51, 89]) pour réduire le problème au cas univarié, Seuls les auteurs de [36] proposent une méthode permettant de calculer la composante de plus grande dimension en utilisant des méthodes d'algèbre homologique. Or comme le remarque Bayer et Mumford en 1993 dans [6], cette stratégie est coûteuse en pratique :

> *The general experience is that taking projections can be very time consuming. One reason is that the degree of the generators may go up substantially and that sparse defining polynomials may be replaced by more or less generic polynomials.*

Nous présentons dans ce chapitre le premier algorithme depuis [36] permettant de calculer une décomposition équidimensionnelle d'un idéal sans calculer de polynômes d'élimination. Une implantation a en outre été réalisée dans le cadre de cette thèse en SINGULAR et en MAPLE.

Une partie de ce travail est présentée dans [103].

Chapitre 8 : Complexité. Nous donnons dans ce chapitre une analyse de la complexité de la décomposition régulière minimale d'un idéal I, dans le cas où I est engendré par une suite *pseudo-régulière* S_r (voir [13] ou section 8.1 pour la définition précise). On peut noter que l'on peut toujours se ramener à ce cas par une combinaisons linéaires générique des générateurs d'un idéal (voir lemme 26 ou [77, 13]).

En notant d le degré maximal des polynômes de la suite pseudo-régulière, et n le nombre de variables, soit (S, F) un ensemble régulier de codimension c, produite par l'algorithme de décomposition régulière minimale appliquée à S_r. On peut alors majoré le degré des polynômes apparaissant dans (S, F) par :

$$\deg(p) \leq \begin{cases} d \text{ si } p \in S \\ d^c \text{ si } p \in F \end{cases}$$

Par ailleurs, nous exprimons la complexité du calcul de la décomposition régulière minimale en fonction du calcul de la saturation d'un idéal par un polynôme. Si I est un idéal engendré par au plus n polynômes de degrés au plus d, et g un polynôme de degré au plus d^n. Et si $\mathcal{T}_\zeta(n, d)$ représente la complexité de la saturation de I par g, alors, le nombre d'opérations nécessaires pour obtenir la DRM de S_r est majoré par :

$$\mathcal{O}\left(n^2 d^n \mathcal{T}_\zeta(n, d)\right)$$

Les chapitres suivants présentent deux applications de systèmes non bien posés. La première est issue de la robotique, la deuxième provient de la géométrie.

Chapite 9 : Robots parallèles. Les robots parallèles font l'objet d'une activité de recherche intense depuis ces vingt dernières années. Le livre [100] par exemple constitue une introduction à ce domaine. Les robots parallèles sont dotés d'une géométrie complexe, et leur étude passe par la résolution de systèmes paramétrés complexes.

Dans [99, 145], les auteurs étudient les configurations dites *cuspidales* des robots parallèles de type $3 - RPR$, en utilisant des méthodes de discrétisation de l'espace des paramètres.

Après un travail préalable de modélisation du problème plus adaptée à nos méthodes, nous avons été confronté au calcul de la variété discriminante d'un système de 9 équations, 6 inconnues et 1 paramètre. Nous avons réussi à calculer sa décomposition régulière minimale ainsi que sa variété discriminante. Cela nous a permis de décrire de façon certifiée toutes les configurations cuspidales du robot $3 - RPR$ étudié dans [99, 145]. Nous avons notamment ainsi exhibé certaines configurations que les méthodes de discrétisation n'avaient pas permis de détecter.

Chapite 10 : Surface d'Enneper. Le problème considéré ici consiste à étudier la variété définissant implicitement une variété paramétrée. Nous montrons comment l'utilisation récursive du calcul de la variété discriminante permet de prouver que les deux variétés considérées sont égales.

Première partie

Systèmes bien posés

Chapitre 2

Introduction

Les modèles paramétrés apparaissent naturellement dans de nombreux domaines comme la robotique [27, 145], la cartographie [144, 47], la biologie [10, 106], la théorie du contrôle [3], l'optimisation [45], etc...

Pour ces applications, on veut classer les différents comportements possibles d'un problème physique en fonction des paramètres.

2.1 Modélisation

La première étape importante est la modélisation du problème sous la forme d'un système paramétré.

Soit $t_1, \ldots, t_s$ un ensemble de variable paramétrique, $x_1, \ldots, x_n$ un ensemble de variable indéterminée. On considérera dans cette partie uniquement les systèmes bien posés, de la forme :

$$(E)\begin{cases} f_1(\mathbf{T}, \mathbf{X}) = 0 \\ \vdots \\ f_n(\mathbf{T}, \mathbf{X}) = 0 \end{cases} \quad \text{et} \quad (I)\begin{cases} g_1(\mathbf{T}, \mathbf{X}) \gneq 0 \\ \vdots \\ g_r(\mathbf{T}, \mathbf{X}) \gneq 0 \end{cases}$$

où $f_1, \ldots, f_n, g_1, \ldots, g_r$ sont des polynômes de $\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]$, tels que pour presque toute spécialisation des paramètres, le système correspondant est radical et zéro-dimensionnel.

Lors de la modélisation il est important de prendre en compte les inégalités, les variables considérées pouvant représenter des longueurs ($x > 0$) ou des variables trigonométriques ($-1 < x = \cos(\theta) < 1$) par exemple.

Une fois écrit sous forme d'un système paramétré S, un problème récurent est celui de la classification des valeurs des paramètres en fonction du nombre de solution réelle de S, présenté en introduction générale.

De même qu'il existe pour les méthodes numériques des notions de conditionnement depuis Rice ([120]), la notion de *système bien posé* est une forme de conditionnement pour les méthodes algébriques que nous développons. Lorsque le système S modélisant une application est bien posé, nous allons montrer que nous pouvons exploiter cette structure pour obtenir en

pratique et en complexité un algorithme efficace de discrimination des paramètres en fonction du nombre de solutions de S.

2.1.1 Variété discriminante pour les systèmes bien posé

Les systèmes bien posés possèdent autant d'équations que d'inconnues et sont génériquement 0-dimensionnels et radical. Soit S un tel système. Dans ce cas, la variété discriminante minimale de S se compose des trois composantes $V_{ineq}(S), V_{inf}(S), V_{crit}(S)$, que l'on peut en outre décrire algébriquement.

Notations

Les notations suivantes sont introduites pour la réécriture algébrique des différentes composantes apparaissant dans la variété discriminante minimale de S.

Notations 2. *Soit S un ensemble paramétré. On note alors :*

- *$\mathbb{P}_n$ la clôture projective de $\mathbb{C}^n$*
- *$\overline{\mathcal{C}_S}$ la clôture projective de $\mathcal{C}_S$ dans $\mathbb{C}^s \times \mathbb{P}_n$*
- *$\mathcal{H}_\infty$ l'hypersurface à l'infini $\mathbb{C}^s \times (\mathbb{P}_n \setminus \mathbb{C}^n) \subset \mathbb{C}^s \times \mathbb{P}_n$*
- *$\overline{\pi}$ la projection canonique de $\mathbb{C}^s \times \mathbb{P}_n$ sur $\mathbb{C}^s$*
- *Si I est un idéal de $\mathbb{Q}[t_1, \ldots, t_s][x_0, x_1, \ldots, x_n]$ homogène en $x_0, x_1, \ldots, x_n$, on note $\overline{\mathcal{V}}(I)$ la variété de $\mathbb{C}^s \times \mathbb{P}_n$ définie par I*
- *j_S est le déterminant de la matrice jacobienne*

$$\begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial f_k}{\partial x_1} & \cdots & \frac{\partial f_k}{\partial x_n} \end{pmatrix}$$

- *g_S est le produit des polynômes $g_1, \ldots, g_r$*

□

Remarque 1. *Avec les notations ci-dessus, on a $\mathcal{H}_\infty = \overline{\mathcal{V}}(\langle x_0 \rangle)$.*

Critère jacobien

Étant donné un idéal I zéro dimensionnel, le critère jacobien permet de détecter si I est radical. D'après les résultats de [35, chapitre 16,§6] on a le résultat suivant.

Théorème 2. *Soient k,n deux entiers tels que $k \leq n$, et $f_1, \ldots, f_k$ une suite de polynômes de $\mathbb{Q}[x_1, \ldots, x_n]$ engendrant un idéal I de dimension zéro. Soit en outre J l'idéal engendré par $f_1, \ldots, f_k$ ainsi que par les polynômes de la forme :*

$$\begin{vmatrix} \frac{\partial f_{i_1}}{\partial X_1} & \cdots & \frac{\partial f_{i_1}}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial f_{i_n}}{\partial X_1} & \cdots & \frac{\partial f_{i_n}}{\partial X_n} \end{vmatrix}$$

où $i_1, \ldots, i_n$ est une suite strictement croissante d'entiers compris entre 1 et k.

Alors, I est radical si et seulement si l'idéal J est l'idéal trivial contenant 1. □

En particulier, si l'idéal I que nous considérons dépend de paramètres, on peut alors en déduire un critère permettant de caractériser l'ensemble des valeurs des paramètres tel que la spécialisation de I en ces paramètres est radical. Dans le cas où le système considéré est bien posé, l'ensemble de ces valeurs correspond alors exactement à la composante $V_{crit}(S)$ décrite en [87].

Description algébrique

Ainsi pour un système bien posé, sa variété discriminante minimale peut alors se définir en utilisant les notations précédentes comme suit.

Définition 5. *(Variété discriminante minimale d'un système bien posé) Soit S un système bien posé. On les trois variétés $V_{ineq}(S), V_{crit}(S), V_{inf}(S) \subset \mathbb{C}^s$ peuvent s'écrire ainsi :*

$$\begin{aligned} V_{ineq}(S) &:= \mathcal{V}\left((I_S + \langle g_S \rangle) \cap \mathbb{Q}[t_1, \ldots, t_s]\right) \\ V_{crit}(S) &:= \mathcal{V}\left((I_S + \langle j_S \rangle) \cap \mathbb{Q}[t_1, \ldots, t_s]\right) \\ V_{inf}(S) &:= \overline{\pi}(\overline{\mathcal{C}_S} \cap \mathcal{H}_\infty) \end{aligned}$$

Dans ce cas, la variété discriminante minimale de S vérifie alors :

$$\mathcal{D}_S = V_{ineq}(S) \cup V_{inf}(S) \cup V_{crit}(S)$$

□

Dans le chapitre 3, on montrera une borne fine du degré de la variété discriminante minimale d'un tel système bien posé, ainsi qu'un algorithme de réduction de son calcul au calcul de l'élimination de variables.

2.2 Organisation de la première partie

Cette partie est décomposée en 2 chapitres. Le premier chapitre présente les résultats de complexité du calcul de la variété discriminante minimale d'un système paramétré bien posé. Le deuxième chapitre présente deux avancées, dans le domaine de la robotique d'une part et de celui des polynômes creux d'autre part.

2.2.1 Variété discriminante et complexité

Dans le cadre des systèmes bien posé, un des résultats principaux de cette thèse est l'exhibition pour la première fois des bornes fines sur la complexité de la variété discriminante minimale.

Principalement, si d est une borne supérieure du degré des polynômes de S, alors, sa variété discriminante minimale est de degré au plus :

$$D := (n+r)d^{(n+1)}$$

et elle se calcule en au plus :

$$(n+r)^{\mathcal{O}(s)}d^{\mathcal{O}(sn)}$$

opérations arithmétiques.

Dans le cadre de cette thèse, j'ai aussi développé avec Fabrice Rouillier un programme permettant de calculer la variété discriminante minimale d'un système bien posé, qui est maintenant intégré dans la suite d'outils de résolutions de systèmes paramétrés du logiciel MAPLE 12.

2.2.2 Applications

Dans le cadre des systèmes bien posé, nous présentons deux problèmes paramétrés issus d'applications. Dans chacune de ses applications nous avons fait un travail de modélisation et de résolution, qui nous a permis d'améliorer l'état de l'art des domaines correspondant.

Cartographie Considérons trois points de référence A, B, C dans l'espace réelle à trois dimension, et un point de contrôle P. Le problème original, appelé *Perspective three Point*, consiste à retrouver la position de P en fonction des angles $\widehat{APB}, \widehat{BPC}, \widehat{CPA}$, et des longueurs AB, BC, AC.

Cependant, si on connait les valeurs des paramètres $\widehat{APB}, \widehat{BPC}, \widehat{CPA}, AB, BC, AC$, on ne peut pas toujours déterminer la position du point P de manière unique.

Soit S le système d'équation paramétré dont les solutions sont la position de P. Nous avons pu pour la première fois résoudre le problème 1 correspondant à ce système. Notamment nous avons exhiber 5 points dans l'espace des paramètres autour desquels le système admet respectivement $0, 2, 4, 6, 8$ solutions.

Polynômes creux La théorie des polynômes creux fait le lien entre le nombre de monôme d'un système d'équations 0-dimensionnel et le nombre de ses solutions. Dans ce cadre, Haas [60] puis Dickenstein et al. [32] ont présenté une famille de systèmes paramétrés creux :

$$H_{(a,b,k)} := \begin{cases} x^{2k} + ay^k - y = 0 \\ y^{2k} + bx^k - x = 0 \\ a \neq 0, b \neq 0, x > 0, y > 0 \end{cases}$$

dont la classification des paramètres a, b en fonction du nombre de solution s'avère particulièrement difficile. En utilisant des méthodes ad hoc basées sur des méthodes de points critiques ([24]) couplée avec la théorie des $\mathcal{A}$-discriminants ([49, 32]), ils arrivent pour $k = 3$ à exhiber un ouvert $\mathcal{U}_3$ de l'espace des paramètres où le système $H_{(a_0,b_0,k)}$ admet exactement 5 solutions pour tout $(a_0, b_0) \in \mathcal{U}$.

Après un travail de modélisation équivalente des systèmes de Haas, nous avons réussi à exhiber un ouvert $\mathcal{U}_k$ jusqu'à $k = 9$, et nous avons pu calculer la variété discriminante minimale de ces systèmes pour $k \leq 13$.

Chapitre 3

Variété discriminante et complexité

3.1 Introduction

3.1.1 Présentation des résultats

La variété discriminante (voir définition 1) est un outil mathématique présenté dans [87] permettant de classifier le nombre de solutions réelles d'un système paramétré. Lazard et Rouillier exhibent en outre dans leur article un algorithme permettant de calculer la variété discriminante minimale d'un systèmes paramétré. Pour des raisons d'efficacité pratique, leur algorithme est basé sur des calculs de base de Gröbner, dont la complexité du calcul est dans le pire des cas doublement exponentielle en le nombre de variables.

Nous verrons dans cette partie comment réduire le calcul de la variété discriminante d'un *système bien posé* au calcul de projection, dont la complexité dans le pire cas donnée dans [5] est meilleure que celle du calcul général des bases de Gröbner.

Notations. *Soient $f_1, \ldots, f_k$ des polynômes de $\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]$. Alors, la fonction de projection est définie par :*
PROJECTION$([f_1, \ldots, f_k], [t_1, \ldots, t_s])$:

- Entrée *:* $\begin{cases} f_1, \ldots, f_k \in \mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]; \\ t_1, \ldots, t_s \end{cases}$
- Sortie *:* $q_1, \cdots, q_t \in \mathbb{Q}[t_1, \ldots, t_s]$ *tels que* $\mathcal{V}(\langle q_1, \cdots, q_t \rangle) = \mathcal{V}(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]}(f_1, \ldots, f_k))$.

□

Pour la réduction du calcul de la variété discriminante au calcul de projection, on se place dans le cas des *système bien posé* définis en introduction, dont les hypothèses sont souvent vérifiées dans les applications.

Les principaux résultats de ce chapitre sont, pour S un système bien posé :

- Une borne fine sur le degré de la variété discriminante minimale de S
- Un algorithme de réduction du calcul de la variété discriminante minimale de S au calcul de projection.

Degré Si S est un système bien posé, et si les polynômes de S sont de degré au plus d, alors le degré de la variété discriminante minimale de S est au plus :

$$(n+r)d^{(n+1)}$$

Réduction Dans le cas où S est bien posé, nous montrons que le calcul de sa variété discriminante minimale peut se réduire en espace polynomial à la fonction de projection présentée ci-dessus. Dans ce cas nous en déduisons en corollaire une borne sur le temps de calcul d'une variété discriminante. En notant d le degré maximal des polynômes $f_1, \ldots, f_n, g_1, \ldots, g_r$ et $\sigma_{\max}$ la taille binaire maximale de leurs coefficients, le calcul de la variété discriminante minimale de S est alors majoré par :

$$\sigma_{\max}^{\mathcal{O}(1)}(n+r)^{\mathcal{O}(s)}d^{\mathcal{O}(sn)}$$

3.1.2 Méthodes de projection

Un de nos principaux résultats est la réduction du calcul de la variété discriminante au calcul de projection. Le problème de projection a été intensivement étudié et a donné lieu à de nombreux travaux théoriques et ainsi que de nombreuses implantations logicielles.

Géométriquement, si I est un idéal de $\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]$, $\mathcal{V}(I)$ la variété de ses zéros dans $\mathbb{C}^s \times \mathbb{C}^n$, et π la fonction de projection triviale de $\mathbb{C}^s \times \mathbb{C}^n$ dans $\mathbb{C}^s$, alors on a :

$$\overline{\pi(\mathcal{V}(I))} = \mathcal{V}(I \cap \mathbb{Q}[t_1, \ldots, t_s])$$

où $\overline{V}$ est l'adhérence de la variété V pour la topologie usuelle.

Nous rappelons ici les principales méthodes permettant de calculer la fonction de projection.

Bases de Gröbner Soit I un idéal de $\mathbb{Q}[x_1, \ldots, x_n]$, $\mathbf{T}$ l'ensemble des monômes de $\mathbb{Q}[x_1, \ldots, x_n]$. Les bases de Gröbner fournissent une représentation de l'anneau quotient $\mathbb{Q}[x_1, \ldots, x_n]/I$. Elles ont été introduites de façon indépendante par Buchberger ([15, 14]) en 1965 sous la direction de Gröbner, et Hironaka dans le cadre des anneaux locaux en 1964 ([64]) sous le nom de bases standards.

Une base de Gröbner de I est un ensemble fini de polynômes générateurs de I, définie par rapport à un ordre *monomial* sur les monômes de $\mathbb{Q}[x_1, \ldots, x_n]$.

Définition 6. *(Ordre monomial)*
Soit $<_{\mathbf{T}}$ un ordre sur $\mathbf{T}$, strict, totale, bien fondé, vérifiant en outre pour tout $t_0, t_1, t_2 \in \mathbf{T}$:

$$t_1 <_{\mathbf{T}} t_2 \Rightarrow t_0 t_1 <_{\mathbf{T}} t_0 t_2$$

On dit alors que que $<_{\mathbf{T}}$ est un ordre monomial.
□

Dans ce cas, on peut définir pour chaque polynôme p de I sont monôme de tête par :

$$\mathrm{M}(p) = \max_{<_{\mathbf{T}}}\{t \mid t\text{est monôme de } p\}$$

et par extension, l'ensemble des monômes de têtes de I est :

$$\mathrm{M}(I) = \{\mathrm{M}(p) \mid p \in I\}$$

Définition 7. *(Base de Gröbner)*
Soit $<_{\mathbf{T}}$ un ordre monomial. On dit que l'ensemble des polynômes $f_1, \ldots, f_m$ forme une base de Gröbner *de I pour l'ordre $<_{\mathbf{T}}$ si et seulement si :*

i) $\{f_1, \ldots, f_m\} \subset I$

ii) $\langle \mathrm{M}(f_1), \ldots, \mathrm{M}(f_m)\rangle = \mathrm{M}(I)$

□

Les bases de Gröbner de certains ordres possèdent en outre une propriété importante qui en font un outil bien adapté pour calculer la projection $I \cap \mathbb{Q}[t_1, \ldots, t_s]$ d'un idéal $I \subset \mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]$.

Définition 8. *(Ordre d'élimination) Soit $<_{t,x}$ un ordre monomial sur les monômes de $\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]$ vérifiant en outre pour tout t_0, t_0' monôme de $\mathbb{Q}[t_1, \ldots, t_s]$, t_1, t_2 monôme de $\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]$:*

$$t_1 <_{t,x} t_2 \Rightarrow t_0 t_1 <_{t,x} t_0' t_2$$

Dans ce cas, on dit que $<_{t,x}$ est un ordre monomial par bloc ou ordre d'élimination.
□

Une propriété importante d'un tel ordre est la suivante. Si G est une base de Gröbner de l'idéal $I \subset \mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]$ pour l'ordre $<_{t,x}$, alors :

$$\langle f \mid f \in G \cap \mathbb{Q}[t_1, \ldots, t_s]\rangle = I \cap \mathbb{Q}[t_1, \ldots, t_s]$$

Ainsi pour obtenir une base de générateurs de $I \cap \mathbb{Q}[t_1, \ldots, t_s]$, il suffit de calculer une base de Gröbner de I pour l'ordre $<_{t,x}$, et de n'en garder que les polynômes de $\mathbb{Q}[t_1, \ldots, t_s]$.

Une description des premiers algorithmes de calcul de bases de Gröbner est présentée dans les livres [8, 28] et les références incluses. Depuis, plusieurs améliorations algorithmiques ont été apportées, notamment dans les travaux [39, 40]. D'un point de vue de la complexité, le calcul d'une base de Gröbner peut dans le pire des cas être doublement exponentiel en le nombre de variables ([97, 7]). Lorsque l'idéal considéré est 0-dimensionnel, les auteurs de [84, 83] montrent que le calcul de sa base de Gröbner peut s'effectuer au moyen d'un algorithme probabiliste en temps simplement exponentiel en le nombre de variables.

Différentes implantations de calculs de bases de Gröbner existent, on peut notamment citer FGb ([42]), MAGMA ([94]) ou encore SINGULAR ([132]).

Ensembles triangulaires réguliers Les ensembles triangulaires, lorsqu'ils sont réguliers, permettent aussi d'effectuer le calcul de projection. Si I est un idéal de $\mathbb{Q}[x_1, \ldots, x_n]$, une décomposition triangulaire D de l'idéal I selon l'ordre $x_1 < \cdots < x_n$ est un ensemble fini de suites de polynômes $\mathbf{T}_1, \ldots, \mathbf{T}_m$ où chaque $\mathbf{T} \in D$ est de la forme :

$$(\mathbf{T}) \begin{cases} p_1 := h_1 x_{v(1)}^{d_1} + p_n(x_1, \ldots, x_{v(1)-1}, x_{v(1)}) \\ \vdots \\ p_k := h_k x_{v(k)}^{d_k} + p_n(x_1, \ldots\ldots\ldots, x_{v(k)-1}, x_{v(k)}) \end{cases}$$

où v est une fonction strictement croissante à valeur dans $\{1, \ldots, n\}$, et $h_i \in \mathbb{Q}[x_1, \ldots, x_{v(i)-1}]$. On note de plus $h(\mathbf{T}) := \prod_{i=1}^{k} h_{x_{v(i)}}$. Les ensembles triangulaires de D vérifient alors :

$$\mathcal{V}(I) = \bigcup_{i=1}^{m} \mathcal{V}(\mathbf{T}_i : h(\mathbf{T}_i)^\infty)$$

Par ailleurs, $\mathbf{T}$ est un ensemble triangulaire dit *régulier* si pour tout $l, 1 \leq l \leq k$:

$$\langle p_1, \ldots, p_{l-1} \rangle : \prod_{i=1}^{l-1} h_i^\infty = \langle p_1, \ldots, p_{l-1} \rangle : \prod_{i=1}^{l} h_i^\infty$$

Dans ce cas, on a alors la propriété que pour tout $j, 1 \leq j \leq n$:

$$(\mathbf{T} : h(\mathbf{T})^\infty) \cap \mathbb{Q}[x_1, \ldots, x_j] = (\mathbf{T} \cap \mathbb{Q}[x_1, \ldots, x_j]) : h(\mathbf{T} \cap \mathbb{Q}[x_1, \ldots, x_j]$$

Pour I est un idéal de $\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]$ et D est une décomposition de I en ensembles triangulaires réguliers, cette propriété nous permet d'obtenir directement une décomposition triangulaire de $I \cap \mathbb{Q}[t_1, \ldots, t_s]$, donnée par $\{\mathbf{T} \cap \mathbb{Q}[t_1, \ldots, t_s] \mid \mathbf{T} \in D\}$.

Plus de détails sur ces méthodes sont présentés dans [110, 4, 141, 98] entre autres. Parmi les logiciels permettant de calculer une décomposition triangulaire régulière, on peut notamment citer la bibliothèque `RegularChains` de MAPLE ([117, 101]), MAGMA ([94]) et la bibliothèque `primdec.lib` de SINGULAR (9.2).

Résultants Le terme *résultant* recouvre une famille de méthodes dédiées à l'élimination de variable dans un système de polynômes. La notion résultant remonte jusqu'aux travaux de Sylvester, dans la continuité de travaux de Bézout, Euler, Lagrange, Cayley, pour le cas de l'élimination d'une variable ([19, 136, 137, 109]). Cette notion a ensuite rapidement été généralisée au résultant multivarié, notamment par Macaulay ([92, 93]) et par Dixon ([33]). On distingue maintenant plusieurs notion théorique de résultant, ainsi que différentes méthodes constructives permettant de calculer ces résultants, soit de manière exact, soit à un multiple polynomial près.

On définit le résultant classique d'une suite de polynômes homogènes $f_1, \ldots, f_{n+1}$ de $K[x_0, \ldots, x_n]$, dont les coefficients sont des variables indéterminées indépendantes $c_1, \ldots, c_N$, comme le polynômes $R \subset \mathbb{Z}[c_1, \ldots, c_N]$, unique à la multiplication par un scalaire près, tel que :

$$R(c_1^0, \ldots, c_N^0) = 0 \Leftrightarrow \exists x^0 = (x_0^0 : \cdots : x_n^0) \in \mathbb{P}_n \mid f_1(x^0) = \cdots = f_{n+1}(x^0) = 0$$

Cette notion peut se généraliser en remplaçant dans la définition ci-dessus $\mathbb{P}_n$ par une variété X vérifiant certaines propriétés. En fonction de la variété X, on sera alors dans le cadre des résultant toriques, unirationnels, ou encore résiduels. Plus de précisions sur ces notions sont présentées dans [72, 135, 75, 49, 18, 17].

D'un point de vue constructif, ces résultants peuvent s'obtenir dans certains cas comme le déterminant d'une matrice construite à partir des polynômes $f_1, \ldots, f_{n+1}$. Il existe différent type de matrices, dont principalement les matrices de Macaulay, de Newton ou encore de Dixon. On peut notamment se référer à [95, 38, 37] et aux références incluses pour une présentation de différentes approches ainsi que leurs applications.

Ces méthodes permettent dans certains cas d'exploiter le caractère creux des polynômes d'entrée, et ont été implantées notamment dans SYNAPS ([138]), dans la bibliothèque `multires` de MAPLE ([105]).

Déformation Les méthodes de déformations ont permis d'améliorer significativement la complexité des méthodes d'éliminations de variables dans le cadre d'un système possédant un nombre fini de zéros affines. En effet, les méthodes basées sur les résultants permettent d'éliminer $n-1$ variables parmi n équations polynomiales homogènes de degré au plus d en $d^{\mathcal{O}(n)}$ opérations, à conditions que ces équations admettent un nombre fini de zéros projectifs en commun ([93, 86]).

Considérons maintenant le cas plus général d'un système de n équations $f_1 = 0, \ldots, f_n = 0$, $f_i \in \mathbb{Q}[x_1, \ldots, x_n]$ non nécessairement homogène, admettant un nombre fini de solutions complexes affines. On sait que l'on peut écrire un polynôme univarié g sous la forme $g = q_1 f_1 + \cdots + q_n f_n$ avec $\deg(g), \deg(q_i f_i) \leq d^n$ grâce aux travaux sur le Nullstellensatz effectif ([12, 79, 44, 13, 70]). En particulier, trouver une telle écriture peut se faire en temps polynomial en $\binom{d^n+n}{n} = d^{\mathcal{O}(n^2)}$, ce qui est beaucoup moins efficace que la borne obtenu dans le cas projectif.

Les techniques de déformations permettent de réduire le problème général au cas projectif afin de retrouver une borne polynomiale en d^n. On note $\mathcal{H}(f_i)$ le polynôme homogénéisé de f_i par x_0 et d_i son degré. L'idée de la déformation, utilisée notamment dans [23, 22], consiste à remplacer pour $i, 1 \leq i \leq n$ les polynômes f_i par $\mathcal{H}(f_i) + Z x^{d_i}$. Dans [22] par exemple, l'auteur considère le u-résultant du système déformé et en déduit un polynôme univarié s'annulant sur les solutions du systèmes original, en temps polynomial en d^n.

Ces méthodes ont notamment été utilisées dans la théorie de l'élimination des quantificateurs dans les corps algébriquement clos ([24]) ainsi que dans la théorie de l'élimination des quantificateurs dans les réels ([119, 21, 5]).

Dans le cas d'un système de $n+1$ équations de $\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]$, on peut notamment trouver une relation de $\mathbb{Q}[t_1, \ldots, t_s]$ s'annulant sur les zéros de ce système en $d^{\mathcal{O}(sn)}$ opérations arithmétiques.

Élimination incrémentale La borne de Bézout indique que l'élimination de $n-1$ variables, dans un système 0-dimensionnel de n polynômes de degrés respectifs $d_1, \ldots, d_n$, produit un polynôme univarié de degré au plus $d_1 \cdots d_n$. Les méthodes de déformations permettent d'obtenir des bornes de complexité polynomiales en la borne de Bézout sur cette procédure d'élimination. Cependant, le polynôme de sortie peut souvent avoir un degré bien

inférieur à la borne de Bézout. Dans ces cas, les auteurs de [54, 55, 52, 53, 56] ont introduit un algorithme probabiliste dont la complexité dépend directement du degré des variétés définis par $f_1, \ldots, f_i, 1 \leq i \leq n$, qui est toujours inférieur à la borne de Bézout.

L'idée consiste à calculer successivement les paramétrisation rationnelle des variétés $f_1, \ldots, f_i, 1 \leq i \leq n$. Par son caractère incrémental, l'algorithme élimine à chaque étape les *zéros à l'infini* au moyen d'une méthode adaptative. Cette méthode n'améliore pas la complexité dans le pire cas, mais permet d'éviter l'ajout artificiel de composantes induit par les méthodes de déformation.

Dans le cas de l'élimination de n variables dans un systèmes de $n+1$ équations de $\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]$, ces méthodes sont probabilistes et permettent de trouver une relation de $\mathbb{Q}[t_1, \ldots, t_s]$ s'annulant sur les zéros de ce système en $d^{\mathcal{O}(sn)}$ opérations arithmétiques.

3.2 Résultat principal

Tout au long de ce chapitre, S désignera un système de n équations polynomiales $f_1 = 0, \ldots, f_n$ et r inéquations polynomiales $g_1 \neq 0, \ldots, g_r \neq 0$, tel que les polynômes de S appartiennent à $\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]$.

Étant donné un système paramétré bien posé (voire Définition 4 en introduction), on va montrer dans ce chapitre comment borner le degré et le temps de calcul de sa *variété discriminante minimale*.

3.2.1 Notations

On introduit d'abord les notations liées à la taille d'un système dépendant de paramètres, complétant les notations introduites en introduction générale.

Notations 3. *Soit S un système de n équations polynomiales $f_1 = 0, \ldots, f_n$ et r inéquations polynomiales $g_1 \neq 0, \ldots, g_r \neq 0$, tel que les polynômes de S appartiennent à $\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]$.*

On note alors :

- *σ_S est la taille maximale des coefficients des polynômes de S, de j_S et de g_S*
- *Pour i allant de 1 à n, d_i est le degré du polynôme f_i*
- *Pour i allant de 1 à r, d'_i est le degré du polynôme f_i*
- *δ est le degré de j_S, inférieur à $\sum_{i=1}^{n}(d_i - 1)$*
- *δ' est le degré de g_S, inférieur à $\sum_{i=1}^{r}(d'_i - 1)$*

□

On utilise aussi les notations suivantes pour désigner les opérations usuelles sur les idéaux.

Notations 4.

- $\mathcal{V} : \begin{array}{ccc} \mathcal{P}(\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]) & \rightarrow & \mathcal{P}(\mathbb{C}^s \times \mathbb{C}^n) \\ I & \mapsto & \mathcal{V}(I) \end{array}$

  associe à I l'ensemble des zéros (ou variété algébrique) de I. Par abus de notations, si $p_1, \ldots, p_k$ sont des polynômes de $\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]$, on notera $\mathcal{V}(p_1, \ldots, p_k)$ la

variété de l'idéal $\langle p_1, \ldots, p_k \rangle$. Il en sera de même pour les fonctions φ et ζ.

- $\begin{array}{rccc} \mathcal{H} : & \mathcal{P}(\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]) & \to & \mathcal{P}(\mathbb{Q}[t_1, \ldots, t_s][x_0, x_1, \ldots, x_n]) \\ & I & \mapsto & \mathcal{H}(I) \end{array}$
associe à l'idéal I l'idéal des polynômes de I homogénéisés par la variable x_0 par rapport aux variables $x_1, \ldots, x_n$. Par abus de notation, si p est un polynômes de $\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]$, on notera $\mathcal{H}(p)$ l'homogénéiser de p.

- $\begin{array}{rccc} \mathcal{H}_i : & \mathcal{P}(\mathbb{Q}[t_1, \ldots, t_s][x_0, \ldots, \widehat{x_i}, \ldots, x_n]) & \to & \mathcal{P}(\mathbb{Q}[t_1, \ldots, t_s][x_0, x_1, \ldots, x_n]) \\ & I & \mapsto & \mathcal{H}_i(I) \end{array}$
associe à l'idéal I l'idéal des polynômes de I homogénéisés par la variable x_i par rapport aux variables $x_0, \ldots, \widehat{x_i}, \ldots, x_n$. Par abus de notation, si p est un polynômes de $\mathbb{Q}[t_1, \ldots, t_s][x_0, \ldots, \widehat{x_i}, \ldots, x_n]$, on notera $\mathcal{H}_i(p)$ l'homogénéiser de p.

- $\begin{array}{rccc} \varphi_A : & \mathcal{P}(\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]) & \to & \mathcal{P}(A) \\ & I & \mapsto & \varphi_A(I) \end{array}$
où A est un sous-anneau de $\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]$, associe à l'idéal I l'idéal d'élimination $I \cap A$. Par abus de notation, on étendra parfois le domaine de définition de cette fonction à $\mathcal{P}(\mathbb{Q}[t_1, \ldots, t_s][x_0, x_1, \ldots, x_n])$ ou $\mathcal{P}(\mathbb{Q}[t_1, \ldots, t_s][x_0, x_1, \ldots, x_n, x_{n+1}])$.

- $\begin{array}{rccc} \sigma^q_{x_i} : & \mathcal{P}(\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]) & \to & \mathcal{P}(\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, \widehat{x_i}, \ldots, x_n]) \\ & I & \mapsto & \sigma^q_{x_i}(I) \end{array}$
où q est une rationnel, associe à l'idéal I l'idéal des polynômes de I où la variable x_i est spécialisée par q. $\sigma^q_{x_i}$ appliquée à un polynômes désignera le polynôme où x_i a été spécialisé par q.

- $\begin{array}{rccc} \zeta_f : & \mathcal{P}(\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]) & \to & \mathcal{P}(\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]) \\ & I & \mapsto & \zeta_f(I) \end{array}$
où f est un polynômes de $\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]$, associe à l'idéal I l'idéal saturé $I : f^\infty$. Par abus de notation, si J est un idéal, $\zeta_J(I)$ désigne l'idéal I saturé par J (i.e l'ensemble des polynômes g tels que il existe un entier k vérifiant que pour toute suite $j_1, \ldots, j_k$ de polynômes de J, $gj_1 \cdots j_k \in I$)

□

Enfin, dans les algorithmes que nous présentons, nous représenterons une variété algébrique V par un ensemble de polynômes s'annulant exactement sur V.

Nous introduisons alors naturellement les opérateurs suivant.

Notations 5. *Soient I et J deux idéaux d'un anneau polynomial $\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]$.*

- *$\overset{\surd}{=}$ désigne la relation d'équivalence sur $\mathcal{P}(\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n])$ définie par :*

$$I \overset{\surd}{=} J \text{ si et seulement si } \sqrt{I} = \sqrt{J}$$

– *la notation* $\overset{\surd}{\subset}$ *est définie par :*

$$I \overset{\surd}{\subset} J \text{ si et seulement si } \sqrt{I} \subset \sqrt{J}$$

□

3.2.2 Définitions

La variété discriminante d'un système paramétré S peut être vue comme une généralisation de la notion de discriminant pour un polynôme paramétré.

On s'intéresse ici à la notion de variété discriminante, au sens de Lazard et Rouillier, d'un système paramétré dépendant d'équations et d'inéquations, possédant génériquement un nombre fini de solutions.

Nous restreignons notre étude aux cas des systèmes paramétrés dit *bien posés* .

Degré

Nous nous intéressons à borner le degré d'une variété. La notion de degré que l'on utilisera est celle présentée en [63].

Définition 9. *Soit $V \subset \mathbb{C}^k$ une variété algébrique irréductible de dimension r. Alors le degré de V que l'on notera* $\deg(V)$ *est défini par :*

$$\deg(V) = \max\{|E \cap V| \mid E \text{ est un sous-espace affine de codimension } r, \text{ tel que } E \cap V \text{ est fini}\}$$

□

En particulier, étant donné un idéal I quelconque, la variété de chacun de ses premiers isolés est irréductible. On peut ainsi définir le degré de $\mathcal{V}(I)$.

Définition 10. *(Degré)*
Soit I un idéal. Alors le degré de $\mathcal{V}(I)$, noté $\deg(\mathcal{V}(I))$*, est défini par :*

$$\deg(\mathcal{V}(I)) = \sum_{P \in \text{minass}(I)} \deg(\mathcal{V}(P))$$

□

3.2.3 Complexité de la variété discriminante

On peut maintenant définir précisément les théorèmes de majoration du degré et du temps de calcul de la variété discriminante minimale d'un système bien posé.

Théorème 3. *Soit S un système paramétré bien posé. Alors, en utilisant les notations 3, le degré de la variété discriminante minimale de S est majoré par :*

$$d_1 \cdots d_n(1 + \delta + \delta')$$

□

Le théorème suivant explicite la réduction du calcul de la variété discriminante minimal de S au calcul d'élimination de variable.

Théorème 4. *Soit S un système paramétré bien posé. Alors, la variété discriminante minimale de S est définie par :*

$$\bigcup_{i=0}^{n} \mathcal{V}(\sigma_{x_0}^0 \circ \varphi_{\mathbb{Q}[t_1,\ldots,t_s,x_0]}(I_i^S))$$

où $I_0^S, \ldots, I_n^S$ sont définis par :

$$\begin{aligned} I_0^S &:= \langle f_1, \ldots, f_n, j_S g_S - x_0, Z x_0 - 1 \rangle \\ I_1^S &:= \sigma_{x_1}^1(\mathcal{H}(f_1), \ldots, \mathcal{H}(f_n), Z x_0 \mathcal{H}(g_S) - 1) \\ &\vdots \\ I_n^S &:= \sigma_{x_n}^1(\mathcal{H}(f_1), \ldots, \mathcal{H}(f_n), Z x_0 \mathcal{H}(g_S) - 1) \end{aligned}$$

□

Ainsi, cela nous permet de borner le temps et l'espace de calcul de la variété discriminante minimale d'un système bien posé S en fonction de la complexité du calcul d'élimination de variables.

Notations 6. *Soient $f_1, \ldots, f_k$ des polynômes de $\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]$, de degrés $\mathbf{d} = (d_1, \ldots, d_k)$, et dont la taille des coefficients est majorée par $\sigma_{\max}$. Alors, on note :*

$$\mathcal{T}_{\text{PROJ}}(\sigma_{\max}, s, n, \mathbf{d})$$

une borne sur le temps de calcul de la fonction PROJECTION$(f_1, \ldots, f_k, [t_1, \ldots, t_s])$.
□

Corollaire 1. *Soit S uns système paramétré bien posé. Alors on peut calculer la variété discriminante minimale de S en au plus :*

$$\begin{array}{rcccccc} & \mathcal{T}_{\text{PROJ}}(& 2\sigma_S, & s+1, & n+1, & (d_1, \ldots, d_n, 2, \delta + \delta') &) \\ & & & + & & & \\ n & \mathcal{T}_{\text{PROJ}}(& 2\sigma_S, & s+1, & n, & (d_1, \ldots, d_n, \delta' + 2) &) \end{array}$$

étapes sur une machine de Türing déterministe. □

Remarque 2. *En utilisant pour $\mathcal{T}_{\text{PROJ}}$ la borne présentée dans [5], et en notant d le degré maximal des polynômes $f_1, \ldots, f_n, g_1, \ldots, g_r$, $\sigma_{\max}$ la taille binaire maximale de leurs coefficients, on obtient alors comme borne :*

$$\sigma_{\max}^{\mathcal{O}(1)}(n + r)^{\mathcal{O}(s)} d^{\mathcal{O}(sn)}$$

Corollaire 2. *Le calcul de la variété discriminante minimale d'un système bien posé peut se faire en espace polynomial* □

*preuve :*Ce corollaire directement en utilisant le résultat de [96] qui prouve que l'élimination de variable peut se faire en espace polynomiale en la taille de l'entrée.
□

3.3 Analyse de la variété discriminante

3.3.1 Préliminaires

On énonce ici diverses propriétés vérifiées par les opérations $\mathcal{H}$, φ, σ et ζ. Ces propriétés seront utilisées souvent au cours des différentes preuves dans les sections suivantes.

Propriété 2. *(Passage à l'intersection)*
Les fonctions définies en 4 commutent avec l'intersection. Étant donné I,J deux idéaux de $\mathbb{Q}[t_1,\ldots,t_s][x_1,\ldots,x_n]$, *A un sous-anneau de* $\mathbb{Q}[t_1,\ldots,t_s][x_1,\ldots,x_n]$, *f un polynôme de* $\mathbb{Q}[t_1,\ldots,t_s][x_1,\ldots,x_n]$ *et q un rationnel, on a :*

- $\mathcal{H}(I \cap J) = \mathcal{H}(I) \cap \mathcal{H}(J)$
- $\varphi_A(I \cap J) = \varphi_A(I) \cap \varphi_A(J)$
- $\sigma^q_{x_i}(I \cap J) \overset{\surd}{=} \sigma^q_{x_i}(I) \cap \sigma^q_{x_i}(J)$
- $\zeta_f(I \cap J) = \zeta_f(I) \cap \zeta_f(J)$

Ainsi que :

- $\mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J)$

□

*preuve :*Chaque égalité s'obtient facilement en raisonnant par double inclusion.
□

Propriété 3. *(Commutation)*
Les fonctions définies en 4 peuvent commuter entre elles dans certains cas. Soit I un idéal, f,g deux polynômes et a,b deux rationnels. Alors :

i) $\zeta_f \circ \zeta_g(I) = \zeta_g \circ \zeta_f(I)$

ii) $\sigma^a_f \circ \sigma^b_g(I) = \sigma^b_g \circ \sigma^a_f(I)$

iii) $\mathcal{H} \circ \zeta_f(I) = \zeta_{\mathcal{H}(f)} \circ \mathcal{H}(I)$

□

*preuve :*L'égalité *i)* s'obtient en remarquant que $\zeta_f \circ \zeta_g(I) = \zeta_{fg}(I)$. Les égalités *ii)* et *iii)* s'obtiennent facilement par double inclusion.
□

Enfin, la propriété suivante énonce quelques règles de réductions qui s'avèrent utiles dans un cadre algorithmique.

Propriété 4. *(Simplifications affines)*
Soit I un idéal de $\mathbb{Q}[t_1,\dots,t_s][x_1,\dots,x_n]$, $f, p_1,\dots,p_m$ des polynômes et Z une variable supplémentaire. Alors :

i) $\varphi_A \circ \zeta_f(I) = \varphi_A(I + \langle Zf - 1\rangle)$

ii) $\sigma^1_{x_0} \circ \mathcal{H}(I) = I$

iii) $\mathcal{H}(p_1,\dots,p_m) = \zeta_{x_0}(\mathcal{H}(p_1),\dots,\mathcal{H}(p_m))$

□

*preuve :*L'égalité *i*) s'obtient en utilisant le critère de Rabinowitsch [115] selon lequel

$$\zeta_f(I) = (I + \langle Zf - 1\rangle) \cap \mathbb{Q}[t_1,\dots,t_s][x_1,\dots,x_n]$$

et donc :

$$\begin{aligned}\varphi_A \circ \zeta_f(I) &= (I + \langle Zf - 1\rangle) \cap \mathbb{Q}[t_1,\dots,t_s][x_1,\dots,x_n] \cap A \\ &= \varphi_A(I + \langle Zf - 1\rangle)\end{aligned}$$

L'égalité *ii*) s'obtient par double inclusion. Pour l'inclusion de droite à gauche, il suffit d'exhiber pour chaque élément f de I un polynôme g de I tel que $\sigma^1_{x_0} \circ \mathcal{H}(g) = f$. En choisissant $g = f$ on obtient directement le résultat voulu.

Pour l'autre inclusion, soit $f \in \sigma^1_{x_0} \circ \mathcal{H}(I)$. Alors, il existe $g \in I$ tel que $\sigma^1_{x_0} \circ \mathcal{H}(g) = f$. On va montrer que f appartient bien à I en montrant que $g = f$. D'abord, on sait que $f = \sigma^1_{x_0} \circ \mathcal{H}(f)$ et que la fonction $\sigma^1_{x_0}$ est linéaire, ce qui entraîne :

$$\sigma^1_{x_0}(\mathcal{H}(g) - \mathcal{H}(f)) = 0$$

Par ailleurs on peut vérifier que $\deg(g) = \deg(\sigma^1_{x_0} \circ \mathcal{H}(g)) = \deg(\sigma^1_{x_0} \circ \mathcal{H}(f)) = \deg(f)$. D'où $\mathcal{H}(g) - \mathcal{H}(f) = \mathcal{H}(g - f)$ et donc :

$$\sigma^1_{x_0} \circ \mathcal{H}(g - f) = 0$$

Ce qui signifie que le terme de degré maximal de $g - f$ est 0, donc $g = f$ ce qui nous permet de conclure la preuve de l'égalité.

Enfin, on démontre l'égalité *iii*) par double inclusion. Comme les deuw idéaux considérés sont homogènes, on peut sans restriction de généralité ne considérer que le cas où les polynômes choisis sont homogènes. L'inclusion de droite à gauche s'obtient en remarquant que si $f \in \zeta_{x_0}(\mathcal{H}(p_1),\dots,\mathcal{H}(p_m))$ est homogène en $x_0,\dots,x_n$, alors $\sigma^1_{x_0}(f) \in \langle p_1,\dots,p_m\rangle$, donc $f \in \mathcal{H}(p_1,\dots,p_m)$.

Pour l'autre inclusion, on remarque d'abord que si $f \in \mathbb{Q}[t_1,\dots,t_s][x_1,\dots,x_n]$, alors :

$$\mathcal{H}(f(t_1,\dots,t_s,x_1,\dots,x_n)) = x_0^{\deg(f)} f(t_1,\dots,t_s,\frac{x_1}{x_0},\dots,\frac{x_n}{x_0})$$

Ainsi, si $f \in \mathcal{H}(p_1, \ldots, p_m)$ est homogène en $x_0, \ldots, x_n$, alors, il existe $q_1, \ldots, q_m \in \mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]$ tels que :

$$\begin{aligned} p &= \mathcal{H}(q_1 p_1 + \cdots + q_m p_m) \\ &= x_0^{\deg(p)}(q_1 p_1)(t_1, \ldots, t_s, \frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}) + \cdots + x_0^{\deg(p)}(q_m p_m)(t_1, \ldots, t_s, \frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}) \\ &= x_0^{\deg(p)-\deg(q_1 p_1)}\mathcal{H}(q_1 p_) + \cdots + x_0^{\deg(p-\deg(q_m p_m))}\mathcal{H}(q_m p_m) \end{aligned}$$

D'où, en notant n le maximum des $\deg(q_i p_i)$, on a $x_0^n p \in \langle \mathcal{H}(p_1), \ldots, \mathcal{H}(p_m) \rangle$, ce qui nous permet de conclure.
□

Propriété 5. *(Simplifications projectives)*
Soient J un idéal et f un polynôme de $\mathbb{Q}[t_1, \ldots, t_s][x_0, x_1, \ldots, x_n]$, homogènes en $x_0, x_1, \ldots, x_n$. Soit A un sous-anneau de $\mathbb{Q}[t_1, \ldots, t_s][x_0, x_1, \ldots, x_n]$. Alors :

i) $\mathcal{H}_i \circ \sigma^1_{x_i}(J) = \zeta_{x_i}(J)$

ii) $\sigma^1_{x_i} \circ \zeta_f(J) = \zeta_{\sigma^1_{x_i}(f)} \circ \sigma^1_{x_i}(J)$

iii) $\varphi_A \circ \zeta_{x_i}(J) = \varphi_A \circ \sigma^1_{x_i}(J)$

iv) $\varphi_A \circ \sigma^1_{x_i}(J) = \sigma^1_{x_i} \circ \varphi_{A[x_i]}(J)$

□

*preuve :*Ces égalités sont des extensions des théorèmes donnés par exemple dans le livre [28, chapitre 8].
□

3.3.2 Degré

Préliminaires

Le degré d'une variété tel que défini Définition 9.2 vérifient plusieurs propriétés que l'on rappelle ici.

Propriété 6. *(Degrés)*
Soient I,J deux idéaux de $\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]$, A un sous-anneau de A, f un polynôme de degré d. Alors :

i) $\deg(\mathcal{V}(I) \cup \mathcal{V}(J)) \leq \deg(\mathcal{V}(I)) + \deg(\mathcal{V}(J))$

ii) $\deg(\mathcal{V}(I) \cap \mathcal{V}(J)) \leq \deg(\mathcal{V}(I)) \deg(\mathcal{V}(J))$

iii) $\deg(\mathcal{V}(\zeta_f(I))) \leq \deg(\mathcal{V}(I))$

iv) $\deg(\mathcal{V}(\varphi_A(I))) \leq \deg(\mathcal{V}(I))$

v) $\deg(\mathcal{V}(\langle f \rangle)) = d$

□

*preuve :*La première égalité est une conséquence directe de la définition du degré comme somme des degrés des composantes irréductibles d'une variété.

La deuxième inégalité est connue sous le nom d'inégalité de Bézout. J.Heintz prouve cette inégalité dans le cas général dans [63].

La troisième inégalité s'obtient en utilisant le lemme 24. En effet, comme l'ensemble des premiers isolés de $\zeta_f(I)$ est un sous-ensemble des premiers isolés de I, la définition 9.2 nous permet directement de conclure que le degré de $\mathcal{V}(\zeta_f(I))$ est inférieur au degré de $\mathcal{V}(I)$.

Pour la quatrième inégalité, on remarque que la fonction φ_A est linéaire, ce qui permet de prouver l'inégalité en utilisant le lemme 2 de [63].

Enfin, l'égalité v) peut s'obtenir facilement en remarquant qu'un espace affine E de dimension 1 peut s'exprimer sous forme paramétrique. Dans ce cas, les points d'intersections de E avec $\mathcal{V}(\langle f\rangle)$ sont solutions d'une équation polynomiale de degré au plus d, et exactement d en choisissant E de manière appropriée.
□

Degré des inéquations et valeurs critiques

Afin de prouver le théorème 3 sur le degré de la variété discriminante minimale d'un système paramétré S, on utilise la propriété 1 selon laquelle :

$$\mathcal{D}_S = V_{ineq}(S) \cup V_{crit}(S) \cup V_{inf}(S)$$

et on majore les degrés de chacune des variétés $V_{ineq}(S), V_{crit}(S), V_{inf}(S)$. La propriété 6 nous permettra alors de conclure que :

$$\deg(\mathcal{D}_S) = \deg(V_{ineq}(S)) + \deg(V_{crit}(S)) + \deg(V_{inf}(S))$$

On borne d'abord les degrés des variétés $V_{ineq}(S)$ et $V_{crit}(S)$.

Lemme 1. *Soit S un système paramétré bien posé. Alors, en utilisant les notations 3 et 5, on a les majorations suivantes :*

$$\deg(V_{ineq}(S)) \leq d_1 \cdots d_n \delta'$$
$$\deg(V_{crit}(S)) \leq d_1 \cdots d_n \delta$$

□

*preuve :*Par définition,

$$V_{ineq}(S) = \mathcal{V}(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]}(I_S + \langle g_S\rangle))$$
$$V_{crit}(S) = \mathcal{V}(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]}(I_S + \langle j_S\rangle))$$

ce qui implique, en utilisant les inégalités $ii), iv)$ et l'égalité v) de la propriété 6 :

$$\deg(V_{ineq}(S)) \leq \deg(I_S)\delta' \quad \text{et} \quad \deg(V_{crit}(S)) \leq \deg(I_S)\delta$$

Ensuite, I_S est défini en notations 3 par $I_S = \zeta_{g_S}(\langle f_1, \ldots, f_n\rangle)$. Ainsi, les inégalités $ii)$ et $iii)$ de la propriété 6 impliquent :

$$\deg(I_S) \leq d_1 \cdots d_n$$

Ce qui permet de conclure la preuve.
□

Degré des points à l'infini

La composante $V_{inf}(S)$ est obtenu par la projection d'une variété projective. On peut en particulier utiliser la théorie de l'élimination projective présentée dans [28, chapitre 8 §5] pour reformuler de façon plus algébrique $V_{inf}(S)$.

Lemme 2. *Soit S un système paramétré. Alors,*

$$V_{inf}(S) = \mathcal{V}\left(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]}\left(\bigcap_{i=1}^{n} \zeta_{x_i} \circ \sigma^0_{x_0} \circ \mathcal{H}(I_S)\right)\right)$$

□

*preuve :*D'abord, on a par construction $\mathcal{C}^p_S = \mathcal{V}(\mathcal{H}(I_S))$ et $\mathcal{H}_\infty = \mathcal{V}(\langle x_0 \rangle)$, ce qui implique :

$$\overline{\mathcal{C}_S} \cap \mathcal{H}_\infty = \overline{\mathcal{V}}\left(\sigma^0_{x_0} \circ \mathcal{H}(I_S)\right)$$

Ensuite, le théorème 6 et la proposition 8 du paragraphe 5 de [28, chapitre 8] prouvent que si I est un idéal de $\mathbb{Q}[t_1, \ldots, t_s][x_0, x_1, \ldots, x_n]$ homogène en $x_0, x_1, \ldots, x_n$, alors :

$$\overline{\pi}(\overline{\mathcal{V}}(I)) = \mathcal{V}\left(\bigcap_{i=0}^{n} \varphi_{\mathbb{Q}[t_1,\ldots,t_s]} \circ \sigma^1_{x_i}(I)\right)$$

En appliquant ce résultat à $\sigma^0_{x_0} \circ \mathcal{H}(I_S)$, on obtient alors :

$$V_{inf}(S) = \mathcal{V}\left(\bigcap_{i=1}^{n} \varphi_{\mathbb{Q}[t_1,\ldots,t_s]} \circ \sigma^1_{x_i} \circ \sigma^0_{x_0} \circ \mathcal{H}(I_S)\right)$$

Puis, en utilisant l'égalité *iii*) de la propriété 5, on obtient alors l'égalité voulue.
□

Cela nous permet de borner le degré de la composante $V_{inf}(S)$.

Lemme 3. *Soit S un système bien posé. Alors, avec les notations 3 et 5, on a :*

$$V_{inf}(S) \leq d_1 \cdots d_n$$

□

*preuve :*D'après le lemme 2 et en utilisant l'inégalité *iv*) du lemme 6, on sait que le degré de $V_{inf}(S)$ est majoré par le degré de :

$$V := \mathcal{V}(\bigcap_{i=1}^{n} \zeta_{x_i} \circ \sigma^0_{x_0} \circ \mathcal{H}(I_S))$$

En particulier, minass$(\bigcap_{i=1}^{n} \zeta_{x_i} \circ \sigma^0_{x_0} \circ \mathcal{H}(I_S))$ est l'ensemble des idéaux premiers isolés de chacun des $\zeta_{x_i} \circ \sigma^0_{x_0} \circ \mathcal{H}(I_S)$, qui sont aussi des premiers isolés de $\sigma^0_{x_0} \circ \mathcal{H}(I_S)$ d'après le lemme 24. Ainsi, le degré de V est majoré par le degré de :

$$\mathcal{V}(\sigma^0_{x_0} \circ \mathcal{H}(I_S))$$

Enfin, la variété de $\sigma^0_{x_0} \circ \mathcal{H}(I_S)$ est de degré inférieur à celui de la variété de $\mathcal{H}(I_S) = \zeta_{x_0\mathcal{H}(g_S)}(\langle \mathcal{H}(f_1), \ldots, \mathcal{H}(f_n)\rangle)$.

Ainsi, en utilisant l'inégalité de Bézout, on a :

$$\deg(\mathcal{V}(\sigma^0_{x_0} \circ \mathcal{H}(I_S))) \leq d_1 \cdots d_n$$

ce qui nous permet de conclure.
□

3.3.3 Algorithme de réduction

On s'attache maintenant à réduire le calcul de la variété discriminante minimale d'un système bien posé à $n+1$ calculs d'élimination de variables. Le précédent algorithme donné en [87] pour le calcul d'une variété discriminante s'appuyait sur des calculs de bases de Gröbner, qui peuvent s'avérer efficace en pratique, mais dont la complexité dans le pire cas est doublement exponentielle en le nombre de variables.

Le calcul d'élimination de variables possède de meilleurs bornes de complexité ([96, 5]), ce qui guide notre réduction du calcul de la variété discriminante minimale à cette fonction.

Réduction de V_{crit}

Le calcul des composantes $V_{crit}(S) \cup V_{ineq}(S)$ peut se ramener au calcul de $V_{ineq}(S')$ où S' est le système S auquel on a rajouté l'inéquation j_S.

Proposition 2. *Soit S un système paramétré bien posé. Avec les notations 3, on définit S' comme le système paramétré donné par les équations et les inéquations de S augmenté de l'inéquation $j_S \neq 0$. Alors, en utilisant les notations 5, on a :*

$$V_{ineq}(S) \cup V_{crit}(S) \cup V_{inf}(S) = V_{inf}(S) \cup V_{ineq}(S')$$

□

*preuve :*On raisonne par double inclusion. Pour l'inclusion de droite à gauche, on remarque que par construction on a $V_{ineq}(S') \subset V_{ineq}(S) \cup V_{crit}(S)$.

Pour l'autre inclusion, comme S est bien posé, on sait que l'idéal J engendré par I_S dans $\mathbb{Q}(t_1, \ldots, t_s)[x_1, \ldots, x_n]$ est radical. En particulier, si P est un premier isolé de I_S tel que $\varphi_{\mathbb{Q}[t_1,\ldots,t_s]}(P) = \{0\}$, alors l'idéal engendré par P dans $\mathbb{Q}(t_1, \ldots, t_s)[x_1, \ldots, x_n]$ est un premier isolé de J. Comme J est radical, le critère jacobien implique $j_S \notin P$. Ainsi :

$$\mathcal{V}(\bigcap_{\substack{P \in \text{minass}(I_S) \\ \varphi_{\mathbb{Q}[t_1,\ldots,t_s]}(P)=\{0\}}} P) \subset \mathcal{V}(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]}(I_S))$$

Par ailleurs, on a par construction :

$$\mathcal{V}(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]}(\bigcap_{\substack{P \in \text{minass}(I_S) \\ \varphi_{\mathbb{Q}[t_1,\ldots,t_s]}(P)\neq\{0\}}} P)) \subset V_{inf}(S)$$

Cela entraîne pour tout polynôme p de $\mathbb{Q}[t_1,\ldots,t_s][x_1,\ldots,x_n]$:

$$\mathcal{V}(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]}(I_S+\langle p\rangle)) \subset V_{inf}(S)\cup\mathcal{V}(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]}(\zeta_{j_S}(I_S)+\langle p\rangle)$$

Ainsi, on peut en déduire :

$$\begin{aligned} V_{ineq}(S)\cup V_{crit}(S) &= \mathcal{V}(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]}(I_S+\langle j_S g_S\rangle)) \\ &\subset V_{inf}(S)\cup\mathcal{V}(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]}(\zeta_{j_S}(I_S)+\langle j_S g_S\rangle)) \\ &\subset V_{inf}(S)\cup V_{ineq}(S') \end{aligned}$$

□

Réduction de V_{inf}

On montre dans cette section comment réduire le calcul de la composante $V_{inf}(S)$ à un calcul d'élimination de variables.

Préliminaires Étant donné un système paramétré S, le lemme 2 et la propriété 2 nous permettent d'écrire :

$$V_{inf}(S)=\bigcup_{i=1}^{n}\mathcal{V}(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]}\circ\zeta_{x_i}\circ\sigma^0_{x_0}\circ\mathcal{H}(I_S))$$

Afin d'économiser le coût des saturations, on peut aussi réécrire $V_{inf}(S)$ de la manière suivante :

Lemme 4. *Étant donné un système paramétré S, avec les notations du théorème 4 :*

$$V_{inf}(S)=\bigcup_{i=1}^{n}\mathcal{V}(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]}\circ\sigma^0_{x_0}\circ\varphi_{\mathbb{Q}[t_1,\ldots,t_s][x_1,\ldots,x_n]}(I_i^S))$$

□

*preuve :*D'après le lemme 2, on a :

$$V_{inf}(S)=\bigcup_{i=1}^{n}\mathcal{V}(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]}\circ\zeta_{x_i}\circ\sigma^0_{x_0}\circ\mathcal{H}(I_S))$$

Soit J_i l'idéal $\varphi_{\mathbb{Q}[t_1,\ldots,t_s]}\circ\zeta_{x_i}\circ\sigma^0_{x_0}\circ\mathcal{H}(I_S))$. Afin de prouver le lemme, on doit montrer que $J_i=\varphi_{\mathbb{Q}[t_1,\ldots,t_s]}\circ\sigma^0_{x_0}\circ\varphi_{\mathbb{Q}[t_1,\ldots,t_s][x_1,\ldots,x_n]}(I_i^S)$.
L'idéal $\sigma^0_{x_0}\circ\mathcal{H}(I_S)$ est homogène, donc d'après l'égalité *iii*) de la propriété 5, on a :

$$\begin{aligned} J_i &= \varphi_{\mathbb{Q}[t_1,\ldots,t_s]}\circ\zeta_{x_i}\circ\sigma^0_{x_0}\circ\mathcal{H}(I_S) \\ &= \varphi_{\mathbb{Q}[t_1,\ldots,t_s]}\circ\sigma^1_{x_i}\circ\sigma^0_{x_0}\circ\mathcal{H}(I_S)) \end{aligned}$$

Ensuite, par définition de I_S, et en utilisant l'égalité *iii*) de la propriété 4 :

$$J_i=\varphi_{\mathbb{Q}[t_1,\ldots,t_s]}\circ\sigma^1_{x_i}\circ\sigma^0_{x_0}\circ\zeta_{x_0\mathcal{H}(g_S)}\left(\langle\mathcal{H}(f_1),\ldots,\mathcal{H}(f_n)\rangle\right)$$

d'où, d'après l'égalité i) de la propriété 4 :

$$J_i = \varphi_{\mathbb{Q}[t_1,\ldots,t_s]} \circ \sigma^1_{x_i} \circ \sigma^0_{x_0} \circ \varphi_{\mathbb{Q}[t_1,\ldots,t_s][x_1,\ldots,x_n]} \left(\langle \mathcal{H}(f_1), \ldots, \mathcal{H}(f_n), Zx_0\mathcal{H}(g_S) - 1\rangle\right)$$

Enfin, par définition,

$$I_i^S = \sigma^1_{x_i}(\mathcal{H}(f_1), \ldots, \mathcal{H}(f_n), Zx_0\mathcal{H}(g_S) - 1)$$

d'où, en faisant commutant la fonction $\sigma^1_{x_i}$ avec les lemme 3 et 5 :

$$J_i = \varphi_{\mathbb{Q}[t_1,\ldots,t_s]} \circ \sigma^0_{x_0} \circ \varphi_{\mathbb{Q}[t_1,\ldots,t_s][x_1,\ldots,x_n]}(I_i^S)$$

□

D'un point de vue algorithmique, les formulations ci-dessus ne constituent cependant pas une réduction à l'algorithme d'élimination de variables, car pour calculer l'idéal homogène engendré par I_S, une saturation par x_0 est toujours nécessaire. Cependant, la variété suivante se calcule directement par élimination de variables.

Notations 7. *Si S est un système paramétré, avec les notations du théorème 4, on note $V^\star_{inf}(S)$ la variété définie par :*

$$V^\star_{inf}(S) = \bigcup_{i=1}^{n} \mathcal{V}(\sigma^0_{x_0} \circ \varphi_{\mathbb{Q}[t_1,\ldots,t_s,x_0]}(I_i^S))$$

□

La proposition suivante montre que l'on peut commuter les fonctions $\varphi_{\mathbb{Q}[t_1,\ldots,t_s]}$ et $\sigma^0_{x_0}$, ce qui est cruciale pour réduire le calcul des points à l'infini à n calculs d'élimination de variables.

Proposition 3. *Soit S un système paramétré. Alors, en utilisant les notations 5, on a :*

$$V_{inf}(S) = V^\star_{inf}(S)$$

□

On va montrer la proposition par double inclusion.

Inclusion de V_{inf} dans $V^\star_{inf}$ Le lemme suivant nous permet de montrer que $V_{inf}(S) \subset V^\star_{inf}(S)$.

Lemme 5. *Soit I un idéal de $\mathbb{Q}[t_1, \ldots, t_s][x_0, x_1, \ldots, x_n]$. Alors :*

$$\sigma^0_{x_0} \circ \varphi_{\mathbb{Q}[t_1,\ldots,t_s,x_0]}(I) \subset \varphi_{\mathbb{Q}[t_1,\ldots,t_s]} \circ \sigma^0_{x_0}(I)$$

□

*preuve :*Soit p un polynôme de $\sigma^0_{x_0} \circ \varphi_{\mathbb{Q}[t_1,\ldots,t_s,x_0]}(I)$. Alors, par hypothèse, $p \in \sigma^0_{x_0}(I)$ et $p \in \mathbb{Q}[t_1,\ldots,t_s]$, d'où $p \in \varphi_{\mathbb{Q}[t_1,\ldots,t_s]} \circ \sigma^0_{x_0}(I)$.
□

Ainsi, ces lemmes nous permettent de déduire la première inclusion nécessaire pour prouver la réduction.

Lemme 6. *Soit S un système paramétré.*

$$V_{inf}(S) \subset V^\star_{inf}(S)$$

□

*preuve :*Avec les notations du théorème 4, on a d'après le lemme 4 :

$$V_{inf}(S) = \bigcup_{i=1}^{n} \mathcal{V}(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]} \circ \sigma^0_{x_0} \circ \varphi_{\mathbb{Q}[t_1,\ldots,t_s][x_1,\ldots,x_n]}(I_i^S))$$

En appliquant le lemme 5 à chacun des I_i^S, on en déduit :

$$V_{inf}(S) \subset \bigcup_{i=1}^{n} \mathcal{V}(\sigma^0_{x_0} \circ \varphi_{\mathbb{Q}[t_1,\ldots,t_s,x_0]}(I_i^S)) = V^\star_{inf}(S)$$

□

Inclusion de $V^\star_{inf}$ dans V_{inf} L'inclusion de $V^\star_{inf}(S)$ dans $V_{inf}(S)$ est plus délicate.

Le lemme suivant est essentiel pour prouver que l'on peut commuter les fonctions $\varphi_{\mathbb{Q}[t_1,\ldots,t_s,x_0]}$ et $\sigma^0_{x_0}$ dans l'écriture de $V_{inf}(S)$.

Lemme 7. *Soient K un corps, A un sous-anneau de K et I un idéal 0-dimensionnel de $K[x_1,\ldots,x_n]$. Supposons en outre qu'il existe G une base de Gröbner de I telle que :*

- *$G \subset A[x_1,\ldots,x_n]$*
- *l'inverse des coefficients de têtes des polynômes de G appartiennent à A*

Alors, il existe un polynôme $p \in I$ tel que :

i) le coefficient de tête de p est 1

ii) $p \in A[x_1]$

iii) $p \in J$ où J est l'idéal engendré par G dans $A[x_1,\ldots,x_n]$

□

Remarque 3. *Dans le cas où $A = K$, on retrouve le lemme classique montrant que l'on peut toujours trouver un polynôme univarié, de coefficient de tête 1 dans un idéal 0-dimensionnel.*

*preuve :*Comme I est de dimension 0, l'anneau quotient $K[x_1,\ldots,x_n]/I$ est aussi un K-espace vectoriel de dimension finie. Si f est un polynôme de $K[x_1,\ldots,x_n]$, on note $\hat{f}$ la classe de f dans $K[x_1,\ldots,x_n]/I$. On note $\mathbf{T}$ l'ensemble des monômes de $K[x_1,\ldots,x_n]$ et $\mathbf{T}(G)$ l'ensemble des monômes de $K[x_1,\ldots,x_n]$ divisibles par le monôme de tête d'un des

polynômes de G. Comme G est une base de Gröbner, cela implique directement que la famille $\mathbf{e}$ de $K[x_1, \ldots, x_n]/I$:

$$\mathbf{e} = \{\hat{m} \mid m \in \mathbf{T} \setminus \mathbf{T}(G)\}$$

est une base de l'espace vectoriel $K[x_1, \ldots, x_n]/I$. En particulier, si f est un polynôme de $K[x_1, \ldots, x_n]$, les coordonnées de $\hat{f}$ dans la base $\mathbf{e}$ sont les coefficients de la forme normale de f modulo la base de Gröbner G.

Pour l'assertion i), on considère m_{x_1} la fonction de multiplication définie par :

$$\begin{array}{rccc} m_{x_1} : & K[x_1, \ldots, x_n]/I & \rightarrow & K[x_1, \ldots, x_n]/I \\ & e & \mapsto & \hat{x_1} e \end{array}$$

C'est une application linéaire que l'on introduit classiquement pour construire un polynôme unitaire et univarié en x_1 de l'idéal I. On considère ensuite la matrice M_{x_1} de m_{x_1} dans la base e, et on note χ_{x_1} son polynôme caractéristique. D'après le théorème de Cayley-Hamilton :

$$\chi_{x_1}(M_{x_1}) = 0$$

Ainsi, l'application qui à $e \in K[x_1, \ldots, x_n]/I$ associe $\chi_{x_1}(\hat{x_1})e$ est l'application nulle. En particulier, pour $e = \hat{1}$, on a $\chi_{x_1}(\hat{x_1}) = \hat{0}$, et donc :

$$\chi_{x_1}(x_1) \in I$$

et le coefficient de tête est 1.

Pour l'assertion ii), on doit montrer que les coefficients de $\chi_{x_1}(x_1)$ appartiennent à A. Pour cela, il suffit de prouver que les coefficients de la matrice M_{x_1} sont dans A. Ces coefficients sont ceux des formes normales des monômes $x_1 m$ pour $m \in \mathbf{T}$. Soit $m \in \mathbf{T}$. Alors les règles de réduction permettant de calculer la forme normale de $x_1 m$ consistent à ajouter successivement à $x_1 m$ des polynômes de la forme :

$$\frac{1}{c(g)} rtg$$

où g appartient à G, $c(g)$ est le coefficient de tête de g, r un élément de A et t un monôme. En particulier, par hypothèse, tous les coefficients de ce polynôme appartiennent à A. Cela permet de conclure que tous les coefficients de la forme normale de $x_1 m$ sont dans A, ce qui achève la preuve du l'assertion.

Enfin, pour l'assertion iii), on sait que p appartient à l'idéal contracté $A[x_1, \ldots, x_n] \cap I$. En particulier, le calcul de sa forme normale selon la base G vaut zéro. En utilisant le même argument que ci-dessus, on en déduit que p s'écrit comme une combinaison des polynômes de G de la forme :

$$p = \sum_{g \in G} q_g g \text{ où } q_g \in A[x_1, \ldots, x_n] \text{ pour tout } g \in G$$

ce qui permet de conclure.

□

On peut maintenant étudier l'effet de la commutation des fonctions $\varphi_{\mathbb{Q}[t_1,\ldots,t_s,x_0]}$ et $\sigma^0_{x_0}$ plus précisément.

Lemme 8. *Soit I un idéal de $\mathbb{Q}[t_1,\dots,t_s][x_0,\dots,\widehat{x_j},\dots,x_n]$. Alors, avec les notations 3 et 5 on a :*

$$\sigma^0_{x_0}\circ\varphi_{\mathbb{Q}[t_1,\dots,t_s,x_0]}(I)\overset{\surd}{\supset}\varphi_{\mathbb{Q}[t_1,\dots,t_s]}\circ\sigma^0_{x_0}\left(\bigcap_{i=1}^{n}\sigma^1_{x_i}\circ\mathcal{H}_j(I)\right)$$

□

*preuve :*D'abord, d'après les propriétés de $\sigma^1_{x_i}$ vue en Propriété 3 et 5, l'ensemble de droite peut se réécrire :

$$\varphi_{\mathbb{Q}[t_1,\dots,t_s]}\circ\sigma^0_{x_0}\left(\bigcap_{i=1}^{n}\sigma^1_{x_i}\circ\mathcal{H}_j(I)\right)=\bigcap_{i=1}^{n}\varphi_{\mathbb{Q}[t_1,\dots,t_s]}\circ\zeta_{x_i}\circ\sigma^0_{x_0}\circ\mathcal{H}_j(I)$$

Alors, soit p un élément de $\bigcap_{i=1}^{n}\varphi_{\mathbb{Q}[t_1,\dots,t_s]}\circ\zeta_{x_i}\circ\sigma^0_{x_0}\circ\mathcal{H}_j(I)$. Par hypothèse, il existe $q_1,\dots,q_n\in\mathbb{Q}[t_1,\dots,t_s][x_0,x_1,\dots,x_n]$ et $k_1,\dots,k_n\in\mathbb{N}$ tels que $p_1,\dots,p_n$ sont définis par :

$$\begin{cases}p_1:=px_1^{k_1}+x_0q_1\\ \quad\vdots\\ p_n:=px_n^{k_n}+x_0q_n\end{cases}\in\mathcal{H}_j(I)$$

Comme $\mathcal{H}_j(I)$ est homogène en $x_0,\dots,x_n$, la partie homogène de degré k_i de p_i appartient aussi à $\mathcal{H}_j(I)$, et on peut supposer sans restriction de généralité que $p_1,\dots,p_n$ sont homogènes en $x_0,\dots,x_n$, de degrés k_i, et en particulier :

$$\deg_{x_0,\dots,x_n}(x_0q_i)=k_i\Rightarrow\deg_{x_1,\dots,x_n}(q_i)<k_i$$

Soit K le corps de fractions $\mathbb{Q}(t_1,\dots,t_s,x_0)$. On considère alors $G\subset\mathbb{Q}(t_1,\dots,t_s,x_0)[x_1,\dots,x_n]$ l'ensemble des polynômes $p_1,\dots,p_n$. Soit $\mathbf{T}$ l'ensemble des monômes de $K[x_1,\dots,x_n]$ et $<_{\mathbf{T}}$ un ordre admissible sur $\mathbf{T}$ compatible avec l'ordre du degré. Alors, le terme de tête de p_i est $px_i^{k_i}$ et G est une base de Gröbner selon l'ordre $<_{\mathbf{T}}$ car les monômes de têtes de chacun des p_i sont étrangers. L'ensemble des coefficients de têtes des polynômes de G est $\{p\}$.

Soit S l'ensemble multiplicativement clos :

$$S:=\bigcup_{i=0}^{\infty}\{p^i\}$$

On note A l'anneau de fraction $S^{-1}\mathbb{Q}[t_1,\dots,t_s,x_0]\subset K$. Alors, on vérifie facilement que G satisfait toutes les conditions du lemme 7. On peut ainsi en déduire qu'il existe un polynôme q dans l'idéal engendré par G dans $A[x_1,\dots,x_n]$ tel que $q\in A[x_j]$ et son coefficient de tête est 1.

En particulier, il existe un entier k tel que :

$$p^kq\in\mathcal{H}_j(I)\cap\mathbb{Q}[t_1,\dots,t_s][x_0,x_j]$$

En notant r la partie homogène de plus haut degré de $p^k q$, on a $r \in \mathcal{H}_j(I) \cap \mathbb{Q}[t_1, \ldots, t_s][x_0, x_j]$, qui peut s'écrire sous la forme :

$$r = p^k x_j^l + x_0 s \text{ où } l \in \mathbb{N} \text{ et } s \in \mathbb{Q}[t_1, \ldots, t_s][x_0, x_j]$$

Ainsi, $\sigma^1_{x_j}(r) \in I \cap \mathbb{Q}[t_1, \ldots, t_s, x_0]$ et d'après l'égalité $ii)$ de la propriété 4, d'où :

$$p^k + x_0 \sigma^1_{x_j}(s) \in I \cap \mathbb{Q}[t_1, \ldots, t_s, x_0] \Rightarrow p \in \sqrt{\sigma^0_{x_0} \circ \varphi_{\mathbb{Q}[t_1,\ldots,t_s,x_0]}(I)}$$

ce qui achève la preuve du lemme.
□

Nous pouvons maintenant prouver l'inclusion de $V^\star_{inf}(S)$ dans $V_{inf}(S)$.

Lemme 9. *Soit S un système paramétré.*

$$V^\star_{inf}(S) \subset V_{inf}(S)$$

□

*preuve :*D'après le lemme 4, on sait que :

$$V_{inf}(S) = \mathcal{V}\left(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]} \circ \sigma^0_{x_0}\left(\bigcap_{i=1}^{n} \varphi_{\mathbb{Q}[t_1,\ldots,t_s][x_1,\ldots,x_n]}(I_i^S)\right)\right) \qquad (*)$$

Par ailleurs, d'après le lemme 4 on a :

$$\varphi_{\mathbb{Q}[t_1,\ldots,t_s][x_1,\ldots,x_n]}(I_i^S) = \sigma^1_{x_i} \circ \mathcal{H}(I_S)$$

ce qui entraîne que pour tout i, j entre 1 et n on a :

$$\varphi_{\mathbb{Q}[t_1,\ldots,t_s][x_1,\ldots,x_n]}(I_i^S) = \sigma^1_{x_i} \circ \mathcal{H}_j \circ \varphi_{\mathbb{Q}[t_1,\ldots,t_s][x_1,\ldots,x_n]}(I_j^S)$$

Ainsi, pour tout j entre 1 et n, en remplaçant $\varphi_{\mathbb{Q}[t_1,\ldots,t_s][x_1,\ldots,x_n]}(I_i^S)$ par $\sigma^1_{x_i} \circ \mathcal{H}_j \circ \varphi_{\mathbb{Q}[t_1,\ldots,t_s][x_1,\ldots,x_n]}(I_j^S)$ dans l'équation (*), on déduit d'après le lemme 8 :

$$V_{inf}(S) \supset \mathcal{V}\left(\sigma^0_{x_0} \circ \varphi_{\mathbb{Q}[t_1,\ldots,t_s]} \circ \varphi_{\mathbb{Q}[t_1,\ldots,t_s][x_1,\ldots,x_n]}(I_j^S)\right)$$

On en conclut que $V_{inf}(S)$ contient l'union des $\mathcal{V}\left(\sigma^0_{x_0} \circ \varphi_{\mathbb{Q}[t_1,\ldots,t_s]}(I_j^S)\right)$ pour tous les j entre 1 et n, ce qui constitue exactement la variété $V^\star_{inf}(S)$.
□

Réduction de V_{ineq}

On montre ici comment réduire le calcul de la variété $V_{ineq}(S)$ à un calcul d'élimination de variables.

Préliminaire Par définition 5, on a :

$$V_{ineq}(S) = \mathcal{V}\left(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]}(\zeta_{g_S}(f_1,\ldots,f_n) + \langle g_S\rangle)\right)$$

Cette définition ne permet pas directement de calculer $V_{ineq}(S)$ par un algorithme d'élimination de variables. On introduit alors la variété $V^\star_{ineq}$.

Notations 8. *Soit S un système paramétré. On note $V^\star_{ineq}(S)$ la variété définie par :*

$$V^\star_{ineq}(S) = \mathcal{V}\left(\sigma^0_{x_0} \circ \varphi_{\mathbb{Q}[t_1,\ldots,t_s,x_0]}(f_1,\ldots,f_n, g_S - x_0, Zx_0 - 1)\right)$$

□

Le calcul de cette variété est une élimination de variables. La proposition suivante montre de plus que le calcul de $V_{ineq}(S)$ peut se réduire à celui de $V^\star_{ineq}(S)$ pour le calcul de la variété discriminante $\mathcal{D}_S$.

Proposition 4. *Soit S un système paramétré. Alors, avec la notation 8 on a :*

$$V_{ineq}(S) \subset V^\star_{ineq}(S) \subset V_{ineq}(S) \cup V_{inf}(S)$$

□

On va montrer cette égalité par double inclusion.

Inclusion de V_{ineq} dans $V^\star_{ineq}$ Afin de démontrer l'inclusion de $V_{ineq}(S)$ dans $V^\star_{ineq}(S)$, on montre d'abord que l'on peut réécrire $V_{ineq}(S)$ sous une forme différente qui nous permettra d'utiliser directement le lemme 5 pour conclure.

Lemme 10. *Soient $p_1,\ldots,p_m,q,r \in \mathbb{Q}[t_1,\ldots,t_s][x_0,x_1,\ldots,x_n]$. Soient $\mathbf{T}$ l'ensemble des monômes de $\mathbb{Q}[t_1,\ldots,t_s][x_0,x_1,\ldots,x_n]$ et $<_{\mathbf{T}}$ un ordre sur les monômes. Supposons que le monôme de tête de q ne possède aucune variable en commun avec les polynômes $p_1,\ldots,p_m$ et r. Alors :*

$$\zeta_r(p_1,\ldots,p_m) + \langle q\rangle = \zeta_r(p_1,\ldots,p_m,q)$$

□

Corollaire 3. *Soient S un système paramétré. Alors :*

$$V_{ineq}(S) = \mathcal{V}\left(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]} \circ \sigma^0_{x_0} \circ \zeta_{x_0}(f_1,\ldots,f_n, x_0 - g_S)\right)$$

□

preuve du corollaire: Par définition,

$$V_{ineq}(S) = \mathcal{V}\left(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]}(\zeta_{g_S}(f_1,\ldots,f_n) + \langle g_S\rangle)\right)$$

et en particulier, on peut même écrire

$$V_{ineq}(S) = \mathcal{V}\left(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]} \circ \sigma^0_{x_0}(\zeta_{g_S}(f_1,\ldots,f_n) + \langle x_0 - g_S\rangle)\right)$$

ce qui nous permet d'obtenir en utilisant le lemme 10 avec $m = n$ et $f_1, \ldots, f_n, x_0 - g_S, g_S$ à la place de $p_1, \ldots, p_m, q, r$:

$$V_{ineq}(S) = \mathcal{V}\left(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]} \circ \sigma^0_{x_0} \circ \zeta_{g_S}(f_1, \ldots, f_n, x_0 - g_S)\right)$$

Enfin, comme $x_0 - g_S$ est dans l'idéal que l'on sature par g_S, une saturation par x_0 est équivalente, d'où l'égalité finale.
□ *preuve du lemme:* D'abord, l'inclusion de gauche à droite est toujours vraie.

Pour l'autre inclusion, soit $p \in \zeta_r(p_1, \ldots, p_m, q)$. Alors, il existe un entier l et des polynômes $c_1, \ldots, c_m, c$ tels que :

$$r^l p = c_1 p_1 + \cdots + c_m p_m + cq$$

En utilisant l'ordre $<_{\mathbf{T}}$, on divise chacun des polynômes $p, c_1, \ldots, c_m$ par q, et on note respectivement $p', c'_1, \ldots, c'_m$ les restes de ces divisions. Ainsi, il existe un polynômes c' tel que :

$$r^l p' = c'_1 p_1 + \cdots + c'_m p_m + c'q$$

En outre, si on note $\mathrm{M}(q)$ le monôme de tête de q, on peut remarquer que tous les monômes de $p', c'_1, \ldots, c'_m$ sont strictement plus petits que $\mathrm{M}(q)$. En particulier, comme $r, p_1, \ldots, p_m$ n'ont pas de variable en commun avec $\mathrm{M}(q)$, on peut en déduire qu'aucun monôme de $r^l p', c'_1 p_1, \ldots, c'_m p_m$ n'est multiple de $\mathrm{M}(q)$. Or

$$c'q = r^l p' - c'_1 p_1 - \cdots - c'_m p_m$$

donc en notant $\mathrm{M}(c')$ le monôme de tête de c', on en déduit que le monôme de tête de $r^l p - c_1 p_1 - \cdots - c_m p_m$ est $\mathrm{M}(c')\ \mathrm{M}(q)$. Comme le terme de tête de cette expression ne peut pas être un multiple de $\mathrm{M}(q)$, cela signifie que $\mathrm{M}(c') = 0$ et donc :

$$p' \in \zeta_r(p_1, \ldots, p_m)$$

ce qui permet de conclure que p est bien dans l'ensemble de gauche de l'égalité du lemme.
□

Nous avons maintenant les éléments suffisant pour prouver la première inclusion de la proposition 4.

Lemme 11. *Soit S un système paramétré. Alors, avec la notation 8 on a :*

$$V_{ineq}(S) \subset V^{\star}_{ineq}(S)$$

□

*preuve :*D'après le corollaire 3, on peut réécrire $V_{ineq}(S)$:

$$V_{ineq}(S) = \mathcal{V}\left(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]} \circ \sigma^0_{x_0} \circ \zeta_{x_0}(f_1, \ldots, f_n, x_0 - g_S)\right)$$

En utilisant le lemme 5 on a alors directement :

$$V_{ineq}(S) \subset \mathcal{V}\left(\sigma^0_{x_0} \circ \varphi_{\mathbb{Q}[t_1,\ldots,t_s,x_0]} \circ \zeta_{x_0}(f_1, \ldots, f_n, x_0 - g_S)\right)$$

ce qui nous permet de conclure en utilisant l'égalité $i)$ de la propriété 4.
□

Inclusion de $V^{\star}_{ineq}$ dans $V_{ineq} \cup V_{inf}$ L'inclusion de $V^{\star}_{ineq}(S)$ dans $V_{ineq}(S) \cup V_{inf}(S)$ est un peu plus technique. Pour la démontrer, on va utiliser la décomposition vue en Lemme 8.Puis avec le lemme suivant on scindera chaque composante en deux variétés qui seront respectivement incluses dans $V_{ineq}(S)$ et $V_{inf}(S)$.

Lemme 12. *Soit I un idéal de $\mathbb{Q}[t_1, \ldots, t_s][x_1, \ldots, x_n]$, et P,q deux polynômes. Alors :*

$$I + \langle pq \rangle \overset{\surd}{=} (I + \langle p \rangle) \cap \zeta_p(I + \langle q \rangle)$$

□

*preuve :*D'abord, si $f \in I + \langle pq \rangle$, on en déduit directement que $f \in I + \langle p \rangle$ et $f \in I+ \subset \zeta_p(I + \langle q \rangle)$.

Pour l'autre inclusion, soit $f \in (I + \langle p \rangle) \cap \zeta_p(I + \langle q \rangle)$. Alors, il existe $i, i' \in I$, $k, k' \in \mathbb{Q}[t_1, \ldots, t_s]$ et $l \in \mathbb{N}$ tels que :

$$\begin{cases} f = i + kp \\ p^l x = a' + k'q \end{cases}$$

En développant f^l, on en déduit qu'il existe $i'' \in I$ tel que $f^l = i'' + k^l p^l$. Ainsi, on peut alors vérifier que $f^{l+1} \in I + \langle q \rangle$ et que $f^{l+2} \in I + \langle pq \rangle$.
□

On peut maintenant démontrer le dernier lemme permettant d'achever la preuve de la proposition 4.

Lemme 13. *Soit S un système paramétré. Alors,*

$$V^{\star}_{ineq}(S) \subset V_{ineq}(S) \cup V_{inf}(S)$$

□

*preuve :*En reprenant la notation 8 et en la modifiant avec l'égalité $i)$ de la propriété 4, $V^{\star}_{ineq}(S)$ peut s'écrire :

$$V^{\star}_{ineq}(S) = \mathcal{V}\left(\sigma^0_{x_0} \circ \varphi_{\mathbb{Q}[t_1,\ldots,t_s,x_0]} \circ \zeta_{g_S}(f_1, \ldots, f_n, g_S - x_0)\right)$$

En utilisant le lemme 8, on en déduit :

$$V^{\star}_{ineq}(S) \subset \bigcup_{i=1}^{n+1} \mathcal{V}\left(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]} \circ \sigma^0_{x_0} \circ \sigma^1_{x_i} \circ \mathcal{H}_{n+1} \circ \zeta_{g_S}(f_1, \ldots, f_n, g_S - x_0)\right)$$

Par ailleurs, on peut remarquer que :

$$\sigma^0_{x_0} \circ \mathcal{H}_{n+1} \circ \zeta_{g_S}(f_1, \ldots, f_n, g_S - x_0) \supset \mathcal{H}_{n+1} \circ \zeta_{g_S}(f_1, \ldots, f_n) + \langle x_{n+1} \mathcal{H}_{n+1}(g_S) \rangle$$

Et d'après le lemme 12, en notant :

$$\begin{cases} I_1 = \mathcal{H}_{n+1}(I_S) + \langle x_{n+1} \rangle \\ I_2 = \zeta_{x_{n+1}}\left(\mathcal{H}_{n+1} \circ \zeta_{g_S}(f_1, \ldots, f_n) + \langle \mathcal{H}_{n+1}(g_S) \rangle\right) \end{cases}$$

on a donc :

$$\sigma^0_{x_0} \circ \mathcal{H}_{n+1} \circ \zeta_{g_S}(f_1, \ldots, f_n, g_S - x_0) \overset{\sqrt{}}{\supset} I_1 \cap I_2$$

Cela nous permet de déduire :

$$V^\star_{ineq}(S) \subset \bigcup_{i=1}^{n+1} \mathcal{V}\left(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]} \circ \sigma^1_{x_i}(I_1)\right) \cup \bigcup_{i=1}^{n+1} \mathcal{V}\left(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]} \circ \sigma^1_{x_i}(I_2)\right)$$

En utilisant la formulation $V_{inf}(S)$ présentée en Lemme 2, on en déduit que pour tout i,$1 \leq i \leq n+1$, on a :

$$\mathcal{V}\left(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]} \circ \sigma^1_{x_i}(I_1)\right) \subset V_{inf}(S)$$

Enfin on a :

$$\begin{aligned}
\mathcal{V}\left(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]} \circ \sigma^1_{x_i}(I_2)\right) &= \mathcal{V}\left(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]} \circ \zeta_{x_i} \circ \zeta_{x_{n+1}}\left(\mathcal{H}_{n+1} \circ \zeta_{g_S}(f_1, \ldots, f_n) + \langle \mathcal{H}_{n+1}(g_S)\rangle\right)\right) \\
&= \mathcal{V}\left(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]} \circ \sigma^1_{x_{n+1}} \circ \zeta_{x_i}\left(\mathcal{H}_{n+1} \circ \zeta_{g_S}(f_1, \ldots, f_n) + \langle \mathcal{H}_{n+1}(g_S)\rangle\right)\right) \\
&= \mathcal{V}\left(\varphi_{\mathbb{Q}[t_1,\ldots,t_s]} \circ \zeta_{x_i}\left(\zeta_{g_S}(f_1, \ldots, f_n) + \langle g_S\rangle\right)\right) \\
&\subset V_{ineq}(S)
\end{aligned}$$

Ce qui achève la démonstration.

□

Réduction complète

On peut maintenant prouver la réduction du calcul de la variété discriminante énoncée au théorème 4.

Lemme 14. *Soit S un système paramétré bien posé. Soit S' le système S augmenté de l'inéquation $j_S \neq 0$. Alors, en utilisant les notations 3, 7 et 8, on a :*

$$\mathcal{D}_S = V^\star_{inf}(S) \cup V^\star_{ineq}(S')$$

□

*preuve :*D'abord, la proposition 2 nous permet d'affirmer que :

$$\mathcal{D}_S = V_{inf}(S) \cup V_{ineq}(S')$$

Puis, la proposition 3 nous permet de remplacer $V_{inf}(S)$ par $V^\star_{inf}(S)$. Enfin la proposition 4 implique :

$$V^\star_{inf}(S) \cup V_{ineq}(S') \subset V^\star_{inf}(S) \cup V^\star_{ineq}(S') \subset V^\star_{inf}(S) \cup V_{ineq}(S') \cup V_{inf}(S')$$

Or on remarque que $I_S \subset I_{S'}$, d'où, en utilisant la formulation de V_{inf} données en lemme 2 :

$$V_{inf}(S') \subset V_{inf}(S)$$

D'où, l'égalité :

$$\mathcal{D}_S = V^\star_{inf}(S) \cup V^\star_{ineq}(S')$$

□

Ainsi le calcul de $V^\star_{inf}(S)$ et $V^\star_{ineq}(S')$ nous permet de réduire le calcul de la variété discriminante de S au calcul d'élimination de variables dans un idéal.

3.4 Exemple

Afin d'illustrer le comportement de notre algorithme, nous présentons ici un exemple d'élimination de quantificateur ([65, 11]).

Soit S le système d'équations $f = 0, g = 0$ et $h \neq 0$, où :

$$\begin{aligned} f &:= ux^2 + vx + 1 \\ g &:= vx^3 + wx + u \\ h &:= wx^2 + vx + u \end{aligned}$$

Les paramètres de S sont les variables u et v. Les inconnues sont les variables w et x. Nous allons ici montrer comment notre algorithme calcule la variété discriminante minimale de ce système $\mathcal{D}_S$. Notamment, pour chaque composante connexe de $A^2 \setminus \mathcal{D}_S$, le nombre de solution réelles de S est constant. Nous allons construire chacune des composantes présentées au théorème 4

D'abord, nous calculons les polynômes g_S et j_S associés à S :

$$\begin{aligned} g_S &:= h = wx^2 + vx + u \\ j_S &:= \begin{vmatrix} \frac{\partial f}{\partial w} & \frac{\partial f}{\partial x} \\ \frac{\partial g}{\partial w} & \frac{\partial g}{\partial x} \end{vmatrix} = -x(2ux + v) \end{aligned}$$

Ensuite, en utilisant les notations du théorème 4 on calcule les idéaux $\sigma^0_{x_0} \circ \varphi_{\mathbb{Q}[u,v,x_0]}(I)$, pour $I \in \{I_0^S, I_1^S, I_2^S\}$.

On utilise ici le logiciel FGb pour calculer la fonction $\varphi_{\mathbb{Q}[u,v,x_0]}$ en utilisant un ordre d'élimination $<_{[u,v,x_0],[w,x]}$ sur les monômes de $\mathbb{Q}[u, v, x_0, w, x]$.

$$
\begin{aligned}
\sigma^0_{x_0} \circ \varphi_{\mathbb{Q}[u,v,x_0]}(I_0^S) &:= \sigma^0_{x_0} \circ \varphi_{\mathbb{Q}[u,v,x_0]}(f, g, j_S g_S - x_0, Z x_0 - 1) \\
&= \sigma^0_{x_0}(-x_0u^3v^4 + x_0u^4v^3 - 13x_0u^2v^3 + 4x_0u^3v + x_0u^5v^2 - 4x_0u^5v \\
&\quad +4x_0u^4v^2 + 7x_0uv^5 - v^4 + 12u^3v^2 - 12u^2v^3 + 4uv^2 - v^7 + 4u^7 + uv^6 \\
&\quad -8u^5v + 4u^4v^2 + 18u^3v^3 - 7u^2v^4 + 7uv^5 - 8u^4v - u^6v^2 + 4u^6 - u^5v^3 \\
&\quad +u^4v^4 + uv^7 + 4u^6v - 5u^5v^2 + 2u^4v^3 - u^3v^4 - 8u^2v^5 - 4x_0u^6 + x_0^2u^5 \\
&\quad -x_0v^7) \\
&= \left\langle -v^7 + 4uv^2 + u^4v^4 + uv^7 + 4u^6v - 5u^5v^2 + 2u^4v^3 - u^3v^4 - 8u^2v^5 \right. \\
&\quad +uv^6 + 4u^7 - u^6v^2 - u^5v^3 - 7u^2v^4 - v^4 + 18u^3v^3 - 8u^5v + 4u^4v^2 \\
&\quad \left. +7uv^5 - 8u^4v + 12u^3v^2 - 12u^2v^3 + 4u^6 \right\rangle \\
\sigma^0_{x_0} \circ \varphi_{\mathbb{Q}[u,v,x_0]}(I_1^S) &:= \sigma^0_{x_0} \circ \varphi_{\mathbb{Q}[u,v,x_0]}(\mathcal{H}(f), \mathcal{H}(g), Z x_0 \mathcal{H}(g_S) - 1, w - 1) \\
&= \sigma^0_{x_0}(x_0^2u^5 - x_0^2uv^4 + 3x_0^2u^2v^2 - x_0u^3v + x_0^2v^2 + x_0v^3 - 2x_0uv + u^2) \\
&= \left\langle u^2 \right\rangle \\
\sigma^0_{x_0} \circ \varphi_{\mathbb{Q}[u,v,x_0]}(I_2^S) &:= \sigma^0_{x_0} \circ \varphi_{\mathbb{Q}[u,v,x_0]}(\mathcal{H}(f), \mathcal{H}(g), Z x_0 \mathcal{H}(g_S) - 1, x - 1) \\
&= \sigma^0_{x_0}(x_0^2 + x_0v + u) \\
&= \langle u \rangle
\end{aligned}
$$

Enfin, nous présentons Figure 3.1 la courbe implicite, union des variétés $\mathcal{V}\left(\sigma^0_{x_0} \circ \varphi_{\mathbb{Q}[u,v,x_0]}(I)\right)$, pour $I \in \{I_0^S, I_1^S, I_2^S\}$. Le complémentaire de cette courbe peut alors être partitionner en cellules connexes homéomorphes à $]0,1[^2$. Si $\mathcal{U}$ est une telle cellule, pour tout point p de $\mathcal{U}$, le système S dont les paramètres sont spécialisés par les valeurs de p admet un nombre constant de solutions réelles, ne dépendant que de la cellule $\mathcal{U}$.

En particulier, on appelle *vecteur générique* l'ensemble V des entiers tels que $k \in V$ si et seulement si il existe un ouvert $\mathcal{U}$ de l'ensemble des valeurs des paramètres, tel que pour tout p de $\mathcal{U}$, le système S spécialisé en p admet exactement k solutions.

Dans ce cas, si on arrive à exhiber un ensemble fini E de point tests intersectant chacune des composantes connexes de $A^2 \setminus \mathcal{D}_S$, alors il suffit de résoudre le système S pour chacun des points E pour calculer l'ensemble des valeurs génériques V. On peut notamment citer le logiciel RAGLIB ([116]) permettant de calculer un point par composante connexe dans le complémentaire d'une hypersurface.

La partie suivante illustre l'utilisation de ces méthodes sur un exemple plus important. Nous verrons notamment là que le calcul de la variété discriminante *minimale* permet de faciliter le calcul des points tests et nous permet de retrouver le vecteur générique associé au système paramétré considéré.

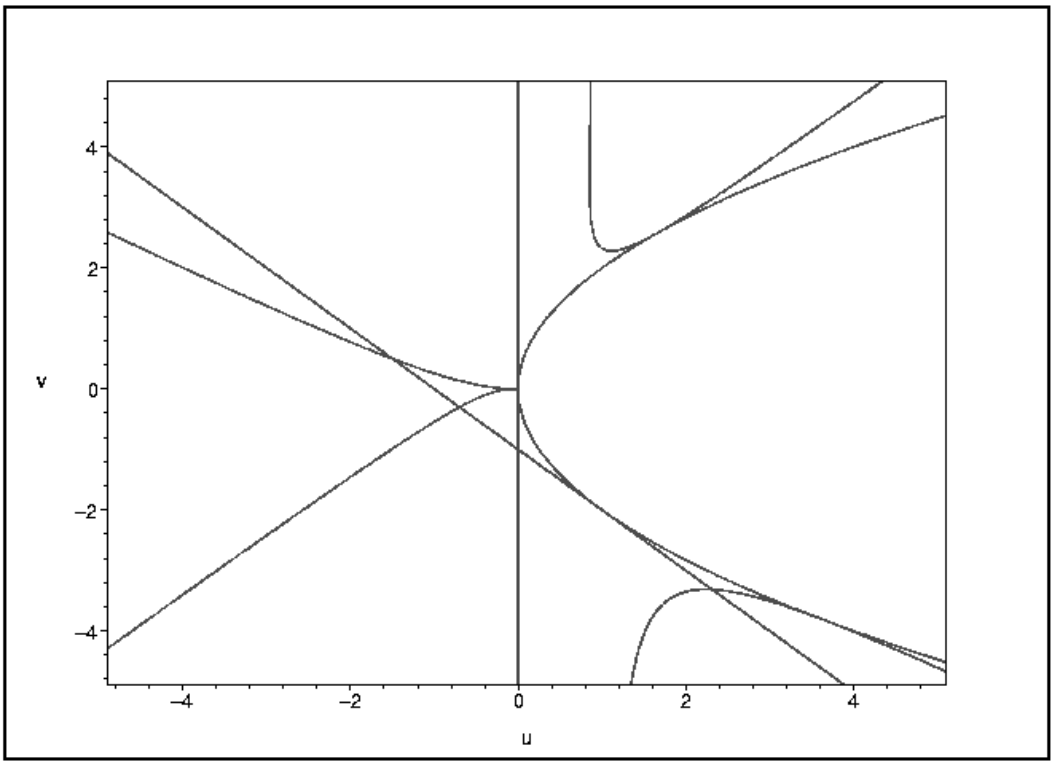


FIG. 3.1 – La variété discriminante minimale du système de Hong

Chapitre 4

Calibration photographique

4.1 Introduction

Le problème perspective-n-point a fait l'objet de nombreuses études au cours des 30 dernières années [43, 61, 144, 47]. Le but est de déterminer la position d'un appareil photo, étant donné la position apparente de n points. Ce problème a de nombreuses applications, en vision par ordinateur [82] ou encore an cartographie [43] par exemple. Le problème dans le cas général peut s'énoncer de la manière suivante :
"Étant donné la position relative de n points de contrôle, et connaissant l'angle formé par chaque paire de points de contrôle avec un point de référence appelé centre de perspective (CP), quelle est la distance du centre de perspective à chacun des points de contrôles ?"

En 1984, les auteurs de [46] ont prouvé que pour $n \neq 6$, la position du centre de perspective est déterminée de manière unique par les angles formés par les paires de points de contrôles avec CP. Il existe de nombreux algorithmes conçus pour le calcul direct des distances. Harllick et al. présentent les principales méthodes publiées avant 1991 dans [61]. Plus récemment, le calcul direct a fait l'objet de nombreuses amélioration dans [113], [2], [118] et les références incluses notamment.

Cependant, dans [43], Fischler et Bolles observent que le problème P3P peut avoir jusqu'à 4 solutions. De plus, dans [67] et les références incluses, Z.Y. Wu et F.C. Hu montrent que le problème P5P peut avoir 2 solutions et le problème $P4P$ jusqu'à 5 solutions. Ces résultats sont implicites, et l'ensemble des paramètres pour lequel le problème admet plusieurs solutions n'est pas calculé.

Dans [48], X.-S. Gao et J. Tang ont finallement prouvé que pour $n \geq 4$, l'ensemble des paramètres pour lesquels le problème PnP admet plus d'une solutions est de mesure nulle.

Dans [144] et [47] Yang, Gao et al. exhibent respectivement un ensemble partiel et exhaustif de conditions polynômiales déterminant le nombre de solutions du problème P3P. Ces conditions sont obtenues au moyen d'une décomposition triangulaire, des calculs de résultants et d'une utilisation attentionnée de la règle des signes de Descartes et des suites de Sylvester-Habicht. Cependant ces conditions sont complexes et ne fournissent pas d'information sur la géométrie des cellules. En particulier, tester la satisfiabilité de ces conditions n'est pas possible avec les programmes actuels de décomposition cylindrique algébrique générique.

Récemment, dans [146] et [143], les auteurs exhibent des conditions géométriques pour lesquelles le problème P3P admet 4 solutions, et fournissent un guide pour placer les points de contrôle dans des applications réelles.

Dans ce chapitre, nous présentons une méthode efficace et certifiée, basée sur le calcul de la variété discriminante, permettant d'obtenir une classification plus intuitive des paramètres d'un système en fonction du nombre de ses solutions réelles. On applique ensuite cette méthode au problème P3P dans le cas où les trois points forment un triangle isocèle. Notre classification est constituée de la variété discriminante minimale du sytsème d'une part, et d'un ensemble fini de points dans l'espace des paramètres. En particulier, si le problème admet génériquement k solutions, nous exhibons explicitement un point dans l'espace des paramètres pour lequel le problème admet exactement k solutions réelles.

Résultat principal. Nous exhibons la classification des paramètres du problème P3P pour un triangle isocèle. L'ensemble des calculs a nécessité près de 3 jours. Le résultat renvoyé est un polynôme de degré 29 et un ensemble de 60086 points.

Le premier outil important nous permettant de résoudre ce problème est la variété discriminante. Pour son calcul, nous avons implanté en MAPLE le programme DV permettant de calculé la variété discriminante d'un système bien posé.

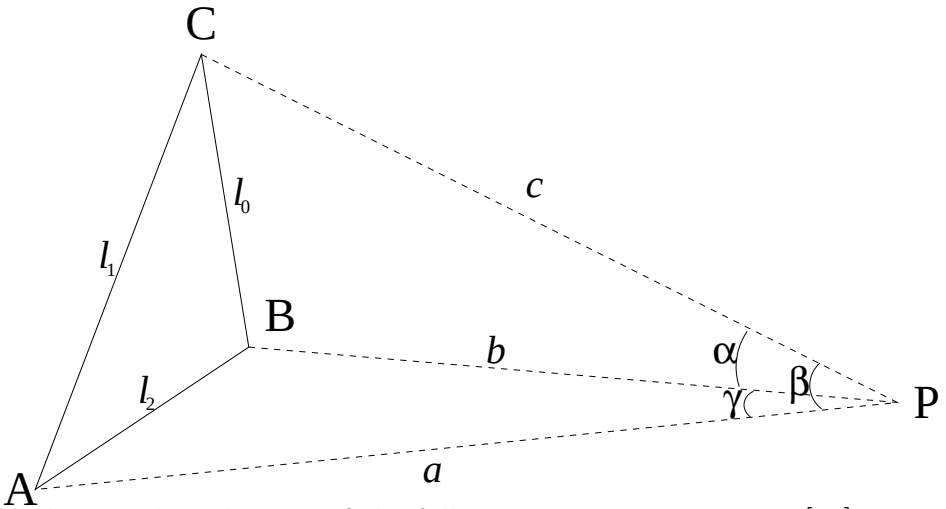
Nous calculons ensuite un point par composante connexe du complémentaire de la variété discriminante dans l'espace réel des paramètres. La décomposition cylindrique algébrique permet en théorie d'exhiber de tels points. Cependant, les implantations actuels de la CAD ne permettent pas de traiter notre variété discriminante, notamment à cause du nombre inabordable de cellules (et du temps) induit par le comportement doublement exponentiel en le nombre de variable de l'algorithme sous-jacent. Les algorithmes basés sur les méthodes de points critiques ont une meilleure complexité asymptotique (voir [5, Chapter 13] et les références incluses). Cependant, ces méthodes utilisent des déformations infinitésimales ([5, 58, 62]), ce qui induit une arithmétique lente et rend finalement difficilement praticable cette méthode. Deux améliorations de ces méthodes sont présentées dans [126] et [41] où l'auteur présente un algorithme conservant une borne asymptotique simplement exponentielle en le nombre de variables sans utiliser de nombres infinitésimaux. Ce sont ces algorithmes qui nous ont finalement permis d'exhiber un point dans chaque composante connexe du complémentaire de la variété discriminante. Pour les calculs, nous utilisons le programme RAGLIB développé par Safey El din.

Dans la première partie, nous décrivons la modélisation du problème P3P. Ensuite, nous présentons notre stratégie de classification. Enfin, nous détaillons l'application de notre méthode sur l'exemple du problème P3P.

4.2 Description of the Perspective Three Point Problem

Let A,B and C be the three control points, P be the perspective point and α,β, γ be respectively the three angles $\widehat{BPC}$,$\widehat{APC}$ and $\widehat{APB}$. Furthermore, let $a = PA$, $b = PB$,

$c = PC$, $l_0 = AB$, $l_1 = BC$ and $l_2 = AC$.



The lengths a,b,c are the solutions of the following equations given in [43] :

$$\begin{cases} l_0^2 &= a^2 + b^2 - 2ab\cos(\alpha) \\ l_1^2 &= b^2 + c^2 - 2bc\cos(\beta) \\ l_2^2 &= a^2 + c^2 - 2ac\cos(\gamma) \end{cases}$$

We denote by u,v and w the expressions $2\cos(\alpha)$, $2\cos(\beta)$ and $2\cos(\gamma)$. Moreover, as in [47], we express all the lengths of our problem relatively to l_0. Thus we introduce $A = \frac{a}{l_0}$, $B = \frac{b}{l_0}$, $C = \frac{c}{l_0}$. And for the length of the triangle, we use $x = \frac{l_2^2}{l_0^2}$ and $t = \frac{l_1^2}{l_0^2}$. Thus we get the following simplified system :

$$\begin{cases} 1 &= A^2 + B^2 - ABu \\ t &= B^2 + C^2 - BCv \\ x &= A^2 + C^2 - ACw \end{cases}$$

with the following constraints :

$$x > 0, t > 0, -2 < u < 2, -2 < v < 2, -2 < w < 2$$

where :
- A, B, C are the *unknowns*
- x, t, u, v, w are the *parameters*

We will present a general method to classify the parameters of such a system. Given a number k, this method allows us to say if there exists an open set of the parameters where the system admit exactly k solutions.

We will show the application of this method for the classification of the parameters of the P3P problem, in the case where the triangle is isosceles.

4.3 Classification method - Discriminant Variety

Goal Let $S_{\mathbf{T}}(\mathbf{X})$ be a parametric system of polynomial equalities and inequalities in $\mathbb{Q}[\mathbf{T}][\mathbf{X}]$, where $\mathbf{T} = T_1, \ldots, T_s$ are the parameters and $\mathbf{X} = X_1, \ldots, X_n$ the unknowns. We want to be

able to answer to the following question :
"Given a parametric system $S_{\mathbf{T}}$ and an integer i, does there exist an open set $\mathcal{O}$ in the parameters' space such that for all $p_0 \in \mathcal{O}$, the number of solutions of S_{p_0} is i ? If yes, give explicitly a point $a \in \mathcal{O}$". For this purpose, we present a method to classify the parametric values p_0 of a dense open set of $\mathcal{P}$ according to the number of real solutions of S_{p_0}. In the following, $\mathcal{P}$ will denote the real parameters' space. The method we describe in this article computes exactly an *open classification* of $\mathcal{P}$ with relation to $S_{\mathbf{T}}$ according to the following definition :

Définition 11. *(*Open classification*) Let $S_{\mathbf{T}}(\mathbf{X})$ be a parametric system. Let $k \in \mathbb{N}$ and $\mathcal{O}_0, \ldots, \mathcal{O}_k$ be open sets (for the euclidean topology) in the parameters' space such that :*

$$\begin{cases} \forall p_0 \in \mathcal{O}_i, S_{p_0} \text{ has } i \text{ real solutions} \\ \bigcup_{i=0}^{k} \mathcal{O}_i \text{ is dense in the parameters' space} \end{cases}$$

We call the family $(\mathcal{O}_i)_{0 \leq i \leq k}$ an open classification *of $\mathcal{P}$ with relation to $S_{\mathbf{T}}$.*
□

As announced in the introduction, the proposed methods will be based on the discriminant variety introduced in [87].

Définition 12. *(Discriminant variety) Given a constructible set $\mathcal{C}$, a discriminant variety of $\mathcal{C}$ is an algebraic set in the parameter's space such that a restriction of the trivial projection from $\mathcal{C}$ onto the complementary of the discriminant variety in the parameters' space defines an analytic cover.*
□

In addition, a discriminant variety is the parameters' space itself if and only if each of the (complex) fibers are infinite.

Définition 13. *(Minimal discriminant variety) The minimal discriminant variety is the intersection of all the discriminant varieties (and is thus a discriminant variety).*
□

Remarque 4. *In particular, the complementary of a discriminant variety defines an open classification of $\mathcal{P}$ with relation to $S_{\mathbf{T}}$.*

Computing an open classification Given a parametric system $S_{\mathbf{T}}$, we show that an *open classification* of $S_{\mathbf{T}}$ can be represented by (q, F, ϕ), which are defined as follows :

- q is a polynomial and a discriminant variety of $S_{\mathbf{T}}$;
- F a set of rational points in each connected component of $q \neq 0$;
- ϕ is a table which associates to each point p_0 of F the number of solutions of the 0-dimensional systems S_{p_0}.

In this representation, each $\mathcal{O}_i$ is represented by q and the subset of points $\phi^{-1}(i) \subset F$ such that :

$$\mathcal{O}_i = \{\ x \in \mathcal{P} \mid \text{ there exists } p \in \phi^{-1}(i) \text{ and a continuous path from } p \text{ to } x \text{ included in } q \neq 0\}$$

To compute this representation, our algorithm is naturally decomposed in three steps :
Input : a parametric system $S_{\mathbf{T}}$, the set of parameters $\mathbf{T}$, and the set of unknowns $\mathbf{X}$.
Output : the 3-tuple (q, F, ϕ)
Main algorithm :
Step a : The discriminant variety q. For the first step, we compute q as a polynomial vanishing at the discriminant variety of $S_{\mathbf{T}}$. The full algorithm may be found in [87] and the main ideas of its computation are recalled in the appendix. It is implemented in the maple DVLIB package and is available in the release 12 of Maple.
Step b : The sampling points F. The critical point method allows to compute at least one point in each connected component of a semi-algebraic set defined by strict inequalities. An algorithm using these methods is given in [126].this algorithm. In this step, F is a finite set of point in each connected component of the semi-algebraic set defined by $q \neq 0$. This function is implemented in the maple RAGLIB package.
Step c : The table ϕ Finally, we compute a table where each point p_0 of F is associated to the number of real solutions of the system S_{p_0}. For this step, we use the Rational Univariate Representation presented in [123] and implemented in the RS software which gives a list of non overlapping boxes with rational bounds, containing the real solutions of a zero-dimensional system.

From a theoretical point of view, the first step has the largest complexity upper bound. However, in practice the behavior of the three steps does not follow the same scheme. In particular, the first step is not often slower than the other steps.

4.4 Solving systems of polynomial inequalities

In order to compute one point in each connected set of an open semi-algebraic set, we use two algorithms based on the critical points computation. We briefly give here the main idea of each algorithm. More details on these algorithms in the general case are given in [41].

Let V be a real hypersurface of $\mathbb{R}^n$, smooth, bounded, defined implicitely by one polynomial $p \in \mathbb{Q}[x_1, \ldots, x_n]$. Moreover, let L be the coordinate line correspondinf to the first variable x_1. If H is a hypersurface, we denote by π_H the projection map from H onto L.

For the first algorithm, let m_+ (resp. m_-) be the local extrema of $p > 0$ (resp. $p < 0$), and let e_+ (resp. e_-) be a rational of $]0; m_+[$ (resp. $]m_-; 0[$). In this case, the varieties V_+ and V_- defined respectiveley by $p - e_+ = 0$ and $p - e_- = 0$ meet every connected components of $\mathbb{R} \setminus V$. Then, the computation of the critical locus of π_{V_+} and π_{V_-} gives us at least one point per connected component of each variety, which also gives us one point in each connected component of $\mathbb{R}^n \setminus V$.

The second strategy consists in computing directly the critical values of π_V. Let $r_1 < \cdots < r_k$ be those ordered critical values. Let $s_0, \ldots, s_k$ be a set of rationals such that $s_0 < r_1 < s_1 < \cdots < r_k < s_k$. Then the union of the varieties defined by $x_1 = s_i$, $0 < i < k$, intersects each connected component of $\mathbb{R}^n \setminus V$. For $0 \leq i \leq k$, let V_i be the variety defined by $p = 0$ and $x_1 = s_i$. We can now apply recursively the same procedure on each of the variety V_i. By recurrence on the dimension, we can see that this algorithm finally returns a finite set of points in each connected componnent of $\mathbb{R}^n \setminus V$.

For the general case, and when the polynomial p defining V can be factorized, the corresponding algorithms are given in [41].

4.5 Computations and results

We show here the results of the computations we obtained solving the P3P problem. We do the computation by restriction to the case where the triangle we observe is isosceles, that is : $l_0 = l_1$. The system we consider is :

$$\begin{cases} 1 &= A^2 + B^2 - ABu \\ 1 &= B^2 + C^2 - BCv \\ x &= A^2 + C^2 - ACw \end{cases} \tag{4.1}$$

It has 4 parameters u,v,w,x and 3 unknowns A,B,C.

All the computations have been performed on a PC Intel(R) Xeon(TM) CPU 3.20GHz with 6Gb of RAM.

The minimal discriminant variety

We first compute the minimal discriminant variety with the *DV* software in about 1 minute. The result is the polynomial D given in appendix. It is the minimal discriminant variety of the P3P parametric system when the triangle is isosceles. We can notice that D has 7 factors of respective degrees $1, 1, 1, 2, 2, 3, 13$, and whose number of terms is at most 153. Along with the constraints on the parameters, the discriminant variety allows us to define the following semi-algebraic set :

$$D \neq 0, x > 0 - 2 < u < 2, -2 < v < 2, -2 < w < 2$$

The parametric system has a constant number of solutions on each connected component of this semi-algebraic set.

Remarque 5. *The above semi-algebraic set is not bounded in the variable x, which is needed to apply the methods presented in [41].*

Thus we split this set into $x < 1$ and $x > 1$. Using the variable $y = \frac{1}{x}$, this leads to the study of two bounded semi-algebraic set :

$$\mathcal{H}_x \begin{cases} D \neq 0 \\ 0 < x < 1 \\ -2 < u < 2 \\ -2 < v < 2 \\ -2 < w < 2 \end{cases} \quad \text{and} \quad \mathcal{H}_y \begin{cases} D_y \neq 0 \\ 0 < y < 1 \\ -2 < u < 2 \\ -2 < v < 2 \\ -2 < w < 2 \end{cases}$$

where D_y denotes the polynomial obtained by the substitution of x by $\frac{1}{y}$ in $y^5 D$.

Solving polynomial systems of inequalities

We now consider the two semi-algebraic sets $\mathcal{H}_x$ and $\mathcal{H}_y$. Thanks to the property of the discriminant variety D, we know that on each connected component of these semi-algebraic sets, the parametric system has a constant number of solutions.

To get a *open classification* we first tried to compute a Cylindrical Algebraic Decomposition. However, after one month of computation, we could only complete the projection phase, but not the lifting phase neither with *Maple* nor with *Magma* software. Finally, we used the implementation of the algorithms computing sampling points described in [41] in semi-algebraic sets defined by the systems $\mathcal{H}_x$ and $\mathcal{H}_y$. The first algorithm returned a result after 3 weeks of computations, and the second after 3 days. As explained above, this is mainly due to the fact that the discriminant variety contains singularities of high dimension. More generally, we observed that the computation of critical values of the projection π_E considered in Section 5 were particularly difficult. The critical loci of this projection restricted to the varieties considered in Subsection 5.1 have a big dimension. Most of the time spent by the first algorithm described in Subsection 5.1 is spent in these computations. The second algorithm described in Subsection 5.2 avoids the computations of the singularities which appear during the running of the first algorithm. Moreover, as explained in Subsection 5.2, its complexity depends on the *real* geometry of the considered semi-algebraic set. This probably explains why it is so efficient in our case.

These implementations will be soon available in the next release of the RAGLIB Maple package. We successfully got one point in each connected components of $\mathcal{H}_x$ and $\mathcal{H}_y$. As a result we get 13612 points distributed in every connected cell of $\mathcal{H}_x$ and 46474 points in $\mathcal{H}_y$. These points can be downloaded at

`http ://www-spiral.lip6.fr/~moroz/P3P.html`

Note that contrarily to polynomials generated randomly, the minimal discriminant variety contains singularities of high dimensions which makes them more difficult to study. Moreover, since D is a minimal discriminant variety , this also ensures us that all conditions on the parameters discriminating the parameters' space according to the number of solutions of the system would contain such singularities.

As we can see on the figures 4.1 and 4.2, some connected cells seem very small and almost intractable with random approximations. The drawings show the graph of $\mathcal{H}_x$ around p_0, one of the points returned by our computation and whose coordinates are :

$$\begin{array}{rl} & (x,u,v,w) \\ = & (\frac{452735729}{9148876946}, \frac{3371082457}{1706654848}, \frac{2763844376}{1399264123}, \frac{26504177576}{13260182015}) \\ \simeq & (0.0494853, 1.97525, 1.97521, 1.99877) \end{array}$$

On each figure, we present 2 slices centered on p_0. The first figure shows a global view of $\mathcal{H}_x$ and p_0, while the second figure shows a much closer neighborhood of p_0. According to the slices, we can see that we have detected here a very small connected cell of $\mathcal{H}_x$.

More generally, the set of points we computed intersects each connected component of $\mathcal{H}_x$ and $\mathcal{H}_y$, and we now need to compute the number of solutions of the parametric system specialized in each point to achieve our classification.

Number of solutions	x	u	v	w
0	$\frac{452735729}{9148876946}$	$-\frac{1087810617}{4897634788}$	$-\frac{2322378129}{10447926511}$	$\frac{4610994663}{2334015862}$
1	$\frac{452735729}{9148876946}$	$-\frac{1087810617}{4897634788}$	$-\frac{2322378129}{10447926511}$	$-\frac{10016606887}{5135366188}$
2	$\frac{452735729}{9148876946}$	$-\frac{1087810617}{4897634788}$	$\frac{2322378129}{10447926511}$	$\frac{10016606887}{5135366188}$
3	$\frac{452735729}{9148876946}$	$-\frac{1087810617}{4897634788}$	$\frac{1270625905}{5709068079}$	$\frac{2776826855}{1423637843}$
4	$\frac{1415953531}{12404789665}$	$\frac{4824522087}{13860411335}$	$\frac{2413516911}{4607583958}$	$\frac{11184766673}{5921669493}$

TAB. 4.1 – Sample parametric points corresponding to a wanted number of solutions

Zero-dimensional system solving

In this step, we compute the number of real solutions satisfying the constraint of the problem for 60086 parameters' values. The mean time to solve each corresponding 0-dimensional system is about 0.05 second.

Finally, we can recover the fact that the parametric system of our problem may have exactly $0, 1, 2, 3$ or 4 solutions satisfying the inequalities' constraints. We present in table 4.1 a sample point in the parameters' space where the system has i solutions for i from 0 to 4.

Moreover, even if we do not have a complete CAD of the discriminant variety, we can have a geometric view of each connected cell of the parameters' space associated to a given number of solutions by drawing the neighborhood of each computed point. As we saw in the previous section, this allowed us for example to exhibit a very small cell, and to compute the number of distinct solutions of the system restricted to this cell, which is exactly 4.

APPENDIX

Elements of discriminant variety theory

The discriminant variety is presented in [87]. We recall here how to compute it for a *well-behaved* parametric system.

Définition 14. *A parametric system $S_{\mathbf{T}}$ is said well-behaved if and only if :*
- *The number of equations equals the number of unknowns*
- *For all p_0 outside a Zariski closed set, S_{p_0} is radical and zero-dimensional.*

□

Remarque 6. *The P3P problem and most of the problems coming from applications are modeled by well-behaved systems.*

Given a *well-behaved* parametric system $S_{\mathbf{T}}$, let g denote the product of the polynomial inequations of $S_{\mathbf{T}}$. and π the projection map from the solutions of $S_{\mathbf{T}}$ to the parameters' space. If $\mathcal{F}$ is a subset of the parameters' space, then $S_{\mathcal{F}}$ denotes the restriction of the parametric system $S_{\mathbf{T}}$ to $\mathcal{F}$. The discriminant variety can be decomposed in four algebraic components :

- V_{ineq} is the projection of the zeros of the polynomial equations and g
- V_{sing} is the Zariski closure of the projection of the singular locus of π
- V_c is the closure of the critical values of π
- V_∞ is the set of parameters' values p_0 such that for all neighborhood B_0 of p_0, the real solutions of S_{B_0} are not bounded.

The components V_{ineq}, V_{sing}, V_c may be computed by saturation and elimination of variables, which may be handled with Gröbner bases computations (see [8] for example). The component V_∞ may be obtained by extracting some coefficients of a gröbner basis with relation to a block ordering satisfying $\mathbf{X} >> \mathbf{T}$. More details on these computation may be found in [87]. Beside, complexity results of this method are given in [102].

Discriminant variety for the isosceles P3P problem

$$
\begin{aligned}
D :=\ & x(-x+2+w)(x-2+w)\\
& (-x+u^2)(-x+v^2)(-uvw+w^2-4+v^2+u^2)\\
& (-2x^2u^3v^5w^3-72xuv^5w-8u^3v^3w^3-96x^4u^3vw+\\
& 6x^2uv^5w^3+4x^3u^4v^4w^2-8x^2u^3v^3w^3+1248xu^2v^2-\\
& 24x^3u^4v^2-4x^3u^6w^2-4x^3v^6w^2-24x^3u^2v^4-\\
& 96xu^2v^4-128x^5v^2-18x^3u^2v^4w^2-384xu^3vw-\\
& 18x^3u^4v^2w^2-12uv^5w^3-96xu^4v^2+24x^3v^4w^2-\\
& 240xv^4+576xu^4+x^5u^4v^4-768x^2u^2+\\
& 64x^5u^2v^2+576x^2v^4-768x^2v^2+64x^4u^4-\\
& 416x^3v^4+64x^3v^6-96x^4uv^3w+256x^4uvw+\\
& 48x^2u^3vw^3+8x^2uv^5w+12x^2u^6v^2+168xv^4w^2-\\
& 2x^2u^2v^6w^2+12x^2v^6w^2+12x^2u^2v^6-40x^2u^4v^4+\\
& 168xu^4w^2+12x^2u^6w^2-8xu^4v^4+16x^5v^4+\\
& xu^6v^2w^2-768x^3uvw+32x^4u^3v^3w-4xu^6v^2-\\
& 12xu^6w^2-12xv^6w^2+96xu^3vw^3+16x^2u^4v^4w^2+\\
& 8x^4u^5vw+48x^2uv^3w^3+96x^3u^3vw-2x^2u^6v^2w^2+\\
& 96x^3uv^3w+60xu^4v^2w^2+96xuv^3w^3+60xu^2v^4w^2+\\
& 6xu^2v^2w^4+8x^4uv^5w-336xu^2v^2w^2-384xuv^3w-\\
& 2xu^4vw^2-4xu^2v^6-1152x^2u^2v^2-27xu^4w^4-\\
& 16x^4u^6-96x^2v^6+64x^3u^6+64xu^6+\\
& 64xv^6-240xu^4-128x^5u^2-1024x^4+\\
& 1024x^3+768x^2uvw+xu^2v^6w^2+8xu^5v^3w+\\
& 6xu^4v^2w^4+48u^5vw+8x^3u^5vw+16x^5u^4-\\
& 27xv^4w^4+24x^3u^4w^2+4x^4u^6v+192x^2v^2w^2-\\
& 128x^4u^2v^2+4v^6w^2-4x^4u^4v^4+64x^4v^4+\\
& 6xu^2v^4w^4+8xu^3v^5w-2xu^5v^3w^3+192x^2u^3vw+\\
& 6xu^5vw^3+96u^3v^3w+192x^2uvw+32x^3u^3v^3w-\\
& 2xu^3v^5w^3+4u^6w^2+256x^3u^2v^2+96x^3v^2w^2+\\
& 48uv^5w-36u^4v^2w^2+256x^4u^2-8x^5u^4v^2-\\
& 416x^3u^4+256x^4v^2+384x^3v^2-96x^2u^6-\\
& 72xu^5vw-76xu^3v^3w^3+12u^4v^2w^4+4x^4u^2v^6-\\
& 12x^3u^6v^2+96x^3u^2w^2-256x^3w^2-8x^5u^2v^4-\\
& 16v^6-16x^4v^6+384x^3u^2-16u^6+\\
& 8x^3uv^5w+xu^4v^4w^4+6xuv^5w^3-36u^2v^4w^2+\\
& 12u^2v^4w^4-4u^3v^3w^5-2x^4u^3v^5w+x^3u^6v^2w^2-\\
& 6x^3u^5v^3w-192x^2v^4w^2-48u^2v^4-12x^3u^2v^6-\\
& 192x^2u^4w^2+8x^2u^5vw+192x^2u^2w^2-48u^4v^2+\\
& 144xu^3v^3w-2x^4u^5v^3w-192x^2uvw^3+176x^2uv^2+\\
& 24x^3u^4v^4+176x^2u^2v^4-160x^2u^3v^3w-6x^3u^3v^5w+\\
& 6x^2u^5vw^3-12u^5vw^3+x^3u^2v^6w^2-2x^2u^5v^3w^3+\\
& 256x^5)
\end{aligned}
$$

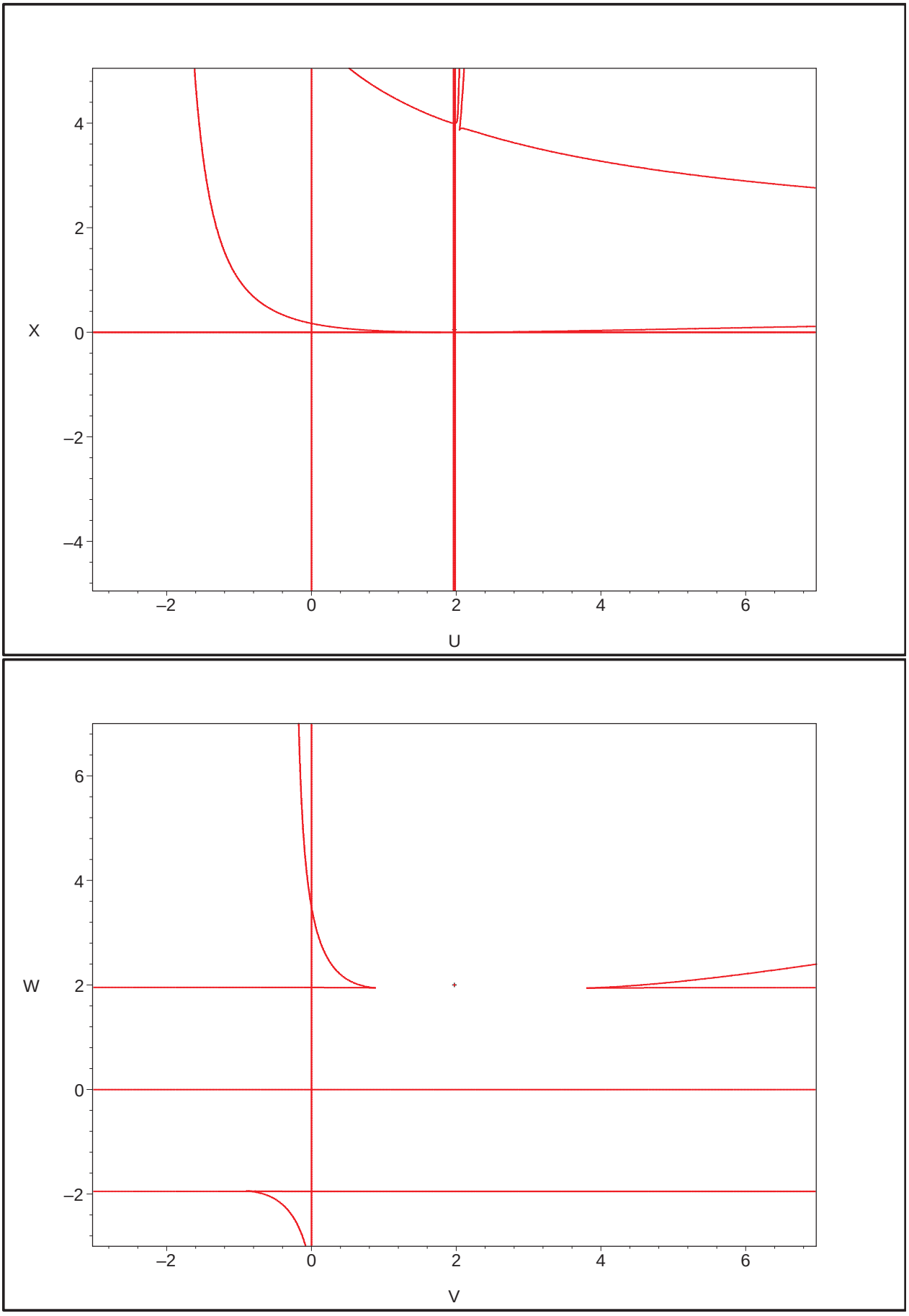


FIG. 4.1 – Two slices of $\mathcal{H}$ partly specialized in $p_0 : -$ in the first, the variables v and w are

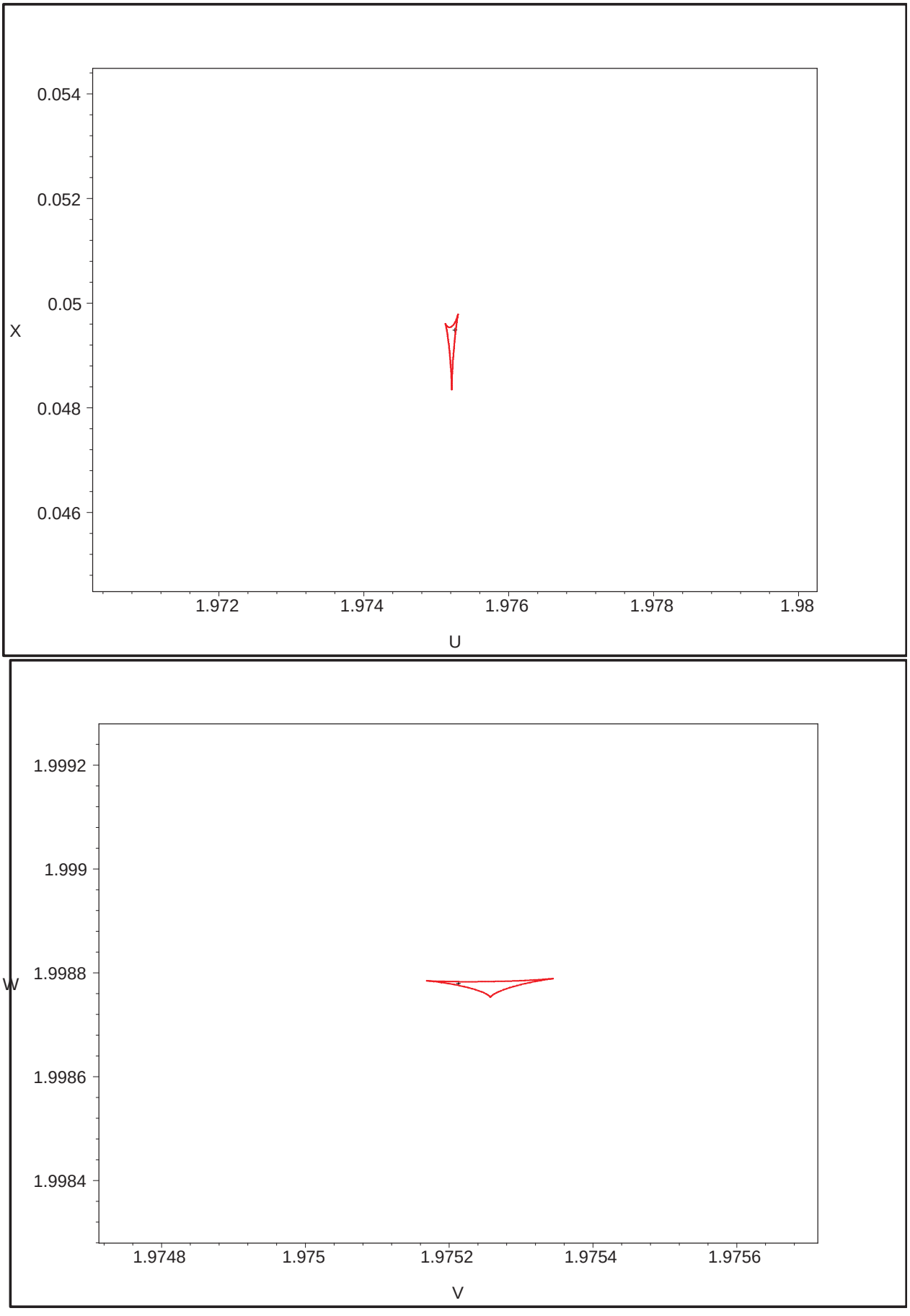


FIG. 4.2 – Two closer slices of $\mathcal{H}$ partly specialized in p_0

Chapitre 5

Polynômes creux

5.1 General Problem

The goal of this article is to show some advances in the study of a family of parametric algebraic systems introduced in [32] (in its parametric form), following the work of Haas [60] whose original objective was to find a system of 2 bi-variate trinomials (polynomials with 3 terms) with 5 roots in the positive quadrant (maximal number according to [91]). In particular, these polynomial systems provide a counter-example to the Kushnirenko's conjecture [76] which has remained opened for three decades (at most 4 solutions).

Définition 15. *Let a, b be two positive real, and k be an integer. Then the Haas system with parameters (a, b, k) is given by :*

$$H_{(a,b,k)} := \begin{cases} x^{2k} + ay^k - y = 0 \\ y^{2k} + bx^k - x = 0 \\ a \neq 0, b \neq 0, x > 0, y > 0 \end{cases} \tag{5.1}$$

□

Dickenstein et al. showed in [32] that the Haas family could provide an infinite number of trinomial systems with 5 real roots when the parameters a and b are specified adequately. However, finding explicit values for a and b appeared to be surprisingly hard. For $k = 3$, the subset of parameters a_0, b_0 such that $H_{(a_0,b_0,3)}$ admits 5 roots in the positive quadrant is contained in a bowl of radius less than 10^{-6}.

Computing instances for the case $k = 3$ appear to be the highest degree which could be reached using their computational strategy.(they mentioned about 5 days of computation to get a certified partition of the parameter's space).

Also, the Haas family not only gives interesting examples for the theory of the fewnomials, but it also provides a challenging family of parametric systems for classification methods.

In this article, our main objective is to show that one can provide all the subsets of non null measure (outside an algebraic curve) in the parameter's space where the system has 5 admissible solutions up to $d = 9$. We solve the problem by means of *Discriminant Varieties* (introduced in [87]) and compute the distributions of the roots using existing general software.

We first show that the results obtained in [32] can be straightforwardly and efficiently be recovered ($k = 3$) using our DV Maple package and that the case $k = 4$ can be solved in the same (easy) way.

For solving the next (from $k = 5$ to $k = 9$) one had to change the way that some intermediate computations were done but also the the way the equations were initially set (by applying a simple change of variables which allowed to decrease strongly the degree of the equations arising in intermediate computations).

5.2 Experimental results

In this section, we detail the results we obtain with 2 different strategies.

The first strategy consists in using discriminant varieties and cylindrical algebraic decomposition tools on the original Haas systems.

The second strategy is a more specific adaptation of these general tools. In particular, we will use the change of variable and the properties presented in section 5.2.2.

All our computations are done on an 3.2Ghz Intel Xeon computer with 6Gb memory using the SALSA library for maple[1], which includes :

- FGb software by J.-C. Faugère for Gröbner bases computations (algorithm F_4 [39])
- RS software by F. Rouillier for real roots of univariate polynomials and zero-dimensional systems ;
- DV Package by the authors of this article for computing discriminant varieties.

Our general computation scheme is summarized as follows :

Discriminant Variety	**(A)**	Computation of the minimal discriminant variety of $H_{(a,b,k)}$. It will be represented as the zeroes of the bivariate polynomial P_{DV}.
Open CAD	**(B)**	Computation of the projection of the critical and singular points of P_{DV}. They will be represented as the zeroes of the univariate polynomial P_{crit}.
	(C)	Computation of one representative point in each open cell of the CAD of $\mathbb{R}^2$ adapted to P_{DV}. They will be represented as a set of rational couples *Sample*.
RUR	**(D)**	Computation of the *RUR* of $H_{(a_i,b_i,k)}$ for each (a_i, b_i) being a representative point. Thus we can compute for each representative point the number of solutions of the Haas system in the positive quadrant *Sols* denotes the possible numbers of solutions

[1] http://fgbrs.lip6.fr/salsa/Software

k	Degree		Cardinal of *Sample*	Numbers of *Sols*	Time (in seconds)			
	P_{DV}	P_{crit}			A	B_1 / B_2	C	D
3	92	1646	125	1,3,5	31	855/ 20	7	13
4	58	589	56	1,3,5	5	55 / 2	1	8
5	272	14454	183	1,3,5	2937	- /19914	1	80

TAB. 5.1 – The results of the open classification on the original Haas system

5.2.1 Original Haas system

Recovering $k = 3$, solving the case $k = 4$

We can recover the case $k = 3$ and even solving the case $k = 4$ using generic tools. The step (A) is performed using the *DV* package. The step (B) consists in eliminating the variable b from the equations defining the ideal :

$$\left\langle P_{DV}, \frac{\partial P_{DV}}{\partial b} \right\rangle$$

This may be done directly through a resultant computation (Maple function) : this strategy will be denoted by (B_1).

The steps (C) and (D) are performed using `rs_isolate` and `rs_rur` functions from the *Salsa library*.

The different steps are summarized in the table 5.1. We can see that we recover easily the case $k = 3$ with generic tools, and can even classify the solutions for $k = 4$.

The case $k = 5$

However, for the case $k = 5$, only the Gröbner bases computations allowed us to complete the computations.

More precisely, we used Gröbner bases to project separately the singular points :

$$\left\langle P_{DV}, \frac{\partial P_{DV}}{\partial b}, \frac{\partial P_{DV}}{\partial a} \right\rangle \cap \mathbb{C}[a]$$

and the critical (regular) points

$$\left\langle P_{DV}, \frac{\partial P_{DV}}{\partial b}, T\frac{\partial P_{DV}}{\partial a} - 1 \right\rangle \cap \mathbb{C}[a]$$

.

The Gröbner bases are computed with the *FGb* package of the *Salsa library*.

We see in table 5.1 that this strategy is always more efficient than direct resultant computations and in particular allows us to reach the case $k = 5$:

5.2.2 Haas system after a change of variable

An equivalent system

A special change of variable was a key extension which allowed us to classify the solutions of the Haas systems up to $k = 9$. It was guessed by observing the results of our computations up to $k = 5$ and extending the remark 4.5 of [32].

Precisely, the original Haas system is written as follows :

$$H_{(a,b,k)} := \begin{cases} x^{2k} + ay^k - y = 0 \\ y^{2k} + bx^k - x = 0 \\ a \neq 0, b \neq 0, x > 0, y > 0 \end{cases}$$

Let

$$\begin{aligned} f_k :(\mathbb{R}^\star)^2 &\to (\mathbb{R}^\star)^2 \\ (u, v) &\mapsto (\frac{u^{2k}}{v}, \frac{v^{2k}}{u}) \end{aligned}$$

Let $(X, Y) = f_k(x, y)$ and $(A, B) = f_k(a, b)$, then, the following system is equivalent to the Haas system :

$$H'_{(A,B,k)} := \begin{cases} h'_1(X, Y) := (X - 1)^{2k} + AY^{k-1}(Y - 1) = 0 \\ h'_2(X, Y) := (Y - 1)^{2k} + BX^{k-1}(X - 1) = 0 \\ X > 0, Y > 0, X - 1 \neq 0, Y - 1 \neq 0 \end{cases}$$

Moreover, for the discriminant variety computation, we need to eliminate the variables X, Y from the Jacobian ideal :

$$\left\langle h'_1, h'_2, \begin{vmatrix} \frac{\partial h'_1}{\partial X} & \frac{\partial h'_2}{\partial X} \\ \frac{\partial h'_1}{\partial Y} & \frac{\partial h'_2}{\partial Y} \end{vmatrix} \right\rangle$$

Using the fact that $(X - 1)^{2k} = -AY^{k-1}(Y - 1)$ and $(Y - 1)^{2k} = -BX^{k-1}(X - 1)$, we can observe that :.

$$\begin{aligned} &(X - 1)(Y - 1) \begin{vmatrix} \frac{\partial h'_1}{\partial X} & \frac{\partial h'_2}{\partial X} \\ \frac{\partial h'_1}{\partial Y} & \frac{\partial h'_2}{\partial Y} \end{vmatrix} \\ &= 4k^2(X - 1)^{2k}(Y - 1)^{2k} - AB(X - 1)(Y - 1)X^{k-2}Y^{k-2}(kX - k + 1)(kY - k + 1) \\ &= AB(X - 1)(Y - 1)X^{k-2}Y^{k-2}(4k^2XY - (kX - k + 1)(kY - k + 1)) \end{aligned}$$

The squarefree part of this expression will allow us to compute more efficiently the discriminant variety.

	Degree		Cardinal	Numbers	Time (in seconds)			
k	P_{DV}	P_{crit}	of *Sample*	of *Sols*	A	B_2	C	D
3	20	48	125	1,3,5	1	1	1	15
4	26	91	84	1,3,5	1	3	1	16
5	32	148	183	1,3,5	5	31	1	81
6	38	219	160	1,3,5	26	305	2	210
7	44	304	321	1,3,5	69	1011	4	1189
8	50	403	270	1,3,5	105	1249	17	3144
9	56	516	453	1,3,5	349	4010	60	7945
10	62	-	-	-	322	-	-	-
11	68	-	-	-	881	-	-	-
12	74	-	-	-	1310	-	-	-
13	80	-	-	-	2011	-	-	-

TAB. 5.2 – The results of the open classification on the modified Haas system

The cases $k = 6, 7, 8$ and 9

To classify the parameters for $k >= 6$, we use the equivalent system presented in the previous section.

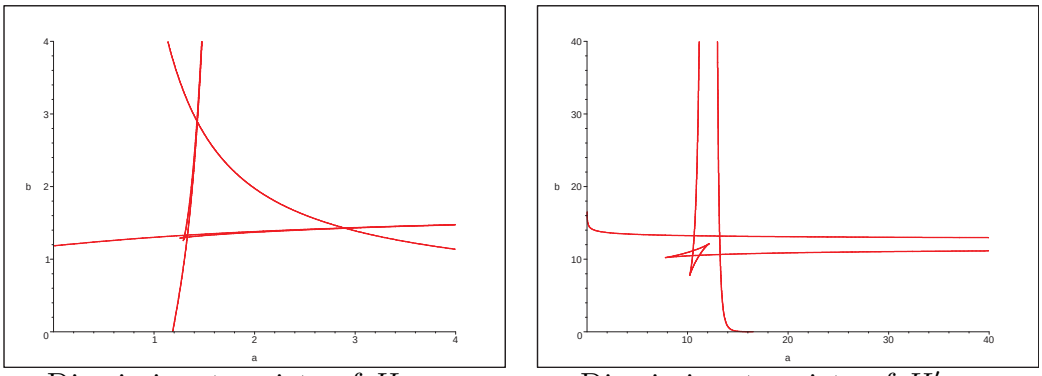
For the discriminant variety in step (A), we use the modified expression of the Jacobian rewritten in the previous section. For the (B) step, the projection of the critical and singular points is handled as in section 5.2.1. Finally, the (C) and (D) are performed with the real solving functions of the *Salsa library*.

Thus, although the equivalent Haas systems are no more trinomials, we could compute their classification up to $k = 9$, while the minimal discriminant variety can be computed up to $d = 13$. The results of our computations are summarized in table 5.2.

5.3 Some discriminant varieties

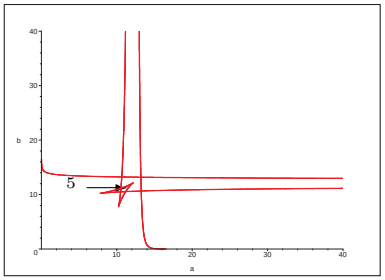
By comparing the drawings of the discriminant varieties for the original and the modified Haas system for $k = 5$ in figure 5.1, we can observe that the transformation enlarges the cells in the complementary of the discriminant variety.

Moreover, by observing in figure 5.2 the evolution of the discriminant varieties of the modified Haas system for k from 5 to 13, we can see that the small area where the number of solutions is 5 grows with k. This explains partly why it is easier to find counter-examples to the Kushnirenko's conjecture for larger k.

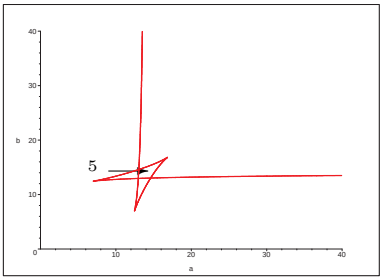


Discriminant variety of $H_{(a,b,5)}$ Discriminant variety of $H'_{(a,b,5)}$

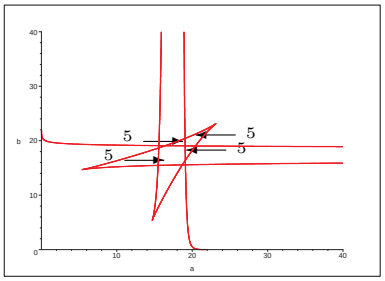
FIG. 5.1 – Discriminant varieties of the original and modified Haas system for $d = 5$



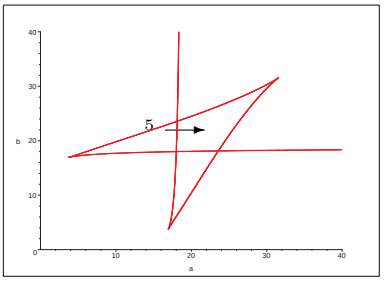
$d = 5$



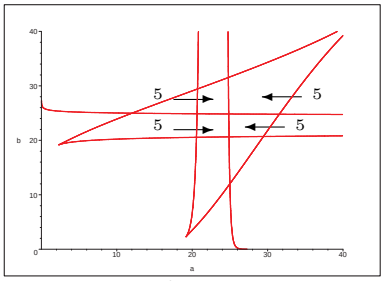
$d = 6$



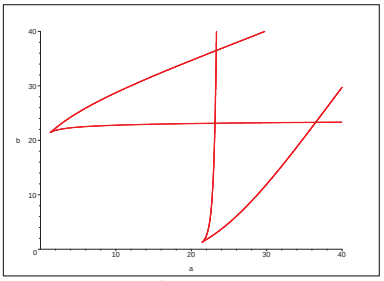
$d = 7$



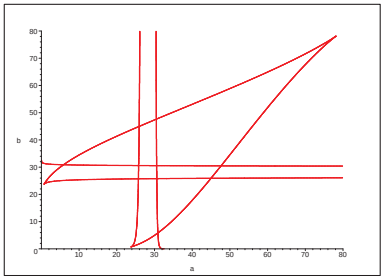
$d = 8$



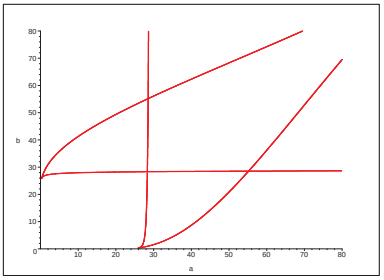
$d = 9$



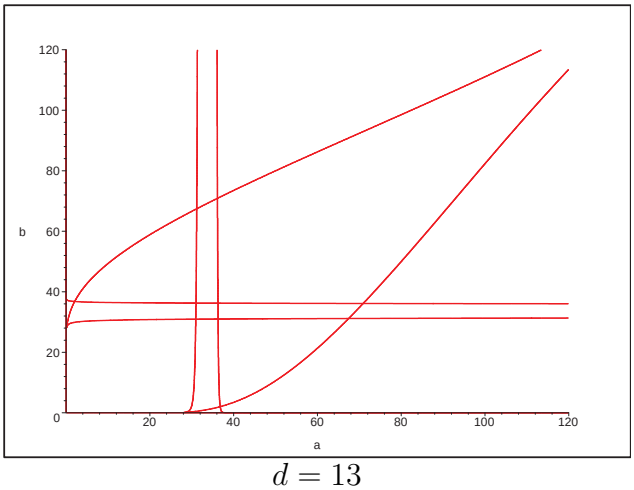
$d = 10$



$d = 11$



$d = 12$



$d = 13$

Deuxième partie

Systèmes surdéterminés

Chapitre 6

Introduction

6.0.1 Problématique

Cette partie est consacrée au traitement plus général des systèmes paramétrés surdéterminés.

Définition 16. *On dira dans cette partie qu'un système paramétré S est* surdéterminé *lorsque :*

- *S est génériquement* 0*-dimensionnel*
- *le nombre d'équations m de S est* quelconque

□

Les systèmes surdéterminés sont moins fréquents dans les applications, mais comme nous le verrons par exemple au chapitre 9, ils peuvent arriver directement (mise en équations) ou indirectement (résultat d'un calcul) et il est nécessaire de les considérer.

Par ailleurs, les calculs de bases de Gröbner s'avèrent relativement efficaces en pratique et sont de plus en plus utilisés dans le processus de modélisation de problèmes paramétrés. Le calcul d'une base de Gröbner par bloc permet par exemple d'éliminer des variables ([28, chapitre 3]) ou encore de retirer des composantes dues à des artefacts de modélisation ([28, chapitre 4, §4]). Dans ces cas où les équations considérées sont issues d'un calcul de base de Gröbner, le système est alors souvent surdéterminé.

Lorsque les systèmes paramétrés sont surdéterminés, leur étude fait apparaître de nouveaux problèmes.

Poblème 2. *Soit S est un système paramétré surdéterminé :*

i) les zéros de S dans $\mathbb{C}^s \times \mathbb{C}^n$ peuvent contenir des composantes isolées de dimension strictement inférieure à s le nombre de paramètres

ii) si S est génériquement radical, le calcul d'une variété contenant $V_{crit}(S)$, calculée avec le critère jacobien, fait intervenir le facteur combinatoire

$$\binom{m}{n}$$

qui rend le calcul très vite impraticable lorsque le système d'équations est donné sous forme d'une base de Gröbner où le nombre d'équations m est souvent très grand devant le nombre de variables n.

iii) lorsque S n'est pas génériquement radical, le critère jacobien ne permet pas de calculer $V_{crit}(S)$

□

Une première solution, pragmatique vis-à-vis de l'état de l'art, consiste à calculer dans ce cas une décomposition triangulaire (voir Section 6.0.2) de l'ensemble d'équations donné en entrée. Cette solution, présentée dans [87], a l'avantage de séparer complètement les composantes de petites dimensions de la composante principale (celle dont la projection sur l'espace des paramètres est dense). De plus, un ensemble triangulaire régulier est en particulier un système bien posé, possédant autant d'équations que d'inconnues. Cela permet ainsi de lever complètement les problèmes *i*) et *ii*). Si de plus cet ensemble triangulaire est régulier et séparable, on peut alors appliquer le critère jacobien et résoudre le point *iii*).

Cependant, la structure triangulaire n'est pas nécessaire pour éviter les difficultés évoquées et peut s'avérer difficile à calculer dans certains cas. Nous n'avons par exemple pas réussi à calculer la décomposition triangulaire du système 9.7 considéré au chapitre 9.

Nous nous sommes alors intéressé à une représentation sous forme de suites localement régulières, non nécessairement triangulaires, qui sont aussi des systèmes bien posés, et suffisent pour traiter les problèmes *i*) et *ii*). De plus, la représentation sous forme de suites localement régulières permet aussi de calculer le radical des composantes qui nous intéresse en utilisant les travaux de [36].

Nous avons développé un algorithme dit de *décomposition régulière* basée sur une représentation en suites localement régulières, plus adaptée à nos besoins. Cet algorithme peut être vu comme une variante plus générale de la décomposition triangulaire. Nous décomposons ainsi un système d'équation non pas en composantes triangulaires, mais en *composantes régulières*.

Notre algorithme de décomposition est général et ne requière aucune hypothèse sur le système d'équations polynômiales traité. De plus, dans le cas d'un système paramétré 0-dimensionnels S, nous verrons en section 7.3.3 que l'algorithme que nous présentons peut être facilement adapté pour séparer les composantes de dimension maximale des composantes de petites dimensions sans les décomposer, permettant ainsi un gain de temps en pratique pour le calcul de la variété discriminante.

Nous verrons que cette approche possède des avantages en pratique tout en conservant des bornes raisonnables de complexité.

6.0.2 Contexte

Il existe de nombreux algorithmes de décomposition dans la littérature. Nous rappelons ici les principaux algorithmes permettant d'obtenir une décomposition équidimensionnelle d'un idéal I et replaçons notre algorithme dans ce contexte.

Décomposition triangulaire

La décomposition triangulaire est peut-être celle qui se rapproche le plus de la décomposition régulière présentée ici. Initiées en 1984 par W.T. Wu ([140]), dans la prolongation des travaux de Ritt([121, 122]), ces méthodes ont beaucoup évoluées au cours des 20 dernières années. On peut notamment citer les contributions indépendantes de D.Lazard ([85]) et M.Kalkbrenner ([73]), qui ont tous les deux étendu la notion de décomposition triangulaire. On peut trouver une étude comparative des différentes méthodes calculant une décomposition triangulaire dans [4], ainsi que des améliorations algorithmiques plus récentes dans [141, 98].

Le principe d'une décomposition triangulaire est de décomposer un idéal I en un ensemble de composantes équidimensionnelles, où chaque composante est représentée par un ensemble triangulaire.

Si f est un polynôme de $K[x_1, \ldots, x_n]$, on note $vars(f)$ l'ensemble des variables apparaissant dans f. Un ensemble triangulaire est alors une suite de polynômes $f_1, \ldots, f_c$ vérifiant pour tout $i, 1 \leq i \leq c$:

- $vars(f_i) \subsetneq vars(f_{i+1})$
- $vars(f_i) \neq \emptyset$

Cette notion a notamment l'avantage de ramener les problèmes de décompositions d'idéaux à des problèmes de factorisation de polynômes. Sous certaines hypothèses de généricité, les auteurs de [30] prouvent qu'en utilisant les paramétrisations rationnelles ([1, 123, 56]), on peut exhiber une représentation triangulaire de C où les degrés des polynômes sont majorés par d^c, identique à la borne que nous obtenons pour les décompositions régulières minimales.

En pratique, nous pouvons remarquer que nous n'avons par exemple pas réussi à calculer la décomposition triangulaire du système 9.7 dans le cadre de l'application robotique présentée au chapitre 9. La décomposition régulière minimale de ce système a cependant été obtenu relativement rapidement.

Décomposition de Gianni, Trager et Zacharias

La décomposition de Gianni, Trager et Zacharias [50] utilise la théorie des bases de Gröbner par block pour scinder récursivement les différentes composantes. Cette méthode est originellement dédiée à la décomposition primaire d'un idéal, et permet d'obtenir les bases de Gröbner des composantes équidimensionnelles de I.

Une variante de cette méthode est donnée dans le livre [8, chapitre 8]. Plus récemment, dans [20], les auteurs présentent des amélioration de cette méthode pour le calcul d'une décomposition équidimensionnelle,en étudiant plus finement le lien entre une base de Gröbner par bloc et le morphisme de projection. Dans [130, 107], les auteurs améliorent aussi cette méthode, en éliminant rapidement les branches correspondant à des composantes redondantes au cours de l'algorithme, dans le but de calculer une décomposition primaire et première de l'idéal considéré. Dans ce type de décompositions, chacune des composantes est représentée par une base de Gröbner.

Cette approche permet de résoudre le problème i), mais ne résout pas le problème combinatoire ii) qui sera induit lors du calcul de V_{crit}, une base de Gröbner étant en général un système sur-contraint.

Décomposition de Eisenbud, Huneke et Vasconcelos

Dans [36], les auteurs présentent une méthode pour extraire la composante de dimension maximale d'un idéal I, en utilisant des outils d'algèbre homologique. Plus de détails sur ces méthodes sont disponibles dans [35, Appendix 3] ou [57, chapitre 7].

Cette méthode a notamment été implantée dans le logiciel SINGULAR. Elle permet ainsi d'isoler la composante de plus grande dimension des autre composantes de I. Cependant, la représentation de cette composante peut la aussi être surdéterminée.

Les auteurs de [36] soulèvent d'ailleurs ce problème en 1992 :

> There are many interesting problems remaining in the area of effective computation in commutative algebra and algebraic geometry. Here are a few of our current favorites :
>
> 1) What is a good method of finding a "simple" maximal regular sequence in an ideal $I \subset S = k[x_1, \ldots, x_n]$? One can start with an element of least degree and adjoin generators one at a time to the ideal, adding a general linear combination of the generators already taken to the regular sequence whenever the codimension of the ideal increases. Unfortunately, this leads to highly non-sparse regular sequences [...]

Nous allons voir que la décomposition régulière permet dans une certaine mesure de répondre à cette question en évitant autant que possible les combinaisons linéaires génériques des polynômes d'entrée.

Décomposition par résolution géométrique

Une autre approche consiste à décomposer un idéal à l'aide de méthodes d'élimination de variables et de pgcd. Initiée dans l'article [51], l'idée consiste à projeter la variété V de dimension d qui nous intéresse sur un espace affine de dimension $d+1$. Si la projection est suffisamment générique, la composante de dimension maximale de V est alors une hypersurface que l'on peut retrouver grâce à des calculs de pgcd. Cependant, comme l'indique la remarque de Eisenbud et al. reportée ci-dessus, les changements génériques de variables font disparaître le caractère creux des polynômes d'entrée, ce qui se traduit en souvent par une lourde pénalité dans le temps d'exécution en pratique.

Cette méthode a ensuite été couplée à une structure de donnée où les polynômes sont donnés des programmes sans divisions afin de contourner ce problème (voir [16] pour une présentation plus détaillée de cette structure de donnée). Avec la *résolution géométrique*, dans la continuité des travaux sur l'élimination [54, 52, 53], l'auteur de [90] présente un algorithme de décomposition équidimensionnel où chaque composante est représentée par une paramétrisation rationnelle, encodée sous forme de programmes sans divisions. Un des intérêts de cette méthode est de garantir une complexité en temps polynômiale en md^n où m est le nombre d'équations, d le degré maximal des polynômes d'entrée et n le nombre de variable.

Pour obtenir aussi de bonnes performances en pratique, les méthodes d'évaluations et de remontées des coefficients, introduites notamment dans [139, 142], ont alors été étendues pour la décomposition équidimensionnelle dans [89]. Cependant, malgré l'utilisation de ces

structures de données compactes, le calcul d'élimination de variables restent couteux en pratique. De plus, la représentation sous forme de paramétrisation rationnelles n'est pas nécessaire pour le calcul de la variété discriminante.

Décomposition symboliques numériques

Nous mentionnons aussi une autre approche de décomposition équidimensionnelle d'un idéal I, basée sur des méthodes dites symboliques numériques. Ces méthodes sont présentées dans [133], dans les références incluses, et se retrouvent aussi en partie dans [89]. Principalement, chaque composante équidimensionnelle I_c de codimension c est représentée par l'ensemble des points d'intersection deI_c avec un espace affine (ou fibre) générique de dimension c. Ces points sont appelés les points témoins de la composante.

Ces méthodes, couplées à des techniques d'interpolation, permettent de retrouver une représentation polynômiale des composantes équidimensionnelles du système d'entrée ([89]). On peut trouver une implantation des méthodes de décompositions sous forme de points test dans le logiciel `PHCpack` ([111]). Les méthodes de décompositions permettant en outre l'interpolation sont implantées dans le logiciel `Kronecker` ([80]).

6.0.3 Organisation

Dans le premier chapitre de cette partie, nous présentons la notion de décomposition régulière. Ensuite nous étudions sa complexité sous certaines hypothèses. Enfin, nous présentons une application importante de robotique donnant lieu un l'étude d'un système paramétré surdéterminé.

Décomposition régulière

La *décomposition régulière* d'un idéal est une décomposition équidimensionnelle d'un idéal I où chaque composantes est représentée par le couple (S, F) où S est une suite régulière de polynômes, et F un ensemble de polynômes. Un tel couple est alors appelé *ensemble régulier*. Comme pour les ensembles triangulaires, on distingue alors deux types de décompositions :

- la *décomposition régulière stricte* : étant donné un idéal I, sa décomposition régulière stricte D est un ensemble de couples (S, F), représentant chacun la variété constructible $\mathcal{C}(S, F) = \mathcal{V}(S) \setminus \mathcal{V}(\prod_{f \in F} f)$. et vérifiant :

$$\mathcal{V}(I) = \bigcup_{(S,F) \in D} \mathcal{C}(S, F)$$

  En outre, on impose que les intersections deux à deux des variétés constructibles $\mathcal{C}(S_1, F_1)$ et $\mathcal{C}(S_2, F_2)$ pour $(S_1, F_1), (S_2, F_2) \in D$ soient vides.
- la *décomposition régulière minimale* : étant donné un idéal I, sa décomposition régulière minimale D est un ensemble de couples (S, F),représentant cette fois chacun la variété algébrique $\mathcal{Z}(S, F) = \overline{\mathcal{V}(S) \setminus \mathcal{V}(\prod_{f \in F} f)}$. et vérifiant :

$$\mathcal{V}(I) = \bigcup_{(S,F) \in D} \mathcal{Z}(S, F)$$

En outre, on impose que les composantes irréductibles de chacune des variétés $\mathcal{Z}(S_0, F_0)$ pour $(S_0, F_0) \in D$ ne soit incluses dans aucunes des variétés $\mathcal{Z}(S, F)$ pour $(S, F) \in D, (S, F) \neq (S_0, F_0)$.

Les décompositions régulières minimales ou DRM sont particulièrement bien adaptées pour le pré-traiter un système surdéterminé avant de calculer sa variété discriminante. Dans le cadre de cette thèse, je me suis donc concentrés sur l'implantation de la décomposition régulière minimal. J'ai écrit un premier programme en SINGULAR afin de comparer cette méthode aux nombreux algorithmes de décomposition implantés dans SINGULAR. J'ai aussi écrit une deuxième version MAPLE afin de tirer partie de la bibliothèque de calcul de base de Gröbner FGB présente dans MAPLE.

Complexité

Nous donnons aussi une analyse de la complexité de la décomposition régulière minimale d'un idéal I, dans le cas où I est engendré par une suite *pseudo-régulière* S_r (voir [13] ou section 8.1 pour la définition précise). On peut noter que l'on peut toujours se ramener à ce cas par une combinaisons linéaires générique des générateurs d'un idéal (voir lemme 26 ou [77, 13]).

En notant d le degré maximal des polynômes de la suite pseudo-régulière, et n le nombre de variables, soit (S, F) un ensemble régulier de codimension c, produite par l'algorithme de décomposition régulière minimale appliquée à S_r. On peut alors majoré le degré des polynômes apparaissant dans (S, F) par :

$$\deg(p) \leq \begin{cases} d \text{ si } p \in S \\ d^c \text{ si } p \in F \end{cases}$$

Si I est un idéal engendré par au plus n polynômes de degrés au plus d, et g un polynôme de degré au plus d^n. Et si $\mathcal{T}_\zeta(n, d)$ représente la complexité de la saturation de I par g, alors, le nombre d'opérations nécessaires pour obtenir la DRM de S_r est majoré par :

$$\mathcal{O}\left(n^2 d^n \mathcal{T}_\zeta(n, d)\right)$$

Dans le cas où nous représentons nos données de manière dense, le nombre d'opérations binaires nécessaires pour obtenir la DRM de S_r est alors majoré par :

$$\sigma_{\max}^{\mathcal{O}(1)} d^{\mathcal{O}\left(n^2\right)}$$

On remarquera que dans le modèle de représentation dense la taille d'un polynôme de degré d^n, dont les coefficients ont une taille binaire majorée par $\sigma_{\max}$, est :

$$\sigma_{\max} \binom{d^n + n}{n} = \sigma_{\max} d^{\theta(n^2)}$$

Robots parallèles

Les robots parallèles font l'objet d'une activité de recherche intense depuis ces vingt dernières années. Le livre [100] par exemple constitue une introduction à ce domaine. Les robots parallèles sont dotés d'une géométrie complexe, et leur étude passe par la résolution de systèmes paramétrés complexes.

Dans [99, 145], les auteurs étudient les configurations dites *cuspidales* des robots parallèles de type $3 - RPR$, en utilisant des méthodes de discrétisation de l'espace des paramètres.

Après un travail préalable de modélisation du problème plus adaptée à nos méthodes, nous avons été confronté au calcul de la variété discriminante d'un système de 9 équations, 6 inconnues et 1 paramètre. Nous avons réussi à calculer sa décomposition régulière minimale ainsi que sa variété discriminante. Cela nous a permis de décrire de façon certifiée toutes les configurations cuspidales du robot $3 - RPR$ étudié dans [99, 145]. Nous avons notamment ainsi exhibé certaines configurations que les méthodes de discrétisation n'avaient pas permis de détecter.

Surface d'Enneper

Le problème considéré ici consiste à étudier la variété définissant implicitement une variété paramétrée. Nous montrons comment l'utilisation récursive du calcul de la variété discriminante permet de prouver que les deux variétés considérées sont égales.

Chapitre 7

Décomposition régulière

7.1 Introduction

Soit V une variété algébrique de $\mathbb{C}^n$ définie par les équations polynomiales :

$$\begin{cases} f_1 &= 0 \\ & \vdots \\ f_m &= 0 \end{cases}$$

Lorsque cette variété est de dimension zéro, sa description géométrique peut se faire par l'énumération finie de ses points. Lorsqu'elle est de dimension positive, afin de décrire cette variété, nous devons d'abord répondre aux questions suivantes : : la variété est elle équidimensionnelle ? Si oui quelle est sa dimension ? Sinon, quelles sont ses différentes composantes équidimensionnelles ? Ensuite, nous devons donner une représentation de chacune de ses composantes.

La *décomposition équidimensionnelle* d'une variété algébrique est une étape nécessaire à la description des solutions d'un système d'équations polynomiales de dimension positive. Dans [20], [134] ou encore [88, chapitre IV], les auteurs étudient des systèmes d'équations de dimension positive modélisant des problèmes de domaines aussi variés que la robotique, la physique théorique, la géométrie, la simulation, ... La décomposition équidimensionnelle de ces systèmes est un étape incontournable menant à leur résolution.

Ces enjeux ont motivé de nombreux travaux sur la décomposition équidimensionnelle et ont donné naissance à plusieurs algorithmes (purement symboliques [140, 51, 85, 73, 50, 20, 36] ou symbolique-numériques [89, 134] parmi les principaux) et logiciels ([112, 80, 117, 116] entre autres).

On peut remarquer que une grande partie des travaux sur la décomposition équidimensionnelle s'appuie sur des méthodes d'élimination de variables pour réduire le problème à la factorisation polynômiale ([140, 85, 73, 50, 20, 51, 89]). Seule les auteurs de [36] proposent une méthode permettant de calculer la composante de plus grande dimension en utilisant des méthodes d'algèbre homologique. D'un point de vue pratique, l'élimination de variables peut s'avérer couteuse comme le remarque Bayer et Mumford en 1993 dans [6] :

> The general experience is that taking projections can be very time consuming. One reason is that the degree of the generators may go up substantially and that sparse defining polynomials may be replaced by more or less generic polynomials.

C'est avec l'objectif pragmatique d'éviter l'élimination de variables et de limiter la création de polynôme générique que nous introduisons les *décompositions régulières* ainsi que les algorithmes permettant de les calculer. À notre connaissance, nous proposons ici le premier algorithme depuis [36] permettant de calculer une décomposition équidimensionnelle d'un idéal sans calculer de polynômes d'élimination. En pratique, nous avons pu observer l'avantage d'une telle approche, notamment sur des exemples comme celui présenté au chapitre 9.

L'idée principale de notre algorithme permettant d'éviter l'élimination de variables est basée sur la remarque suivante. Soit I un idéal équidimensionnel de $K[x_1, \ldots, x_n]$, dont la variété $\mathcal{V}(I)$ se décompose en les composantes irréductibles $V_1, \ldots, V_m \subset \mathbb{C}^n$. Soit g un polynôme de $K[x_1, \ldots, x_n]$ tel que g s'annule sur les k composantes $V_1, \ldots, V_k$. Si f est un polynôme :

i) s'annulant sur les $m - k$ composantes $V_{k+1}, \ldots, V_m$

ii) prenant une valeur non nulle sur chacune des composantes $V_1, \ldots, V_k$

, alors :

$$\mathcal{V}(I + \langle g \rangle) = \mathcal{V}(I : f^\infty) \cup \mathcal{V}(I + \langle f + g \rangle)$$

et chacune des variétés $\mathcal{V}(I : f^\infty)$ et $\mathcal{V}(I + \langle f + g \rangle)$ est équidimensionnelle. Un polynôme f vérifiant la condition i) peut s'obtenir parmi les générateurs de $I : g^\infty$. La condition ii) est plus difficile à garantir. Dans la section 7.3.1 on montre que si on sait exhiber un polynôme f satisfaisant la condition i) et prenant une valeur non nulle sur *un* point de $\mathcal{V}(I)$, alors on peut construire un polynôme vérifiant les conditions i) et ii).

Les algorithmes que nous présentons ici peuvent être utilisés directement dans un anneau de Cohen-Macaulay quelconque. Nous nous restreindrons dans la présentation aux anneaux de polynômes.

7.1.1 Opérations usuelles

La description des algorithmes de ce chapitre s'appuie essentiellement sur :
- La saturation d'un idéal par un polynôme
- Le test d'appartenance au radical d'un idéal
- Le calcul d'intersection d'idéaux

Nous présentons ici un rapide aperçu des méthodes permettant d'effectuer ces opérations dans un anneau de polynômes.

Saturation Soit I un idéal de $K[x_1, \ldots, x_n]$ et g un polynôme. L'idéal I saturé par g se note $I : g^\infty$ et est défini par :

$$I : g^\infty = \{p \in K[x_1, \ldots, x_n] \mid \exists d \in \mathbb{N} \text{ tel que } g^d p \in I\}$$

Dans nos algorithmes, nous utiliserons une fonction de saturation renvoyant un idéal dont le radical est $I : g^\infty$.

SATURATION $([f_1, \ldots, f_k], [g])$:

- *Entrée* : $\begin{cases} f_1, \ldots, f_k \in \mathbb{Q}[x_1, \ldots, x_n]; \\ g \in \mathbb{Q}[x_1, \ldots, x_n] \end{cases}$
- *Sortie* : $q_1, \cdots, q_t \in \mathbb{Q}[t_1, \ldots, t_s]$ tels que $\sqrt{\langle q_1, \cdots, q_t \rangle} = \langle f_1, \ldots, f_k \rangle : g^\infty$.

La saturation d'un idéal par un polynômes peut être vue comme l'élimination d'une variable. Soit $f_1, \ldots, f_k$ des polynômes de $K[x_1, \ldots, x_n]$ générateurs de I. Alors la saturation de I par g est exactement :

$$\langle f_1, \ldots, f_k, Zg - 1 \rangle \cap K[x_1, \ldots, x_n]$$

Pour calculer la fonction SATURATION, on peut ainsi utiliser n'importe quelle méthode d'élimination vues à la section 3.1.2 du chapitre 3. En particulier, on peut calculer les générateurs de $I : g^\infty$ en éliminant une variable, grâce aux algorithmes de bases de Gröbner en utilisant un ordre d'élimination $<_{[Z],[x_1,\ldots,x_n]}$. On peut aussi utiliser les méthodes incrémentiels de calcul de paramétrisation rationnelle, ou encore les méthodes de déformations. Pour ces dernières méthodes, on sera amené à éliminer autant de variable que la codimension de I afin de pouvoir obtenir un ensemble de générateurs de J tel que $\sqrt{J} = I : g^\infty$.

Appartenance au radical Étant donné un idéal I, et un polynôme g de $K[x_1, \ldots, x_n]$, on est induit à tester au cours de notre algorithme si le polynôme g appartient au radical de l'idéal I. Le lemme suivant nous permet de réduire ce test à un calcul de saturation d'idéal par un polynôme.

Lemme 15. *(Appartenance au radical)*
Soit I un idéal et g un polynôme de $K[x_1, \ldots, x_n]$. Les deux propositions suivantes sont alors équivalentes :

i) $g \in \sqrt{I}$

ii) $1 \in I : g^\infty$

□

Ainsi, en utilisant un algorithme de calcul de saturation, on peut directement tester si le polynôme g appartient au radical de I.

Intersection Nous utilisons l'intersections d'idéaux en section 7.3.2 pour le calcul d'une *décomposition régulière minimale*. Soient I_1, I_2 deux idéaux de $\mathbb{Q}[x_1, \ldots, x_n]$. Comme on peu le lire dans [28, chapitre 4,§3] par exemple, le calcul de leur intersection peut se faire par l'élimination d'une variable.

Lemme 16. *(Intersection)*
Soient $f_1, \ldots, f_k$ et $g_1, \ldots, g_l$ des polynômes de $K[x_1, \ldots, x_n]$ engendrant respectivement les idéaux I et J. Alors, l'intersection de I et J vérifie :

$$I \cap J = \langle Zf_1, \ldots, Zf_k, (1-Z)g_1, \ldots, (1-Z)g_l \rangle \cap K[x_1, \ldots, x_n]$$

□

Ainsi, comme pour la saturation, on peut utiliser les méthodes d'éliminations présentées en section 3.1.2 pour calculer l'intersection d'idéaux. En particulier, le calcul de Gröbner permet de calculer cette intersection en éliminant une variable.

7.1.2 Organisation

Ce chapitre est réparti en trois parties.

Dans la première partie, nous rappelons les définitions des notions mathématiques fondamentales sur lesquels nous nous appuyons, et introduisons les notions de *décomposition régulière stricte* (ou DRS) et *décomposition régulière minimale* (ou DRM). Dans la deuxième partie, nous présentons deux algorithmes permettant de calculer respectivement les DRS et les DRM.

Au cours de ma thèse j'ai implanté l'algorithme de décomposition régulière minimale présentée en section 7.3.2 en MAPLE et en SINGULAR. Pour les opérations de saturation et d'intersection, j'ai utilisé des algorithmes basés sur le calcul de bases de Gröbner. La troisième partie présente une comparaison de l'implantation en SINGULAR avec les autres algorithmes de décomposition implantés dans ce système de calcul formel.

7.2 Résultat principal

7.2.1 Préliminaires

Dimension

Soit A un anneau commutatif noethérien. Nous rappelons ici les résultats d'algèbre commutative essentiels pour la définition de la dimension d'un idéal.

Notations 9. *Si F est une partie de A, on note $\langle F \rangle_A$ l'idéal engendré par les éléments de F dans A. Lorsqu'il n'y a pas d'ambigüité sur l'anneau dans lequel on se place, on omettra l'anneau en indice.*
□

Définition 17. *[35, Chapitre 17](Suite régulière)*
Une suite $f_1, \ldots, f_k$ d'éléments de A est dite régulière si et seulement si :
- *$\langle f_1, \ldots, f_k \rangle \neq A$*
- *pour tout i entre 1 et k, f_i n'est pas un diviseur de zéro dans $A/\langle f_1, \cdots, f_{i-1} \rangle$*

□

Définition 18. *[74](Idéal premier)*
Un idéal P de A est dit premier *si et seulement si A/P est un anneau intègre.*
□

Définition 19. *[74](Premier isolé)*
Soit I un idéal de A. Soit $\mathcal{P}_I$ l'ensemble des idéaux premiers contenant I. On dit que P est un premier isolé *(ou* minimal*) de I si et seulement si P est un élément minimal pour l'inclusion de $\mathcal{P}_I$.*
□

Notations 10. *Soit I un idéal de A. On notera* $\mathrm{minass}(I)$ *l'ensemble des idéaux premiers minimaux de I.*
□

Lemme 17. *[74](Unicité de la représentation première)*
Soit I un idéal. Si il existe un ensemble d'idéaux premiers $P_1, \ldots, P_k$ tels que :

$$\begin{cases} \sqrt{I} = \bigcap_{i=1}^{k} P_i \\ \forall 1 \leq i, j \leq k, P_i \not\subset P_j \end{cases}$$

alors, $\{P_1, \ldots, P_k\} = \mathrm{minass}(I)$
□

Définition 20. *(Hauteur d'un idéal premier)*
La hauteur d'un idéal premier P de A est la longueur k de la plus grande suite strictement décroissante d'idéaux premiers de la forme :

$$P \supsetneq P_1 \supsetneq \cdots \supsetneq P_k$$

□

Définition 21. *(Profondeur d'un idéal premier)*
La profondeur d'un idéal premier P de A est la longueur k de la plus grande suite régulière d'éléments de P.
□

Définition 22. *[35, Chapitre 18](Anneau de Cohen Macaulay)*
Soit A un anneau commutatif noethérien. On dit que A est un anneau de Cohen-Macaulay si et seulement si la hauteur de tout idéal premier P de A est égale à sa profondeur.
□

Les anneaux de polynômes multivariés $K[x_1, \ldots, x_n]$, les anneaux de séries formelles $K[[t]]$ sont des exemples d'anneaux de Cohen-Macaulay.

Dans la suite, A désignera toujours un anneau de Cohen-Macaulay. Ce cadre nous permet de définir facilement la dimension d'un idéal.

Définition 23. *(Dimension)*
Soit A un anneau de Cohen-Macaulay et I un idéal de A. La codimension de I est la plus petite hauteurs des idéaux premiers minimaux de I.

La dimension de I est la codimension de A moins la codimension de I.
□

Extension

Définition 24. *(Clôture multiplicative)*
Soit F une partie non vide de A. On note $\widetilde{F}$ la clôture multiplicative de F définie par :

$$\widetilde{F} = \{f_1^{n_1} \cdots f_k^{n_k} \mid k \geq 1, n_1 \geq 0, \ldots, n_k \geq 0, f_1 \in F, \ldots, f_k \in F\}$$

Lorsque $F = \emptyset$, on définit par convention $\widetilde{F} = \{1_A\}$
□

Notations 11. *(Extension)*
Soit S une partie multiplicativement close de A. On note $S^{-1}A$ l'anneau des fractions de la forme r/s où $r \in A$ et $s \in S$. Si f un élément de $S^{-1}A$, et est donné sous une représentation $f = r/s$ où $r \in A$ et $s \in S$, alors num(f) *désignera par abus de notation l'élément r.*
□

Lemme 18. *[74]*
Si A est un anneau de Cohen-Macaulay et S une partie multiplicativement close de A, alors $S^{-1}A$ est un anneau de Cohen-Macaulay.
□

Remarque 7. *Lorsque F est un ensemble fini, et A une algèbre de corps alors, en notant p le produit des éléments de F, les algèbres suivantes sont isomorphes :*
- $\widetilde{F}^{-1}A$
- $A[\frac{1}{p}]$
- $A[T]/\langle Tp - 1\rangle$

Géométrie

Définition 25. *[74](Idéal maximal)*
Un idéal $\mathfrak{m}$ de A est dit maximal *si et seulement si $A/\mathfrak{m}$ est un corps.*
□

Remarque 8. *Lorsque A est un anneau polynômial $\overline{K}[x_1, \ldots, x_n]$ et $\overline{K}$ un corps algébriquement clos, les idéaux maximaux de $\overline{K}[x_1, \ldots, x_n]$ sont alors en bijections avec les points de $\overline{K}^n$.*

Notations 12. *(Variété algébrique)*
Soit A est un anneau polynômial $K[x_1, \ldots, x_n]$, $\overline{K}$ la clôture algébrique de K, et I un idéal de A. On note $\mathcal{V}(I)$ l'ensemble des zéros de I dans $\overline{K}^n$. On dit que $\mathcal{V}(I)$ est la variété algébrique *de I.*
□

Remarque 9. *Dans le cas où A est un anneau de Cohen-Macaulay, on peut définir* Specmax(A) *l'ensemble des idéaux maximaux de A et définir la variété algébrique d'un idéal I dans* Specmax(A) *par :*

$$\mathcal{V}(I) = \{\mathfrak{m} \in \text{Specmax}(A) \mid I \subset \mathfrak{m}\}$$

Notations 13. *(Radical)*
Soit I un idéal de A. On note sqrtI le radical de I défini par :

$$\sqrt{I} = \{p \in A \mid \exists k \in \mathbb{N} \text{ tel que } p^k \in I\}$$

□

Propriété 7. *[28]*
Si I est un idéal de A, alors, son radical $\sqrt{I}$ vérifie les propriétés suivantes :
- $\mathcal{V}(\sqrt{I}) = \mathcal{V}(I)$
- $\sqrt{I} = \bigcap_{P \in \text{minass}(I)} P$
- $\text{minass}(\sqrt{I}) = \text{minass}(I)$

□

Notations 14. *(Division,Saturation)*
Soient I, J deux idéaux de A.

On note $I : J$ l'idéal I divisé par J, défini par :

$$I : J = \{x \in A \mid xJ \subset I\}$$

On note $I : J^\infty$ l'idéal I saturé par J, défini par :

$$I : J^\infty = \{x \in A \mid \exists k \in \mathbb{N} \text{ tel que } xJ^k \subset I\}$$

Si p est un polynôme de A, on notera par abus de notation $I : p$ l'idéal I divisé par $\langle p \rangle$ et $I : p^\infty$ l'idéal I saturé par $\langle p \rangle$.

□

Notations 15. *(Clôture de Zariski)*
Soit V un ensemble de points de $\overline{K}^n$. La clôture de Zariski *$\widetilde{V}$ de V est la plus petite variété algébrique contenant V.*

□

Remarque 10. *Dans le cas d'un anneau de Cohen-Macaulay A, la clôture de Zariski d'un ensemble V de* Specmax(A) *est définie de la même manière comme la plus petite variété algébrique contenant V.*

7.2.2 Définitions

Dans cette section, A désigne un anneau de Cohen-Macaulay.

Définition 26. *(Ensemble régulier)*
Soit S une suite $s_1, \ldots, s_k$ de k éléments de A et F une partie finie de A.

La paire (S, F) est appelée ensemble régulier *si et seulement si S est une suite régulière dans $\widetilde{F}^{-1}A$.*

□

Géométriquement, un ensemble régulier est une suite S régulière en dehors de l'hypersurface définie par le produit des polynômes de F.

Exemple 1. *On se place dans l'anneau $A = \mathbb{C}[x, y]$. Soient $F = \emptyset$ et S la suite constituée des 2 polynômes s_1 et s_2 :*

$$\begin{aligned} s_1 &= x(y^2 - x^2) \\ s_2 &= (y-1)(y^2 - x^2) \end{aligned}$$

La suite S n'est pas régulière dans $\mathbb{C}[x, y]$, car xs_2 est divisible par s_1, donc vaut zéro dans $\mathbb{C}[x, y]/\langle s_1 \rangle_A$.

La paire (S, F) n'est donc pas un ensemble régulier.

□

Exemple 2. *Soient $F = \{y - x, y + x\}$ et S la suite (s_1, s_2) définie dans l'exemple 1 dans $\mathbb{C}[x, y]$.*

Dans ce cas, en notant $A' = \widetilde{F}^{-1}\mathbb{C}[x, y]$, on peut remarquer que s_2 n'est pas un diviseur de zéro dans $A'/\langle s_1 \rangle_{A'}$. En effet l'idéal engendré par s_1 vérifie :

$$\langle s_1 \rangle_{A'} = \langle x \rangle_{A'}$$

C'est un idéal premier, l'anneau $A'/\langle s_1 \rangle_{A'}$ est intègre et s_2 n'est pas diviseur de zéro dans $A'/\langle s_1 \rangle_{A'}$. Ainsi la suite S est régulière dans A'.

La paire (S, F) est un ensemble régulier.

□

Définition 27. *(Géométrie des ensembles réguliers)*
Soit (S, F) un ensemble régulier.

- *On appelle* idéal saturé *de (S, F) et on note $\mathcal{I}(S, F)$ l'idéal*

$$\langle S \rangle : \prod_{f \in F} f^\infty$$

Dans le cas où A est une algèbre polynômiale sur un corps K, on peut définir les notions suivantes.

- *On appelle* zéros constructibles *de (S, F) et on note $\mathcal{C}(S, F)$ la variété semi-algébrique*

$$\mathcal{V}(S) \setminus \bigcup_{f \in F} \mathcal{V}(f)$$

- *On appelle* zéros algébriques *de (S, F) et on note $\mathcal{Z}(S, F)$ la variété algébrique*

$$\overline{\mathcal{V}(S) \setminus \bigcup_{f \in F} \mathcal{V}(f)}$$

- *Le nombre de polynômes de la suite S est appelé* hauteur *de (S, F).*

□

Remarque 11. *On peut noter que dans le cas où A est une algèbre polynomiale, la variété algébrique $\mathcal{V}$ $(\mathcal{I}(S, F))$ est exactement $\mathcal{Z}(S, F)$.*

On peut maintenant définir la notion fondamentale de cette partie.

Définition 28. *(Décomposition Régulière)*
Soit I un idéal de A. Soit D un ensemble fini de paires (S, F) telles que :
(i) $\forall (S,F) \in D, (S,F)$ *est un ensemble régulier*
(ii) $\sqrt{I} = \bigcap_{(S,F)\in D} \sqrt{\mathcal{I}(S,F)}$
On dit alors que D est une décomposition régulière *ou* DR *de I.*
□

Remarque 12. *Si A est un anneau polynomial, on peut remplacer (ii) de manière équivalente par :*
(ii) $\mathcal{V}(I) = \bigcup_{(S,F)\in D} \mathcal{Z}(S,F)$

Définition 29. *(Décomposition Régulière Minimale)*
Soient I un idéal de A et D une décomposition régulière de I. On dit que D est une décomposition régulière minimale *ou* DRM *de I si et seulement si pour tout (S_1, F_1) et (S_2, F_2) deux ensembles réguliers différents dans D on a :*

$$P \in \text{minass}(\mathcal{I}(S_1, F_1)) \Rightarrow P \not\supset \mathcal{I}(S_2, F_2)$$

□

Définition 30. *(Décomposition Régulière Stricte)*
Soient $K[x_1, \ldots, x_n]$ un anneau polynomial et I un idéal de $K[x_1, \ldots, x_n]$. Soit D une décomposition régulière de I. On dit que D est une décomposition régulière stricte *ou* DRS *de I si et seulement si pour tout (S_1, F_1) et (S_2, F_2) deux ensembles réguliers différents dans D on a :*

$$\mathcal{C}(S_1, F_1) \cap \mathcal{C}(S_2, F_2) = \emptyset$$

□

7.2.3 Propriétés

Propriété 8. *(Équidimensionnelle)*
Soit (S, F) un ensemble régulier. Alors l'idéal saturé $\mathcal{I}(S, F)$ est équidimensionnelle (ses idéaux premiers isolés sont tous de même dimension) et sa codimension est la hauteur de (S, F).
On appelle dimension *de (S, F) la dimension $\mathcal{I}(S, F)$.* □

Propriété 9. *(Calcul du radical)*
Soit A l'anneau de polynômes $K[x_1, \ldots, x_n]$ et K un corps de caractéristique 0. Soit (S, F) un ensemble régulier de hauteur k. On note J l'idéal Jacobien engendré par les mineurs $k \times k$ de la matrice jacobienne de S. Alors, l'idéal

$$\mathcal{I}(S, F) : J$$

est le radical de $\mathcal{I}(S, F)$. □

Remarque 13. *Cette propriété est fausse dans le cas d'un idéal général.*

*preuve :*Comme S est régulière dans $\widetilde{F}^{-1}A$, le théorème 2.1 de [36] nous permet de conclure. □

Exemple 3. *Soit $A = \mathbb{C}[x, y]$. On considère l'ensemble régulier $(S, F) = ((x^2, y^2), \emptyset)$. La matrice Jacobienne de S est :*

$$\begin{bmatrix} 2x & 0 \\ 0 & 2y \end{bmatrix}$$

La hauteur de (S, F) est 2, et l'idéal jacobien engendré par les mineurs 2×2 de M est :

$$J = \langle 4xy \rangle$$

On peut alors vérifier que $I : J = \langle x, y \rangle = \sqrt{I}$.
□

Exemple 4. *Soit $A = \mathbb{C}[x, y]$. Cet exemple est illustre le cas général où l'idéal n'est pas régulier.*

Soit $I = \langle x^2, y^2, xy \rangle$. Alors I est 0-dimensionnel et $\sqrt{I} = \langle x, y \rangle$. Or sa matrice Jacobienne M est :

$$\begin{bmatrix} 2x & 0 \\ 0 & 2y \\ y & x \end{bmatrix}$$

L'idéal Jacobien J est engendré par les mineurs 2×2 de M :

$$J = \left\langle 4xy, 2x^2, -2y^2 \right\rangle$$

Alors $I : J = \langle 1 \rangle \neq \sqrt{I}$.
□

7.3 Algorithmes

Nous supposerons ici que A est un anneau polynomial $K[x_1, \ldots, x_n]$, où K est un corps quelconque. On pourra penser par exemple à :

- $\mathbb{Q}$
- $\mathbb{Q}(x_1, \ldots, x_k)$
- $\mathbb{Z}/p\mathbb{Z}$
- $\mathbb{Z}/p\mathbb{Z}(x_1, \ldots, x_k)$

Les algorithmes que nous présentons dans cette section prennent en entrée une liste de polynômes et renvoient une décomposition régulière stricte (resp. minimale) de l'idéal qu'ils engendrent.

7.3.1 Décomposition régulière stricte

L'algorithme de décomposition régulière stricte est incrémentiel en les polynômes d'entrée. La description de notre algorithme utilisera exclusivement les boîtes noires présentée ci-dessus.

Présentation générale de l'algorithme

Soit $I = \langle g_1, \ldots, g_m \rangle$ un idéal de A engendré par m polynômes. L'idée de notre algorithme est de calculer successivement les décompositions régulières strictes D_c de $\langle g_1, \ldots, g_c \rangle$ pour $1 \leq c \leq m$.

D'abord, il est facile de voir que la paire formée de la suite (g_1) et de l'ensemble vide est un ensemble régulier qui forme trivialement une décomposition régulière D_1 de $\langle g_1 \rangle$.

Supposons maintenant que nous ayons calculé une décomposition régulière stricte D_c de $\langle g_1, \ldots, g_c \rangle$. L'étape incrémentielle de notre algorithme consiste alors à calculer une DRS D_{c+1} de $\langle g_1, \ldots, g_{c+1} \rangle$ à partir de D_c.

Plus précisément, soit $(S, F) \in D_c$. On se place alors dans l'anneau $\widetilde{F}^{-1}A$ et on note $D_{(S,F),g_{c+1}}$ une DRS de :

$$\langle S \rangle_{\widetilde{F}^{-1}A} + \langle g_{c+1} \rangle_{\widetilde{F}^{-1}A}$$

dans $\widetilde{F}^{-1}A$.

Ainsi, par le calcul des $D_{(S,F),g_{c+1}}$, on retrouve D_{c+1} avec :

$$D_{c+1} = \bigcup_{(S,F) \in D_c} \{(\mathrm{num}(S'), \mathrm{num}(F') \cup F) \mid (S', F') \in D_{(S,F),g_{c+1}}\}$$

où $\mathrm{num}(S')$ désigne la suite des numérateur des éléments de S' et $\mathrm{num}(F')$ l'ensemble des numérateurs de F'.

L'étape cruciale de notre algorithme est donc, étant donné un ensemble régulier (S, F) et un polynôme p de calculer une décomposition régulière stricte de $D_{(S,F),p}$ de l'idéal engendré par S et p dans $\widetilde{F}^{-1}A$.

Scindage

Distinction de cas Soit (S, F) un ensemble régulier et p un polynôme de $K[x_1, \ldots, x_n]$. On note A l'anneau $\widetilde{F}^{-1}K[x_1, \ldots, x_n]$, et I (resp. J) l'idéal engendré par S (resp. S et p) dans A.

L'enjeu est de calculer une décomposition régulière stricte de J. Nous distinguons alors deux cas :

– p ne divise pas zéro dans A/I A

– p divise zéro dans A/I A

Dans le premier cas, la séquence S'=S,p est régulière sur A, et $(S', \emptyset)$ est trivialement une DRS de J dans A.

Dans le second cas, nous scindons I en deux ensembles réguliers. L'idée est de calculer un polynôme $h \in A$ tel que :

$$\begin{cases} h \in I : p^\infty \\ p + h \text{ ne divise pas zéro dans } A/I \ A \end{cases} \tag{C}$$

Ce calcul est effectué par l'*algorithme de scindage* présenté dans la section suivante. Ainsi, si h vérifie les conditions (C), on montrera que :

$$D_{(S,F),p} = \{(S, \{h\}), ((S, p + h), \emptyset)\}$$

est une DRS de J dans A.

Lemme préparatoires Avant de présenter l'algorithme, nous introduisons quelques lemmes nécessaires à la preuve de la terminaison et de la correction de l'algorithme.

Lemme 19. *Soient $p \in A$ et I un idéal de A engendré par une suite régulière. Les propositions suivantes sont alors équivalentes :*

i) p divise zéro dans A/IA
ii) $\dim(I) = \dim(I + \langle p \rangle)$
iii) $\exists P \in \text{minass}(I)$ tel que $p \in P$

Dans ce cas, on remarque en outre que $I : p^\infty$ n'est pas inclus dans $\sqrt{I}$
□

*preuve :*Pour la preuve de ce lemme, on utilise la décomposition primaire d'une suite régulière décrite dans [35] par exemple. Principalement, il existe un nombre fini d'idéaux $Q_1, \ldots, Q_k$ tels que :

- $I = \bigcap_{i=1}^{k} Q_i$
- Si $r \in A \setminus \sqrt{Q_i}$ alors $Q_i : r = Q_i$
- $\text{minass}(I) = \{\sqrt{Q}_1, \ldots, \sqrt{Q}_k\}$
- $\forall P \in \text{minass}(I), \dim(P) = \dim(I)$

En utilisant cette décomposition primaire on prouve alors :

i) $\Rightarrow$ iii) Si p divise zéro dans A/IA, alors il existe $q \notin I$ tel que $qp \in I$. En particulier, il existe Q_i tel que $q \notin Q_i$. Ainsi $\sqrt{Q_i} \in \text{minass}(I)$ et $p \in \sqrt{Q_i}$.

iii) $\Rightarrow$ ii) La dimension de I est toujours supérieure à la dimension de $I + \langle p \rangle$. Par ailleurs, s'il existe $P \in \text{minass}(I)$ tel que $p \in P$, on sait alors que $I + \langle p \rangle \subset P$, ce qui entraîne $\dim(I + \langle p \rangle) \geq \dim(P) = \dim(I)$.

ii) $\Rightarrow$ i) Si p ne divise pas zéro dans A/IA alors la suite formé par les générateurs de I et p est régulière. En particulier, la profondeur des idéaux premiers isolés de $I + \langle p \rangle$ est strictement supérieure à celle des idéaux premiers de I, ce qui implique $\dim(I) > \dim(I + \langle p \rangle)$.

Enfin, s'il existe $P \in \text{minass}(I)$ tel que $p \in P$, on conclue facilement que $I : p^\infty \not\subset P$ donc en particulier, $I : p^\infty \not\subset \sqrt{I}$.
□

Le lemme suivant est au coeur de l'algorithme de scindage.

Lemme 20. *Soit I un idéal et p,q deux éléments de A tels que $pq \in I$. On a alors l'galité suivante :*

$$\sqrt{I + \langle p, q \rangle} = \sqrt{I + \langle p + q \rangle}$$

□

*preuve :*L'inclusion de la gauche vers la droite est évidente. Pour l'autre sens, on peut remarquer que les éléments pq, $p(p+q)$ et $q(p+q)$ appartiennent à $\sqrt{I + \langle p + q \rangle}$, et donc p^2 et q^2 aussi. Le passage au radical permet de conclure la preuve.
□

Géométriquement, ce lemme peut s'énoncer ainsi : si $\mathcal{V}(I) \subset \mathcal{V}(p) \cup \mathcal{V}(q)$, alors $\mathcal{V}(I) \cap \mathcal{V}(p) \cap \mathcal{V}(q) = \mathcal{V}(I) \cap \mathcal{V}(p+q)$. C'est cette propriété qui nous permettra d'obtenir une séquence régulière sans utiliser une combinaison générique des générateurs.

Algorithme de scindage L'algorithme de scindage constitue la partie principale de l'étape de récurrence. Étant donné un ensemble régulier (S, F) et un polynôme p, soit I l'idéal engendré par S dans $A := \widetilde{F}^{-1}K[x_1, \ldots, x_n]$. L'algorithme suivant calcule un polynôme h de $K[x_1, \ldots, x_n]$ tel que :

$$h \in I : p^\infty \tag{1}$$

$$p + h \text{ ne divise pas zéro dans } A/I\ A \tag{2}$$

Algorithme 1 SCINDAGE

ENTRÉE : un ensemble régulier (S, F) et un polynôme p de $K[x_1, \ldots, x_n]$
($A := \widetilde{F}^{-1}K[x_1, \ldots, x_n]$ et I désigne l'idéal engendré par S dans A)
SORTIE : un élément h dans $I : p^\infty$
tel que $p + h$ ne divise pas zéro dans A/SA

- $h := 0$
- TANT QUE $\dim(I + \langle p + h \rangle) = \dim(I)$
  - $J := I : (p + h)^\infty$
  - POUR $g \in$ Générateurs de J
    SI $g \notin \sqrt{I}$ ALORS
    SORTIR
    FIN SI
  - FIN POUR
  - $h := h + g$
- FIN TANT
- RENVOYER h

Remarque 14.

- *On peut remarquer qu'il n'est pas nécessaire de calculer tous les générateurs de $J = I : (p+h)^\infty$: on peut s'arrêter dès que l'on a trouvé un générateur de J qui n'est pas dans le radical de I.*
- *En utilisant le lemme 19, il est facile de vérifier que l'élément h renvoyé en sortie est tel que $p + h$ ne divise pas zéro dans A/SA .*
- *Le nombre d'itération de la boucle principale* TANT QUE *est majoré par le nombre de premiers isolés de I (cf. preuve ci-dessous).*

*preuve :*Afin de prouver la correction de cet algorithme, nous devons nous assurer que le polynôme renvoyé h appartient à $I : p^\infty$, et que l'algorithme termine bien.

Correction. Nous prouvons la première assertion par récurrence en remarquant que J est toujours inclus dans $I : p^\infty$.

Supposons que $h \in I : p^\infty$ et soit $x \in I : (p+h)^\infty = J$. Dans ce cas, il existe k et l deux entiers tels que $p^k h \in I$ et $(p+h)^l x \in I$. En développant $p^{kl}(p+h)^l x = (p^{k+1} + p^k h)^l x$, on peut alors remarquer que $x \in I : p^\infty$, ce qui permet de conclure que si $h \in I : p^\infty$ alors $J = I : (p+h)^\infty \subset I : p^\infty$.

Puis par récurrence, on a :

- Lorsque $h = 0$, par définition d'un idéal $h \in I : p^\infty$.
- Supposons que $h \in I : p^\infty$ au début de la boucle TANT QUE. Dans ce cas, on a vu que $J = I : (p+h)^\infty \subset I : p^\infty$. En particulier, le polynôme $g \in J$ appartient lui aussi à $I : p^\infty$. Ainsi le nouveau polynôme $h + g$, qui sera le nouveau h, appartient lui aussi à $I : p^\infty$.

Terminaison. Pour la preuve de terminaison de l'algorithme, nous utilisons les équivalences données dans le lemme 19 pour montrer que le nombre d'itérations de la boucle TANT QUE est majoré par le nombre de premiers isolés de I.

Plus précisément, soit $h \in A$ tel que $\dim(I + \langle p+h \rangle) = \dim(I)$, et soit k le nombre de premiers isolés de I contenant $p+h$. Sans restriction de généralité, on peut écrire :

$$\text{minass}(I) = \{P_1, \ldots, P_k, Q_1, \ldots, Q_s\}$$

où $p + h \in \bigcap_{i=1}^k P_i$ et $I : (p+h)^\infty \subset \bigcap_{i=1}^s Q_i$.

Comme dans l'algorithme, soit $g \in I : (p+h)^\infty$ tel que $g \notin \sqrt{I}$. Le lemme 19 nous garanti qu'un tel élément existe toujours. Dans ce cas, on montre que $p + h + g$ est contenu dans au plus $k - 1$ premiers isolés de I.

Pour $1 \leq i \leq s$, on sait que $g \in Q_i$ et $p + h \notin Q_i$, ce qui implique :

$$p + h + g \notin Q_i$$

Par ailleurs, puisque $g \notin \sqrt{I}$, il existe $1 \leq i_0 \leq k$ tel que $g \notin P_{i_0}$. Comme $p + h \in P_{i_0}$, on a alors :

$$p + h + g \notin P_{i_0}$$

Ainsi, $p + h + g$ est contenu dans au plus $k - 1$ premiers isolés de I.

À chaque itération de boucle, on remplace h par $h + g$, ce qui nous permet de conclure que le nombre de premiers isolés de I contenant $p + h$ diminue strictement jusqu'à ce qu'il soit nul, auquel cas $\dim(I + \langle p+h \rangle) \neq \dim(I)$ d'après le lemme 19 et l'algorithme termine. □

Algorithme complet

Nous revenons maintenant sur l'algorithme principale de calcul de décomposition régulière stricte. Nous montrons d'abord dans le lemme suivant que l'algorithme de scindage calcule bien une décomposition stricte.

Lemme 21. *Soient (S, F) un ensemble régulier, A l'anneau $\widetilde{F}^{-1}K[x_1, \ldots, x_n]$. Soit p un polynôme de $K[x_1, \ldots, x_n]$ divisant zéro dans A/SA. On note I (resp. J) l'idéal engendré*

par S (resp. S et p) dans A. Soit h est le polynôme renvoyé par l'algorithme de scindage. On définit l'ensemble D par :

$$D := \begin{cases} \{(S, \{h\}), ((S, p+h), \emptyset)\} & si\ \langle S, p+h\rangle \neq A \\ \{(S, \{h\})\} & sinon \end{cases}$$

Alors, D est une DRS de J dans A.
□

*preuve :*Par construction, les éléments de D sont des ensembles réguliers.

Ensuite, pour prouver que D est une décomposition régulière de J, nous devons vérifier que l'union des zéros constructibles des ensembles réguliers sont les zéros de J. Nous montrons d'abord l'égalité des clôtures algébriques, ce qui revient à prouver :

$$\sqrt{I + \langle p\rangle} = \sqrt{I} : h^\infty \cap \sqrt{I + \langle p + h\rangle}$$

Pour l'inclusion de la gauche vers la droite, puisque $h \in I : p^\infty$, nous avons $ph \in \sqrt{I}$, ce qui nous permet de conclure d'après le lemme 20 que $\sqrt{I + \langle p + h\rangle} = \sqrt{I + \langle p, h\rangle}$ donc en particulier, $\sqrt{I + \langle p\rangle} \subset \sqrt{I + \langle p + h\rangle}$. Par ailleurs, comme $p \in \sqrt{I} : h^\infty$, on a bien

$$\sqrt{I + \langle p\rangle} \subset \sqrt{I} : h^\infty \cap \sqrt{I + \langle p + h\rangle}$$

Pour l'autre inclusion, soit $x \in \sqrt{I} : h^\infty \cap \sqrt{I + \langle p + h\rangle}$. Alors, il existe $q \in I, r \in A$ et deux entiers k et l tels que

$$\begin{cases} x^k = q + r(p + h) \\ h^l x^k \in I \end{cases}$$

Il nous suffit donc de prouver que rh appartient à $\sqrt{I + \langle p\rangle}$ pour vérifier l'inclusion de droite vers la gauche. Or par construction, $h^l r(p+h) \in I$, donc $h^{l+1} r \in I + \langle p\rangle$, ce qui nous permet de conclure.

Nous devons maintenant prouver que cette décomposition régulière est stricte. Pour cela, il suffit de remarquer que d'après le lemme 20, $h \in \sqrt{I + \langle p, h\rangle} = \sqrt{I + \langle p + h\rangle}$. Ainsi, les zéros constructible de l'ensemble régulier $((S, p + h), \emptyset)$ sont naturellement distincts de ceux de (S, h).
□

Nous avons maintenant tous les éléments pour écrire l'algorithme final de décomposition régulière stricte.

Théorème 5. *Soit I un idéal engendré par les polynômes $f_1, \ldots, f_k$. Alors, la fonction :*

$$\textsc{Drs}(((f_1), \emptyset), (f_2, \ldots, f_k))$$

renvoie un décomposition régulière stricte de I. □

Algorithme 2 DRS

ENTRÉE : - un ensemble régulier (S, F)
- une liste L de polynômes $g_c, \ldots, g_m$

SORTIE : une DRS de $(S + \langle g_c, \ldots, g_m \rangle) : \prod_{f \in F} f^\infty$

- SI la liste L est vide, ALORS
  - RENVOYER $\{(S, F)\}$
- FIN SI
- $D := \emptyset$
- $J := \mathcal{I}(S, F)$
- SI $\dim(J + \langle g_c \rangle) \neq \dim(J)$ ALORS
  - $S' := S, g_c$
- SINON
  - $h :=$ SCINDAGE$((S, F), g_c)$
  - $S' := S, g_c + h$
  - $F' := F \cup \{h\}$
  - $D := \{(S, F')\}$
- FIN SI
- SI $1 \notin \langle S' \rangle : \prod_{f \in F} f^\infty$ ALORS
  - $D := D \cup \{(S', F)\}$
- FIN SI
- RENVOYER $\bigcup_{e \in D}$ DRS$(e, (g_{c+1}, \ldots, g_m))$

*preuve :*Nous montrons par récurrence sur le nombre de polynôme de la liste L que la fonction DRS calcule correctement une décomposition régulière stricte de :

$$(S + \langle g_c, \ldots, g_m \rangle) : \prod_{f \in F} f^\infty$$

D'abord, si la liste L est vide, alors DRS renvoie l'ensemble $\{(S, F)\}$ qui est trivialement une décomposition régulière stricte de $\mathcal{I}(S, F)$.

Ensuite, supposons que la sortie de DRS soit correcte lorsque le nombre de polynôme de L est $m - c$, et montrons que l'algorithme se comporte toujours correctement pour $m - c + 1$ polynômes.

Soient (S, F) et $L = (g_c, \ldots, g_m)$ les entrées de l'algorithme DRS. Si les dimension de $\mathcal{I}(S, F)$ et $\mathcal{I}(S, F) + \langle g_c \rangle$ sont différentes, alors, le lemme 19 nous assure que g_c est un non diviseur de zéro dans $A/\mathcal{I}(S, F)A$. Si l'idéal engendré par $S + \langle g_c \rangle$ dans $A/\mathcal{I}(S, F)A$ est l'anneau tout entier, alors on renvoie l'ensemble vide, qui est bien la décomposition régulière stricte de l'idéal trivial. Sinon, $\{(S + \langle g_c \rangle, F)\}$ est un ensemble régulier, et par hypothèse de récurrence, DRS$((S + \langle g_c \rangle, F), (g_{c+1}, \ldots, g_m))$ renvoie bien une décomposition régulière stricte de $(S + \langle g_c, \ldots, g_m \rangle) : \prod_{f \in F} f^\infty$.

Si les dimension de $\mathcal{I}(S, F)$ et $\mathcal{I}(S, F) + \langle g_c \rangle$ sont égales, alors on note h le polynôme renvoyé par SCINDAGE$((S, F), g_c)$ et on définit l'ensemble D par :

$$D := \begin{cases} \{(S, F \cup \{h\}), ((S, g_c + h), F)\} & \text{si } \langle S, g_c + h \rangle : \prod_{f \in F} f^\infty \neq A \\ \{(S, F')\} & \text{sinon} \end{cases}$$

Le lemme 21 nous assure alors que D forme une décomposition régulière stricte de $(S + \langle g_c \rangle) : \prod_{f \in F} f^\infty$. Puis par hypothèse de récurrence, on conclut que

$$\bigcup_{e \in D} \textsc{Drs}(e, (g_{c+1}, \ldots, g_m))$$

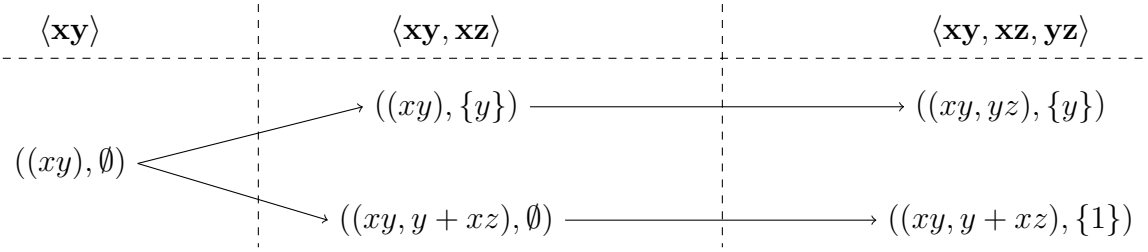
est une décomposition régulière stricte de $(S + \langle g_c, \ldots, g_m \rangle) : \prod_{f \in F} f^\infty$.
□

On illustre le comportement de cet algorithme sur des exemples jouets. L'algorithme étant récursif, on représente les étapes intermédiaires de calcul sous la forme d'un arbre dont la racine à gauche représente l'entrée de l'algorithme et les feuilles à droite forment la décomposition régulière renvoyée en sortie.

Exemple 5.
Soit l'idéal $I = \langle xy, xz, yz \rangle$ dans l'anneau polynômial $\mathbb{Q}[x, y, z]$. Pour calculer une décomposition régulière stricte de I, on calcule le résultat de la fonction $\textsc{Drs}(((xy), \emptyset), (xz, yz))$. *Dans cette exemple, S désigne la suite (xy, xz, yz).*

Les résultats intermédiaires peuvent être représenter sous la forme d'un arbre où :

- *L'entête de la k^e colonne est la liste préfixe des k premiers polynômes de S. On note cette liste S_k*
- *Chaque nœud représente un appel à la fonction* Drs
- *L'étiquette d'un nœud représente l'ensemble régulier donné en entrée à la fonction* Drs
- *La liste de polynômes donnée en entrée à la fonction* Drs *appliquée à un nœud de la k^e colonne est la liste suffixe de S privée de S_k*



Ainsi, la fonction appliquée sur le premier nœud de la 2^e colonne par exemple est $\textsc{Drs}\,(((xy), \{y\}), (yz))$.

Finalement, on lit directement dans la dernière colonne la décomposition régulière stricte de $\langle xy, xz, yz \rangle$.

De plus, on peut remarquer que les ensembles réguliers de la deuxième colonne forment une décomposition régulière de $\langle xy, xz \rangle$. De manière général, les ensembles réguliers de la k^e colonne représentent la décomposition régulière stricte de l'idéal engendré par S_k.

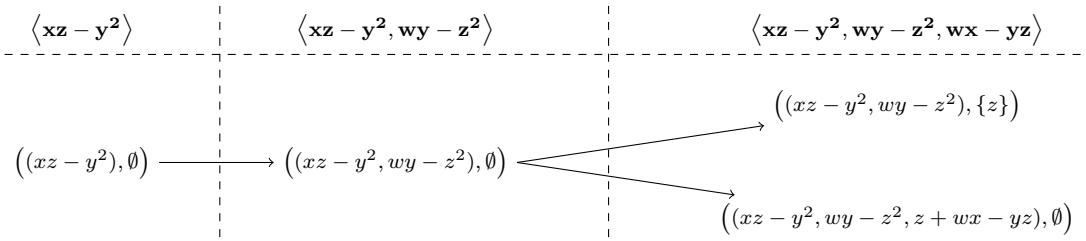
D'un point de vue géométrique, les zéros algébriques des deux ensembles réguliers de la dernière colonnes sont respectivement :

- *la droite support de l'axe y*
- *les deux droites supports des axes x et z*

□

La courbe gauche est un exemple classique de courbe projective qui n'est pas une intersection complète. Cette courbe est définie comme les zéros des polynômes $xz-y^2, wy-z^2, wx-yz$.

Exemple 6.
Soit S la suite de polynômes $(xz-y^2, wy-z^2, wx-yz)$ dans $\mathbb{Q}[x,y,z,w]$. Comme pour l'exemple précédent, on obtient une décomposition régulière stricte de l'idéal engendré par S en calculant $\textsc{Drs}\,(((xz-y^2),\emptyset),(wy-z^2, wx-yz))$.



On peut lire sur la dernière colonne la décomposition de la courbe gauche en deux ensembles réguliers.

Géométriquement, les zéros algébriques de $((xz-y^2, wy-z^2),\{z\})$ forment exactement la courbe gauche. Les zéros algébriques du deuxième ensemble régulier $((xz-y^2, wy-z^2, z+wx-yz),\emptyset)$ sont inclus dans ceux du premier.
□

On peut voir avec l'exemple précédent que la décomposition régulière stricte d'un idéal peut être constituée d'ensembles réguliers dont les zéros algébriques sont inclus dans les autres. C'est pour éliminer ces composantes que l'on s'intéresse à la notion de décomposition régulière minimale.

7.3.2 Décomposition régulière minimale

Dans cette section, on va voir que l'on peut modifier l'algorithme 2 pour obtenir une décomposition régulière minimale (Définition 29).

On considère d'abord le cas plus simple où l'idéal I que l'on veut décomposer est 0-dimensionnel.

Cas 0-dimensionnel

Dans le cas d'un idéal I de dimension zéro, on va montrer qu'une décomposition régulière stricte est équivalente à une décomposition régulière minimale.

Lemme 22. *Soit (S,F) un ensemble régulier de $K[x_1,\ldots,x_n]$, de hauteur n. Alors :*

$$\mathcal{Z}(S,F) = \mathcal{C}(S,F)$$

□

preuve :Par hypothèse, $\mathcal{Z}(S,F)$ est une variété de dimension 0 et $\mathcal{C}(S,F) \subset \mathcal{Z}(S,F)$. Supposons par l'absurde que l'inclusion est stricte. Alors il existe un point p dans $\mathcal{Z}(S,F) \setminus \mathcal{C}(S,F)$. Comme $\mathcal{Z}(S,F)$ est zéro dimensionnel, le point p est isolé et en particulier, $p \notin \overline{\mathcal{C}(S,F)}$. Or $\overline{\mathcal{C}(S,F)} = \mathcal{Z}(S,F)$, donc $p \notin \mathcal{Z}(S,F)$ ce qui est une contradiction.
□

Ce lemme nous permet de prouver l'équivalence des décomposition régulières strictes et minimales.

Théorème 6. *Soit I un idéal de dimension zéro.*

1. *Si D est une décomposition régulière stricte de I, alors elle est aussi minimale*
2. *Si D est une décomposition régulière minimale de I, elle est aussi stricte.*

□

preuve :

1. Soit D une décomposition régulière stricte de I. Soient (S_1,F_1) et (S_2,F_2) deux ensembles réguliers distincts quelconque de D. Par définition, on sait que $\mathcal{C}(S_1,F_1) \cap \mathcal{C}(S_2,F_2) = \emptyset$. De plus, on peut conclure d'après le lemme 22 que $\mathcal{Z}(S_1,F_1) \cap \mathcal{Z}(S_2,F_2) = \emptyset$. En particulier cela implique que si P est un idéal premier de minass$(\mathcal{I}(S_1,F_1))$, alors $P \not\supset \mathcal{I}(S_2,F_2)$, car sinon on aurait $\mathcal{V}(P) \subset \mathcal{Z}(S_1,F_1) \cap \mathcal{Z}(S_2,F_2)$. Cela prouve donc que D est aussi une décomposition minimale.
2. Soit D une décomposition régulière minimale de I. De la même manière, soient (S_1,F_1) et (S_2,F_2) deux ensembles réguliers distincts quelconque de D. Par définition, si $P \in$ minass$(\mathcal{I}(S_1,F_1))$ alors $P \not\supset \mathcal{I}(S_2,F_2)$. Et comme les premiers associés à $\mathcal{I}(S_1,F_1)$ sont de dimension 0, ils sont maximaux et on a donc : $\mathcal{I}(S_1,F_1) + \mathcal{I}(S_2,F_2) = K[x_1,\ldots,x_n]$. Cela équivaut à dire que $\mathcal{Z}(S_1,F_1) \cap \mathcal{Z}(S_2,F_2) = \emptyset$. Puis par le lemme 22, on a $\mathcal{C}(S_1,F_1) \cap \mathcal{C}(S_2,F_2) = \emptyset$, ce qui nous permet de conclure que D est aussi une décomposition stricte.

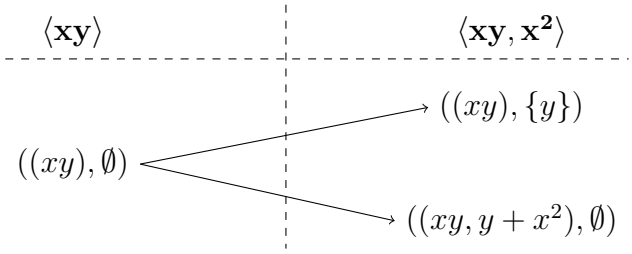
□

Ainsi, dans le cas où l'idéal I considéré est de dimension 0, on peut calculer une décomposition régulière minimale de I en utilisant directement l'algorithme 2.

Cas général

Dans le cas général, l'algorithme 2 ne renvoie pas de décomposition régulière minimale, comme le montre l'exemple suivant.

Exemple 7. *Soit I l'idéal engendré par (xy, x^2) dans $\mathbb{Q}[x,y]$. En utilisant l'algorithme 2 pour calculer une décomposition régulière stricte de I, on obtient l'arbre de calcul suivant :*



Dans cet exemple, la DRS de I est constituée des deux ensembles réguliers $((xy), \{y\})$ et $((xy, y + x^2), \emptyset)$. On peut facilement vérifier que :

– $\mathcal{C}((xy), \{y\})$ *est la droite support de l'axe y privée de l'origine*

– $\mathcal{C}((xy, y + x^2), \emptyset)$ *est le point origine du repère.*

On voit dans cet exemple où I n'est pas zéro dimensionnel, on voit que les zéros algébriques du second ensemble régulier sont inclus dans les zéros algébriques du premier. Plus formellement, on peut remarquer $P = \langle x, y\rangle$ est un premier isolé associé à $\mathcal{I}((xy, y + x^2), \emptyset)$. Et $P \supset \langle x\rangle = \mathcal{I}((xy), \{y\})$. Ainsi cette décomposition n'est pas une décomposition régulière minimale de I.

□

Cependant, étant donné une DRS d'un idéal I, on peut montrer que si on ne considère que les ensembles réguliers de hauteur minimale, alors ils forment une décomposition régulière minimale de la partie équidimensionnelle maximale de I.

Définition 31. *(Partie équidimensionnelle maximale)*
Soit I un idéal et d sa dimension. On définit sa partie équidimensionnelle maximale et note EQUI(I) *l'idéal :*

$$\text{EQUI}(I) := \bigcap_{\substack{P \in \text{minass}(I) \\ \dim(P) = d}} P$$

□

Le lemme suivant est fondamental pour la construction d'un algorithme de décomposition régulière minimale.

Lemme 23. *Soit I un idéal de codimension c et D un décomposition régulière stricte de I. Si (S_1, F_1) et (S_2, F_2) sont deux ensembles réguliers distincts de D, de hauteur c, alors on a :*

$$P \in \text{minass}(\mathcal{I}(S_1, F_1)) \Rightarrow P \not\supset \mathcal{I}(S_2, F_2)$$

Ainsi, l'ensemble $D' := \{(S, F) \in D \mid$ la hauteur de (S, F) est $c\}$ est une décomposition régulière minimale de EQUI(I).

□

*preuve :*Soit d la hauteur de (S_1, F_1) et (S_2, F_2). Soit P un idéal premier isolé associé $\mathcal{I}(S_1, F_1)$. Supposons par l'absurde que $\mathcal{I}(S_2, F_2) \subset P$. On va montrer que la hauteur de P est alors strictement supérieur à d, ce qui contredit, d'après le lemme 8, le fait que P appartient à minass$(\mathcal{I}(S_1, F_1))$.

On note $f_1 = \prod_{f \in F_1} f$ et $f_2 = \prod_{f \in F_2} f$ en prenant comme convention qu'un produit sur un ensemble vide vaut 1. Par définition, $\mathcal{C}(S_1, F_1) \cap \mathcal{C}(S_2, F_2) = \emptyset$. En particulier, cela signifie que $\mathcal{Z}(S_1, F_1) \cap \mathcal{Z}(S_2, F_2) \subset \mathcal{V}(\langle f_1 f_2\rangle)$. Ou de façon plus algébrique : $f_1 f_2 \subset \sqrt{\mathcal{I}(S_1, F_1) + \mathcal{I}(S_2, F_2)}$. On peut ainsi déduire d'après l'hypothèse par l'absurde que :

$$\sqrt{\mathcal{I}(S_1, F_1) + \mathcal{I}(S_2, F_2) + \langle f_1 f_2\rangle} = \sqrt{\mathcal{I}(S_1, F_1) + \mathcal{I}(S_2, F_2)} \subset P$$

Par ailleurs, soit $J = (\mathcal{I}(S_1, F_1) + \langle f_1 \rangle) \cap (\mathcal{I}(S_2, F_2) + \langle f_2 \rangle)$. Par construction, f_1 (resp. f_2) n'est pas un diviseur de zéro dans $A/\mathcal{I}(S_1, F_1)A$ (resp. $A/\mathcal{I}(S_2, F_2)A$). Ainsi la codimension de l'idéal J est strictement supérieure à d. Or on peut remarquer que :

$$J \subset \sqrt{\mathcal{I}(S_1, F_1) + \mathcal{I}(S_2, F_2) + \langle f_1 f_2 \rangle}$$

En effet, si $e \in J$, alors, il existe $i_1, q_1, i_2, q_2 \in A$ tels que $e = i_1 + q_1 f_1$ et $e = i_2 + q_2 f_2$. En particulier :

$$e^2 = i_1 i_2 + i_1 q_2 f_2 + i_2 q_1 f_1 + q_1 q_2 f_1 f_2 \in \sqrt{\mathcal{I}(S_1, F_1) + \mathcal{I}(S_2, F_2) + \langle f_1 f_2 \rangle}$$

Ainsi, $J \subset P$, ce qui implique que la hauteur de P est supérieure ou égale à la codimension de J, donc supérieure stricte à d, d'où la contradiction.
□

Ce lemme nous permet directement de construire un algorithme pour calculer une décomposition régulière minimale de EQUI(I), en modifiant légèrement l'algorithme 2.

Algorithme 3 DRM-MAX

ENTRÉE : - un ensemble régulier (S, F)
- une liste L de polynômes $g_c, \ldots, g_m$
- d un entier

SORTIE : une DRM de EQUI $\left((S + \langle g_c, \ldots, g_m \rangle) : \prod_{f \in F} f^\infty\right)$

- SI la liste L est vide, ALORS
  - RENVOYER $\{(S, F)\}$
- FIN SI
- $D := \emptyset$
- $J := \mathcal{I}(S, F)$
- SI $\dim(J + \langle g_c \rangle) \neq \dim(J)$ ALORS
  - $S' := S, g_c$
- SINON
  - $h :=$ SCINDAGE$((S, F), g_c)$
  - $S' := S, g_c + h$
  - $F' := F \cup \{h\}$
  - $D := \{(S, F')\}$
- FIN SI
- SI $1 \notin \langle S' \rangle : \prod_{f \in F} f^\infty$ ET $\mathbf{\dim(J) > d}$ ALORS
  - $D := D \cup \{(S', F)\}$
- FIN SI
- RENVOYER $\bigcup_{e \in D}$ DRM-MAX$(e, (g_{c+1}, \ldots, g_m), d)$

Cet algorithme permet ainsi de calculer une décomposition régulière minimale de EQUI(I).

Théorème 7. *Soit I un idéal engendré par les polynômes $f_1, \ldots, f_k$, d sa dimension et F un ensemble de polynôme. Alors, la fonction :*

$$\text{DRM-MAX}(((f_1), F), (f_2, \ldots, f_k), d)$$

renvoie un décomposition régulière minimale de EQUI$(I : \prod_{f\in F} f^\infty)$. □

Remarque 15. *Si on utilise un entier d quelconque, alors la fonction* DRM-MAX$(((f_1),\emptyset),(f_2,\ldots,f_k),d)$ *renvoie exactement les ensembles réguliers de dimension supérieure ou égale à d d'une décomposition régulière stricte de I. En particulier, si $d > \dim(I)$, la fonction renvoie l'ensemble vide.*

*preuve :*Il suffit de remarquer que cette fonction renvoie exactement les ensembles réguliers de hauteurs minimales d'une décomposition stricte de $I : \prod_{f\in F} f^\infty$, ce qui nous permet de conclure en utilisant le lemme 23.
□

En utilisant l'algorithme 3, nous pouvons maintenant présenter un algorithme complet de calcul de décomposition régulière minimale d'un idéal I. L'idée de cet algorithme est de calculer un décomposition régulière minimale des différentes partie équidimensionnelles de I successivement.

Algorithme 4 DRM

ENTRÉE : Un idéal I engendré par les polynômes $f_1,\ldots,f_k$
SORTIE : Un décomposition régulière minimale de I
- $D := \emptyset$
- $J := \langle 1\rangle$
- $g := 1$
- $fini$:=FAUX
- TANT QUE NON $fini$
  - $d := \dim(I : g^\infty)$
  - D_{equi} := DRM-MAX$(((f_1),\{g\}),(f_2,\ldots,f_k),d)$
  - $D := D \cup D_{equi}$
  - $J := J \cap \bigcap_{(S,F)\in D_{equi}} \mathcal{I}(S,F)$
  - POUR $g \in$ Générateurs de J
    SI $g \notin \sqrt{I}$ ALORS
    SORTIR
    FIN SI
  - FIN POUR
  - SI $J \subset \sqrt{I}$ ALORS
    $fini$:=VRAI
  - FIN SI
- FIN TANT
- RENVOYER D

Théorème 8. *Soit I un idéal. La fonction :*

$$\text{DRM}(I)$$

renvoie une décomposition régulière minimale de I. □

Remarque 16. *Le nombre d'itérations dans la boucle* TANT QUE *est majoré par le nombre de premiers associés à I.*

Pour prouver le théorème 8, on aura besoin des deux lemmes suivants.

Lemme 24. *Soient I un idéal, f un polynôme. Alors,*

$$\text{minass}(I : f^\infty) = \{P \in \text{minass}(I) \mid f \notin P\}$$

□

*preuve :*L'implication de droite à gauche se voit en remarquant d'abord que si P est un idéal premier isolé de I ne contenant pas f, alors P contient $I : f^\infty$. En effet, pour tout $e \in I : f^\infty$, il existe k tel que $f^k e \in I \subset P$. Comme P est premier et ne contient pas f, alors $e \in P$. Maintenant, pour montrer que P est un premier minimal, soit Q un idéal premier tel que $P \supset Q \supset I : f^\infty$. Alors $P \supset Q \supset I$ et par minimalité de P parmi les idéaux premiers contenant I, on a donc $Q = P$. Et ainsi, on a bien : $P \in \text{minass}(I : f^\infty)$.

Pour l'autre implication, soit P un premier isolé de $I : f^\infty$. D'abord on montre que P ne contient pas f. En effet, supposons par l'absurde que $f \in P$. Soit $e \in \bigcap_{\substack{Q \in \text{minass}(I:f^\infty) \\ Q \neq P}} Q$ (si $\text{minass}(I : f^\infty)$ est réduit à $\{P\}$, on choisit $e = 1$). Dans ce cas, on a : $ef \in \sqrt{I : f^\infty}$ et donc $e \in \sqrt{I : f^\infty}$. Ce qui implique : $\bigcap_{\substack{Q \in \text{minass}(I:f^\infty) \\ Q \neq P}} Q = \sqrt{I : f^\infty}$, ce qui contredit l'unicité de la décomposition en premiers isolés.

Ensuite on montre que si P est un premier isolé de $I : f^\infty$, alors P est aussi dans $\text{minass}(I)$. Par hypothèse, P contient $I : f^\infty \supset I$. Puis supposons que Q est un idéal premier tel que $P \supset Q \supset I$. Il nous suffit de montrer que Q contient $I : f^\infty$ pour conclure par minimalité de P parmi les idéaux premiers contenant $I : f^\infty$ que $Q = P$. Et en effet, si e est un élément de $I : f^\infty$, alors, il existe k tel que $f^k e \in I \subset Q$. Or $f \notin P$ donc $f \notin Q$. D'où $e \in Q$ par définition d'un idéal premier et donc $Q \supset I : f^\infty$.
□

On montre aussi le lemme suivant.

Lemme 25. *Soient I un idéal et D une décomposition régulière minimale de I. Alors, les ensembles d'idéaux premiers* $\text{minass}(\mathcal{I}(S, F))$ *pour $(S, F) \in D$ forment une partition de* $\text{minass}(I)$.
□

*preuve :*Soit D un décomposition première minimale de I. Alors, par définition d'une décomposition régulière minimale, on sait que si (S_1, F_1) et (S_2, F_2) sont deux ensembles réguliers de D, on a :

$$P \in \text{minass}(\mathcal{I}(S_1, F_1)) \Rightarrow P \not\supset \mathcal{I}(S_2, F_2)$$

En particulier, par définition d'un idéal premier isolé, si $P \not\supset \mathcal{I}(S_2, F_2)$, alors $P \notin \text{minass}\mathcal{I}(S_2, F_2)$. Ainsi, les ensembles $\text{minass}(\mathcal{I}(S, F))$ pour $(S, F) \in D$ sont disjoints.

Par ailleurs, par définition d'une décomposition régulière on sait aussi que :

$$\sqrt{I} = \bigcap_{(S,F) \in D} \sqrt{\mathcal{I}(S, F)}$$

Cela implique en particulier que $\sqrt{I} = \bigcap_{(S,F)\in D} \bigcap_{P\in \text{minass}(\mathcal{I}(S,F))} P$.

Les idéaux premiers $P \in \text{minass}(\mathcal{I}(S,F))$ tels que $(S,F) \in D$ forment donc une décomposition non redondante de $\sqrt{I}$. Ainsi, par unicité de la décomposition d'un idéal en idéaux premiers non redondants, on a bien :

$$\text{minass}(I) = \{P \in \text{minass}(\mathcal{I}(S,F)) \mid (S,F) \in D\}$$

□

On a maintenant tous les outils pour démontrer le théorème de correction de l'algorithme 4.

preuve du théorème 8:
Soit I l'idéal considéré en entrée de l'algorithme 4. On va d'abord montrer que au début de la boucle TANT QUE, l'ensemble D est toujours une décomposition régulière minimale de J.

D'abord, par construction, on voit facilement que D est constitué d'ensembles réguliers tels que :

$$J = \bigcap_{(S,F)\in D} \mathcal{I}(S,F)$$

ce qui prouve que D est une décomposition régulière de J.

Pour prouver la minimalité de D, on montre par récurrence sur le nombre d'itérations de la boucle TANT QUE que :

$$\begin{cases} (1) & \bigcup_{(S,F)\in D} \text{minass}(\mathcal{I}(S,F)) \subset \text{minass}(I) \\ (2) & D \text{ est une DRM de } J \end{cases}$$

D'abord, pour le cas 0, J vaut $\langle 1\rangle$ et $D = \emptyset$ est donc bien une DRM de J et évidemment $\emptyset \subset \text{minass}(I)$.

Puis par récurrence, en utilisant les notation de l'algorithme 4, supposons que D est une DRM de J et $\bigcup_{(S,F)\in D} \text{minass}(\mathcal{I}(S,F)) \subset \text{minass}(I)$. On veut alors montrer que $D \cup D_{equi}$ est une DRM de $J \cap \bigcap_{(S,F)\in D_{equi}} \mathcal{I}(S,F)$ et $\bigcup_{(S,F)\in D_{equi}} \text{minass}(\mathcal{I}(S,F)) \subset \text{minass}(I)$.

D'abord, pour l'assertion (1), si $(S,F) \in D_{equi}$ alors $\text{minass}((S,F)) \subset \text{minass}(\text{EQUI}(I : g^\infty)) \subset \text{minass}(I : g^\infty) \subset \text{minass}(I)$.

Puis, pour l'assertion (2). Soient (S_1,F_1) et (S_2,F_2) deux ensembles réguliers de D. On distingue alors deux cas.

Si (S_1,F_1) et (S_2,F_2) appartiennent tous les deux à D_{equi}, alors le théorème 7 nous permet directement de conclure que (S_1,F_1) et (S_2,F_2) satisfont les critères nécessaire pour une décomposition régulière minimale.

Sinon, on suppose sans restriction de généralité que $(S_1,F_1) \in D$ et $(S_2,F_2) \in D_{equi}$. On doit alors montrer :

$$\begin{cases} P \in \text{minass}(\mathcal{I}(S_1,F_1)) \Rightarrow P \not\supset \mathcal{I}(S_2,F_2) \\ P \in \text{minass}(\mathcal{I}(S_2,F_2)) \Rightarrow P \not\supset \mathcal{I}(S_1,F_1) \end{cases}$$

On remarque d'abord que par construction, $g \in J \subset \mathcal{I}(S_1, F_1)$ et $\mathcal{I}(S_2, F_2) \in I : g^\infty$. Ainsi on peut en déduire, en utilisant l'hypothèse de récurrence et le lemme 24 que :

$$\begin{cases} \text{minass}(\mathcal{I}(S_1, F_1)) \subset \{P \in \text{minass}(I) \mid g \in P\} \\ \text{minass}(\mathcal{I}(S_2, F_2)) \subset \{P \in \text{minass}(I) \mid g \notin P\} \end{cases}$$

Ainsi, soit P un idéal premier isolé de $\mathcal{I}(S_1, F_1)$. Si P contenait $\mathcal{I}(S_2, F_2)$, il contiendrait un premier isolé de $\mathcal{I}(S_2, F_2)$, donc un premier isolé de I. Or comme P est lui-même un premier isolé de I, on aurait $P = Q$ ce qui contredit le fait que $g \in P$ et $g \notin Q$. Donc $P \not\supset \mathcal{I}(S_2, F_2)$. Réciproquement, soit Q un idéal premier de $\mathcal{I}(S_2, F_2)$. Les mêmes arguments nous permettent de conclure que $Q \not\supset \mathcal{I}(S_1, F_1)$.

Maintenant, nous devons montrer que l'algorithme 4 termine et qu'il renvoie bien une DRM de I. D'abord, d'après le lemme 25, les premiers isolés de J sont exactement l'union des premiers isolés des $\mathcal{I}(S, F)$ pour $(S, F) \in D$. En particulier, avec l'assertion (1), cela implique $\text{minass}(J) \subset \text{minass}(I)$. On peut alors remarquer que le nombre de premiers isolés de J augmente strictement à chaque itération de la boucle, et on sort de la boucle dès que $\text{minass}(J) = \text{minass}(I)$. Ainsi, à la fin de l'algorithme, D est une décomposition régulière minimale de J et $\sqrt{(J)} = \sqrt{(I)}$. Cela nous permet donc de conclure que D est bien une décomposition régulière minimale de I.
□

7.3.3 Décomposition pour les systèmes paramétrés

Dans le cadre d'un système paramétré génériquement 0-dimensionnel S, on s'intéresse à séparer les composantes de dimension maximale des composantes de petites dimensions afin de calculer la composante $V_{sd}(S)$ de la variété discriminante minimale de S. On ne veut cependant pas décomposer inutilement l'ensemble des composantes de petites dimensions de S.

L'idée pour séparer les composantes sans les décomposer consiste à adapter l'algorithme 4 de décomposition régulière minimale en supprimant le calcule systématique de la fonction Drm-Max.

L'algorithme qui en découle est donné par la fonction Drm-Sep.

On peut facilement vérifier que l'algorithme 5 calcule d'une part les composantes de dimension maximale exactement comme l'algorithme 4. D'autre part, il calcule ensuite les composantes de petites dimension, comme pour l'algorithme 4, sans les décomposer spécifiquement.

Théorème 9. *Soit I un idéal. La fonction :*

$$\text{Drm-Sep}(I)$$

renvoie une décomposition régulière minimale de $\text{equi}(I)$ *et un idéal J tel que :*

$$\mathcal{V}(J) = \overline{\mathcal{V}(I) \setminus \mathcal{V}(\text{equi}(I))}$$

□

Algorithme 5 DRM-SEP

ENTRÉE : Un idéal I engendré par les polynômes $f_1, \ldots, f_k$
SORTIE : Une composante régulière représentant les composantes de dimension maximale de I, et un idéal dont les zéros sont les autres composantes de I.

- $D := \emptyset$
- $g := 1$
- $fini$:=FAUX
- $d := \dim(I)$
- $D_{equi} :=$ DRM-MAX$(((f_1), \{g\}), (f_2, \ldots, f_k), d)$
- $J_{sd} := \langle 1 \rangle$
- $J := \bigcap_{(S,F) \in D_{equi}} \mathcal{I}(S, F)$
- TANT QUE NON $fini$
  - POUR $g \in$ Générateurs de J
    SI $g \notin \sqrt{I}$ ALORS
    - $J_{sd} := J_{sd} \cap (I : g^\infty)$
    - $J := J \cap (I : g^\infty)$

    SORTIR
    FIN SI
  - FIN POUR
  - SI $J \subset \sqrt{I}$ ALORS
    $fini$:=VRAI
  - FIN SI

– FIN TANT
– RENVOYER D_{equi}, J_{sd}

On peut voir en table 7.3 que cette fonction peut être dans certains cas significativement plus rapide en pratique que l'implantation de la fonction DRM complète.

Cette fonction nous fournit en outre un outil permettant de calculer la composante $V_{sd}(S)$ d'un système S quelconque dépendant de s paramètres.

En effet, si l'on a calculé la composante $V_{inf}(S)$, on peut alors éliminer les composantes de dimensions strictement supérieures à s. Soit I l'idéal obtenu par saturation des équations du système S par les polynômes définissant $V_{inf}(S)$ et par les polynômes des inéquations de S. Ainsi, I est de dimension s et en effectuant la fonction DRM-SEP(I), on obtient exactement l'idéal J_{sd} des composantes de dimensions strictement inférieures à s. La projection de $\mathcal{V}(J_{sd})$ sur l'espace des paramètres est exactement $V_{sd}(S)$.

Dans ce cadre, la fonction DRM-SEP(I) renvoie aussi la décomposition régulière $D_{equi} = \{(S_1, F_1), \ldots, (S_k, F_k)\}$ des composantes de S, de dimension s, dont la projection sur l'espace des paramètres est dense. On note alors V_c l'union des points critiques des variétés $\mathcal{Z}(S_1, F_1), \ldots, \mathcal{Z}(S_k, F_k)$, V_s l'union des singularités de $\mathcal{Z}(S_1, F_1), \ldots, \mathcal{Z}(S_k, F_k)$ et V_i l'union des intersections deux à deux des variétés $\mathcal{Z}(S_1, F_1), \ldots, \mathcal{Z}(S_k, F_k)$. La composante $V_{crit}(S)$ est alors exactement la projection de l'union des variétés $V_c \cup V_s \cup V_i$.

7.3.4 Implantation

Afin de valider expérimentalement notre approche, nous avons implanté l'algorithme DRM dans les logiciels MAPLE et SINGULAR. Nous avons ainsi pu répertorié et comparer les temps de calcul de notre implantation sur la suite d'exemples présentée dans l'article [31].

Les exemples considérés ici sont facilement résolubles par les algorithmes de l'état de l'art. Ils permettent de vérifier que notre algorithme se comporte de manière satisfaisante dans les cas simples, tout en renvoyant une sortie adaptée au calcul de la variété discriminante.

On peut remarquer en table 7.1 pour l'implantation en SINGULAR que les temps de calcul de notre algorithme de décomposition régulière minimale est plus rapide sur certains exemples et plus lent sur d'autres que les algorithmes de décomposition de SINGULAR. Par ailleurs, on peut remarquer que les temps de calcul de cette première implantation sont toujours inférieurs à 5 secondes. Dans la table 7.2, on applique ces algorithmes sur les trois principaux exemples traités dans cette thèse. En particulier, on remarque que lorsque le système considéré est bien posé, le temps de décomposition régulière minimale est alors négligeable. Ainsi la décomposition systématique par une DRM des systèmes paramétrés ne semble pas pénaliser le calcul général de la variété discriminante lorsque le système considéré est bien posé. Dans le cas du système surdéterminé présenté au chapitre 9, équation 9.7, le calcul de la DRM permet dans un temps raisonnable d'obtenir une représentation compact du système considéré. En particulier, on peut ensuite calculer facilement la composante critique de la variété discriminante correspondant à ce système.

La fonction de décomposition partielle DRM-SEP a été implantée en MAPLE. En table 7.3, on a comparé les temps de calcul des implantations MAPLE de la décomposition régulière minimale complète (fonction DRM) avec celui de la décomposition partielle (fonction DRM-SEP). On observe ainsi en pratique que l'on peut gagner en temps un facteur non négligeable en évitant la décomposition des composantes de petites dimension avec la fonction DRM-

SEP. Pour les systèmes $2, 3, 7, 23, 24$ par exemple, on observe un gain de facteur 2 (systèmes $2, 3, 7, 23, 24$), et on gagne même un facteur 10 en temps pour le système 16.

	minAssGTZ	minAssChar	equidim	equidim-EHV	DRM
DGP1	13	7	1	1	25
DGP2	20	16	41	16	42
DGP3	3	1	4	5	3
DGP4	9	3	4	2	7
DGP5	37	*	238	*	88
DGP6	7	19	473	*	213
DGP7	12	32	16	16	24
DGP8	3	397	1	1	6
DGP9	32	1916	1	1	6
DGP10	8	*	0	1	7
DGP11	*	*	8	6	64
DGP12	43	*	0	0	3
DGP13	19	*	0	1	6
DGP14	4	5	2	1	0
DGP15	22	281	1	0	47
DGP16	330	3721	153	143	410
DGP17	99	*	0	0	5
DGP18	6	213	1	1	11
DGP19	7	*	4	3	14
DGP20	8	304	5	195	26
DGP21	1	1	10	13	5
DGP22	13	13	59	*	42
DGP23	47	40	30	*	44
DGP24	4	8	9	20	3
DGP25	55	142	921	*	242
DGP26	28	*	0	1	16
DGP27	6	21	0	0	2
DGP28	13	11	1	0	1
DGP29	2	0	2499	*	4
DGP30	91	46	8	*	30
DGP31	5	2	0	0	1
DGP32	5	5	68	*	19
DGP33	4	3	2	1	11
DGP34	*	*	3	3	62

* signifie que les calculs ont duré plus de 60 secondes
(sur un processeur 32 bits, 2.8GHz Intel pentium)

TAB. 7.1 – Temps de décomposition équidimensionnelle des exemples de [31], en SINGULAR (en centièmes de seconde)

	minAssGTZ	minAssChar	equidim	equidim-EHV	DRM
Polynômes creux (Eq. 5.1, k=3)	119	1	0	0	1
Calibration (Eq. 4.1)	0	0	0	0	0
Robots parallèles (Eq. 9.7)	*	*	*	*	1362

* signifie que les calculs ont duré plus de 60 secondes
(sur un processeur 32 bits, 2.8GHz Intel pentium)

TAB. 7.2 – Temps de décomposition équidimensionnelle des applications de cette thèse, en SINGULAR (en centièmes de seconde)

	ratio : $\frac{\text{temps DRM}}{\text{temps DRM-SEP}}$		ratio : $\frac{\text{temps DRM}}{\text{temps DRM-SEP}}$
DGP1	1.41	DGP18	0.93
DGP2	2.09	DGP19	0.98
DGP3	2.50	DGP20	1.05
DGP4	1.89	DGP21	1.02
DGP5	1.63	DGP22	1.49
DGP6	1.02	DGP23	2.34
DGP7	2.15	DGP24	2.68
DGP8	1.05	DGP25	1.84
DGP9	1.05	DGP26	1.01
DGP10	1.06	DGP27	1.04
DGP11	1.07	DGP28	1.06
DGP12	1.04	DGP29	1.03
DGP13	0.99	DGP30	0.99
DGP14	0.94	DGP31	0.95
DGP15	1.61	DGP32	1.91
DGP16	10.29	DGP33	1.09
DGP17	1.05	DGP34	1.00

TAB. 7.3 – Décomposition équidimensionnelle complète et partielle MAPLE

`minAssGTZ`	calcule les idéaux premiers associés à un idéal en utilisant l'algorithme de [50]
`minAssChar`	calcule les idéaux premiers associés à un idéal en utilisant les ensembles caractéristiques de Ritt-Wu ([140])
`equidim`	calcule une décomposition équidimensionnelle d'un idéal en utilisant l'algorithme de [50]
`equidim-EHV`	calcule une décomposition équidimensionnelle d'un idéal en utilisant l'algorithme de [36]

TAB. 7.4 – Fonctions de décompositions du logiciel SINGULAR

Chapitre 8

Complexité des suites pseudo-régulières

Cette section est destinée à prouver que l'algorithme de calcul d'une *décomposition régulière minimale* d'un idéal se place dans une classe de complexité raisonnable vis-à-vis des méthodes existantes.

On se placera pour cette analyse dans le cas où l'idéal d'entrée est engendré par une suite pseudo-régulière, notion définie en section 8.1. La complexité de l'algorithme 4 est plus facile à étudier dans ce cadre particulier dans lequel on peut toujours se ramener (voir lemme 26). Cependant, si nous ne proposons pas de bornes de complexité satisfaisante pour le cas général, cela ne signifie pas pour autant que l'algorithme se comporte moins bien lorsque la suite donnée en entrée n'est pas pseudo-régulière. Notamment, notre étude de complexité se place dans le cas où les polynômes sont représentés sous leur forme dense et ne prend donc pas en compte le caractère creux des polynômes.

L'analyse de complexité en temps et en espace sera exprimée en fonction de la complexité des opérations de bases suivantes :

- le calcul de la *dimension* d'un idéal I
- le calcul de la *saturation* d'un idéal I par un polynôme f.

Notamment, on montre que si $f_1, \ldots, f_k$ est une suite pseudo-régulière engendrant un idéal I, de degrés respectifs $d_1, \ldots, d_k$ alors, on peut calculer une décomposition régulière minimale de I :

- telle que $\forall (S, F) \in D$, $\max(\deg(f) \mid f \in S \cup F) \leq d_1 \cdots d_k$
- en $\mathcal{O}\left(\binom{d_1 \cdots d_k + n}{n}^2\right)$ étapes sur une machine de Türing.

8.1 Suite pseudo-régulière

Les suites pseudo-régulières sont introduites sous le nom de *rather regular sequences* dans [13].

Elles possèdent de bonnes propriétés pour l'étude de complexité qui leur ont valu d'être utilisées pour l'étude d'une variante du Nullstellensatz effectif ([13]) ou encore pour améliorer la borne supérieure du temps de calcul de la décomposition équidimensionnelle ([90]).

Définition 32. *(Suite pseudo-régulière)*
Soit $f_1, \ldots, f_k$ une suite de polynômes engendrant l'idéal I. On dit que la suite est pseudo-régulière si et seulement si :

i) $P \in \text{minass}(\langle f_1, \ldots, f_i \rangle) \setminus \text{minass}(I) \Rightarrow f_{i+1} \notin P$

ii) $\exists P \in \text{minass}(\langle f_1, \ldots, f_i \rangle) \mid f_{i+1} \notin P$

□

Remarque 17.

- *Une suite régulière est aussi une suite pseudo-régulière.*
- *Si la codimension de I est c, alors, les c premiers polynômes de la suite pseudo-régulière forment une suite régulière.*

Exemple 8. *La suite $(xy, x(x-1))$ de polynômes de $\mathbb{Q}[x, y]$ est pseudo-régulière. En effet, soit I l'idéal $\langle xy, x(x-1) \rangle$. Ses premiers isolés sont :*

$$\text{minass}(I) = \{\langle x \rangle, \langle x - 1, y \rangle\}$$

Les premiers isolés de $\langle xy \rangle$ sont $\langle x \rangle$ et $\langle y \rangle$. On remarque que $\langle y \rangle \in \text{minass}(\langle xy \rangle) \setminus \text{minass}(I)$, et $x(x-1) \notin \langle y \rangle$. Ainsi les conditions i) et ii) de la définition des suites pseudo-régulières sont satisfaites.
□

Exemple 9. *(Retour sur la courbe gauche)*
Soient $s_1 = xz - y^2$, $s_2 = wy - z^2$, $s_3 = wx - yz$ les trois polynômes de $\mathbb{Q}[x, y, z, w]$ introduits dans l'exemple 6 et dont les zéros forment la courbe gauche. Nous allons montrer que la suite (s_1, s_2, s_3) est pseudo-régulière.

D'abord, on peut remarquer que s_1 et s_2 n'ont pas de facteur en commun, ce qui satisfait donc les conditions i) et ii) de la définition d'une suite pseudo-régulière pour le cas $i = 1$.

Ensuite, pour $i = 2$, si $P \in \text{minass}(\langle s_1, s_2 \rangle)$, alors on peut vérifier facilement que $s_3 \in P \Leftrightarrow P \in \text{minass}(\langle s_1, s_2, s_3 \rangle)$. Ceci nous montre ainsi que la condition i) est satisfaite. Pour la condition ii), il suffit de remarquer que l'idéal $\langle y, z \rangle$ est un premier isolé de $\langle s_1, s_2 \rangle$ qui ne contient pas s_3
□

Exemple 10. *Soient $f_1 = xy$, $f_2 = x(x + y - 1)$, $f_3 = y(x + y - 1)$ trois polynômes de $\mathbb{Q}[x, y]$ et soit I l'idéal engendré par ces polynômes. On va voir que la suite (f_1, f_2, f_3) n'est pas pseudo-régulière.*

On peut d'abord observer que I est 0-dimensionnel et que ses premiers isolés sont exactement :

$$\text{minass}(I) = \{\langle x, y \rangle, \langle x, y - 1 \rangle, \langle x - 1, y \rangle\}$$

Par ailleurs, les premiers isolés de $\langle f_1, f_2 \rangle$ sont :

$$\text{minass}(\langle f_1 \rangle) = \{\langle x \rangle, \langle y \rangle\}$$

On peut alors voir que l'idéal premier $\langle x \rangle$ est bien dans $\text{minass}(\langle f_1 \rangle) \setminus \text{minass}(I)$ et contient f_2, ce qui contredit la condition i) de la définition d'une suite pseudo-régulière.
□

Le lemme suivant montre que étant donné un idéal I, il existe toujours une suites pseudo-régulières engendrant un idéal J tel que $\sqrt{I} = \sqrt{J}$.

Lemme 26. *[13, Lemma 0]*
Soit I un idéal engendré par $f_1, \ldots, f_m$ dans $K[x_1, \ldots, x_n]$ où K est un corps de caractéristique 0. Alors il existe une suite pseudo-régulière $h_1, \ldots, h_k$ telle que, quitte à changer les indices :

i) $\sqrt{I} = \sqrt{\langle h_1, \ldots, h_k \rangle}$

ii) $\forall 1 \leq i \leq k, \deg(h_i) = \deg(f_i)$

□

Remarque 18.

- *En pratique, une telle suite peut s'obtenir en combinant linéairement et aléatoirement les polynômes $f_1, \ldots, f_m$.*
- *Une telle opération n'a pas d'impact significative sur la complexité théorique du calcul. Ce n'est pas le cas en pratique, où le caractère creux de certains polynômes par exemple peut être perdu par cette opération.*

Exemple 11. *En reprenant les notations de l'exemple 10, la suite :*

$$f_1, f_2 + f_3, f_3$$

est une suite pseudo-régulière.

On remarque que f_1 et $f_2 + f_3$ n'ont pas de facteur en commun, ce qui nous permet de conclure en suivant la même preuve que pour l'exemple 9.

□

Pour l'étude de complexité qui suit, on supposera que la suite donnée en entrée est pseudo-régulière.

8.2 Opérations de bases

L'algorithme 4, s'appuie sur des opérations générales sur les idéaux, comme le calcul de la *dimension* d'un idéal, de sa *saturation* par un polynôme, ou encore de l'*intersection* de plusieurs idéaux.

On utilisera alors les notations suivantes.

Notations 16. *Soient $(f_1, \ldots, f_k)$ une suite pseudo-régulière de polynômes de $K[x_1, \ldots, x_n]$, de degrés $\mathbf{d} = (d_1, \ldots, d_k)$, engendrant l'idéal I. Soit g un polynôme de degré $d' \leq d_1 \cdots d_k$. On note alors :*

$\mathcal{T}_{\dim}(n, \mathbf{d}, d')$: une borne supérieure du temps de calcul de la dimension de $I : g^\infty$ sur une machine de Türing

$\mathcal{T}_\zeta(n, \mathbf{d}, d')$: une borne supérieure du temps de calcul de la fonction ζ

$\mathcal{N}_\zeta(n, \mathbf{d})$: une borne supérieure du nombre de polynômes renvoyés par ζ (ne dépend pas du degré de g)

$\mathcal{D}_\zeta(n, \mathbf{d})$ *: une borne supérieure des degrés des polynômes renvoyés par* ζ *(ne dépend pas du degré de* g*)*
$\mathcal{N}_p(\mathbf{d})$ *: une borne supérieure du nombre de premiers isolés de* I
$\mathcal{N}_p^{max}(\mathbf{d})$ *: une borne supérieure du nombre de premiers isolés de chacun des idéaux* $\langle f_1\rangle, \ldots, \langle f_1, \ldots, f_k\rangle$

□

Remarque 19. *En utilisant le lemme précédent et les résultats de la section 7.1, dans le cas où la représentation des polynômes est dense, on peut expliciter les bornes suivantes :*

- $\mathcal{T}_{\dim}(n, \mathbf{d}, d') = \mathcal{O}\left((n+1)^{2.312} 11^{n+1} \binom{\max(d_1,\ldots,d_k,d'+1)+n+1}{n+1}^{8.376}\right)$
- $\mathcal{T}_\zeta(n, \mathbf{d}, d') = \mathcal{O}\left((k+1)^{\omega+1} \binom{d_1\cdots d_k(d'+1)+n}{n}^{\omega+1}\right)$
- $\mathcal{N}_\zeta(n, \mathbf{d}) = n+1$
- $\mathcal{D}_\zeta(n, \mathbf{d}) = d_1 \cdots d_k$
- $\mathcal{N}_p(\mathbf{d}) = d_1 \cdots d_k$
- $\mathcal{N}_p^{max}(\mathbf{d}) = d_1 \cdots d_k$

On exprimera par la suite la complexité des différentes fonctions en fonction des complexités de ces fonctions de base.

8.2.1 Saturation, Dimension

On a vu en section 7.1 la complexité général du calcul de la *dimension* et de la *saturation*.

Dans l'algorithme 4, on a besoin de calculer la dimension d'un idéal I saturé par un polynôme g.

Le lemme suivant nous montre que l'on peut ramener le calcul de la dimension d'un idéal saturé par un polynôme au calcul direct de la dimension d'un idéal.

Lemme 27. *Soient* $I \subset A$ *un idéal engendré par* $f_1, \ldots, f_k$ *et* g *un polynôme de* A*. Alors, en notant* Z *une nouvelle variable libre, on a :*

$$\dim(I : g^\infty) = \dim(\langle f_1, \ldots, f_k, Zg - 1\rangle_{A[Z]}) - 1$$

□

Remarque 20. *Dans ce cas, en notant* d_i *le degré de* f_i *pour* i *entre* 1 *et* k*,* d' *le degré de* g *et* $\mathbf{d}$ *le vecteur* $(d_1, \ldots, d_k, d')$*, le coût en temps du calcul de la dimension de* $I : g^\infty$ *est :*

$$\mathcal{T}_{\dim}(n+1, \mathbf{d}) = \mathcal{O}\left((n+1)^{2.312} 11^{n+1} \binom{\max(d_1, \ldots, d_k, d'+1)+n+1}{n+1}^{8.376}\right)$$

*preuve :*Ce résultat s'obtient en observant comme dans [115] que

$$I : g^\infty = \langle f_1, \ldots, f_k, Zg - 1\rangle_{A[Z]} \cap A$$

□

Dans le cas où $(f_1, \ldots, f_k)$ forment une suite pseudo-régulière, on peut aussi utiliser l'algorithme suivant qui améliore l'exposant dans la complexité calcul ci-dessus dans le cas où du cas où g est un polynôme dense de degré supérieur à $d_1 \cdots d_k$.

Algorithme 6 DIM-PSEUDO-REG

ENTRÉE : - une suite pseudo-régulière $f_1, \ldots, f_k$
- un polynôme g

SORTIE : la dimension de $\langle f_1, \ldots, f_k \rangle : g^\infty$

- POUR i de 1 à k
  - $J := \langle f_1, \ldots, f_i \rangle : (g f_{i+1})^\infty$
  - POUR $h \in$ Générateurs de J
    - SI $1 \notin \langle f_1, \ldots, f_i \rangle : (gh)^\infty$ ALORS
      - RENVOYER $n - i$
    - FIN SI
  - FIN POUR
- FIN POUR

Lemme 28. *En utilisant les notations de l'algorithme 6, on note* $\mathbf{d} = (d_1, \ldots, d_k)$ *le vecteur des degrés des polynômes* $f_1, \ldots, f_k$, d_g *le degré de* g, *et* $d' = d_g + \mathcal{D}_\zeta(n, \mathbf{d})$. *Alors, l'algorithme 6 calcule la dimension de* $\langle f_1, \ldots, f_k \rangle : g^\infty$ *en temps :*

$$\mathcal{O}\left(k \mathcal{N}_\zeta(n, \mathbf{d}) \mathcal{T}_\zeta(n, \mathbf{d}, d')\right)$$

□

Remarque 21. *Cela permet ainsi de borner le coût du calcul de la dimension en fonction du coût de la saturation.*

*preuve :*D'abord, on montre que l'algorithme 6 calcule bien la dimension de l'idéal $I := \langle f_1, \ldots, f_k \rangle : g^\infty$. En effet, avec les notations de l'algorithme 6 :

$$1 \notin \langle f_1, \ldots, f_i \rangle : (gh)^\infty \Leftrightarrow \langle f_1, \ldots, f_i \rangle (g f_{i+1})^\infty \not\subset \sqrt{\langle f_1, \ldots, f_k \rangle : g^\infty}$$

En particulier, d'après le lemme 24, cela signifie qu'il existe un idéal premier isolé P de $\langle f_1, \ldots, f_i \rangle$, de profondeur inférieure à i, et tel que $g \notin P$ et $f_{i+1} \in P$. Or, d'après la condition $i)$ de la définition d'un suite pseudo-régulière, si P est un premier isolé de $\langle f_1, \ldots, f_i \rangle$ et $f_{i+1} \in P$, alors, P est aussi un premier isolé de $\langle f_1, \ldots, f_k \rangle$, et comme $g \notin P$, on en déduit par le lemme 24 que P est un premier isolé de I et que la dimension de I est minoré par $n - i$. Enfin, par construction, le couple $(S, F) := ((f_1, \ldots, f_i), \{g\})$ est un ensemble régulier tel que $\mathcal{I}(S, F) \subset I$, ce qui prouve que la dimension de I est majoré par $n - i$.

Enfin, pour la complexité de l'algorithme, on remarque que la boucle principale est exécutée au plus k fois. À chaque itération est effectuée :

- une saturation en temps au plus $\mathcal{T}_\zeta(n, \mathbf{d}, d_g + \max_{1 \leq i \leq n}(d_i))$
- puis au plus $\mathcal{N}_\zeta(n, \mathbf{d})$ saturation, chacune en temps majoré par $\mathcal{T}_\zeta(n, \mathbf{d}, d')$ où $d' = d_g + \mathcal{D}_\zeta(n, \mathbf{d})$

En considérant que $\mathcal{D}_\zeta(n, \mathbf{d}) > \max_{1 \leq i \leq n}(d_i)$, on obtient alors la borne de complexité.
□

8.2.2 Intersection

L'intersection d'idéaux est utilisée comme boîte noire dans l'algorithme 4. Étant donné un idéal I et des polynômes $g_1, \ldots, g_p$, nous nous attachons dans cette section à étudier le calcul de l'intersections d'idéaux de la formes :

$$I : g_1^\infty \cap \cdots \cap I : g^\infty$$

Nous verrons en section 8.3 que dans le cas où les polynômes engendrant l'idéal donné en entrée forment une suite pseudo-régulière, les intersections à calculer dans l'algorithme 4 peuvent toujours s'exprimer sous cette forme.

Sous cette forme, l'intersection se réduit à une simple saturation.

Notations 17. *Soit Z une variable libre. On introduit la famille de polynômes univariés suivante :*

$$l_{j,k} = \prod_{\substack{1 \leq i \leq k \\ i \neq j}} (Z - i)$$

□

On montre alors que l'on peut calculer l'intersection d'idéaux de la forme $I : g^\infty$ en effectuant une seule saturation :

- avec un algorithme déterministe et en rajoutant une variable dans le lemme 29
- avec un algorithme probabiliste dans le lemme 30

Lemme 29. *(Déterministe)*
Soit I un idéal et $g_1, \ldots, g_p$ des polynômes de A. Soit h le polynôme $\sum_{j=1}^{p} l_{j,p} g_i \in A[Z]$. Alors :

$$I : g_1^\infty \cap \cdots \cap I : g_p^\infty = \langle I \rangle_{A[Z]} : h^\infty \cap A$$

□

Remarque 22. *Dans le membre de droite, on effectue une saturation par h et on élimine la variable particulière Z. Ces deux opérations peuvent se calculer en une seule passe en simplifiant l'algorithme de saturation vu en section 7.1 : au lieu de calculer tous les générateurs de $\langle I \rangle_{A[Z]} : h$, on se restreint à ceux appartenant à A.*

En particulier, si $\mathbf{d} = (d_1, \ldots, d_k)$ sont les degrés des polynômes générateurs de I, et $d' = \max_{1 \leq i \leq k}(d_i)$, alors le degré du polynôme h est $k + d'$, et les opérations de saturation et d'élimination s'effectuent en temps majoré par $\mathcal{T}_\zeta(n+1, \mathbf{d}, k + d')$.

*preuve :*On procède par double inclusion.

D'abord, l'inclusion de gauche à droite est toujours vraie, quelque soit les polynômes $l_{i,p}$ utilisés. En effet, soit e un élément de $I : g_1^\infty \cap \cdots \cap I : g_p^\infty$. Alors, il existe $m_1, \ldots, m_p$ des entiers tels que :

$$\forall 1 \leq i \leq p, e g_i^{m_i} \in I$$

En particulier, on remarque que dans le développement de

$$(l_{1,p} g_1 + \cdots + l_{p,p} g_p)^{(m_1 + \cdots + m_p)}$$

, chaque terme est un monôme de degré $m_1 + \cdots + m_p$ en les polynômes $g_1, \ldots, g_p$, et contient donc au moins un facteur de la forme g_i^m avec $m \geq m_i$. Ainsi $eh^{(m_1+\cdots+m_p)} \in I$.

Pour l'autre inclusion, soit e un polynôme de $\langle I \rangle_{A[Z]} : h^\infty \cap A$. Alors, il existe m tel que $eh^m \in \langle I \rangle_{A[Z]}$. Et comme les générateurs de de I ne dépendent pas de Z, on peut en déduire que si l'on note h_i le polynôme obtenu en remplaçant Z par i dans h, alors, $eh_i^m \in I$. Or $h_i = (\prod_{\substack{1 \leq j \leq p \\ j \neq i}} (j - i)) f_i$, et donc $e \in I : f_i^\infty$ pour tout i entre 1 et p.
□

Pour la version probabiliste, nous nous plaçons dans le cadre des algorithmes probabilistes de type Monte-Carlo.

Définition 33. *Soient $\phi : E \to F$ une fonction et R une variable aléatoire à valeur dans un ensemble fini selon une loi uniforme. Alors un algorithme A utilisant R est dit probabiliste de type Monte-Carlo si pour toute entrée $e \in E$ il calcule $\phi(e)$ avec une probabilité supérieure à $2/3$.*
□

Le lemme suivant nous montre que nous pouvons calculer l'intersection des idéaux de la forme $I : g^\infty$ avec un algorithme de type Monte-Carlo effectuant une seule saturation.

Lemme 30. *(Probabiliste)*
Soit I un idéal engendrés par les polynômes $f_1, \ldots, f_k$ de degrés respectifs $d_1, \ldots, d_k$. Soit $\mathcal{N}_p$ le nombre de premiers isolés de I. Soient $g_1, \ldots, g_p$ d'autres polynômes. Si $l_1, \ldots, l_p$ sont p entiers choisis entre 1 et $3\mathcal{N}_p$ avec une probabilité uniforme, alors, avec une probabilité supérieure à $2/3$, on a :

$$\sqrt{I : g_1^\infty \cap \cdots \cap I : g_p^\infty} = \sqrt{I : \left(\sum_{i=1}^{p} l_i g_i \right)^\infty}$$

□

Remarque 23.
- *Le nombre $\mathcal{N}_p$ de premiers isolés de I est inférieur à $d_1 \cdots d_k$.*
- *En remplaçant $\mathcal{N}_p$ par le nombre de premiers* associés *à I, on a alors exactement :*

$$I : g_1^\infty \cap \cdots \cap I : g_p^\infty = I : \left(\sum_{i=1}^{p} l_i g_i \right)^\infty$$

avec une probabilité supérieure à $2/3$.

Afin de démontrer ce lemme, nous introduisons ce petit lemme.

Lemme 31. *Soient E un K-espace vectoriel de dimension k muni d'une base $(e_1, \ldots, e_k)$, F un sous-espace strict de E et D un entier. Soient u un vecteur de F et B le réseau défini par :*

$$B = \{u + l_1 e_1 + \cdots + l_k e_k \mid (l_1, \ldots, l_k) \in \{1 \ldots, D\}^k\}$$

Alors, B intersecte F en au plus D^{k-1} points.
□

*preuve :*Comme F ne contient pas tout E, on peut choisir v un vecteur de la base non contenu dans F. Soit v^C l'espace vectoriel de dimension $k-1$ engendré par les vecteurs de la base différents de v. Soit π la projection de E sur v^C parallèle à v et τ la translation qui envoie $e \in E$ sur $e+u$.

Par construction, on peut remarquer que $\tau \circ \pi$ restreinte à F est une injection. En effet, si $u_1, u_2 \in F$ vérifient $\tau \circ \pi(u_1) = \tau \circ \pi(u_2)$, alors il existe $\lambda \in K$ tel que $u_2 - u_1 = \lambda v$. Comme $u_2 - u_1 \in F$, cela implique $\lambda = 0$ et $u_1 = u_2$.

Ainsi, on peut même observer que $\tau \circ \pi$ restreinte à $F \cap B$ est une injection dont l'image est contenue dans $\tau(v^C) \cap B$. Or le cardinal de $\tau(v^C) \cap B$ est D^{k-1}, qui majore donc aussi le cardinal de $F \cap B$.

□

En se ramenant à ce lemme, on va pouvoir maitriser la probabilité du lemme 30.

preuve du lemme 30:

Soient

$$I_1 = I : g_1^\infty \cap \cdots \cap I : g_p^\infty$$

et

$$I_2 = I : \left(\sum_{i=1}^{p} l_i g_i \right)^\infty$$

La preuve du lemme 29 montre que $I_1 \subset I_2$ et donc $\text{minass}(I_1) \supset \text{minass}(I_2)$. Ainsi,

$$\sqrt{I_1} = \sqrt{I_2} \Leftrightarrow \text{minass}(I_1) \subset \text{minass}(I_2)$$

Étant donné un idéal premier P de $\text{minass}(I_1)$, on sait d'après le lemme 24 qu'il appartient aussi à $\text{minass}(I_2)$ si et seulement si $(\sum_{i=1}^{p} l_i g_i) \notin P$.

Soit $D = 3\mathcal{N}_p$. Pour prouver que $\sqrt{I_1} = \sqrt{I_2}$ avec une probabilité supérieure à $2/3$, il nous faut majorer le cardinal de l'ensemble

$$B := \{(l_1, \ldots, l_p) \in \{1, \ldots, D\}^p \mid l_1 g_1 + \ldots + l_p g_p \in \bigcup_{P \in \text{minass}(I_1)} P\}$$

par $D^p/3$. Cela prouvera ainsi que $\sqrt{I_1} \neq \sqrt{I_2}$ avec une probabilité inférieure à $1/3$ et que l'égalité est donc vraie avec une probabilité supérieure à $2/3$.

On considère E l'espace vectoriel des combinaisons linéaires des polynômes $g_1, \ldots, g_p$:

$$E = \{l_1 g_1 + \cdots + l_p g_p \mid (l_1, \ldots, l_p) \in K^p\}$$

Quitte à permuter les indices, on peut supposer que $(g_1, \ldots, g_k)$ est une base de E où $k \leq p$.

Si P un premier isolé de I_1, alors $P \cap E$ est par construction un sous-espace strict de E. Soit $F = P \cap E$. On fixe arbitrairement les entiers $l_{k+1}, \ldots, l_p$ et on note u le vecteur $l_{k+1} g_{k+1} + \cdots + l_p g_p$. Le lemme 31 nous permet alors d'affirmer que :

$$\{l_1 g_1 + \cdots + l_k g_k + u \mid (l_1, \ldots, l_k) \in \{1, \ldots, D\}^k\}$$

intersecte P en au plus D^{k-1} points.

Par ailleurs, le vecteur u peut prendre D^{p-k} valeurs. Ainsi, le nombre de p-uplet $(l_1, \ldots, l_p) \in \{1, \ldots, D\}^p$ tels que :

$$l_1 g_1 + \ldots + l_p g_p \in P$$

est majoré par D^{p-1}.

Enfin, le nombre de premiers isolés $P \in \text{minass}(I_1)$ est inférieur à $\mathcal{N}_p = D/3$, ce qui nous permet de conclure que le cardinal de B est bien majoré par $D^p/3$.

□

8.3 Algorithme dans le cas pseudo-régulier

Dans le cas où I est engendré par une suite pseudo-régulière, au cours de l'algorithme 4 les décompositions régulières minimales D_{equi} ne sont pas quelconques.

Propriété 10. *Soient $(f_1, \ldots, f_k)$ une suite pseudo-régulière, g un polynôme, et d la dimension de l'idéal $I = \langle f_1, \ldots, f_k \rangle$ (on note c sa codimension). Soit D_{equi} la décomposition régulière minimale renvoyée par :*

$$\textsc{Drm-Max}\,(((f_1), \{g\}), (f_2, \ldots, f_k), d)$$

Alors, tout $(S, F) \in D_{equi}$ vérifie :

i) S est une sous-suite préfixe de $(f_1, \ldots, f_k)$

ii) F est un ensemble de cardinal inférieur à 2

iii) $\sqrt{\mathcal{I}(S, F)} = \sqrt{I : \prod_{f \in F} f^\infty}$

□

Remarque 24. *Dans ce cas, le nombre d'appels récursif à la fonction* Drm-Max *est au plus $k - 1$.*

Remarque 25. *Sachant que la suite $f_1, \ldots, f_k$ est pseudo-régulière et connaissant la dimension d de $\langle f_1, \ldots, f_k \rangle : g^\infty$, on peut simplifier l'algorithme de la fonction* Drm-Max *en le remplaçant par l'algorithme suivant qui renvoie le même résultat :*

- si $k = n - d$ alors renvoyer $(f_1, \ldots, f_{n-d}, \{g\})$ fin si
- $h :=$ Scindage $((f_1, \ldots, f_{n-d}, \{g\}), g_{n-d+1})$
- renvoyer $(f_1, \ldots, f_{n-d}, \{g, h\})$

*preuve :*D'après la remarque 17, les c premiers polynômes de I forment une suite régulière. En particulier, en utilisant les notations de l'algorithme 3, les c premiers appels de la fonction Drm-Max se placeront systématiquement dans la branche où $\dim(J + \langle g_c \rangle) \neq \dim(J)$. On a donc :

$$\textsc{Drm-Max}\,(((f_1), \{g\}), (f_2, \ldots, f_k), d) = \textsc{Drm-Max}\,(((f_1, \ldots, f_c), \{g\}), (f_{c+1}, \ldots, f_k), d)$$

Puis, comme la dimension de $\mathcal{I}((f_1, \ldots, f_c), \{g\})$ est d et que la suite $f_1, \ldots, f_k$ est pseudo-régulière, on a alors 2 cas. Soit $k = c$, auquel cas, le résultat renvoyé est :

$$D_{equi} = \{((f_1, \ldots, f_c), \{g\})\}$$

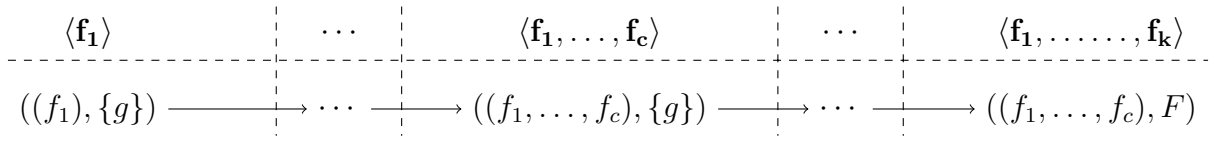
Soit $k > c$, alors l'appel de fonction

$$\textsc{Drm-Max}\,(((f_1, \ldots, f_c), \{g\}), (f_{c+1}, \ldots, f_k), d)$$

va créer un polynôme h et appeler la fonction :

$$\textsc{Drm-Max}\,(((f_1, \ldots, f_c), \{g, h\}), (f_{c+2}, \ldots, f_k), d)$$

Les propriétés d'une suite pseudo-régulière impliquent alors que à partir de là, à chaque appel récursif, l'algorithme 3 ne rajoutera aucun polynômes ni à la suite $(f_1, \ldots, f_c)$, ni à l'ensemble $\{g, h\}$, et ne fera qu'un appel récursif tant qu'il restera des polynômes à traiter. Ainsi, le nombre total d'appels récursifs à la fonction Drm-Max est inférieur à $k - 1$, et l'arbre de calcul de l'algorithme 3, avec les conventions données dans l'exemple 5 est :



Et le résultat final est une décomposition régulière minimale réduite à un ensemble régulier de la forme :

$$D_{equi} = \{((f_1, \ldots, f_c), \{g, h\})\}$$

Ce qui démontre les assertions *i*) et *ii*).

Enfin, pour l'assertion *iii*) on note S la suite $(f_1, \ldots, f_c)$ on montre par double inclusion que

$$\sqrt{\mathcal{I}(S, F)} = \sqrt{I : \prod_{f \in F} f^\infty}$$

D'abord, comme $S \subset I$, on a directement l'inclusion de gauche à droite.

Puis, la condition *ii*) de la définition 28 d'une décomposition régulière implique que $\sqrt{\mathcal{I}(S, F)} \supset I : g^\infty$, et en particulier :

$$\sqrt{\mathcal{I}(S, F)} = \sqrt{\mathcal{I}(S, F)} : \prod_{f \in F} f^\infty \supset I : \prod_{f \in F} f^\infty$$

□

Ainsi, en combinant ce résultat aux résultats de la section 8.2.2, on peut ainsi borner dans l'algorithme 4 le calcul de l'intersection :

$$J \cap \bigcap_{(S,F) \in D_{equi}} \mathcal{I}(S, F)$$

On peut en effet facilement exprimer J comme une intersection d'idéaux de la forme :

$$J := \bigcap_{i=1}^{p} I : g_i^{\infty}$$

De même D_{equi} est réduit à $\{(S, F)\}$ et $\bigcap_{(S,F)\in D_{equi}} \mathcal{I}(S, F)$ est l'idéal $I : \prod_{f\in F} f^{\infty}$.

On note $\mathbf{d} = (d_1, \ldots, d_k)$ le vecteur $(\deg(f_1), \ldots, \deg(f_k))$ des degrés de la suite de polynômes engendrant I, et $d' = \max_{1\leq i\leq p}(\deg(g_i))$.

Ainsi, le calcul d'un idéal ayant le même radical que $J \cap \bigcap_{(S,F)\in D_{equi}} \mathcal{I}(S, F)$ peut se faire en temps majoré par :

- $\mathcal{T}_{\zeta}(n + 1, \mathbf{d}, k + d')$ de manière déterministe en utilisant le lemme 29
- $\mathcal{T}_{\zeta}(n, \mathbf{d}, d')$ avec un algorithme probabiliste de type Monte-Carlo en utilisant le lemme 30

8.4 Analyse de l'algorithme de décomposition minimale

8.4.1 Taille de la sortie

En rassemblant les résultats des précédentes sections, on peut maintenant obtenir des bornes de complexités sur la décomposition régulière minimale d'un idéal.

D'abord, on borne la taille d'une décomposition régulière minimale D calculée par l'algorithme 4 lorsque l'idéal I donné en entrée est engendré par une suite pseudo-régulière $(f_1, \ldots, f_k)$ de degrés $\mathbf{d} = (d_1, \ldots, d_i)$.

On va montrer dans ce cas que le nombre d'ensembles réguliers de D est majoré par $d_1 \cdots d_k$. Et pour chaque $(S, F) \in D$, le nombre de polynômes de S est majoré par n, leurs degrés par $\max_{1\leq i\leq k}(d_i)$, le cardinal de F est inférieur à k, et le degré des polynômes de F est borné par $d_1 \cdots d_k$.

Théorème 10. *Soient I un idéal de codimension c engendré par la suite pseudo-régulière $(f_1, \ldots, f_k)$ de degrés $\mathbf{d} = (d_1, \ldots, d_i)$, et D une DRM de I calculée avec l'algorithme 4.*

Alors en utilisant les notations 16, le cardinal de D est majoré par $\mathcal{N}_p(\mathbf{d})$. Et pour tout $(S, F) \in D$, on a :

i) S est une sous-suite préfixe de $(f_1, \ldots, f_k)$

ii) le cardinal de S est majoré par $\min(k, n)$

iii) le cardinal de F est majoré par 2

iv) $\forall g \in F, \deg(g) \leq \mathcal{D}_{\zeta}(n, \mathbf{d})$

□

Remarque 26.
- *L'assertion i) implique que chaque polynôme de S est majoré par $\max_{1\leq i\leq k}(d_i)$.*

– *De façon plus explicite en utilisant les bornes vues en section 7.1, l'algorithme 4 calcule une décomposition régulière minimale constituée d'au plus* $d_1 \cdots d_k$ *ensembles réguliers où chaque polynôme peut se représenter avec une taille au plus :*

$$\sigma_{\max}\binom{d_1 \cdots d_k + n}{n}^2$$

*preuve :*D'abord, le fait que le cardinal de D est majoré par $\mathcal{N}_p(\mathbf{d})$ s'obtient en utilisant le lemme 25 qui nous dit que les premiers isolés des $\mathcal{I}(S,F)$ tels que $(S,F) \in D$ forment une partition de l'ensemble des premiers isolés de I. Ainsi, comme chaque $\mathcal{I}(S,F)$ a au moins un premier isolé, on en déduit que le cardinal de D est majoré par le nombre $\mathcal{N}_p(\mathbf{d})$ de premiers isolés de I.

Ensuite, les assertions i) et iii) découlent directement de la propriété 10 de la fonction Drm-Max utilisée dans l'algorithme Drm. Puis, comme S est une sous-suite de $(f_1, \ldots, f_k)$, son cardinal est majoré par k. De plus, le fait que (S,F) soit un ensemble régulier entraine que le nombre de polynômes de (S,F) est aussi majoré par n, d'où l'assertion ii).

Enfin, le point iv) provient du fait que si $(S,F) \in D$, chaque polynôme de F a été calculé par la fonction Scindage$((S_0,F_0),p_0)$ (algorithme 1) appelé dans l'algorithme 3 avec à chaque fois en entré un ensemble régulier (S_0,F_0) tel que S_0 est une sous-suite de $(f_1,\ldots,f_k)$. En particulier on vérifie facilement que le polynôme h renvoyé par Scindage$((S_0,F_0),p_0)$ est dans l'idéal résultant de la saturation de S_0 par un polynôme particulier. Ainsi, en utilisant la fonction ζ pour effectuer la saturation, on peut en conclure que le polynôme renvoyé est de degré majoré par $\mathcal{D}_\zeta(n,\mathbf{d})$.
□

8.4.2 Complexité en temps

On va maintenant pouvoir borner la complexité en temps de l'algorithme de décomposition régulière minimale dans le cas où l'idéal pris en entrée est engendré par une suite pseudo-régulière.

On exprimera la complexité en fonction des complexités des fonctions de bases vues en section 7.1, puis nous les expliciterons dans le cas d'une machine de Türing déterministe.

Notations 18.

– $\mathcal{T}_{\text{Scindage}}(n,\mathbf{d},d_F,d_p)$ *:*
est une borne du temps de calcul de la fonction

$$\text{Scindage}((S,F),p)$$

où n *est le nombre de variables,* $\mathbf{d}$ *le vecteurs des degrés des polynômes de* S*,* d_F *la somme des degrés des polynômes de* F *et* d_p *le degré de* p*.*

– $\mathcal{T}_{\text{Drm-Max}}(n,\mathbf{d},d_g)$ *:*
est une borne du temps de calcul de la fonction

$$\text{Drm-Max}\,(((f_1),\{g\}),(f_2,\ldots,f_k),d)$$

où n est le nombre de variables, d la dimension de l'idéal $\langle f_1, \ldots, f_k\rangle : g^\infty$, $(f_1, \ldots, f_k)$ une suite pseudo-régulière de polynômes, $\mathbf{d}$ le vecteur de leurs degrés et d_g le degré de g.

– $\mathcal{T}_{\text{DRM}}(n, \mathbf{d})$:
est une borne du temps de calcul de la fonction

$$\text{DRM}\,(f_1, \ldots, f_k)$$

où n est le nombre de variables et $f_1, \ldots, f_k$ une suite pseudo-régulière de polynômes.

□

On va expliciter dans l'ordre les bornes $\mathcal{T}_{\text{SCINDAGE}}(n, \mathbf{d}, d_F, d_p)$, $\mathcal{T}_{\text{DRM-MAX}}(n, \mathbf{d}, d_g)$ et enfin $\mathcal{T}_{\text{DRM}}(n, \mathbf{d})$.

Lemme 32. *En utilisant les notations 16 et 18, et en notant $d' = d_F + \max(d_p, \mathcal{D}_\zeta(n, \mathbf{d}))$, le temps de calcul de la fonction* SCINDAGE$((S, F), p)$ *est borné par :*

$$\mathcal{T}_{\text{SCINDAGE}}(n, \mathbf{d}, d_F, d_p) = \mathcal{O}\left(\mathcal{N}_p(\mathbf{d})\mathcal{N}_\zeta(n, \mathbf{d})\mathcal{T}_\zeta(n, \mathbf{d}, d')\right)$$

□

*preuve :*La fonction SCINDAGE$((S, F), p)$ effectue une boucle TANT QUE au plus $\mathcal{N}_p(\mathbf{d})$ fois d'après la remarque 14.

Dans la boucle, l'algorithme calcule :
– une saturation $J := S : \left((p + h)\prod_{f\in F} f\right)^\infty$ en temps $\mathcal{T}_\zeta(n, \mathbf{d}, d')$
– un test d'appartenance au radical de $S : \prod_{f\in F} f^\infty$ pour chaque polynômes de l'idéal J (au plus $\mathcal{N}_\zeta(n, \mathbf{d})$) pouvant se faire à chaque fois par une saturation en temps $\mathcal{T}_\zeta(n, \mathbf{d}, d')$

Ainsi, le temps total de l'algorithme est majoré par :

$$\mathcal{N}_p(\mathbf{d})\left(\mathcal{T}_\zeta(n, \mathbf{d}, d') + \mathcal{N}_\zeta(n, \mathbf{d})\mathcal{T}_\zeta(n, \mathbf{d}, d')\right)$$

et la borne finale suit en retirant les termes négligeables.

□

Nous pouvons maintenant borner le temps de calcul de $\mathcal{T}_{\text{DRM-MAX}}(n, \mathbf{d}, d_g)$.

Lemme 33. *En utilisant les notations 16 et 18, et en notant $d' = d_g + 2\mathcal{D}_\zeta(n, \mathbf{d})$, le temps de calcul de la fonction* DRM-MAX $(((f_1), \{g\}), (f_2, \ldots, f_k), d)$ *est borné par :*

$$\mathcal{T}_{\text{DRM-MAX}}(n, \mathbf{d}, d_g) = \mathcal{O}\left(k\mathcal{N}_p^{max}(\mathbf{d})\mathcal{N}_\zeta(n, \mathbf{d})\mathcal{T}_\zeta(n, \mathbf{d}, d')\right)$$

□

Remarque 27. *En utilisant pour la fonction* DRM-MAX *l'algorithme simplifié présenté en remarque 25, et en notant $d' = d_g + \mathcal{D}_\zeta(n, \mathbf{d})$, on peut alors borner le temps de calcul par :*

$$\mathcal{T}_{\text{DRM-MAX}}(n, \mathbf{d}, d_g) = \mathcal{O}\left(\mathcal{N}_p^{max}(\mathbf{d})\mathcal{N}_\zeta(n, \mathbf{d})\mathcal{T}_\zeta(n, \mathbf{d}, d')\right)$$

preuve :D'après la remarque 24, la fonction :

$$\textsc{Drm-Max}\left(((f_1),\{g\}),(f_2,\ldots,f_k)\right)$$

effectue au plus $k-1$ appels récursifs lorsque la suite $(f_1,\ldots,f_k)$ est pseudo-régulière, où chaque appel est de la forme :

$$\begin{array}{ll}(1) & \begin{cases}\textsc{Drm-Max}\left(((f_1,\ldots,f_i),\{g\}),(f_{i+1},\ldots,f_k)\right) & \text{si } i\leq n-d\\ \textsc{Drm-Max}\left(((f_1,\ldots,f_{n-d}),\{g,h\}),(f_{i+1},\ldots,f_k)\right) & \text{si } i>n-d\end{cases}\\ (2) & \end{array}$$

À chaque appel, l'algorithme 3 effectue :

- un calcul de la fonction Scindage en temps au plus $\mathcal{T}_{\textsc{Scindage}}(n,(d_1,\ldots,d_i),d_g,d_{i+1})$ dans le cas (1) et $\mathcal{T}_{\textsc{Scindage}}(n,(d_1,\ldots,d_{n-d}),d_g+\mathcal{D}_\zeta(n,(d_1,\ldots,d_{n-d})),d_{i+1})$ dans le cas 2
- dans le cas (1), un test d'appartenance du polynôme 1 au radical de $\langle f_1,\ldots,f_{i+1}\rangle : g^\infty$ qui peut s'effectuer à l'aide d'une saturation en temps au plus $\mathcal{T}_\zeta(n,(d_1,\ldots,d_i),d_g)$; dans le cas (2), le test n'est pas effectué.

Ainsi, en retirant les temps de saturations qui sont négligeables devant ceux de l'algorithme Scindage, le temps total de calcul est majoré par :

$$\mathcal{O}\left(k\mathcal{T}_{\textsc{Scindage}}(n,\mathbf{d},d_g+\mathcal{D}_\zeta(n,\mathbf{d}),\max_{1\leq i\leq k}d_i)\right)$$

d'où la borne ci-dessus en utilisant le lemme 32.
□

On peut maintenant analyser la complexité de l'algorithme 4 calculant une décomposition régulière minimale d'un idéal engendré par une suite pseudo-régulière.

Théorème 11. *En utilisant les notations 16 et 18, et en notant* $d'=3\mathcal{D}_\zeta(n,\mathbf{d})$*, le temps de calcul de la fonction* $\textsc{Drm}(f_1,\ldots,f_k)$ *est majoré par :*

$$\mathcal{T}_{\textsc{Drm}}(n,\mathbf{d})=\mathcal{O}\left(k\mathcal{N}_p(\mathbf{d})\mathcal{N}_p^{max}(\mathbf{d})\mathcal{N}_\zeta(n,\mathbf{d})\mathcal{T}_\zeta(n,\mathbf{d},d')\right)$$

□

Remarque 28.

- *En utilisant les remarques 25 et 27, et en notant* $d'=2\mathcal{D}_\zeta(n,\mathbf{d})$*, on peut obtenir un algorithme de complexité majorée par :*

$$\mathcal{O}\left(\mathcal{N}_p(\mathbf{d})\mathcal{N}_p^{max}(\mathbf{d})\mathcal{N}_\zeta(n,\mathbf{d})\mathcal{T}_\zeta(n,\mathbf{d},d')\right)$$

- *En explicitant les bornes avec les résultats présentés en section 7.1, on obtient alors comme borne :*

$$\mathcal{O}\left((n+1)(d_1\cdots d_k)^2(k+1)^{\omega+2}\binom{3(d_1\cdots d_k+1)^2+n}{n}^{\omega+1}\right)$$

ou encore :

$$\mathcal{O}\left((n+1)(k+1)^{\omega+2}(6d_1\cdots d_k)^{2(\omega+1)n+2}\right)$$

*preuve :*Pour obtenir cette borne, on remarque que l'algorithme 4 calculant une DRM d'un idéal effectue une boucle au plus $\mathcal{N}_p(\mathbf{d})$ fois d'après la remarque 16. Au cours de cette boucle sont effectués :

- un calcul de dimension en temps majoré par $\mathcal{O}\left(k\mathcal{N}_\zeta(n,\mathbf{d})\mathcal{T}_\zeta(n,\mathbf{d},d')\right)$
- un appel à la fonction Drm-Max en temps majoré par $\mathcal{O}\left(k\mathcal{N}_p^{max}(\mathbf{d})\mathcal{N}_\zeta(n,\mathbf{d})\mathcal{T}_\zeta(n,\mathbf{d},d')\right)$
- un calcul d'intersection que l'on effectue avec une saturation en au plus $\mathcal{T}_\zeta(n+1,\mathbf{d},k+\mathcal{D}_\zeta(n,\mathbf{d}))$
- puis $\mathcal{N}_\zeta(n,\mathbf{d})$ saturations effectuées chacune en au plus $\mathcal{T}_\zeta(n,\mathbf{d},d')$

En utilisant les bornes vues en section 7.1, on constate alors que le calcul Drm-Max est dominant, ce qui induit la complexité finale de l'algorithme calculant la fonction Drm.
□

Chapitre 9

Robot parallèle plan

9.1 Introduction

Nous considérons dans ce chapitre un robot plan parallèle possédant trois degrés de liberté, appelé robot 3-RPR et présenté en figure 9.1.

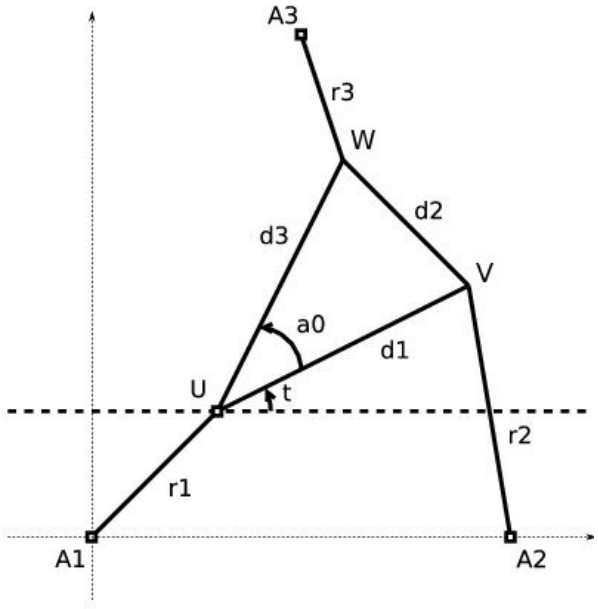


FIG. 9.1 – Parallel robot 3-rpr

Le robot est constitué d'une plateforme triangulaire, manipulée par trois jambes dont attachées au plan. Il est spécifié par les longueurs des trois côtés de la plateforme d_1, d_2, d_3, et par les trois points d'attache A_1, A_2, A_3. Ces variables sont les paramètres géométriques du robot. Ils seront spécialisées par des valeurs rationnelles dans les exemples que nous considérerons.

Les longueurs des jambes $\mathbf{L} = (r_1, r_2, r_3)$ sont les paramètres de contrôle. Le robot 3-RPR possède des moteurs lui permettant de modifier directement la valeur de ces paramètres. Ils

permettent ainsi de modifier la position de la plateforme triangulaire. Cependant, il n'y a pas de de bijection entre les valeurs des paramètres de contrôle et la position de la plateforme. Comme on peut lire dans [100], lorsque les r_1, r_2, r_3 sont spécifiés, le robot peut avoir au plus 6 positions différentes.

Afin de décrire sans ambiguïté la position de la plateforme triangulaire, nous introduisons le point $\mathcal{U}$ et l'angle t (voir figure 9.1). les coordonnées de $\mathcal{U}$ sont notées $(\mathcal{U}_x, \mathcal{U}_y)$, et le cosinus et sinus de t sont notés respectivement t_x et t_y. Les valeurs de ces variables décrivent exactement une configuration du robot. Dans la suite, ces varaiables seront appelées variables de positions et notées $\mathbf{X} = (\mathcal{U}_x, \mathcal{U}_y, t_x, t_y)$.

Ainsi, dans notre modélisation, la configuration du robot est décrite par 7 variables $(\mathbf{L}, \mathbf{X})$. Nous exhibons par ailleurs 4 équations polynômiales en $(\mathbf{L}, \mathbf{X})$ algébriquement indépendantes, modélisant les contraintes du robot. Ainsi, le robot considéré possède bien 3 degrés de liberté, comme montré par exemple dans [99, 100, 145].

État de l'art

Dans [99, 145], les auteurs modélisent le robot 3-RPR par un système de 3 équations en 3 les paramètres $\mathbf{L}$ et 3 variables θ :

$$\Gamma_1(\mathbf{L}, \theta) = 0, \Gamma_2(\mathbf{L}, \theta) = 0, \Gamma_3(\mathbf{L}, \theta) = 0$$

Pour étudier localement le mouvement du robot 3-RPR, les auteurs développent les équations de contrainte en séries. Les termes du premier et deuxième ordre de ces séries permet notamment de détecter respectivement les configurations sungulières et cuspidales du robot 3-RPR.

Le développement de chaque Γ_i en série tronquée après l'ordre 2 s'écrit ainsi :

$$\begin{aligned}
\Delta\Gamma =& \frac{\partial \Gamma}{\partial \theta}\Delta\theta + \frac{\partial \Gamma}{\partial \mathbf{L}}\Delta\mathbf{L} \\
&+ \frac{1}{2}\begin{bmatrix} \Delta\theta^T \frac{\partial^2 \Gamma_1}{\partial \theta^2}\Delta\theta \\ \Delta\theta^T \frac{\partial^2 \Gamma_2}{\partial \theta^2}\Delta\theta \\ \Delta\theta^T \frac{\partial^2 \Gamma_3}{\partial \theta^2}\Delta\theta \end{bmatrix} + \begin{bmatrix} \Delta\theta^T \frac{\partial^2 \Gamma_1}{\partial \theta \partial \mathbf{L}}\Delta\mathbf{L} \\ \Delta\theta^T \frac{\partial^2 \Gamma_2}{\partial \theta \partial \mathbf{L}}\Delta\mathbf{L} \\ \Delta\theta^T \frac{\partial^2 \Gamma_3}{\partial \theta \partial \mathbf{L}}\Delta\mathbf{L} \end{bmatrix} + \frac{1}{2}\begin{bmatrix} \Delta\mathbf{L}^T \frac{\partial^2 \Gamma_1}{\partial \mathbf{L}^2}\Delta\mathbf{L} \\ \Delta\mathbf{L}^T \frac{\partial^2 \Gamma_2}{\partial \mathbf{L}^2}\Delta\mathbf{L} \\ \Delta\mathbf{L}^T \frac{\partial^2 \Gamma_3}{\partial \mathbf{L}^2}\Delta\mathbf{L} \end{bmatrix} \\
&+ \mathcal{O}(\|\Delta\theta\|^3 + \|\Delta\mathbf{L}\|^3) \\
=& 0
\end{aligned} \tag{9.1}$$

Singular configurations Les configurations singulières apparaissent lorsque les termes du premier ordre de la série 9.1 ne permettent pas de décrire localement les mouvements du

robot. Cette situation correspond à la situation où localement, les variables de positions θ ne varient pas linéairement en fonction des variables $\mathbf{L}$.

De manière équivalent, les configurations singulières apparaissent dès lors que la matrice $\frac{\partial \Gamma}{\partial \theta}$ n'est pas inversible, ce qui s'écrit algébriquement par la condition :

$$\det(\frac{\partial \Gamma}{\partial \theta}) = 0 \tag{9.2}$$

D'un point de vue géométrique, les auteurs de [99] ont observé que les configurations satisfaisant l'équation 9.2 correspondent à la limite de 2 modes d'assemblages convergeant vers la même configuration.

Cuspidal configurations Les points dits cuspidaux correspondent à 3 configurations coïncidentes. Pour les exhiber, les idées de [99, 145] consistent à analyser le noyau des matrices des termes du premier et du second ordre de la série 9.1. Les auteurs en déduisent un critère leur permettant de décrire partiellement les configurations cuspidales, en faisant varier numériquement un paramètre de manière discrète.

Une autre idée apparaissant notamment dans [108, 27] consiste à réduire les équations de contrainte à une équation polynômiale p dépendant des paramètres de contrôle et d'une seule variable. Les configurations cuspidales sont alors incluses dans l'ensemble des raines triples de p. Cette approche n'est cependant pas praticable avec le robot $3-RPR$: en particulier, il est possible de calculer le polynôme p, cependant la taille de ce dernier le rend difficilement utilisable pour en extraire ses racines triples, comme l'ont aussi remarqué les auteurs de [99].

Comportements inexpliqués

Dans les travaux précédents, les points cuspidaux sont obtenus à l'aide d'une condition nécessaire mais non suffisante. En particulier, les auteurs de [145] obtiennent ces configurations comme les solutions d'un polynômes de degré 96. Or ce polynôme se factorise en plusieurs facteurs dont un de degré 24 contenant expérimentalement toutes les configurations cuspidales. Cependant, aucune preuve ne permet d'éliminer avec certification les autres facteurs.

Par ailleurs, la description géométrique des configurations cuspidales est difficile. Les auteurs de [145] ont réussi à analyser ces positions en discrétisant l'espace des paramètres. Cependant cette méthode n'est pas exhaustive, en particulier, les auteurs observent que le nombre maximal de configurations cuspidales obtenues en fixant le paramètre r_1 est 8, mais il n'existe pas de preuve garantissant ce résultat.

Résultats principal

Dans ce chapitre, nous présentons une nouvelle approche plus algébrique permettant de décrire les configurations cuspidales par un ensemble de conditions nécessaires et suffisantes.

Le système obtenu est surdéterminé. Nous analysons ce système en utilisant les techniques de variété discriminantes et de décompositions présentées dans les chapitres précédents. Ces

méthodes nous permettent de décrire rigoureusement l'ensemble des configurations cuspidales. Nous montrons notamment que le nombre maximal de points cuspidaux est 10.

Dans la section suivante, nous définissons la notion de degré algébrique que nous utiliserons. Dans la dernière section nous caractérisons algébriquement les configurations singulières, puis cuspidales du robot 3-RPR. Nous analysons en outre la géométrie des configurations cuspidales de manière certifiée à l'aide de la variété discriminante.

D'un point de vue théorique, un des ingrédients important de notre modélisation est une extension du critère jacobien pour caractériser algébriquement les racines de degré supérieur ou égal à 3 d'un système zéro dimensionnel.

D'un point de vue calcul, l'élimination de variables, de résolutions de système zéro-dimensionnel et de calcul de variété discriminante sont fait avec la bibliothèque SALSA pour MAPLE. Les calculs de décomposition régulières sont effectués avec la bibliothèque RD.

9.2 Algebraic tools

Total degree

In the following two sections, we quickly remind the definitions of the *total degree* and *local degree* of a 0-dimensional system. The interested reader may find a good introduction in [37] or in [29, chapter 4].

Given a polynomial system S of polynomial equations in $\mathbb{C}[X_1, \ldots, X_n]$ with finitely many complex solutions, we first present the algebraic definition of the total degree of S.

Notations 19.
- *R denotes the ring $\mathbb{C}[X_1, \ldots, X_n]$*
- *I_S denotes the ideal generated by the polynomials of S in R.*
- *$\mathcal{A}$ denotes the $\mathbb{C}$-vector space R/I_S*

□

With these notations, we can define the total degree of a polynomial system.

Définition 34. *(total degree)*
If S is a system of polynomial equations with finetely many solutions then, using the notations above, we call total degre *of S the dimension of A over the field $\mathbb{C}$.*
□

Remarque 29. *The total degree of a polynomial system is always greater than its number of roots. More precisely, it is exactly the number of roots counted with multiplicities.*

Local degree

To define the degree of a root in S, we use the same construction as for the total degree, except that we replace the global polynomial ring R by the localization of R at α.

Notations 20.

- *If $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n$ is a solution of S, then we denote by M_α the ideal generated by $\langle X_1 - \alpha_1, \ldots, X_n - \alpha_n \rangle$.*
- *S_α denotes the complementary of M_α in $\mathbb{C}[X_1, \ldots, X_n]$.*

□

We first define the localization of the polynomial ring R at a n-tuple of $\mathbb{C}^n$.

Définition 35. *(local ring)*
Let α be a n-tuple of $\mathbb{C}^n$. Using the previous notations, we call local polynomial ring *in α the fraction ring :*

$$S_\alpha^{-1} R = \{r/s \mid r \in R, s \in S_\alpha\}$$

equipped with the usual operations on the fractions. In the following, we denote it by R_α.
□

Remarque 30. *Every polynomial that does not vanish on α is invertible in R_α*

Finally, the degree of a root is defined as follows.

Définition 36. *(local degree)*
Let S be a system of polynomial equations with finetely many solutions, and α be a root of S. Then, the degree of α *in S is the dimension of the $\mathbb{C}$-vector space R_α/I where R_α is the local ring defined in 35, and I is the ideal generated by the polynomial of S in R_α.*
□

Remarque 31. *When S is reduced to a univariate polynomial equation*

$$\prod_{i=1}^{k} (X - c_i)^{\mu_i} = 0 \tag{S}$$

then the reader may check that the local degree of each root c_i is exactly μ_i.

Software

The manipulations and computations of the algebraic objects are done with the SALSA library in MAPLE ([128]).

FGb Given a set of polynomial generating an ideal I, FGB allows the computation of the Gröbner basis of I with relation to a given order on the variables, with the function `fgb_gbasis`.

Computing a Gröbner basis of I is a first step which allows the computation of :
- the dimension and the degree of I, with the function `fgb_hilbert`
- the membership test of a polynomial to I, with the function `fgb_normalForm`

Furthermore, given a subset of the variables, it is possible to compute the polynomials of I depending only on these variables, by using a special elimination ordering with the function `fgb_gbasis_elim`.

RS Given a system of polynomial equations $f_1 = 0, \ldots, f_k = 0$, we say that S is 0-dimensional if its number of complex solutions is finite.

In this case, we can use the `rs_isolate` function ([124])to compute directly the real solutions of S. By default, each solution will be given by a box with rational bounds, with the insurance that no pair of boxes overlaps.

Moreover, in MAPLE, the final size of each box may be control with the global variable *Digits*.

DV Given a parametric system of equations $f_1 = O, \ldots, f_k = 0$ and inequations $g_1 \neq 0, \ldots, g_r \neq 0$, $T_1, \ldots, T_s$ being the parameters and $X_1, \ldots, X_n$ the unknowns. Its minimal discriminant variety is computed with the algorithm presented in [87].

Mainly, the algorithm may split in three steps :

- The computation of the points at infinity. For the 3-rpr manipulator, this kind of points does not appear.
- The computation of the inequation bounds in the parameters' space. In the case of the manipulator, these bounds are trivial since the inequations already depend solely on the parameters.
- The computation of the critical and singular values. In the general case, these values are computed as follows :
  - Let $m_1, \ldots, m_{\binom{k}{n}}$ be the $n \times n$ minors of the Jacobian matrix :

$$\begin{pmatrix} \frac{\partial f_1}{\partial X_1} & \cdots & \frac{\partial f_1}{\partial X_n} \\ \vdots & & \vdots \\ \vdots & & \vdots \\ \frac{\partial f_k}{\partial X_1} & \cdots & \frac{\partial f_k}{\partial X_n} \end{pmatrix}$$

  - Then, the critical and singular values are solutions of the polynomials that depend only on the parameters $T_1, \ldots, T_s$ in the ideal generated by $f_1, \ldots, f_k, m_1, \ldots, m_{\binom{k}{n}}$. This step can be done with the function `fgb_gbasis_elim`.

9.3 New modelling and method

9.3.1 Constraint equations

From the geometrical specifications of the planar 3-RPR manipulator, we deduce the constraint equations that model statically the design of the robot, as in section 1.

We first specify that α_x and α_y are the coordinates of a unit vector by :

$$\alpha_x^2 + \alpha_y^2 - 1 = 0$$

The lengths ρ_1, ρ_2, ρ_3 can be written as the norm of the vectors $\overrightarrow{A_1B}, \overrightarrow{A_2V}, \overrightarrow{A_3W}$:

$$\begin{cases} \|\overrightarrow{A_1B}\| - r_1^2 = 0 \\ \|\overrightarrow{A_2V}\| - r_2^2 = 0 \\ \|\overrightarrow{A_3W}\| - r_3^2 = 0 \end{cases} \tag{9.3}$$

The coordinates of each point is :

$$A_1 \left| \begin{matrix} 0 \\ 0 \end{matrix} \right. \qquad A_2 \left| \begin{matrix} A_{2x} \\ 0 \end{matrix} \right. \qquad A_3 \left| \begin{matrix} A_{3x} \\ A_{3y} \end{matrix} \right. \qquad B \left| \begin{matrix} B_x \\ B_y \end{matrix} \right.$$

$$V \left| \begin{matrix} B_x + d_1 \cos(\alpha) \\ B_y + d_1 \sin(\alpha) \end{matrix} \right. \qquad W \left| \begin{matrix} B_x + d_3 \cos(\alpha + \beta) \\ B_y + d_3 \sin(\alpha + \beta) \end{matrix} \right.$$

Finally, we derive the trigonometric formulas, and replace $\cos(\alpha), \sin(\alpha)$ by α_x, α_y and $\cos(\beta), \sin(\beta)$ by β_x, β_y in Equ. 9.3. Then, the modelling of the manipulator is given by the system :

$$\mathbf{E}(\mathbf{L}, \mathbf{X}) = \begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}^T \tag{9.4}$$

Where

$$\mathbf{E}(\mathbf{L}, \mathbf{X}) := \begin{bmatrix} \alpha_x^2 + \alpha_y^2 - 1 \\ B_x^2 + B_y^2 - \rho_1^2 \\ (B_x + d_1\alpha_x - A_{2x})^2 + (B_y + d_1\alpha_y)^2 - \rho_2^2 \\ (B_x + d_3\alpha_x\beta_x - d_3\alpha_y\beta_y - A_{3x})^2 + (B_y + d_3\alpha_x\beta_y + d_3\alpha_y\beta_x - A_{3y})^2 - \rho_3^2 \end{bmatrix}$$

Due to its particular design, the configurations of a 3-RPR manipulator may be classified into three categories : the regular configurations, the singular configurations and the cuspidal configurations. The description of the special configurations (singular and cuspidal) is important for path planning. First, the regular configurations are the most common ones : these are the configurations where the position of the platform is locally uniquely determined by the values of the control parameters. Then the singular (resp. cuspidal) configurations are two (resp. three or more) coalesced configurations. These configurations were studied through local analysis, but we will see that they can also be described with algebraic methods.

9.3.2 Singular configurations

From a geometrical point of view, we saw in Section 1 that the configuration satisfying Equation (7) are coalesced assemblies, meaning that they are limit of two assemblies.

From an algebraic point of view, this condition can be retrieved in term of multiplicities. When we specialize the variables $\mathbf{L}$ with real numbers, the set of equations 9.4 has finitely many solutions. Moreover, an algebraic degree is associated to each solution (see Section 9.3.2). Using this notion, we can check that the singular assemblies are exactly configurations that are solutions of degree greater than 2. Indeed, the Jacobian criterion [35] states directly that these configurations are the solutions to Equation (7).

Modelling To describe the singular points, we use the notion of algebraic degree in a 0-dimensional system. A system of equation is said 0-dimensional when it has a finite number of complex solutions. This is the case of Equations (9.4) when we fix the lengths ρ_1, ρ_2, ρ_3. In this case, each solution can be associated with an integer greater or equal to 1, called the degree (or multiplicity) of the solution, as defined in section 9.2.

Définition 37. *We say that a configuration* $P_0 = (\rho_1^0, \rho_2^0, \rho_3^0, B_x^0, B_y^0, \alpha_x^0, \alpha_y^0)$ *of the 3-rpr manipulator is singular if and only if* $(B_x^0, B_y^0, \alpha_x^0, \alpha_y^0)$ *is a solution of degree greater or equal to* 2 *of :*

$$\mathbf{E}((\rho_1^0, \rho_2^0, \rho_3^0), \mathbf{X}) = \begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}^T$$

□

To find the singular configurations, we use the Jacobian criterion.

Théorème 12. *Let* $p_1, \ldots, p_m$ *be polynomials of* $\mathbb{C}[x_1, \ldots, x_n]$ *admitting a finite set of common complex roots. Let* J *be the Jacobian matrix :*

$$\begin{bmatrix} \frac{\partial p_1}{\partial x_1} & \cdots & \frac{\partial p_1}{\partial x_n} \\ \vdots & & \vdots \\ \vdots & & \vdots \\ \frac{\partial p_m}{\partial x_1} & \cdots & \frac{\partial p_m}{\partial x_n} \end{bmatrix}$$

If $M_1, \ldots, M_{\binom{m}{n}}$ *denote the* $n \times n$ *minors of* J*, then the roots of degree greater than* 2 *of the system* $p_1 = 0, \ldots, p_m = 0$ *are exactly the roots of :*

$$\begin{cases} p_1 = 0, \ldots, p_m = 0 \\ M_1 = 0, \ldots, M_{\binom{m}{n}} \end{cases}$$

□

Applying the Jacobian criterion ([35]) on the polynomial system 9.4, we deduce that the singular configurations of the cuspidal manipulator are exactly the solutions of the system :

$$\begin{cases} \mathbf{E}(\mathbf{L}, \mathbf{X}) = \begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}^T \\ \det(\frac{\partial \mathbf{E}}{\partial \mathbf{X}}) = 0 \end{cases} \tag{9.5}$$

Remarque 32. *The solutions to Equations (9.4) of degree* 2 *are solutions of degree* 1 *to Equations (9.5), while the solutions of degree greater than* 3 *in Equations (9.4) have a degree greater than* 2 *in Equations (9.5).*

Moreover, using Gröbner basis computations to eliminate variables with the FGb software ([128]), a polynomial in the parametric variables $\mathbf{L}$, denoted P_{sing}, can be computed. Its solutions are exactly the sets of values of lengths for which the manipulator admits singular configurations.

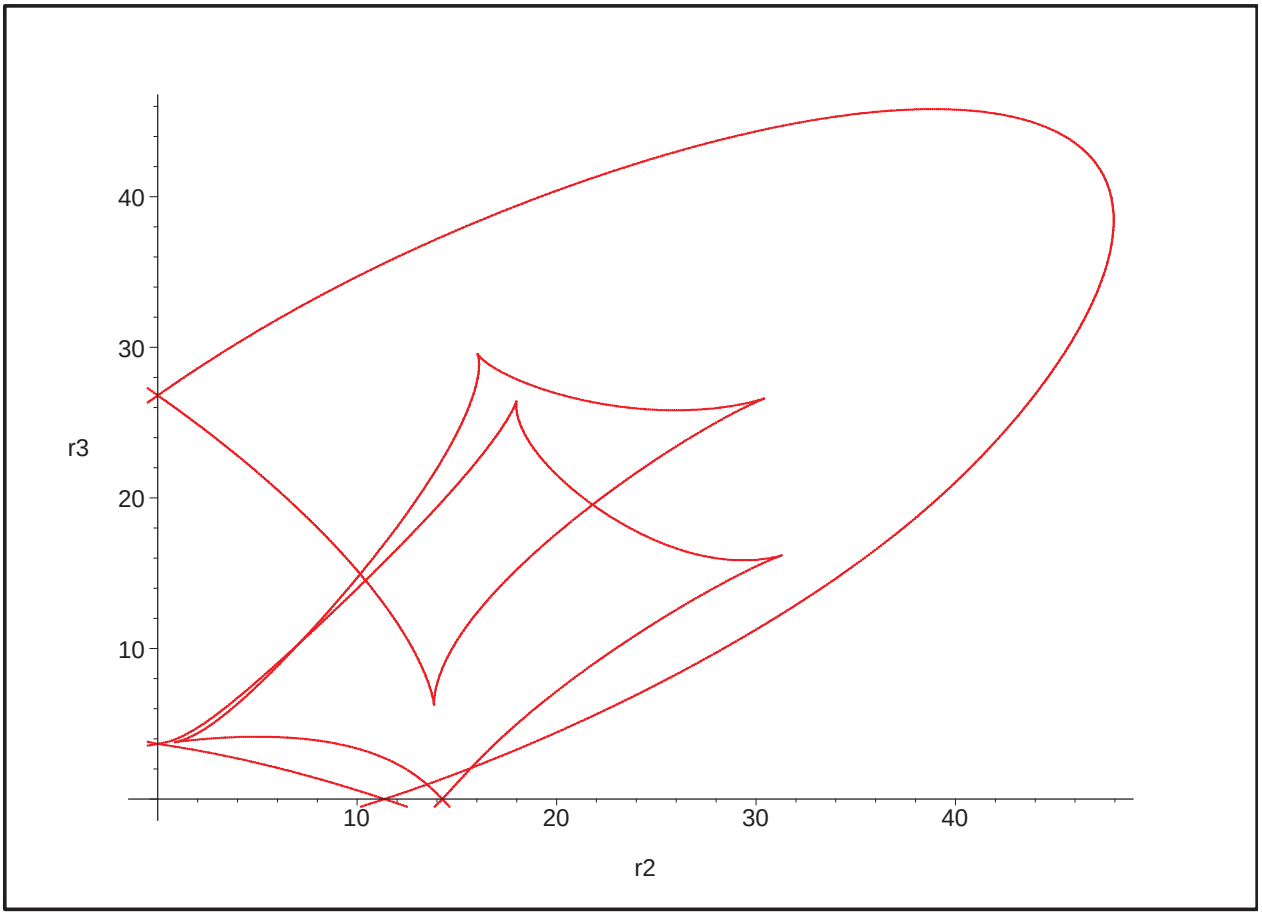


FIG. 9.2 – Singular curve for $\rho_1 = 14.98$

Example We show here the results of our computation for the manipulator presented in [68, 99, 145, 100]. The geometric parameters of this 3-rpr robot are :

$$\begin{aligned} A_1 &= (0,0) & d_1 &= 17.04 \\ A_2 &= (15.91,0) & d_2 &= 16.54 \\ A_3 &= (0,10) & d_3 &= 20.84 \end{aligned} \tag{9.6}$$

By specifying these values in Equations (9.5), we obtain a system, the solutions of which are exactly the singular configurations of the studied manipulator. By eliminating the variables $\mathbf{X}$ with Gröbner bases computation, we obtain a polynomial P_{sing} in $\mathbf{L}$, of degree 24. The zeros of this polynomial define a surface in the space of parameters. By specifying $\rho_1 = 14.98$ as in [145, 99], the corresponding slice of zeroes of P can be plotted. The same curve as in [145, 99] can be observed Figure 9.2.

9.3.3 Cuspidal configurations

Cuspidal configurations are associated with second-order degeneracies that appear for triply coalesced configurations. As shown in [99, 145], these configurations play an important role in path planning.

To find cuspidal configurations, the ideas of [99, 145] was to analyze the kernels of the matrices in the first and second order terms of Equ. (3). It allowed the authors to find automatically the cuspidal configurations when L_1 is specified as a numerical value. However it did not allow them to describe these configurations precisely. We introduce a complete certified description of the cuspidal configurations, which may be seen as an extension of the ideas introduced in [108, 27]. In particular, our approach allows us to find cuspidal configurations that were missed in the previous papers, and to certify that we did find them all.

Modelling As for the singular points, we define algebraically the cuspidal configurations.

Définition 38. *The configuration* $P_0 = (\rho_1^0, \rho_2^0, \rho_3^0, B_x^0, B_y^0, \alpha_x^0, \alpha_y^0)$ *of the 3-rpr manipulator is said cuspidal if and only if* $(B_x^0, B_y^0, \alpha_x^0, \alpha_y^0)$ *is a solution of degree higher or equal to* 3 *of*

$$\mathbf{E}((\rho_1^0, \rho_2^0, \rho_3^0), \mathbf{X}) = \begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}^T$$

.

□

In Section 9.3.2, the Jacobian criterion allowed us to select the configurations of degree higher than 2. However, we now want to compute the configurations of degree higher than 3. Fortunately, we saw in Remark 32 that these configurations are exactly the roots of degree higher than 2 of Equ. (9.5). Thus we can use the Jacobian criterion on Equations (9.5) to get a system describing exactly the cuspidal configurations.

Let $J = \det(\frac{\partial \mathbf{E}}{\partial \mathbf{X}})$, then the following system of 9 equations defines exactly the cuspidal configurations of the 3-rpr manipulator :

	ρ_2	ρ_3	B_x	B_y	α_x	α_y
1	0.845	3.777	5.336	-13.997	0.633	0.773
2	13.851	6.260	-14.963	0.698	0.998	-0.045
3	31.276	16.178	-6.104	13.679	-0.543	-0.839
4	17.988	26.446	14.721	-2.769	-0.985	0.167
5	30.449	26.619	-10.363	10.816	.537	0.843
6	16.027	29.566	14.437	3.995	0.999	-0.010

TAB. 9.1 – The 6 cuspidal configurations (roots of Equations 9.7) for $\rho_1 = 14.98$

$$\begin{cases} \mathbf{E}(\mathbf{L},\mathbf{X}) = \begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}^T \\ J = 0 \\ \det\left(\begin{bmatrix} \frac{\partial \mathbf{E}_1}{\partial \mathbf{X}}^T & \frac{\partial \mathbf{E}_2}{\partial \mathbf{X}}^T & \frac{\partial \mathbf{E}_3}{\partial \mathbf{X}}^T & \frac{\partial J}{\partial \mathbf{X}}^T \end{bmatrix}\right) = 0 \\ \det\left(\begin{bmatrix} \frac{\partial \mathbf{E}_1}{\partial \mathbf{X}}^T & \frac{\partial \mathbf{E}_2}{\partial \mathbf{X}}^T & \frac{\partial \mathbf{E}_4}{\partial \mathbf{X}}^T & \frac{\partial J}{\partial \mathbf{X}}^T \end{bmatrix}\right) = 0 \\ \det\left(\begin{bmatrix} \frac{\partial \mathbf{E}_1}{\partial \mathbf{X}}^T & \frac{\partial \mathbf{E}_3}{\partial \mathbf{X}}^T & \frac{\partial \mathbf{E}_4}{\partial \mathbf{X}}^T & \frac{\partial J}{\partial \mathbf{X}}^T \end{bmatrix}\right) = 0 \\ \det\left(\begin{bmatrix} \frac{\partial \mathbf{E}_2}{\partial \mathbf{X}}^T & \frac{\partial \mathbf{E}_3}{\partial \mathbf{X}}^T & \frac{\partial \mathbf{E}_4}{\partial \mathbf{X}}^T & \frac{\partial J}{\partial \mathbf{X}}^T \end{bmatrix}\right) = 0 \end{cases} \tag{9.7}$$

Remarque 33. *These equations are not algebraically independent. In particular, even if the number of equations is* 9 *and the number of variables is* 7*, the set of solutions is a curve of dimension* 1 *in* $\mathbb{R}^7$*.*

The advantage of the Equations (9.7) is that the degrees of the equations involved are smaller than 5. This will allow us to complete the computations to certify our analysis of the curve in Section 9.3.4.

Example Using the robot specified by the lengths and points of Equ. (9.6), its triple points are exactly the solutions of Equations (9.7).

Moreover, when we specify the length ρ_1, Equ. (9.7) has finitely many solutions. Using the methods of real solving for 0-dimensional systems of the software RS ([128]), we can easily find the roots of Equ. (9.7) for any given ρ_1.

In particular, for $\rho_1 = 14.98$, we get 6 triple points (see Table 9.1), which confirms the results of [145].

9.3.4 Cusps analysis

Equations (9.7) define the cuspidal configurations of the robot. Without further computations, these equations are not sufficient to describe the geometry of the triple roots of the 3-rpr manipulator. In [99, 145], the authors observed that the set of cuspidal configurations is finite in slices of the robot's joint space defined by given values of ρ_1. This leads to the conjecture that the set of cuspidal configurations forms a curve of dimension 1 in the full space of the parameters ρ_1, ρ_2, ρ_3. Furthermore, the authors of [145] described the number of cuspidal configurations for discrete values of ρ_1 in $\mathbb{R}$. This allowed them to find configurations that were omitted in previous works.

In this section, we will give a certified and exhaustive description of the number of cuspidal configurations with respect to the values of ρ_1. In particular, this study allows us to find values of ρ_1 for which the 3-rpr manipulator has 10 cuspidal configurations, while previous works never observed more than 8 cuspidal configurations.

The dimension of the set of solutions of Equ. 9.7 in the complex field is 1. This can be checked by computing and analysing the Gröbner bases of Equ. 9.7 (see [28, chapter 9] for more details).

To describe geometrically the solutions of Equ. 9.7 with respect to the values of ρ_1, we will consider it as a parametric system where :

- the single parameter is ρ_1
- the unknowns are $\rho_2, \rho_3, B_x, B_y, \alpha_x, \alpha_y$

We follow the work of [87, 27, 41] to describe the roots of a parametric system. Our process has 2 steps :

- We first compute its *minimal discriminant variety*. The definition of the discriminant variety in the general case is given in Appendix.
- Then, we compute the number of solutions for sample parameter's values chosen outside the discriminant variety

Discriminant variety of the cuspidal configurations We consider the Equ. 9.7 as a system parametrized with ρ_1. In this case, its minimal discriminant variety is a finite set of values of ρ_1 denoted by :

$$P_{DV} = \{a_1, \ldots, a_k\} \subset \mathbb{R}, k > 0$$

The main property of the discriminant variety is that for each value of ρ_1 in an interval $]a_i, a_{i+1}[$, the Equ. 9.7 have the same number of distinct real solutions.

The points of the discriminant varieties are the real roots of univariate polynomials. The lines ρ_1 of the table 9.2 show numerical approximations of these roots, while the full univariate polynomials may be found in appendix.

The lines #Cusp gives the number of cuspidal configurations when ρ_1 is in an interval of the shape $]a_i, a_{i+1}[$, where the a_i are the real values of ρ_1 defining the discriminant variety P_{DV}.

Number of cuspidal configurations Using the main property of the discriminant variety, we know that to count the number of cuspidal configurations outside the discriminant variety,

#Cusp		0		2		4		2		
ρ_1	0.000	]——[	0.148	]——[	1.655	]——[	1.660	]——[		
#Cusp		4		6		8		6		
ρ_1	2.261	]——[	2.975	]——[	9.18678	]——[	9.18686*	]——[		
#Cusp		8		6		8		6		
ρ_1	9.257662	]——[	9.257677*	]——[	10.9056649	]——[	10.9056683*	]——[		
#Cusp		8		6		8		6		
ρ_1	14.579115749	]——[	14.579115757*	]——[	20.555	]——[	20.562	]——[		
#Cusp		8		10		8		6		
ρ_1	26.786	]——[	28.094	]——[	28.107	]——[	28.257	]——[		
#Cusp		8		6		2				
ρ_1	30.740	]——[	30.779	]——[	30.946	]——————				

* the precision of these values has been increased to distinguish them

TAB. 9.2 – Discriminant variety of the cuspidal configurations (Equ. 9.7) w.r.t. ρ_1 ; the numerical value are truncated

it is sufficient to compute a finite set of sampling points in the complementary of P_{DV} and solve the corresponding zero-dimensional systems. More precisely, we choose a value v_i in each interval of the shape :

$$]a_i, a_{i+1}[, \text{ such that } a_i, a_{i+1} \text{ are consecutive reals of } P_{DV}$$

and compute the number of solution of Equ. 9.7 when $\rho_1 = v_i$. Moreover, we choose a value v_{k+1} in $]a_k, +\infty[$, and count the number of solution of Equ. 9.7 when $\rho_1 = v_{k+1}$. The results of these computations are summarized in the lines #Cusp of Table 9.2. To count the number of real solutions of Equ. 9.7 when $\rho_1 = v_i$, we use the real solver *RS* ([128]).

From Table 9.2 we conclude that, asymptotically, the manipulator has 2 cuspidal configurations, and that this number is stable as soon as ρ_1 is greater than 31. Moreover, we can observe that the robot may have up to 10 cuspidal configurations when ρ_1 is in the interval $]28.095, 28.107[$. Figure 9.3 shows the singular curve of the parallel robot for $\rho_1 = 28.10$ and the corresponding 10 cuspidal configurations.

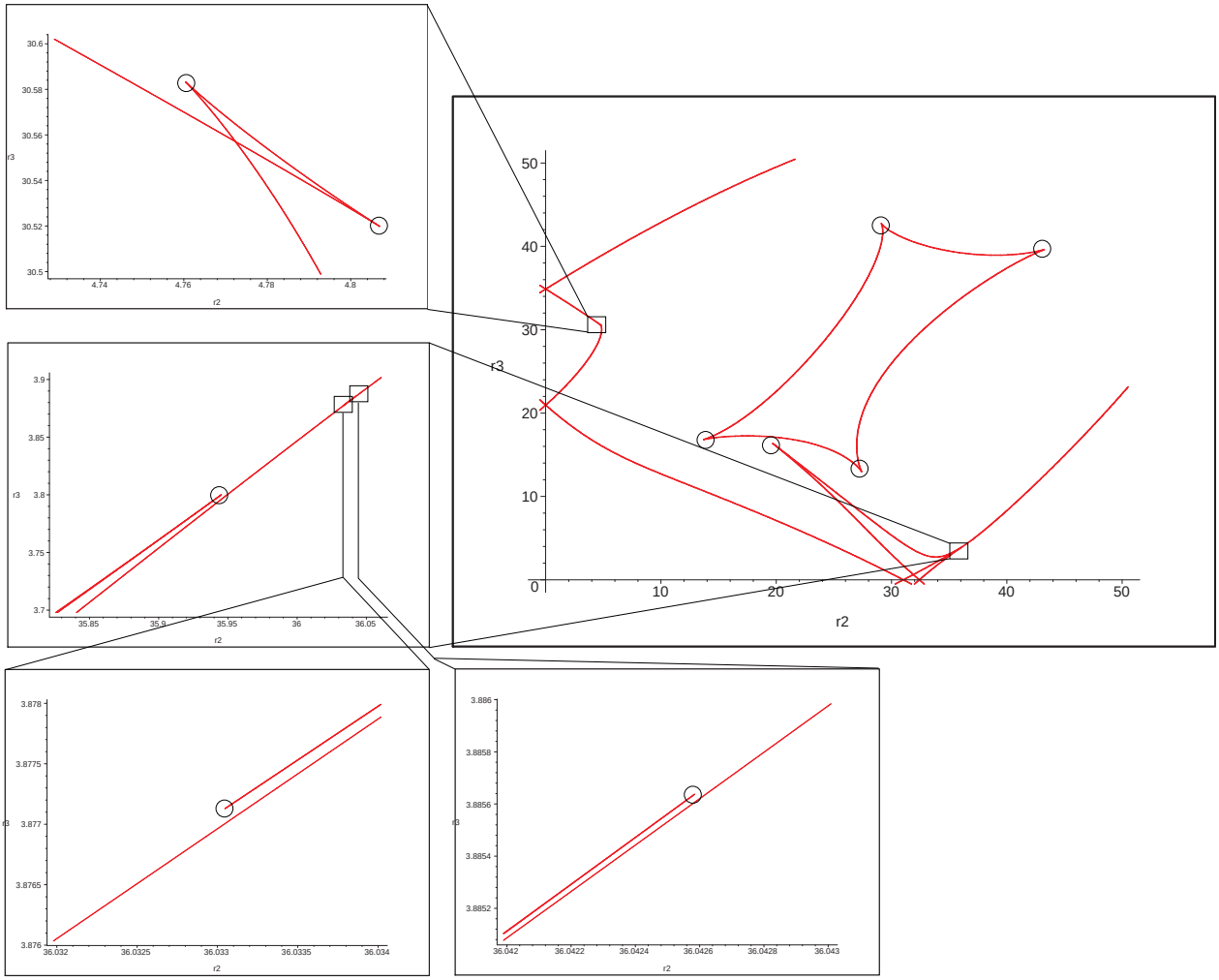


FIG. 9.3 – Singular curve for $\rho_1 = 28.10$. The circles show the 10 cuspidal points in this configuration.

Chapitre 10

Surface d'Enneper

We show here an example of minimal discriminant varieties application in our framework. It will allow us to prove that the real parametrization of the Enneper surface matches its real implicit form. In [34] the author solves this problem with a combination `REDLOG`,`QEPCAD` and `QERRC`. Through the process, he has to simplify formulas whose textual representation contains approximatively 500 000 characters. We will see that our framework allows us to use *minimal* discriminant varieties to solve this problem. Notably, this allows us to keep formulas small. The following computations are done with the `Maple` package `DV`, which uses `FGb` to carry out the elimination function. We also use the factorization functions of `Maple` to take the square-free part of the polynomials given in the input, and to simplify the output. Finally `RS` and the `Maple` package `RAG` allows us to treat the discriminant varieties we compute. All these software are available in the Salsa Software Suite [128].

When E and F are two lists of polynomials, T a list of parameters and X a list of unknowns, we denote by

$$\mathbf{DV}(E, F, T, X)$$

the discriminant variety of the parametric system $S : (p = 0)_{p\in E} \wedge (q \neq 0)_{q\in F}$.

Definition of the Enneper surface

The real Enneper surface $\mathcal{E} \subset \mathbb{R}^3$ has a parametric definition :

$$\mathcal{E} = \Big\{(x(u,v), y(u,v), z(u,v)) \quad | \quad (u,v) \in \mathbb{R}^2\Big\}$$

$$\begin{array}{rcl} x(u,v) & = & 3u + 3uv^2 - u^3 \\ y(u,v) & = & 3v + 3u^2v - v^3 \\ z(u,v) & = & 3u^2 - 3v^2 \end{array}$$

We will also consider the graph of the Enneper surface $\mathcal{E}_g \subset \mathbb{R}^5$ defined as follows :

$$\mathcal{E}_g = \Big\{(x(u,v), y(u,v), z(u,v), u, v) \quad | \quad (u,v) \in \mathbb{R}^2\Big\}$$

Beside, a Gröbner basis computation returns easily its implicit Zarisky closure $\overline{\mathcal{E}}$ [28, 34] :

$$\overline{\mathcal{E}} = \left\{(x,y,z) \in \mathbb{R}^3 \quad | \quad p(x,y,z) = 0\right\}$$

$$\begin{aligned} p(x,y,z) \;=\; & -19683x^6 + 59049x^4y^2 - 10935x^4z^3 - 118098x^4z^2 + 59049x^4z - 59049x^2y^4 \\ & -56862x^2y^2z^3 - 118098x^2y^2z - 1296x^2z^6 - 34992x^2z^5 - 174960x^2z^4 \\ & +314928x^2z^3 + 19683y^6 - 10935y^4z^3 + 118098y^4z^2 + 59049y^4z + 1296y^2z^6 \\ & -34992y^2z^5 + 174960y^2z^4 + 314928y^2z^3 + 64z^9 - 10368z^7 + 419904z^5 \end{aligned}$$

Discriminant varieties

The main idea to compare $\mathcal{E}_\}$ and $\overline{\mathcal{E}}$ is in a first step to compute the union of their discriminant varieties, V. In a second step we compare $\mathcal{E}_g$ and $\overline{\mathcal{E}}$ on a finite number of well chosen test points outside of V. Finally, the properties of the discriminant variety ensure us that the result of our comparison on these test points holds for every points outside of V.

More precisely, $\mathcal{E}_g$ and $\overline{\mathcal{E}}$ are both algebraic varieties of dimension 2. Thus we choose a common subset of 2 variables, x and y for example, which will be the *parameters* for the two discriminant varieties :

$$\begin{aligned} V_1^{xy} &:= \mathbf{DV}(\ [x - x(u,v), y - y(u,v), z - z(u,v)]\ ,\ [\ ]\ ,\ [x,y]\ ,\ [z,u,v]\ ) \\ V_2^{xy} &:= \mathbf{DV}(\ [p(x,y,z)]\ ,\ [\ ]\ ,\ [x,y]\ ,\ [z]\ ) \end{aligned}$$

The number of equations equals the number of unknowns in both case and our algorithm returns a non trivial variety for both systems. This ensures us that the two systems are *generically simple*. Here are the results of the computations, which lasted less than 1 second on a 2.8 GHz Intel Pentium cpu :

$$\begin{aligned} V_1^{xy} = \; & \mathbf{V}(y^6 + 60y^4 + 768y^2 - 4096 + 3x^2y^4 - 312x^2y^2 + 768x^2 + 3x^4y^2 + 60x^4 + x^6) \\ & \cup \mathbf{V}(x^6 + 48x^4 + 3x^4y^2 - 336x^2y^2 + 3x^2y^4 + 768x^2 + 4096 + 768y^2 + 48y^4 + y^6) \end{aligned}$$

$$\begin{aligned} V_2^{xy} = \; & \mathbf{V}(y^6 + 60y^4 + 768y^2 - 4096 + 3x^2y^4 - 312x^2y^2 + 768x^2 + 3x^4y^2 + 60x^4 + x^6) \\ & \cup \mathbf{V}(x^6 + 48x^4 + 3x^4y^2 - 336x^2y^2 + 3x^2y^4 + 768x^2 + 4096 + 768y^2 + 48y^4 + y^6) \\ & \cup \mathbf{V}(x-y) \cup \mathbf{V}(y) \cup \mathbf{V}(x+y) \cup \mathbf{V}(x) \end{aligned}$$

We denote by $\pi_{xy} : \mathbb{R}^3 \to \mathbb{R}^2$ the canonical projection. Then the properties of the discriminant variety ensure us that for each connected component $\mathcal{C}$ of $\mathbb{R}^2 \setminus (V_1^{xy} \cup V_2^{xy})$, $(\pi_{xy}^{-1}(\mathcal{C}) \cap \mathcal{E}, \pi_{xy})$ and $(\pi_{xy}^{-1}(\mathcal{C}) \cap \overline{\mathcal{E}}, \pi_{xy})$ are both analytic covering. Moreover, $\mathcal{E} \subset \overline{\mathcal{E}}$. Thus if $\mathcal{C}$ is a connected component of $\mathbb{R}^2 \setminus (V_1^{xy} \cup V_2^{xy})$, we get the following property :

$$\exists p \in \mathcal{C}, \pi_{xy}^{-1}(p) \cap \mathcal{E} = \pi_{xy}^{-1}(p) \cap \overline{\mathcal{E}} \iff \forall p \in \mathcal{C}, \pi_{xy}^{-1}(p) \cap \mathcal{E} = \pi_{xy}^{-1}(p) \cap \overline{\mathcal{E}}$$

This allows us to prove that $\mathcal{E}$ and $\overline{\mathcal{E}}$ are equal above $\mathbb{R}^2 \setminus (V_1^{xy} \cup V_2^{xy})$: we take one point p in each connected component of $\mathbb{R}^2 \setminus (V_1^{xy} \cup V_2^{xy})$, and check that the number of real solutions of $\pi_{xy}^{-1}(p) \cap \mathcal{E}$ and of $\pi_{xy}^{-1}(p) \cap \overline{\mathcal{E}}$ is the same. We use the `RAG` package to get one

point in each connected component and RS to solve the corresponding zero dimensional real systems. This allows us to prove that

$$\pi_{xy}^{-1}(\mathbb{R}^2 \setminus (V_1^{xy} \cup V_2^{xy})) \cap \mathcal{E} = \pi_{xy}^{-1}(\mathbb{R}^2 \setminus (V_1^{xy} \cup V_2^{xy})) \cap \overline{\mathcal{E}}$$

In order to get more information, we repeat this process using respectively the discriminant varieties on the parameter set $\{x, z\}$ and $\{y, z\}$. This leads to the following computations :

$$\begin{array}{l} V_1^{xz} := \mathbf{DV}(\ [x - x(u,v), y - y(u,v), z - z(u,v)]\ ,\ [\ ]\ ,\ [x,z]\ ,\ [y,u,v]\ ) \\ V_2^{xz} := \mathbf{DV}(\ [p(x,y,z)]\ ,\ [\ ]\ ,\ [x,z]\ ,\ [y]\ ) \end{array}$$

and

$$\begin{array}{l} V_1^{yz} := \mathbf{DV}(\ [x - x(u,v), y - y(u,v), z - z(u,v)]\ ,\ [\ ]\ ,\ [y,z]\ ,\ [x,u,v]\ ) \\ V_2^{yz} := \mathbf{DV}(\ [p(x,y,z)]\ ,\ [\ ]\ ,\ [y,z]\ ,\ [x]\ ) \end{array}$$

The result is shown on Figure 10.1.

Then we compute as above one point in each connected component of the complementary, and this allows us to prove that :

$$\pi_{xz}^{-1}(\mathbb{R}^2 \setminus (V_1^{xz} \cup V_2^{xz})) \cap \mathcal{E} = \pi_{xz}^{-1}(\mathbb{R}^2 \setminus (V_1^{xz} \cup V_2^{xz})) \cap \overline{\mathcal{E}}$$

and

$$\pi_{yz}^{-1}(\mathbb{R}^2 \setminus (V_1^{yz} \cup V_2^{yz})) \cap \mathcal{E} = \pi_{yz}^{-1}(\mathbb{R}^2 \setminus (V_1^{yz} \cup V_2^{yz})) \cap \overline{\mathcal{E}}$$

Using the following notations :

$$\begin{array}{l} V^{xy} := \pi_{yz}^{-1}(V_1^{xy} \cup V_2^{xy}) \\ V^{xz} := \pi_{xz}^{-1}(V_1^{xz} \cup V_2^{xz}) \\ V^{yz} := \pi_{yz}^{-1}(V_1^{yz} \cup V_2^{yz}) \end{array}$$

it remains us to check what happens above each component of

$$V^{xy} \cap V^{xz} \cap V^{yz}$$

An idea is to set apart the linear components from the others. We introduce

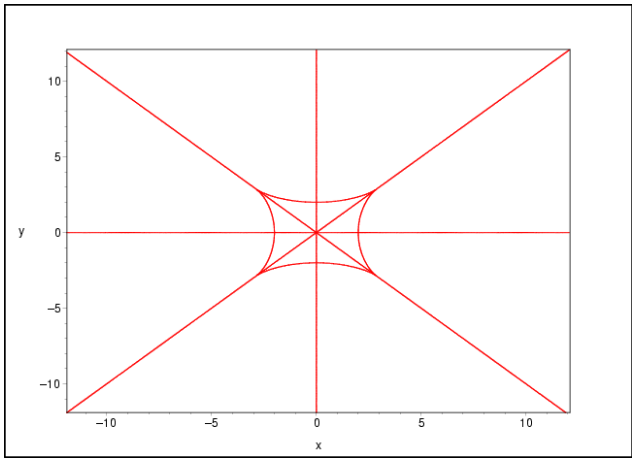
$$V_L := \mathbf{V}(x + y) \cup \mathbf{V}(x - y) \cup \mathbf{V}(x) \cup \mathbf{V}(y) \cup \mathbf{V}(z)$$

and denote respectively $V^{xy} \setminus V_L$,$V^{xz} \setminus V_L$ and $V^{yz} \setminus V_L$ by $\widetilde{V^{xy}}$, $\widetilde{V^{xz}}$ and $\widetilde{V^{yz}}$. Using the RAGlib, we verify that

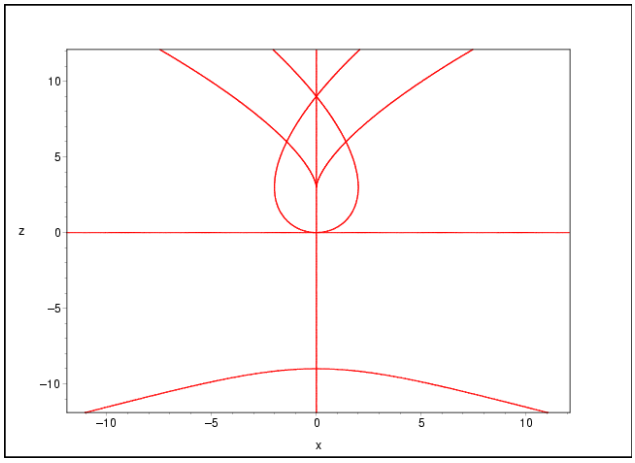
$$\widetilde{V^{xy}} \cap \widetilde{V^{xz}} \cap \widetilde{V^{yz}}$$

has actually no real points.

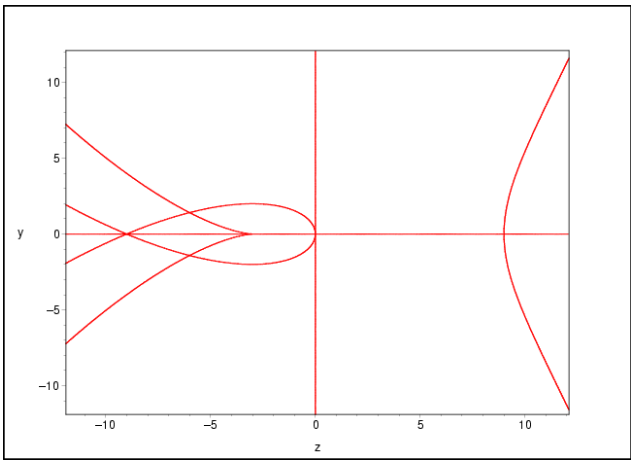
It remains us to check what happens on each of the 5 linear components of V_L. The intersection of $\mathcal{E}_g$ or $\overline{\mathcal{E}}$ with a linear component P may be seen as a linear substitution of a variable. This operation produces 5 pairs of varieties of dimension 2 (Table 10.1). To check their equality, we use the same strategy as above and compute the 5 discriminant varieties with 1 parameter,3 unknowns of $K_1, \ldots, K_5$, respectively $V_{K_1}, \ldots, V_{K_5}$, and the 5 discriminant



$V_1^{xy} \cup V_2^{xy}$



$V_1^{xz} \cup V_2^{xz}$



$V_1^{yz} \cup V_2^{yz}$

FIG. 10.1 – The discriminant varieties for the three possible sets of parameters

varieties with 1 parameter,1 unknown of $L_1, \ldots, L_5$, respectively $V_{L_1}, \ldots, V_{L_5}$. We check that $K_i = L_i$ for each point by connected component of the complementary of $V_{K_i} \cup V_{L_i}$, in less than 1 second. And at last we intersect again the varieties with their discriminant varieties, which reduces the problem to compare 5 pairs of zero dimensional systems. Thus we check that the equality holds for the finitely many points considered. Finally this allows us to conclude that $\mathcal{E} = \overline{\mathcal{E}}$.

	$\mathcal{E}_g$				
W	$\mathbf{V}(x)$	$\mathbf{V}(y)$	$\mathbf{V}(z)$	$\mathbf{V}(y+x)$	$\mathbf{V}(y-x)$
$\mathcal{E}_g \cap W$	K_1	K_2	K_3	K_4	K_5
$System$	$\begin{cases} 0-x(u,v) \\ y-y(u,v) \\ z-z(u,v) \end{cases}$	$\begin{cases} x-x(u,v) \\ 0-y(u,v) \\ z-z(u,v) \end{cases}$	$\begin{cases} x-x(u,v) \\ y-y(u,v) \\ 0-z(u,v) \end{cases}$	$\begin{cases} x-x(u,v) \\ -x-y(u,v) \\ z-z(u,v) \end{cases}$	$\begin{cases} x-x(u,v) \\ x-y(u,v) \\ z-z(u,v) \end{cases}$
$Parameter$	z	z	x	x	x
$Unknowns$	y,u,v	x,u,v	y,u,v	z,u,v	z,u,v
$Minimal$ $Discriminant$ $Variety$	$V_{K_1} =$ $\mathbf{V}(z) \cup \mathbf{V}(z-3)$ $\cup \mathbf{V}(z-9)$	$V_{K_2} =$ $\mathbf{V}(z) \cup \mathbf{V}(z+3)$ $\cup \mathbf{V}(z+9)$	$V_{K_3} =$ $\mathbf{V}(x) \cup \mathbf{V}(x^2+2)$	$V_{K_4} = V_{K_5} =$ $\mathbf{V}(x+4) \cup \mathbf{V}(x-4) \cup \mathbf{V}(x^2-8)$ $\cup \mathbf{V}(x^2+2)$	

	$\overline{\mathcal{E}}$				
W	$\mathbf{V}(x)$	$\mathbf{V}(y)$	$\mathbf{V}(z)$	$\mathbf{V}(y+x)$	$\mathbf{V}(y-x)$
$\overline{\mathcal{E}} \cap W$	L_1	L_2	L_3	L_4	L_5
$System$ $(sqfr =$ $squarefree)$	$sqfr(p(0,y,z))$	$sqfr(p(x,0,z))$	$sqfr(p(x,y,0))$	$sqfr(p(x,-x,z))$	$sqfr(p(x,x,z))$
$Parameter$	z	z	x	x	x
$Unknown$	y	x	y	z	z
$Minimal$ $Discriminant$ $Variety$	$V_{L_1} = \mathbf{V}(z+9)$ $\cup \mathbf{V}(z) \cup \mathbf{V}(z-3)$ $\cup \mathbf{V}(z-9)$	$V_{L_2} = \mathbf{V}(z-9)$ $\cup \mathbf{V}(z) \cup \mathbf{V}(z-3)$ $\cup \mathbf{V}(z+9)$	$V_{L_3} =$ $\mathbf{V}(x)$	$V_{L_4} = V_{L_5} =$ $\mathbf{V}(x+4) \cup \mathbf{V}(x-4) \cup \mathbf{V}(x^2-8)$ $\cup \mathbf{V}(x)$	

TAB. 10.1 – Discriminant varieties of the sub varieties

Chapitre 11

Conclusion

La variété discriminante est un outil théorique permettant de discriminer les paramètres d'un systèmes en fonction du nombre de ses solutions. Moins expressif qu'un décomposition cylindrique algébrique, cette variété est cependant suffisante pour la résolution de nombreuses applications.

D'un point de vue théorique, nous avons donné une borne fine sur le degré de la variété discriminante minimale d'un système bien posé. Nous avons aussi montré que dans ce cas, son calcul se réduit au calcul d'élimination de variables.

Pour traiter le cas des systèmes paramétrés généraux nous avons développé un algorithme de décomposition régulière. Cet algorithme a été conçu avec plusieurs objectifs :

- il permet de fournir une décomposition équidimensionnelle d'un idéal donné
- il permet de séparer les composantes de dimensions maximale des composantes de petites dimensions, sans décomposition supplémentaire
- chaque composante est représentée sous la forme d'une suite localement régulière, ce qui permet ainsi d'utiliser le critère jacobien pour calculer les points critiques et singuliers de cette composante, ou encore pour calculer son radical si elle ne l'est pas
- l'algorithme est basé sur le calcul de saturations pour séparer les composantes de différentes dimension

En particulier, de nombreux algorithmes s'appuyant sur la factorisation polynômiale pour décomposer un idéal nécessitent le calcul d'un polynôme d'élimination qui peut dans certains cas être une étape bloquante. L'algorithme présenté ici est une alternative efficace en pratique permettant de contourner ce problème.

Stratégies adaptées

Étant donné un système paramétré S, sa variété discriminante minimale se compose des quatre composantes $V_{inf}(S), V_{ineq}(S), V_{crit}(S), V_{sd}(S)$. En pratique, le calcul des composantes

$V_{crit}(S)$ et $V_{sd}(S)$ sont souvent les plus coûteuses en temps et en mémoire. De plus on a vu en première partie que l'on pouvait calculer les composantes $V_{inf}(S)$ et $V_{ineq}(S)$ en un temps simplement exponentiel en le nombre de variables, que le système considéré soit bien posé ou seulement génériquement zéro dimensionnel.

En supposant que l'on connaît les idéaux I_{inf} et I_{ineq} des variétés $V_{inf}(S)$ et $V_{ineq}(S)$, on veut calculer les composantes $V_{crit}(S)$ et $V_{sd}(S)$.

De manière générale, ces composantes peuvent se calculer dès lors que l'on connaît la composante principale I_p du système considéré. Dans ce cas, on peut appliquer le critère jacobien sur I_p pour obtenir $V_{crit}(S)$, et $V_{sd}(S)$ peut s'écrire :

$$V_{sd}(S) := \varphi_{\mathbb{Q}[t_1,\ldots,t_s]} \circ \zeta_{I_{inf}} \circ \zeta_{Ip}(I_S)$$

Dans ces conditions, le calcul de I_p et des saturations d'idéaux ci-dessus permette de calculer $V_{sd}(S)$.

La fonction Drm-Sep, variante de l'algorithme général de décomposition régulière, permet précisément de calculer I_p et d'effectuer la saturation de I_S par I_p de manière efficace.

Ce n'est cependant pas la seule stratégie possible.Au vu de la diversité des exemples provenant d'applications, il est important de pouvoir disposer de différentes stratégies de calcul, tirant au mieux parti des propriétés vérifiées par le système paramétré considéré. Par exemple :

- si le système considéré est donné sous forme d'ensemble triangulaire, des algorithmes de décompositions triangulaires pourront s'avérer très efficaces
- si le système est donné sous la forme d'un suite pseudo-régulière, on pourra préféré l'algorithme de décomposition régulière présenté dans cette thèse
- si les polynômes du système sont donné sous la forme de programmes d'évaluation, on pourra se tourner vers les algorithmes de décompositions comme la *résolution géométrique*.

Extension

Lorsque le système considéré S n'est pas génériquement zéro dimensionnel, on est confronté à deux possibilités :

i) S n'admet génériquement pas de solutions complexes

ii) S admet génériquement une infinité de solutions complexes

Projection des solutions complexes non dense. Le cas i) est inévitable si l'on veut décrire les solutions au-dessus de la variété discriminante d'un système donné S. En effet pour ce faire, on ajoute les polynômes de la variété discriminante au système initial, ce qui constitue un nouveau système S' dont la projection des solutions n'est pas dense puisqu'elle est incluse dans la variété discriminante minimale de S.

D'un point de vue algorithmique, ce cas n'est fondamentalement pas plus difficile à traiter que le cas génériquement zéro dimensionnel. En particulier, au moins deux stratégies sont possibles.

La première stratégie consiste à considérer un sous-ensemble des paramètres de cardinal égal à la dimension complexe de solutions de S'. Ainsi, on se retrouve dans le cas des systèmes génériquement zéro dimensionnels, et on peut alors réutiliser directement les outils développés pour ce cas.

En deuxième approche, on peut directement calculer la variété discriminante de S', définie comme sous-variété stricte de la projection des solutions de S'. En particulier nous devons alors considérer une nouvelle composante $V_{sing}(S)$, correspondant essentiellement à un certain idéal jacobien pour le calcul de la variété discriminante minimale (voir [87] pour plus de détails). Les outils de décompositions présentés dans cette thèse restent bien adaptés pour calculer une telle variété discriminante.

Génériquement une infinité de solutions complexes. La situation *ii*) est plus difficile à gérer. Dans le cadre du travail publié dans [9], l'auteur étudie un système paramétré S possédant une infinité de solutions complexes, et veut caractériser l'ensemble des paramètres où le système n'admet pas de solutions réels. De manière plus général, on s'intéresse ici à discriminer les paramètres en fonction de la *dimensions réelle* des solutions de S. Dans le cadre des modélisations admettant génériquement un nombre infini de solutions complexes, la classification des paramètres en fonction de la dimension semble être une étape incontournable de la description des solutions réelles.

Bibliographie

[1] M.-E. Alonso, E. Becker, M.-F. Roy, and T. Wörmann. Zeros, multiplicities, and idempotents for zero-dimensional systems. In Laureano González-Vega and Tomás Recio, editors, *Algorithms in Algebraic Geometry and Applications*, volume 143 of *Progress in Mathematics*, pages 1–15. Birkhäuser Verlag, Boston-Basel-Berlin-Stuttgart, 1996. Paper in the MEGA'94 Conference (Métodos Efectivos en Geometría Algebraica = Effective Methods in Algebraic Geometry).

[2] M.-A. Ameller, B. Triggs, and L. Quan. Camera pose revisited - new linear algorithms, December 13 2000.

[3] Hirokazu Anai, Shinji Hara, and Kazuhiro Yokoyama. Sum of roots with positive real parts. In *ISSAC'05*, pages 21–28, 2005.

[4] Philippe Aubry and Marc Moreno Maza. Triangular sets for solving polynomial systems : a comparative implementation of four methods. *J. Symbolic Comput.*, 28(1-2) :125–154, 1999. Polynomial elimination—algorithms and applications.

[5] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2003.

[6] Dave Bayer and David Mumford. What can be computed in algebraic geometry ? In *Computational algebraic geometry and commutative algebra (Cortona, 1991)*, Sympos. Math., XXXIV, pages 1–48. Cambridge Univ. Press, Cambridge, 1993.

[7] David Bayer and Michael Stillman. On the complexity of computing syzygies. *J. Symbolic Comput.*, 6(2-3) :135–147, 1988. Computational aspects of commutative algebra.

[8] Thomas Becker and Volker Weispfenning. *Gröbner bases*, volume 141 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1993.

[9] Gerald Bourgeois. Algebraic systems of matrices and gröbner basis, 2007.

[10] Christopher W. Brown, M'hammed El Kahoui, Dominik Novotni, and Andreas Weber 0004. Algorithmic methods for investigating equilibria in epidemic modeling. *J. Symb. Comput*, 41(11) :1157–1173, 2006.

[11] Christopher W. Brown and Scott McCallum. On using bi-equational constraints in CAD construction. In Manuel Kauers, editor, *ISSAC '05*, pages 76–83, 2005.

[12] W. Dale Brownawell. Bounds for the degrees in the Nullstellensatz. *Ann. of Math. (2)*, 126(3) :577–591, 1987.

[13] W. Dale Brownawell. A pure power product version of the Hilbert Nullstellensatz. *Michigan Math. J.*, 45(3) :581–597, 1998.

[14] B. Buchberger. Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems. *Aequationes Math.*, 4 :374–383, 1970.

[15] Bruno Buchberger. An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *J. Symbolic Comput.*, 41(3-4) :475–511, 2006. Translated from the 1965 German original by Michael P. Abramson.

[16] Peter Bürgisser, Michael Clausen, and M. Amin Shokrollahi. *Algebraic complexity theory*, volume 315 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1997.

[17] L. Busé, M. Elkadi, and B. Mourrain. Resultant over the residual of a complete intersection. *J. Pure Appl. Algebra*, 164(1-2) :35–57, 2001. Effective methods in algebraic geometry (Bath, 2000).

[18] Laurent Busé, Mohamed Elkadi, and Bernard Mourrain. Generalized resultants over unirational algebraic varieties. *J. Symbolic Comput.*, 29(4-5) :515–526, 2000. Symbolic computation in algebra, analysis, and geometry (Berkeley, CA, 1998).

[19] Étienne Bézout. Recherches sur le degré des équations résultantes de l'évanouissement des inconnues. *Histoire de l'académie royale des sciences*, pages 288–338, 1764. Summary pp. 88-91.

[20] Massimo Caboara, Pasqualina Conti, and Carlo Traverso. Yet another ideal decomposition algorithm. In *Applied algebra, algebraic algorithms and error-correcting codes (Toulouse, 1997)*, volume 1255 of *Lecture Notes in Comput. Sci.*, pages 39–54. Springer, Berlin, 1997.

[21] John Canny. Some algebraic and geometric computations in pspace. In *STOC '88 : Proceedings of the twentieth annual ACM symposium on Theory of computing*, pages 460–469, New York, NY, USA, 1988. ACM.

[22] John Canny. Generalised characteristic polynomials. *J. Symbolic Comput.*, 9(3) :241–250, 1990.

[23] A. L. Chistov and D. Y. Grigoriev. Subexponential time solving systems of algebraic equations. i,ii. Technical report, Steklov Institute, Leningrad, 1983.

[24] Alexander L. Chistov and Dima Grigoriev. Complexity of quantifier elimination in the theory of algebraically closed fields. In Michal Chytil and Václav Koubek, editors, *Mathematical Foundations of Computer Science 1984, Praha, Czechoslovakia, September 3-7, 1984, Proceedings*, volume 176 of *Lecture Notes in Computer Science*, pages 17–31. Springer, 1984.

[25] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, 1993.

[26] George E. Collins. *Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition*. Springer Verlag, 1975.

[27] Solen Corvez and Fabrice Rouillier. Using computer algebra tools to classify serial manipulators. In *Automated Deduction in Geometry*, pages 31–43, 2002.

[28] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Undergraduate Texts in Mathematics. Springer Verlag, 1992.

[29] David Cox, John Little, and Donal O'Shea. *Using algebraic geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1998.

[30] Xavier Dahan and Éric Schost. Sharp estimates for triangular sets. In Jaime Gutierrez, editor, *Symbolic and Algebraic Computation, International Symposium ISSAC 2004, Santander, Spain, July 4-7, 2004, Proceedings*, pages 103–110. ACM, 2004.

[31] Wolfram Decker, Gert-Martin Greuel, and Gerhard Pfister. Primary decomposition : algorithms and comparisons. In *Algorithmic algebra and number theory (Heidelberg, 1997)*, pages 187–220. Springer, Berlin, 1999.

[32] Alicia Dickenstein, J. Maurice Rojas, Korben Rusek, and Justin Shih. Extremal real algebraic geometry and $\mathcal{A}$-discriminants. *Mosc. Math. J.*, 7(3) :425–452, 574, 2007.

[33] A. L. Dixon. The element of three quantics in two independent variables. *Proc. London Math. Soc.*, 7, 1908.

[34] Andreas Dolzmann. Solving geometric problems with real quantifier elimination. In *Automated Deduction in Geometry*, volume 1669 of *Lecture Notes in Computer Science*, pages 14–29, 1998.

[35] David Eisenbud. *Commutative algebra with a view toward algebraic geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin-Heidelberg-London-Paris-Tokyo-Hong Kong-Barcelona-Budapest, 1994.

[36] David Eisenbud, Craig Huneke, and Wolmer Vasconcelos. Direct methods for primary decomposition. *Invent. Math.*, 110(2) :207–235, 1992.

[37] M. Elkadi and B. Mourrain. *Introduction à la résolution des systèmes d'équations algébriques*. Mathématiques et Applications. Springer-Verlag, 2006. to appear.

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

[39] J.-C. Faugère. A new efficient algorithm for computing gröbner bases (f_4). *Journal of Pure and Applied Algebra*, 139(1-3) :61–88, 1999.

[40] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, pages 75–83 (electronic), New York, 2002. ACM.

[41] Jean-Charles Faugère, Guillaume Moroz, Fa brice Rouillier, and Mohab Safey El Din. Classification of the perspective-three-point problem, discrim inant variety and real solving polynomial systems of inequalities. In D. Jeffrey, editor, *ISSAC '08 : Proceedings of the twenty-first international symposium on Symbolic and algebraic computation*, pages 79–86, New York, NY, USA, 2008. ACM.

[42] FGb. Logiciel de calcul de base de gröbner. http ://fgbrs.lip6.fr/salsa/Software/.

[43] M. A. Fischler and R. C. Bolles. Random sample consensus : A paradigm for model fitting with applications to image analysis and automated cartography. *Commun. ACM*, 24(6) :381–395, 1981.

[44] Noaï Fitchas and André Galligo. Nullstellensatz effectif et conjecture de Serre (théorème de Quillen-Suslin) pour le calcul formel. *Math. Nachr.*, 149 :231–253, 1990.

[45] I. A. Fotiou, P. Rostalski, P. A. Parrilo, and M. Morari. Parametric optimization and optimal control using algebraic geometry methods. *Internat. J. Control*, 79(11) :1340–1358, 2006.

[46] S. Ganapathy. Decomposition of transformation matrices for robot vision. In *CRA84*, pages 130–139, 1984.

[47] X.-S. Gao, X. Hou, J. Tang, and Hang-Fei Cheng. Complete solution classification for the perspective-three-point problem. *IEEE Trans. Pattern Anal. Mach. Intell*, 25(8) :930–943, 2003.

[48] X. S. Gao and J. Tang. On the probability of the number of solutions for the P4P problem. *Journal of Mathematical Imaging and Vision*, 25(1) :79–86, July 2006.

[49] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, resultants, and multidimensional determinants*. Mathematics : Theory & Applications. Birkhäuser Boston Inc., Boston, MA, 1994.

[50] Patrizia Gianni, Barry Trager, and Gail Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *J. Symbolic Comput.*, 6(2-3) :149–167, 1988. Computational aspects of commutative algebra.

[51] M. Giusti and J. Heintz. Algorithmes - disons rapides - pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionnelles. In T. Mora and C. Traverso, editors, *Proc. Effective Methods in Algebraic Geometry, MEGA '90*, volume 94 of *Progress in Mathematics*, pages 169–193. Birkhäuser, 1991.

[52] M. Giusti, J. Heintz, K. Hägele, J. E. Morais, L. M. Pardo, and J. L. Montaña. Lower bounds for Diophantine approximations. *J. Pure Appl. Algebra*, 117/118 :277–317, 1997. Algorithms for algebra (Eindhoven, 1996).

[53] M. Giusti, J. Heintz, J. E. Morais, J. Morgenstern, and L. M. Pardo. Straight-line programs in geometric elimination theory. *J. Pure Appl. Algebra*, 124(1-3) :101–146, 1998.

[54] M. Giusti, J. Heintz, J. E. Morais, and L. M. Pardo. When polynomial equation systems can be "solved" fast ? In *Applied algebra, algebraic algorithms and error-correcting codes (Paris, 1995)*, volume 948 of *Lecture Notes in Comput. Sci.*, pages 205–231. Springer, Berlin, 1995.

[55] Marc Giusti, Joos Heintz, Jose Enrique Morais, and Luis Miguel Pardo. Le rôle des structures de données dans les problèmes d'élimination. *C. R. Acad. Sci. Paris Sér. I Math.*, 325(11) :1223–1228, 1997.

[56] Marc Giusti, Grégoire Lecerf, and Bruno Salvy. A gröbner free alternative for polynomial system solving. *J. Complexity*, 17(1) :154–211, 2001.

[57] Gert-Martin Greuel and Gerhard Pfister. *A Singular Introduction to Commutative Algebra*. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2002.

[58] D. Grigoriev and N. Vorobjov. Solving systems of polynomials inequalities in subexponential time. *Journal of Symbolic Computation*, 5 :37–64, 1988.

[59] Dima Grigoriev and Nicolai Vorobjov. Bounds on numbers of vectors of multiplicities for polynomials which are easy to compute. In *ISSAC'00*, pages 137–146, 2000.

[60] Bertrand Haas. A simple counterexample to Kouchnirenko's conjecture. *Beiträge Algebra Geom.*, 43(1) :1–8, 2002.

[61] R. M. Haralick, K. Ottenberg, and M. Nolle. Analysis and solutions of the three point persepective pose estimation problem. In *Proceedings Computer Vision and Pattern Recognition '91*, pages 592–598, Lahaina, Maui, June 1991.

[62] 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.

[63] Joos Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theoret. Comput. Sci.*, 24(3) :239–277, 1983.

[64] Heisuke Hironaka. Resolution of singularities of an algebraic variety over a field of characteristic zero. I, II. *Ann. of Math. (2) 79 (1964), 109–203 ; ibid. (2)*, 79 :205–326, 1964.

[65] H. Hong. Quantifier elimination for formulas constrained by quadratic equati ons via slope resultants. *The Computer Journal*, 36(5) :440–449, 1993.

[66] H. Hong. Generic quantifier elimination. In *Proceedings of IMACS-ACA'95*, 1995.

[67] Z.Y. Hu and F.C. Wu. A note on the number of solutions of the noncoplanar p4p problem. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24(4) :550–555, 2002.

[68] C. Innocenti and V. Parenti-Castelli. Singularity-free evolution from one configuration to another in serial and fully-parallel manipulators. *Journal of Mechanical Design*, 120(1) :73–79, 1998.

[69] Zbigniew Jelonek. On the generalized critical values of a polynomial mapping. *Manuscripta Math.*, 110(2) :145–157, 2003.

[70] Zbigniew Jelonek. On the effective Nullstellensatz. *Invent. Math.*, 162(1) :1–17, 2005.

[71] Zbigniew Jelonek and Krzysztof Kurdyka. Quantitative generalized Bertini-Sard theorem for smooth affine varieties. *Discrete Comput. Geom.*, 34(4) :659–678, 2005.

[72] J.-P. Jouanolou. Le formalisme du résultant. *Adv. Math.*, 90(2) :117–263, 1991.

[73] Michael Kalkbrener. *Three Contributions to Elimination Theory.* PhD thesis, Johannes Kepler University, Linz, Austria, 1991.

[74] Irving Kaplansky. *Commutative rings.* The University of Chicago Press, Chicago, Ill.-London, revised edition, 1974.

[75] M. M. Kapranov, B. Sturmfels, and A. V. Zelevinsky. Chow polytopes and general resultants. *Duke Math. J.*, 67(1) :189–218, 1992.

[76] A. G. Khovanski*u* a. A class of systems of transcendental equations. *Dokl. Akad. Nauk SSSR*, 255(4) :804–807, 1980.

[77] Steven L. Kleiman. Bertini and his two fundamental theorems, April 17 1997. Comment : PLAIN TeX, 29 pages with 3 figures, automatically produced by dvips.

[78] Donald E. Knuth. *The art of computer programming. Vol. 2.* Addison-Wesley Publishing Co., Reading, Mass., second edition, 1981. Seminumerical algorithms, Addison-Wesley Series in Computer Science and Information Processing.

[79] János Kollár. Sharp effective Nullstellensatz. *J. Amer. Math. Soc.*, 1(4) :963–975, 1988.

[80] `Kronecker`. Bibliothèque magma de résolution géométrique. http ://www.math.uvsq.fr/ lecerf/software/kronecker/.

[81] K. Kurdyka, P. Orro, and S. Simon. Semialgebraic Sard theorem for generalized critical values. *J. Differential Geom.*, 56(1) :67–92, 2000.

[82] B. Lacolle, O. Leboulleux, B. Conio, and R. Horaud. An analytic solution for the perspective 4-point problem. *CVGIP : Image Understanding*, 48(2) :277–278, November 1989.

[83] Y. N. Lakshman. A single exponential bound on the complexity of computing Gröbner bases of zero-dimensional ideals. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 227–234. Birkhäuser Boston, Boston, MA, 1991.

[84] Y. N. Lakshman and Daniel Lazard. On the complexity of zero-dimensional algebraic systems. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 217–225. Birkhäuser Boston, Boston, MA, 1991.

[85] D. Lazard. A new method for solving algebraic systems of positive dimension. *Discrete Appl. Math.*, 33(1-3) :147–160, 1991. Applied algebra, algebraic algorithms, and error-correcting codes (Toulouse, 1989).

[86] Daniel Lazard. Résolution des systèmes d'équations algébriques. *Theoret. Comput. Sci.*, 15(1) :77–110, 1981.

[87] Daniel Lazard and Fabrice Rouillier. Solving parametric polynomial systems. *J. Symb. Comput.*, 42(6) :636–667, 2007.

[88] G. Lecerf. *Une alternative aux méthodes de réécriture pour la résolution des systèmes algébriques*. PhD thesis, École polytechnique, 2001.

[89] G. Lecerf. Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers. *Journal of Complexity*, 19(4) :564–596, 2003.

[90] Grégoire Lecerf. Computing an equidimensional decomposition of an algebraic variety by means of geometric resolutions. In *ISSAC*, pages 209–216, 2000.

[91] Tien-Yien Li, J. Maurice Rojas, and Xiaoshen Wang. Counting real connected components of trinomial curve intersections and m-nomial hypersurfaces. *Discrete Comput. Geom.*, 30(3) :379–414, 2003.

[92] F. S. Macaulay. On some formulæ in elimination. *Proceedings of the London Mathematical Society*, 33(1) :3–27, 1902.

[93] F. S. Macaulay. *Algebraic Theory of Modular Systems*, volume 19 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1916.

[94] MAGMA. Logiciel de calcul formel. http ://magma.maths.usyd.edu.au/magma/.

[95] Dinesh Manocha and John F. Canny. Multipolynomial resultant algorithms. *J. Symbolic Comput.*, 15(2) :99–122, 1993.

[96] Guillermo Matera and Jose Maria Turull Torres. The space complexity of elimination theory : upper bounds. In *Foundations of computational mathematics*, pages 267–276. Springer, 1997.

[97] Ernst W. Mayr and Albert R. Meyer. The complexity of the word problems for commutative semigroups and polynomial ideals. *Adv. in Math.*, 46(3) :305–329, 1982.

[98] M.M. Maza. On triangular decompositions of algebraic varieties. *MEGA-2000 Conference, Bath*, 2000.

[99] P. R. McAree and R. W. Daniel. An explanation of never-special assembly changing motions for 3-3 parallel manipulators. *I. J. Robotic Res*, 18(6) :556–574, 1999.

[100] Jean-Pierre Merlet. *Parallel Robots*, volume 74 of *Solid Mechanics and its Applications*. Kluwer Academic Publishers, Boston, 2000. INRIA.

[101] `modpn`. Bibliothèque maple de décomposition triangulaire. présentée à ISSAC '08 par Xin Li,Moreno Maza, Rasheed, É.Schost
http ://www.csd.uwo.ca/ xli96/LMRS-08b.pdf.

[102] Guillaume Moroz. Complexity of the resolution of parametric systems of polynomial equations and inequations. In Barry M. Trager, editor, *Symbolic and Algebraic Computation, International Symposium, ISSAC 2006, Genoa, Italy, July 9-12, 2006, Proceedings*, pages 246–253. ACM, 2006.

[103] Guillaume Moroz. Regular decompositions. In Deepak Kapur, editor, *ASCM*, volume 5081 of *Lecture Notes in Computer Science*, pages 263–277. Springer, 2007.

[104] Guillaume Moroz and Fabrice Rouillier. Explicit classification of the 9 first haas parametric systems. In *Automated Deduction in Geometry*, 2008.

[105] `multires`. Bibliothèque maple de calcul de résultant. http ://www-sop.inria.fr/galaad/software/multires/.

[106] Wei Niu and Dongming Wang. Algebraic approaches to stability analysis of biological systems. *Mathematics in Computer Science*, 1(3) :507–539, 2008.

[107] Masayuki Noro and Kazuhiro Yokoyama. Implementation of prime decomposition of polynomial ideals over small finite fields. *J. Symbolic Comput.*, 38(4) :1227–1246, 2004.

[108] J El Omri and P Wenger. How to recognize simply a non-singular posture changing 3-dof manipulator. In *Proc. 7th Int. Conf. on Advanced Robotics*, pages 215–222, 1995.

[109] K.H. Parshall. The British development of the theory of invariants (1841–1895). *BSHM Bulletin : Journal of the British Society for the History of Mathematics*, 21(3) :186–199, 2006.

[110] P.Aubry. *Ensembles triangulaires de polynômes et résolution de systèmes algébriques. Implantation en Axiom.* PhD thesis, Université P. et M. Curie, 1999.

[111] `PHCpack`. Logiciel de résolution réelle. http ://www.math.uic.edu/ jan/download.html.

[112] `primdec.lib`. Bibliothèque singular de décomposition algébrique. http ://www.singular.uni-kl.de/.

[113] L. Quan and Z.-D. Lan. Linear N-point camera pose determination. *IEEE Trans. Pattern Anal. Mach. Intell*, 21(8) :774–780, 1999.

[114] Patrick J. Rabier. Ehresmann fibrations and Palais-Smale conditions for morphisms of Finsler manifolds. *Ann. of Math. (2)*, 146(3) :647–691, 1997.

[115] J. L. Rabinowitsch. Zum Hilbertschen Nullstellensatz. *Math. Ann.*, 102(1) :520, 1930.

[116] RAGLIB. Bibliothèque maple de géométrie réelle. http ://www-spiral.lip6.fr/ safey/RAGLib/.

[117] `RegularChains`. Bibliothèque maple de décomposition triangulaire. http ://www.maplesoft.com/.

[118] G. Reid, J. Tang, and L. Zhi. A complete symbolic-numeric linear method for camera pose determination. In J. Rafael Senda, editor, *ISSAC 2003*, pages 215–223, pub-ACM :adr, 2003. ACM Press.

[119] James Renegar. On the computational complexity and geometry of the first-order theory of the reals. I. Introduction. Preliminaries. The geometry of semi-algebraic sets. The decision problem for the existential theory of the reals. *J. Symbolic Comput.*, 13(3) :255–299, 1992.

[120] John R. Rice. A theory of condition. *SIAM Journal on Numerical Analysis*, 3(2) :287–310, 1966.

[121] Joseph Fels Ritt. *Differential Equations From The Algebraic Standpoint*, volume XIV of *American Mathematical Society Colloquium Publications*. American Mathematical Society, 1932.

[122] Joseph Fels Ritt. *Differential Algebra*, volume XXXIII of *American Mathematical Society Colloquium Publications*. American Mathematical Society, New York, N. Y., 1950.

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

[124] RS. Logiciel de résolution réelle de système 0-dimensionnel. http ://fg-brs.lip6.fr/salsa/Software/.

[125] Mohab 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.

[126] Mohab Safey El Din. Testing sign conditions on a multivariate polynomial and applications. *Math. Comput. Sci.*, 1(1) :177–207, 2007.

[127] Mohab Safey El Din. Practical and theoretical issues for the computation of genera lized critical values of a polynomial mapping and its applications. In D. Kapur, editor, *8-th Asian Symposium on Computer Mathematics (ASCM 2007)*, Lecture Notes in Artificial Intelligence. Springer-Verlag, Dec. 15-17 2008.

[128] SALSA. Bibliothèque maple de calculs algébriques et réels. http ://fg-brs.lip6.fr/salsa/Software/.

[129] Éric Schost. Complexity results for triangular sets. *J. Symbolic Comput.*, 36(3-4) :555–594, 2003. International Symposium on Symbolic and Algebraic Computation (ISSAC'2002) (Lille).

[130] Takeshi Shimoyama and Kazuhiro Yokoyama. Localization and primary decomposition of polynomial ideals. *J. Symbolic Comput.*, 22(3) :247–277, 1996.

[131] Victor Shoup. *A computational introduction to number theory and algebra*. Cambridge University Press, Cambridge, 2005.

[132] SINGULAR. Logiciel de calcul formel. http ://www.singular.uni-kl.de/.

[133] A.J. Sommese, J. Verschelde, and C.W. Wampler. Introduction to numerical algebraic geometry. In *Solving Polynomial Equations*, volume 14 of *Algorithms and Computation in Mathematics*, pages 301–337. Springer, Berlin Heidelberg, 2005.

[134] Andrew J. Sommese, Jan Verschelde, and Charles W. Wampler. Numerical decomposition of the solution sets of polynomial systems into irreducible components. *SIAM Journal on Numerical Analysis*, 38(6) :2022–2046, December 2001.

[135] Bernd Sturmfels. Sparse elimination theory. In *Computational algebraic geometry and commutative algebra (Cortona, 1991)*, Sympos. Math., XXXIV, pages 264–298. Cambridge Univ. Press, Cambridge, 1993.

[136] J J Sylvester. On the intersections, contacts, and other correlations of two conics expressed by indeterminate coordinates. *Cambridge and Dublin Mathematical Journal*, 5 :262–282, 1850.

[137] James Joseph Sylvester. *The Collected Mathematical Papers of James Joseph Sylvester*, volume 1 (1837–1853). Cambridge University Press, 1904.

[138] SYNAPS. Bibliothèque c++ pour le calcul formel. http ://www-sop.inria.fr/galaad/software/synaps/.

[139] W. Trinks. On improving approximate results of buchberger's algorithm by newton's method. In B. F. Caviness, editor, *EUROCAL '85, European Conference on Computer Algebra, Linz, Austria, April 1-3, 1985, Proceedings Volume 2 : Research Contributions*, volume 204 of *Lecture Notes in Computer Science*, pages 608–612. Springer, 1985.

[140] Wen tsün Wu. *Mechanical theorem proving in geometries*. Springer-Verlag New York, Inc., New York, NY, USA, 1994.

[141] Dongming Wang. Computing triangular systems and regular systems. *J. Symbolic Computation*, 30(2) :221–236, 2000.

[142] Franz Winkler. A geometrical decision algorithm based on the gröbner bases algorithm. In Patrizia M. Gianni, editor, *ISSAC*, volume 358 of *Lecture Notes in Computer Science*, pages 356–363. Springer, 1988.

[143] Y. H. Wu and Z. Y. Hu. PnP problem revisited. *Journal of Mathematical Imaging and Vision*, 24(1) :131–141, January 2006.

[144] L. Yang. A simplified algorithm for solution classification of the perspective-three-point problem, December 1998.

[145] Mazen Zein, Philippe Wenger, and Damien Chablat. Singular curves and cusp points in the joint space of 3-RPR parallel manipulators. In *ICRA*, pages 777–782. IEEE, 2006.

[146] C.-X. Zhang and Z.-Y. Hu. A general sufficient condition of four positive solutions of the p3p problem. *J. Comput. Sci. Technol.*, 20(6) :836–842, 2005.

Table des algorithmes

Table des figures

Table des symboles

Index