Représentations matricielles en théorie de l'élimination et applications à la géométrie

Laurent Busé

UNIVERSITÉ DE NICE - SOPHIA ANTIPOLIS
École Doctorale des Sciences Fondamentales et Appliquées

Représentations Matricielles en Théorie de l'Élimination et Applications à la Géométrie

Mémoire pour l'obtention de l'

Habilitation à Diriger des Recherches

spécialité : Mathématiques

présenté par

Laurent BUSÉ

et soutenu publiquement le 29 avril 2011, à l'INRIA Sophia Antipolis, devant le jury composé de :

Rapporteurs :

Mme Alicia DICKENSTEIN	Professeur à l'Université de Buenos Aires, Argentine
M. Marc GIUSTI	Directeur de recherche CNRS, École Polytechnique, France
M. Frank-Olaf SCHREYER	Professeur à l'Université de Saarbrücken, Allemagne

Examinateurs :

M. Marc CHARDIN	Chargé de recherche CNRS, IMJ & UMPC, France
M. André GALLIGO	Professeur à l'Université de Nice, France
M. Jean-Pierre JOUANOLOU	Professeur émérite à l'Université de Strasbourg, France
M. Bernard MOURRAIN	Directeur de recherche INRIA, Sophia Antipolis, France
Mme Marie-Françoise ROY	Professeur à l'Université de Rennes, France

Remerciements

Je tiens à adresser mes plus sincères remerciements à Alicia Dickenstein, Marc Giusti et Frank-Olaf Schreyer qui ont accepté la difficile tâche de rapporteur. Je les remercie pour leur lecture détaillée de ce mémoire. Un grand merci également à Marc Chardin, André Galligo, Jean-Pierre Jouanolou, Bernard Mourrain et Marie-Françoise Roy pour leur participation à mon jury.

J'exprime toute ma gratitude aux membres du projet GALAAD, plus particulièrement à Bernard Mourrain, chef de l'équipe, et André Galligo pour leurs encouragements constants et pour la confiance qu'ils m'ont accordée.

Je voudrais également remercier très chaleureusement Marc Chardin et Jean-Pierre Jouanolou. Travailler à leurs côtés fût un réel plaisir et surtout une vraie chance. Ils m'ont énormément appris.

Je remercie aussi tous mes collaborateurs et tous les étudiants que j'ai pu encadrer, ou bien juste croiser. Merci également à tous les personnels des services de l'INRIA Sophia Antipolis dont le dévouement fait que les conditions de travail y sont tout simplement exceptionnelles.

Table des matières

Introduction

La rédaction de ce mémoire m'a donné l'occasion de revenir sur une dizaine d'années de pratique de la recherche post-thèse, pour l'essentiel comme chargé de recherche à l'INRIA dans l'équipe Galaad commune au laboratoire J.-A. Dieudonné de l'Université de Nice.

Pour rappel, mon travail de thèse de doctorat consistait à répondre à la question suivante : comment peut-on étendre les méthodes basées sur les résultants pour la résolution des systèmes polynomiaux ? En effet, une des propriétés les plus importantes de ces méthodes, à savoir la production de formules d'élimination closes et universelles, les rendent très sensibles à la présence d'un lieu base : dès qu'il existe une solution commune indépendante des paramètres du système considéré dans la variété projective sous-jacente (espace projective, varieté torique, ...), les résultants classiques sont identiquement nuls. La contribution principale de mon travail de thèse a été de donner une construction générale des résultants qui permette de surmonter cette faiblesse. Des formules explicites pour calculer ces résultants y sont démontrées dans des cas particuliers. Elles ont notamment conduit à des algorithmes pour le calcul d'équations implicites de surfaces rationnelles en la présence de points base et pour la résolution d'une partie zéro-dimensionnelle d'un système polynomial possédant une lieu base arbitraire dans le plan.

À la suite de cette thèse, mon activité de recherche est restée centrée sur la théorie de l'élimination et ses applications aux aspects effectifs de la géométrie algébrique et de l'algèbre commutative. Néanmoins, j'ai délaissé la résolution des systèmes polynomiaux pour me concentrer sur la modélisation géométrique. Ce domaine applicatif s'est révélé être, de mon point de vue, particulièrement intéressant et il a de fait considérablement influencé mes travaux. En effet, dans le contexte de la modélisation géométrique, la théorie de l'élimination permet de changer la représentation d'un objet algébrique pour le mettre sous une forme appropriée à la résolution d'un problème donné. En quelques sortes, on rejoint ici une approche plus générale qui consiste à mettre la problématique de représentation des données au centre du processus de résolution d'un problème d'élimination (voir par exemple [Giusti et al., 1998] et ses références).

Avec cet objectif à l'esprit, je me suis intéressé à une approche matricielle de la théorie de l'élimination qui consiste à obtenir un objet éliminant sous la forme d'une matrice. Ce point de vue transparaît dans la quasi totalité de mes travaux. S'il fallait résumer d'une phrase la mise en oeuvre de cette approche, on pourrait écrire : "éliminer, c'est calculer une présentation d'une certaine composante homogène d'un module gradué". D'un point de vue algorithmique, ces représentations matricielles transposent un problème de géométrie, par exemple un calcul d'intersection ou de lieu singulier, en un problème d'algèbre linéaire. Ce changement de représentation établit ainsi un pont entre la géométrie et l'algèbre linéaire numérique, pont qui permet de livrer des problèmes géométriques à la puissance des algorithmes d'algèbre linéaire numérique qui sont par ailleurs développés, tant au niveau théorique que pratique et logiciel, par une importante communauté depuis de très nombreuses années. Les travaux que j'ai choisis de présenter dans ce mémoire visent à illustrer le mieux possible ce propos.

Le premier chapitre traite du problème d'implicitation d'une hypersurface paramétrée par un espace projectif. Il s'agit de calculer une représentation implicite d'une hypersurface donnée par une représentation paramétrique. On y résume une série de travaux en collaboration notamment avec M. Chardin et J.-P. Jouanolou, dans lesquels nous avons développé une méthode qui produit, sous certaines hypothèses, une représentation implicite de l'hypersurface considérée sous la forme d'une matrice. Cette méthode, dont nous donnerons les grandes lignes, est basée sur l'étude d'une certaine algèbre d'éclatement associée

à la paramétrisation de l'hypersurface en question. Une partie du travail de thèse de Marc Dohm [Dohm, 2008], que j'ai co-encadré avec A. Galligo, portait sur cette méthode.

Dans le deuxième chapitre, sont rassemblées plusieurs contributions autour des courbes algébriques paramétrées par la droite projective. On y explique tout d'abord comment obtenir une représentation implicite matricielle, puis on en illustre l'intérêt au travers d'applications comme le calcul d'intersection ou bien la détection de singularités. Ces travaux ont été conduits dans le cadre de la thèse de T. Luu Ba que je co-encadre avec A. Galligo. La dernière partie de ce chapitre sera consacrée au cas particulier des courbes planes pour lesquelles on peut établir un lien très précis entre singularités et facteurs invariants d'une certaine matrice d'élimination.

Le dernier chapitre revient sur des travaux en collaboration avec G. Chèze dans lesquels nous nous sommes intéressés au test d'irréductibilité absolue pour une hypersurface dans un espace projectif. Revisitant une méthode introduite par W. Ruppert [Ruppert, 1986], nous formulons ce test sous la forme d'une matrice dont nous préciserons quelques propriétés. Puis, nous en illustrerons l'intérêt en l'appliquant au dénombrement des fibres spéciales d'un pinceau d'hypersurfaces algébriques dans un espace projectif dont l'élément générique est absolument irréductible.

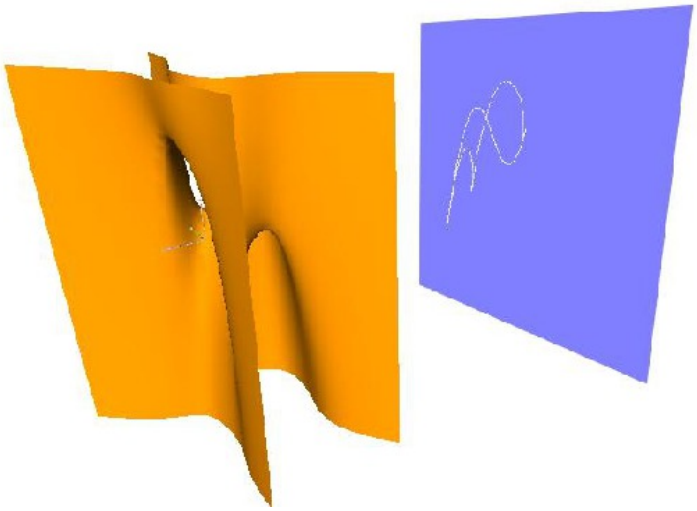


FIGURE 1 – Une surface quartique et son contour apparent [14, §6]

Enfin, je voudrais terminer cette introduction en illustrant par l'exemple ce qui m'attire le plus dans la théorie de l'élimination : son témoignage de consonances remarquables entre algèbre et géométrie. Soit le polynôme

$$P(X,Y) := \sum_{i,j\geq 0,\ i+j\leq d} U_{i,j} X^i Y^j$$

de degré $d \geq 4$. Le discriminant itéré de P, c'est-à-dire le discriminant éliminant X du discriminant éliminant Y du polynôme P, est un polynôme homogène dans l'anneau factoriel $\mathbb{Z}[U_{i,j} : i,j \geq 0,\ i+j \leq d]$ de degré $4(d-1)(d^2-d-1)$ dont la décomposition en produit de facteurs irréductibles est de la forme

$$\mathrm{Disc}_X(\mathrm{Disc}_Y(P(X,Y))) = U_{0,0} F_1(P) F_2(P)^2 F_3(P)^3. \qquad (\star)$$

Ce résultat, obtenu en collaboration avec B. Mourrain [14, Theorem 6.8], semble avoir été énoncé pour la première fois par O. Henrici en 1868 Henrici [1868, 1869], sans toutefois que l'irréductibilité des facteurs F_1, F_2 et F_3 n'y soit mentionnée.

Il est intéressant de rapprocher $(\star)$ d'un résultat datant de 1955 de H. Whitney [Whitney, 1955] en théorie des singularités. Soit S une surface générale de $\mathbb{R}^3$ donnée par l'équation $f(x,y,z) = 0$ où f est un polynôme de degré d, et soit Σ la courbe des points de S où $\partial_y f$ s'annule, c'est-à-dire le lieu singulier de la projection de S sur le plan (Oxz). Alors, la projection de Σ sur le plan (Oxz), appelée le contour apparent de S, ne possède que deux types de singularités (qui sont en nombre fini) : des points doubles ordinaires qui correspondent à la projection de deux plis superposés de S, et des points de

rebroussement qui correspondent aux points-fronces de Σ. Revenant à $(\star)$, on note que l'on peut réaliser $f(x, y, z)$ comme spécialisation du polynôme $P(X, Y)$ en l'écrivant

$$f(x, y, z) = \sum_{i,j \geq 0,\ i+j \leq d} a_{i,j}(z) x^i y^j$$

où $a_{i,j}(z)$ est un polynôme de degré $d - i - j$ dans $\mathbb{R}[z]$. Les descriptions explicites des facteurs F_1, F_2 et F_3 données dans [14, §6] permettent alors de constater que les points de rebroussement de S sont données par le facteur F_3 et les points doubles ordinaires par le facteur F_2. Le facteur F_1 fournit quant à lui les points de S pour lesquels le plan tangent est orthogonal à la direction (Oz).

Chapitre 1

Représentations matricielles d'hypersurfaces rationnelles

La détermination de l'image d'une application rationnelle est un problème d'élimination qui possède une longue histoire. En effet, c'est aux XVIIIième et XIXième siècles que l'on découvre les premiers développements de la théorie du résultant de deux polynômes en une variable par Bézout et Cayley, résultant qui permet de formuler l'équation implicite d'une courbe plane rationnelle à partir d'une de ses paramétrisations. Plus récemment, ce problème a subi un regain d'intérêt pour des applications en modélisation géométrique qui sont devenues pertinentes grâce à l'apparition des ordinateurs et de leur puissance de calcul. Le problème d'implicitation d'une hypersurface, principalement d'une courbe ou d'une surface, rationnelle apparaît donc comme un sujet de recherche très actif de ces trente dernières années avec de nombreuses contributions provenant aussi bien de la communauté de la modélisation géométrique que de l'algèbre commutative et de la géométrie algébrique.

Si le calcul de bases de Gröbner permet en théorie de résoudre le problème d'implicitation, il n'est pas considéré comme une bonne solution algorithmique, notamment à cause d'un coup de calcul non constant suivant l'instance considérée. Les approches à l'aide de la théorie du résultant ont donc été privilégiées pour leur caractère universel (au sens où elles commutent à la spécialisation), mais aussi car elles fournissent des formulations matricielles du résultat de l'élimination. Ces méthodes sont caractérisées par le fait qu'un résultant, correspondant à une compactification particulière de l'espace affine paramétrant une hypersurface, permet de traiter le problème d'implicitation pour une classe d'hypersurfaces particulières. Par exemple, toute paramétrisation régulière après compactification sur une variété algébrique appropriée peut être implicitée par le résultant correspondant sur cette variété. Typiquement, les compactifications les plus répandues sont l'espace projectif, l'espace projectif anisotrope ou bien encore une variété torique projective, et l'on parle alors respectivement de résultant de Macaulay, de résultant anisotrope ou de résultant creux ou torique. Nous renvoyons le lecteur à l'article [6] qui propose un survol de toutes ces notions ainsi que diverses applications en modélisation géométrique.

Mes travaux de thèse consistaient pour l'essentiel à développer de nouveaux types de résultants afin de traiter le problème des paramétrisations rationnelles non régulières, la présence de points base étant le principal obstacle à l'approche du problème d'implicitation par les résultants. J'ai ainsi introduit le résultant résiduel [1,2,3,21] qui revient à compactifier une paramétrisation sur une variété d'éclatement associée au lieu base de cette paramétrisation. Sous certaines hypothèses, on obtient alors de nouvelles classes d'hypersurfaces que l'on peut ainsi impliciter à l'aide d'une formulation universelle. Mais ce caractère universel a un prix : il faut connaître une description explicite du lieu base et une décomposition de la paramétrisation sur celui-ci. Mentionnons également que D. Eisenbud et F.-O. Schreyer ont parallèlement développé une autre méthode permettant, entres autres, d'aboutir à de nouvelles formules pour le résultant de formes homogènes en la présence de points base [Eisenbud et al., 2003].

Après ma thèse, je me suis donc orienté vers une autre méthode pour traiter les paramétrisations rationnelles non régulières. Cette méthode, initiée par J.-P. Jouanolou, permet de construire des matrices semblables aux matrices résultantes qui répondent au problème d'implicitation en la présence de points base, sous certaines hypothèses, mais qui ne conduisent pas à des formulations universelles comme pour

les résultants. Elle est basée sur l'étude de l'algèbre symétrique de l'idéal formé par les coordonnées de la paramétrisation considérée. Cette algèbre est engendrée par les relations entre ces coordonnées, relations qui forment un nouveau système, remplaçant celui formé par les équations usuelles, dont la plupart des points base ont disparu. Cette propriété géométrique est d'ailleurs bien connue puisque l'algèbre symétrique est, tout comme l'algèbre de Rees, une algèbre d'éclatement, c'est-à-dire une algèbre associée à un procédé géométrique permettant de transformer une paramétrisation rationnelle en une paramétrisation régulière sans en changer l'image.

Dans ce chapitre, on présente une succession de travaux [5,10,16,19,26] qui, à partir de l'étude de l'algèbre symétrique d'un idéal engendré par les coordonnées d'une paramétrisation, fournissent une collection de matrices répondant au problème d'implicitation. Ils sont ici résumés en des termes pratiques et orientés pour les applications en modélisation géométrique, une des deux principales motivations qui ont guidé mes recherches vers ce sujet. En termes de représentation, ces matrices remplacent l'habituelle équation implicite d'une hypersurface. Leur étude a été motivée par leur potentiel à enrichir cette représentation classique des hypersurfaces. En effet, cette représentation matricielle est non seulement moins difficile à calculer, mais contient également d'autres informations très utiles sur la surface paramétrée et sa paramétrisation (cf. par exemple [11,24]). Aussi, une part de ce chapitre est consacrée à des travaux sur le calcul de l'intersection d'une surface et d'une courbe algébrique. Ils visent à démontrer que les matrices de représentation obtenues peuvent être performantes pour la manipulation des objets qu'elles représentent. Finalement, on termine par un rapide survol d'un travail effectué dans le cadre de la thèse de Marc Dohm, portant sur les surfaces paramétrées par un produit de deux droites projectives, surfaces qui sont très utilisées en modélisation géométrique.

1.1 Le problème d'implicitation

Soit k un corps et supposons donnée une application rationnelle

$$\begin{array}{rcl} \phi : \mathbb{P}^{n-1} := \mathrm{Proj}(k[X_1, \ldots, X_n]) & \to & \mathbb{P}^n := \mathrm{Proj}(k[T_1, \ldots, T_{n+1}]) \\ (x_1 : \cdots : x_n) & \mapsto & (f_1(x_1, \ldots, x_n) : \cdots : f_{n+1}(x_1, \ldots, x_n)) \end{array} \tag{1.1}$$

où $f_1, \ldots, f_{n+1}$ sont des polynômes homogènes dans $k[X_1, \ldots, X_n]$ de même degré $d \geq 1$. Lorsque l'image fermée de ϕ est une hypersurface $\mathcal{H}$ de $\mathbb{P}^n$ (sur une clôture algébrique de k), le problème d'implicitation consiste à déterminer une équation implicite $H(T_1, \ldots, T_{n+1}) = 0$ de cette hypersurface. Noter que H est un polynôme homogène de $k[T_1, \ldots, T_{n+1}]$ de degré le degré de l'hypersurface $\mathcal{H}$. D'un point de vue plus algébrique, l'application ϕ correspond au morphisme de k-algèbres

$$\begin{array}{rcl} h : k[T_1, \ldots, T_{n+1}] & \to & k[X_1, \ldots, X_n] \\ P(T_1, \ldots, T_{n+1}) & \mapsto & P(f_1, \ldots, f_{n+1}) \end{array} \tag{1.2}$$

dont le noyau $\ker(h)$ est un idéal homogène principal de $k[T_1, \ldots, T_{n+1}]$ engendré par une équation implicite de $\mathcal{H}$.

L'approche que j'ai développée dans la plupart de mes travaux autour de ce problème d'implicitation consiste à substituer au polynôme H, représentation classique de l'hypersurface $\mathcal{H}$, une matrice à coefficients dans $k[T_1, \ldots, T_{n+1}]$. Cette matrice est en général bien plus simple à calculer et fournit une représentation plus compacte de l'hypersurface $\mathcal{H}$. Cependant, elle nécessite le développement de nouveaux algorithmes pour sa manipulation, ce que nous entreverrons plus loin dans ce chapitre.

D'ores et déjà, mentionnons que nous nous limiterons dans la suite au cas où l'idéal

$$I := (f_1, \ldots, f_{n+1}) \subset R := k[X_1, \ldots, X_n]$$

définit un nombre fini, éventuellement nul, de points dans $\mathbb{P}^{n-1}$. Au delà de cette hypothèse, les techniques algébriques que nous allons exposer deviennent beaucoup plus ardues ; voir par exemple [Chardin, 2006, Proposition 6] où l'auteur donne des résultats pour le cas d'un lieu base un peu plus général. Néanmoins, cette hypothèse est suffisante pour obtenir des résultats pertinents lorsque $n = 2$ et $n = 3$, deux cas qui présentent un intérêt tout particulier en modélisation géométrique.

Enfin, rappelons la formule d'intersection associée à l'application ϕ, démontrée dans un contexte plus général dans [5], et qui permet d'appréhender le degré d'une équation implicite de l'hypersurface rationnelle $\mathcal{H}$.

Théorème 1 ([5, Theorem 2.5]). *Si $T = \mathrm{Proj}(R/I)$ est fini sur k alors*

$$d^{n-1} - e(T, \mathbb{P}^{n-1}) = \begin{cases} \deg(\phi)\deg(H) & \text{si } \phi \text{ est génériquement finie} \\ 0 & \text{si } \phi \text{ n'est pas génériquement finie,} \end{cases}$$

où $e(T, \mathrm{Proj}(R))$ désigne la multiplicité de T au sens de Hilbert-Samuel.

1.2 Représentations matricielles en théorie de l'élimination : principe général

Étant donné un anneau (commutatif unitaire) A, on considère l'anneau de polynômes $A[X_1, \ldots, X_n]$ que l'on gradue canoniquement par $\deg(X_i) := 1$ pour tout $i \in \{1, \ldots, n\}$. On pose $\mathfrak{m} := (X_1, \ldots, X_n)$ et on suppose donné un idéal homogène $I := (F_1, \ldots, F_r) \subset \mathfrak{m}$ dans $A[\mathbf{X}]$ avec la notation $\mathbf{X} := (X_1, \ldots, X_n)$. En outre, on définit l'anneau quotient $B := A[\mathbf{X}]/I$ qui est alors naturellement un $A[\mathbf{X}]$-module gradué.

L'anneau A est l'anneau des coefficients des polynômes $F_1, \ldots, F_r$. Ainsi, on peut le voir comme l'anneau des paramètres du système polynomial $\{F_1 = \cdots = F_r = 0\}$ dont on souhaite éliminer les variables homogènes $X_1, \ldots, X_n$. En des termes plus géométriques, on désire calculer l'image du schéma d'incidence

$$\mathrm{Proj}(B) \subset \mathbb{P}^{n-1}_A := \mathrm{Proj}(A[\mathbf{X}])$$

par la projection canonique $\mathbb{P}^{n-1}_A \to \mathrm{Spec}(A)$. Cette image possède une structure naturelle de schéma [Eisenbud and Harris, 2000, §V.1.1] qui est définie par l'idéal

$$\mathfrak{A} := \{s \in A : \exists k \in \mathbb{N} \text{ tel que } \mathfrak{m}^k s =_B 0\} = (I : \mathfrak{m}^\infty) \cap A.$$

Notons que cet idéal s'exprime aussi en termes de la cohomologie locale de B. En effet, rappelant que

$$H^0_{\mathfrak{m}}(B) := \{s \in B : \exists k \in \mathbb{N} \text{ tel que } \mathfrak{m}^k s = 0\}$$

et qu'il hérite naturellement de la structure graduée de B, on observe que $\mathfrak{A} = H^0_{\mathfrak{m}}(B)_0$.

Toutes ces considérations sont classiquement résumées par le théorème suivant dont on peut trouver diverses preuves dans la littérature ; par exemple [Cartier and Tate, 1978] ou [Hartshorne, 1977, chapter II, theorem 4.9].

Théorème 2 (de l'élimination). *Soient $\mathbb{K}$ un corps, $\overline{\mathbb{K}}$ une clôture algébrique de $\mathbb{K}$ et $\rho : A \to \mathbb{K}$ un morphisme d'anneaux (souvent appelé une* spécialisation*). Les assertions suivantes sont équivalentes :*

(i) $\rho(\mathfrak{A}) = 0$.

(ii) *il existe un vecteur non nul $\xi := (\xi_1, \ldots, \xi_n) \in \overline{\mathbb{K}}^n$ tel que $\rho(P)(\xi) = 0$ pour tout $P \in I$.*

Le principe général de l'approche qui sera utilisée par la suite consiste à exploiter le lien entre l'idéal $\mathfrak{A}$ et les parties graduées de l'anneau quotient B. Pour tout $n \in \mathbb{N}$, la multiplication $B_1 \otimes B_n \to B_{n+1}$ est surjective, ce qui implique que l'on a une suite croissante d'idéaux dans A :

$$0 = \mathrm{ann}_A(B_0) \subset \mathrm{ann}_A(B_1) \subset \mathrm{ann}_A(B_2) \subset \cdots \subset \mathrm{ann}_A(B_t) \subset \mathrm{ann}_A(B_{t+1}) \subset \cdots$$

On montre alors le résultat suivant (voir [33, §1]) :

Proposition 3. *Soit $\eta \in \mathbb{N}$ tel que $H^0_{\mathfrak{m}}(B)_\eta = 0$. Alors, pour tout entier $t \geq 0$*

$$\mathfrak{A} = \mathrm{ann}_A(B_\eta) = \mathrm{ann}_A(B_{\eta+t}).$$

Cette proposition suggère une représentation alternative de la solution à notre problème d'élimination : une présentation, au sens algébrique classique, du A-module B_η. Ainsi, le résultat de notre problème d'élimination n'est alors plus un idéal donné par ses générateurs, mais une matrice à coefficients dans A. Toute la suite de ce chapitre consiste donc à montrer comment cette représentation, que nous qualifierons de *matricielle*, peut être mise en oeuvre dans le contexte de l'implicitation d'une hypersurface rationnelle.

Nous serons naturellement amenés à considérer dans la suite deux invariants classiques associés aux A-module B_ν, $\nu \in \mathbb{N}$, et qui sont plus facilement accessibles au calcul :

– l'idéal initial de Fitting [Northcott, 1976; Eisenbud, 1995] de B_ν, que nous noterons $\mathfrak{F}(B_\nu)$; il fournit une approximation intéressante de l'idéal $\mathrm{ann}_A(B_\nu)$ puisque bien que ne définissant, en général, pas les mêmes schémas, ces deux idéaux définissent les mêmes variétés algébriques,
– l'invariant de MacRae [Northcott, 1976] de B_ν, que nous noterons $\mathfrak{S}(B_\nu)$; il correspond à la partie de codimension 1 de $\mathfrak{F}(B_\nu)$, autrement dit au plus grand diviseur commun d'un système de générateurs de l'idéal $\mathfrak{F}(B_\nu) \subset A$.

Terminons en soulignant que la principale difficulté de cette approche réside en la détermination du plus petit entier η satisfaisant à la proposition 3. C'est surtout dans cette perspective que nous introduirons une résolution de B (puis de B_ν).

1.3 Algèbre symétrique et élimination

Afin d'utiliser les techniques énoncées dans le paragraphe précédent, il faut mettre la main sur un anneau quotient B en lien avec notre problème d'élimination. Il existe un candidat bien connu en géométrie algébrique : l'algèbre de Rees de l'idéal $I = (f_1, \ldots, f_{n+1}) \subset R := k[X_1, \ldots, X_n]$ que nous noterons $\mathrm{Rees}_R(I)$. Introduisant une nouvelle indéterminée Z, on peut décrire cette algèbre comme le quotient de l'anneau $R[T_1, \ldots, T_{n+1}]$ par le noyau du morphisme de R-algèbres

$$\begin{array}{rcl} \beta : R[T_1, \ldots, T_{n+1}] & \to & R[Z] \\ T_i & \mapsto & f_i Z. \end{array} \tag{1.3}$$

Il n'est pas difficile de constater que $\ker(\beta) \cap k[T_1, \ldots, T_{n+1}] = \ker(h)$ et par suite, que pour tout $\nu \in \mathbb{N}$

$$\mathrm{ann}_{k[\underline{T}]}(\mathrm{Rees}_R(I)_\nu) = \ker(h).$$

Cependant, l'algèbre $\mathrm{Rees}_R(I)$ est un objet algébrique complexe dont il est délicat d'extraire des équations. En particulier, il est généralement difficile d'obtenir une résolution de l'algèbre de Rees, ce qui est une difficulté importante dans l'application du principe général du paragraphe précédent.

Pour remédier à ce problème, on va considérer une algèbre quotient un peu plus grosse en se restreignant aux équations linéaires de l'algèbre de $\mathrm{Rees}_R(I)$, autrement dit aux relations (ou syzygies) de $I \subset R$. C'est l'algèbre symétrique de I dans R que l'on note $\mathrm{Sym}_R(I)$. On peut la décrire par le morphisme de R-algèbres surjectif

$$\begin{array}{rcl} \alpha : R[T_1, \ldots, T_{n+1}] & \to & \mathrm{Sym}_R(I) \\ T_i & \mapsto & f_i \end{array} \tag{1.4}$$

dont le noyau est donné par

$$\ker(\alpha) = \left\{ g_1 T_1 + g_2 T_2 + \cdots + g_{n+1} T_{n+1}, g_i \in R[T_1, \ldots, T_{n+1}] : \sum_{i=1}^{n+1} g_i f_i = 0 \right\}.$$

L'algèbre symétrique est intéressante dans notre contexte pour au moins deux raisons. La première est que ses équations sont simples et assez facilement accessibles au calcul. En effet, elles sont formées exclusivement de relations entre les polynômes $f_1, \ldots, f_{n+1}$. La deuxième raison réside en la propriété suivante, point clé de notre approche au problème d'implicitation.

Théorème 4 ([5]). *Soit η un entier tel que $H^0_{\mathfrak{m}}(\mathrm{Sym}_R(I))_\nu = 0$ pour tout $\nu \geq \eta$, alors*

$$\mathrm{ann}_{k[\underline{T}]}(\mathrm{Sym}_R(I)_\nu) \subset \ker(h) \quad \textit{pour tout } \nu \geq \eta.$$

De plus, si T est fini et forme localement une intersection complète, alors

$$\mathrm{ann}_{k[\underline{T}]}(\mathrm{Sym}_R(I)_\nu) = \ker(h) \quad \textit{pour tout } \nu \geq \eta.$$

D'après les méthodes exposées au paragraphe 1.2, on déduit qu'une équation implicite de notre hypersurface $\mathcal{H}$ peut être obtenue en éliminant les variables homogènes $X_1, \ldots, X_n$ des équations (dans $R[T_1, \ldots, T_{n+1}]$) de l'algèbre symétrique $\mathrm{Sym}_R(I)$ (cette même algèbre joue le rôle de l'algèbre quotient B dans les notations du paragraphe 1.2). Dans cet objectif, il reste encore à estimer l'entier η du théorème ci-dessus, puis à déterminer les multiplicités pouvant intervenir dans l'invariant de MacRae associé à $\mathrm{Sym}_R(I)_\nu$, $\nu \geq \eta$, et aussi les éventuels termes parasites pouvant apparaître lorsque T, bien que fini, ne forme pas localement une intersection complète.

1.3.1 L'indice de saturation

Le résultat qui suit permet de contrôler l'annulation des parties graduées du module de cohomologie locale $H^0_{\mathfrak{m}}(\mathrm{Sym}_R(I))$. Si M est un module $\mathbb{N}$-gradué sur un anneau gradué, son *degré initial* désignera l'entier

$$\mathrm{indeg}(M) := \min\{\nu \in \mathbb{N} : M_\nu \neq 0\}.$$

Théorème 5 ([10, Theorem 4])**.** *Si T est fini et forme localement une presque intersection complète, alors pour tout entier*

$$\nu \geq \eta_0 := (n-1)(d-1) - \mathrm{indeg}(I :_A \mathfrak{m}^\infty)$$

on a $H^0_{\mathfrak{m}}(\mathrm{Sym}_A(I))_\nu = 0$.

Sous l'hypothèse de finitude de T, on peut donner une interprétation géométrique du degré initial du saturé de I par rapport à $\mathfrak{m}$. En effet, soit T est vide et alors $\mathrm{indeg}(I :_A \mathfrak{m}^\infty) = 0$, soit T est non vide et alors $\mathrm{indeg}(I :_A \mathfrak{m}^\infty)$ correspond au plus petit degré (≥ 1) d'une hypersurface homogène dans $\mathbb{P}^{n+1}$ qui contient (le schéma zéro-dimensionnel) T.

Il est important en pratique de noter que

$$(n-1)(d-1) - d \leq \eta_0 \leq (n-1)(d-1).$$

La borne supérieure est atteinte lorsque T est vide, ce qui est le cas d'une paramétrisation ϕ suffisamment générale, et la borne inférieure lorsque l'idéal I est saturé, i.e. $I = (I : \mathfrak{m}^\infty)$. Ce dernier cas est atteint, par exemple si $n = 3$ en appliquant le théorème de structure de Hilbert-Burch.

La preuve du théorème 5 repose sur la connaissance d'une résolution de l'algèbre symétrique. À partir de cette résolution, on construit un complexe double qui permet à son tour de définir deux suites spectrales ayant même aboutissement. C'est leur comparaison qui fournit l'entier η_0 et le théorème. La résolution de l'algèbre symétrique dont nous parlons est connue sous le nom de *complexe d'approximation des cycles*.

1.3.2 Complexes d'approximation

Ces complexes ont été introduits par A. Simis et W. Vasconcelos dans [Simis and Vasconcelos, 1981], puis étudiés en détails par J. Herzog, A. Simis et W. Vasconcelos dans [Herzog et al., 1982] et [Herzog et al., 1983a] (voir aussi [Herzog et al., 1983b; Vasconcelos, 1994]). Nous rappelons ici très rapidement leur définition puis leur intérêt dans notre contexte.

Soit A un anneau, J un idéal de A engendré par r éléments $\mathbf{a} := (a_1, \ldots, a_r)$ et introduisons des indéterminées $\mathbf{T} := (T_1, \ldots, T_r)$. Aux deux morphismes

$$u : A[T_1, \ldots, T_r]^r \xrightarrow{(a_1,\ldots,a_r)} A[T_1, \ldots, T_r] : (b_1, \ldots, b_r) \mapsto \sum_{i=1}^{r} b_i a_i,$$

$$v : A[T_1, \ldots, T_r]^r \xrightarrow{(T_1,\ldots,T_r)} A[T_1, \ldots, T_r] : (b_1, \ldots, b_r) \mapsto \sum_{i=1}^{r} b_i T_i,$$

correspondent deux complexes de Koszul $K(\mathbf{a}; A[\mathbf{T}])$ et $K(\mathbf{T}; A[\mathbf{T}])$ dont nous noterons les différentielles $d_{\mathbf{a}}$ et $d_{\mathbf{T}}$ respectivement. Ces différentielles vérifiant l'égalité $d_{\mathbf{a}} \circ d_{\mathbf{T}} + d_{\mathbf{T}} \circ d_{\mathbf{a}} = 0$, on déduit qu'il existe trois complexes, appelés *complexes d'approximation*, habituellement notés

$$\begin{aligned}
\mathcal{Z}_\bullet &:= (\ker d_{\mathbf{a}}, d_{\mathbf{T}}),\\
\mathcal{B}_\bullet &:= (\mathrm{Im}\, d_{\mathbf{a}}, d_{\mathbf{T}}),\\
\mathcal{M}_\bullet &:= (H_\bullet(K(\mathbf{a}; A[\mathbf{T}])), d_{\mathbf{T}}).
\end{aligned}$$

C'est surtout le complexe $\mathcal{Z}_\bullet$ qui est intéressant dans notre contexte. La raison en est simple : le complexe $\mathcal{Z}_\bullet$ se termine par la suite

$$\ker(u) \xrightarrow{v} A[T_1, \ldots, T_r] \to 0$$

et puisque, par définition

$$v(\ker(u)) = \left\{ \sum_{i=1}^{r} b_i T_i \ \text{ tel que } \ \sum_{i=1}^{r} b_i a_i = 0 \right\}, \tag{1.5}$$

on déduit que

$$H_0(\mathcal{Z}) = \frac{A[T_1, \ldots, T_r]}{v(\ker(u))} \simeq \mathrm{Sym}_A(J).$$

Ainsi, lorsque le complexe $\mathcal{Z}_\bullet$ est acyclique, il fournit une résolution projective de l'algèbre symétrique de J dans A.

Mentionnons que ces complexes d'approximation possèdent de très nombreuses propriétés. Par exemple, il n'est pas difficile de vérifier que $v(\ker(u))$ annule tous les modules d'homologie (sur $A[\mathbf{T}]$) de $\mathcal{Z}_\bullet, \mathcal{B}_\bullet$ et $\mathcal{M}_\bullet$ qui possèdent donc une structure de $\mathrm{Sym}_A(J)$-modules. La propriété sans doute la plus remarquable de ces trois complexes est le fait que leur homologie ne dépende que de l'idéal J (ils sont indépendants du choix de r et de $\mathbf{a}$).

Revenant à notre problème d'implicitation et à ses notations, le résultat suivant permet de caractériser l'acyclicité du $\mathcal{Z}$-complexe, et donc l'existence d'une résolution projective de l'algèbre symétrique correspondante dans notre contexte.

Théorème 6 ([10, Theorem 4]). *Si T est fini, alors le complexe $\mathcal{Z}_\bullet$ est acyclique si et seulement si T forme localement une presque intersection complète (i.e. localement engendré par – au plus – n éléments).*

1.3.3 Invariants de MacRae associés

Les théorèmes 4 et 5 mettent en évidence que le support du $k[T_1, \ldots, T_{n+1}]$-module $\mathrm{Sym}_R(I)_\nu$, $\nu \geq \eta_0$, est lié à notre problème d'implicitation. Notre objectif étant de construire à partir de là une représentation matricielle, on s'intéresse à l'idéal de Fitting initial $\mathfrak{F}(\mathrm{Sym}_R(I)_\nu)$ car il a même support que $\mathrm{Sym}_R(I)_\nu$ et correspond à l'idéal des mineurs maximaux d'une présentation $k[T_1, \ldots, T_{n+1}]$-libre de $\mathrm{Sym}_R(I)_\nu$. En fait, on va surtout s'intéresser à sa partie purement de codimension 1, c'est-à-dire à l'invariant de MacRae $\mathfrak{S}(\mathrm{Sym}_R(I)_\nu)$.

Pour commencer, rappelons que pour chaque point $\mathfrak{p} \in T$, toujours supposé fini, on peut associer deux multiplicités, à savoir

- son degré, que nous noterons $d_\mathfrak{p}$ et qui vaut $\dim_{R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}}(R_\mathfrak{p}/I_\mathfrak{p})$,
- sa multiplicité, que nous noterons $e_\mathfrak{p}$ et qui correspond à la multiplicité $e(I_\mathfrak{p}, R_\mathfrak{p})$ au sens de Hilbert-Samuel.

Il est important de noter que l'on a toujours $e_\mathfrak{p} \geq d_\mathfrak{p}$ et que $e_\mathfrak{p} = d_\mathfrak{p}$ si et seulement si $\mathfrak{p}$ peut être engendré par une suite régulière (voir [Bruns and Herzog, 1993, corollary 4.5.10]), autrement dit si $\mathfrak{p}$ est une intersection complète.

Ces rappels faits, observons que nous avons d'un côté le théorème 1 qui fournit l'isomorphisme gradué

$$\ker(h)^{\deg(\phi)} \simeq k[\mathbf{T}](-d^{n-1} + \sum_{\mathfrak{p} \in T} e_p) \tag{1.6}$$

et d'un autre côté le résultat suivant qui est un simple calcul de degré à partir d'une résolution libre obtenue à l'aide d'une partie graduée du complexe $\mathcal{Z}_\bullet$.

Théorème 7 ([5],[10],[33,§4]). *Si T est fini et forme localement une presque intersection complète alors, pour tout entier $\nu \geq \eta_0$ on a*

$$\ker(h)^{\deg(\phi)} \supseteq \mathfrak{S}(\mathrm{Sym}_A(I)_\nu) = \mathfrak{S}(\mathrm{Sym}_A(I)_{\eta_0}) \simeq k[\mathbf{T}](-d^{n-1} + \sum_{\mathfrak{p} \in T} d_\mathfrak{p})$$

où le dernier isomorphisme est un isomorphisme gradué de $k[\mathbf{T}]$-modules.

De plus, supposant toujours T fini, l'inclusion ci-dessus est une égalité si et seulement si T forme localement une intersection complète.

Mentionnons au passage que l'indice de saturation η_0 que nous avons défini et qui intervient dans le théorème ci-dessus est optimal au sens suivant :

$$\mathfrak{S}(\mathrm{Sym}_A(I)_\nu) = \mathfrak{S}(\mathrm{Sym}_A(I)_{\eta_0}) \text{ si et seulement si } \nu \geq \eta_0.$$

Cette propriété est montrée dans [16], sous les hypothèses du théorème ci-dessus.

On déduit de (1.6) et du théorème 7 que nécessairement $\mathfrak{S}(\mathrm{Sym}_A(I)_{\eta_0})$, et donc $\mathfrak{S}(\mathrm{Sym}_A(I)_\nu)$ pour tout $\nu \geq \eta$, est engendré par le produit d'une équation implicite de $\mathcal{H}$ élevée à la puissance $\deg(\phi)$ et d'un polynôme homogène non nul, disons $G \in k[T_1, \ldots, T_{n+1}]$, de degré $\sum_{\mathfrak{p}\in T} e_\mathfrak{p} - d_\mathfrak{p}$. Précisons un peu plus la situation, toujours avec l'hypothèse de finitude sur T.

Si T est localement une intersection complète. Dans ce cas, $e_\mathfrak{p} = d_\mathfrak{p}$ pour tout $\mathfrak{p} \in T$, T étant d'ailleurs possiblement vide. Le polynôme G est donc un élément non nul dans k. Par suite,

$$\mathfrak{S}(\mathrm{Sym}_A(I)_\nu) \simeq \ker(h)^{\deg(\phi)} \text{ pour tout } \nu \geq \eta.$$

C'est le cas idéal, où même la multiplicité qui est introduite possède une signification géométrique : le degré de la paramétrisation ϕ.

Si T est localement une presque intersection complète. Soit un point $\mathfrak{p} \in T$ tel que $\mathfrak{p}$ n'est pas une intersection complète. Ce point est donc engendré par n éléments et pas moins. En ce point, les générateurs de I (i.e. $f_1, \ldots, f_{n+1}$) sont donc liés par une unique relation qui, évaluée au point $\mathfrak{p}$, fournit une forme linéaire $L_\mathfrak{p}(T_1, \ldots, T_{n+1}) \in k[T_1, \ldots, T_{n+1}]$ unique à multiplication près par une constante non nulle dans k.

Proposition 8 ([16])**.** *Si k est supposé algébriquement clos et que T est fini et est localement une presque intersection complète, alors*

$$G = \prod_{\mathfrak{p}\in S} L_\mathfrak{p}^{e_\mathfrak{p} - d_\mathfrak{p}}$$

où $S \subset T$ est le sous-schéma de T des points non intersection complète.

Bien que l'on n'obtienne pas exactement une équation implicite de $\mathcal{H}$ élevée à la puissance $\deg(\phi)$, il faut remarquer que le facteur parasite qui intervient a lui aussi une interprétation géométrique : il correspond aux fibres de la projection $\mathrm{Proj}(\mathrm{Sym}_A(I)) \to \mathbb{P}^{n-1}$ qui sont des hyperplans. De plus ce facteur parasite peut être calculé indépendamment de $\mathfrak{S}(\mathrm{Sym}_A(I)_{\eta_0})$, bien que cela ne soit pas vraiment souhaitable en pratique.

Si T n'est pas localement une presque intersection complète. Dans ce cas, $\mathfrak{S}(\mathrm{Sym}_A(I)_{\eta_0})$ est l'idéal nul. On peut l'expliquer géométriquement de la façon suivante : si $\mathfrak{p}$ est un point de T engendré par $n+1$ éléments et pas moins, alors la fibre de la projection $\mathrm{Proj}(\mathrm{Sym}_A(I)) \to \mathbb{P}^{n-1}$ en ce point est $\mathbb{P}^n$ tout entier et par suite, l'autre projection canonique $\mathrm{Proj}(\mathrm{Sym}_A(I)) \to \mathbb{P}^n$ devient surjective. Par conséquent, les matrices de représentation n'ont plus les propriétés annoncées.

1.4 Matrices de représentations à coefficients des formes linéaires

Nous avons maintenant tous les ingrédients pour définir une famille de matrices ayant les propriétés de représentation annoncées pour l'hypersurface $\mathcal{H}$.

Définition. Pour tout entier ν, une présentation de $k[T_1, \ldots, T_{n+1}]$-modules libres de $\mathrm{Sym}_R(I)_\nu$ est donnée par

$$(\mathcal{Z}_1)_\nu \to (\mathcal{Z}_0)_\nu = (R[T_1, \ldots; T_{n+1}])_\nu \to \mathrm{Sym}_R(I)_\nu \to 0.$$

On définit alors la matrice $\mathbf{L}(\phi)_\nu$ comme étant une matrice de $(\mathcal{Z}_1)_\nu \to (\mathcal{Z}_0)_\nu$ que nous qualifierons de matrice de représentation de ϕ (parfois de $\mathcal{H}$ par abus) lorsque $\nu \geq \eta_0$. Bien sûr, $\mathbf{L}(\phi)_\nu$ dépend du choix des $k[T_1, \ldots, T_{n+1}]$-bases de $(\mathcal{Z}_1)_\nu$ et $(\mathcal{Z}_0)_\nu$.

Une base pour $(\mathcal{Z}_0)_\nu$ correspond à un choix de base pour les polynômes homogènes en les variables $X_1, \ldots, X_n$, ce qui ne pose aucun problème. Calculer une base de $(\mathcal{Z}_1)_\nu$ revient à calculer une k-base des relations de I en degré ν. Elle est donc obtenue en résolvant un système linéaire sur k.

Propriétés. On suppose ici que T est fini et qu'il forme localement une presque intersection complète. Pour tout $\nu \geq \eta_0$, les faits suivants découlent des résultats énoncés précédemment.

- la matrice $\mathbf{L}(\phi)_\nu$ est à coefficients des formes linéaires dans $k[T_1, \ldots, T_{n+1}]$,
- la matrice $\mathbf{L}(\phi)_\nu$ est constituée de $\binom{n-1+\nu}{n-1}$ lignes et d'au moins autant de colonnes.
- le rang de $\mathbf{L}(\phi)_\nu$ est génériquement $\binom{n-1+\nu}{n-1}$ et chute exactement sur $\mathcal{H} \cup_{\mathfrak{p}\in T} V(L_\mathfrak{p}) \subset \mathbb{P}^n$.
- le PGCD des mineurs maximaux (i.e. des mineurs de taille $\binom{n-1+\nu}{n-1}$) de $\mathbf{L}(\phi)_\nu$ est égal au produit

$$H(T_1, \ldots, T_{n+1})^{\deg(\phi)} \prod_{\mathfrak{p}\in T} L_\mathfrak{p}(T_1, \ldots, T_{n+1})^{e_\mathfrak{p} - d_\mathfrak{p}}$$

  (avec la convention $L_\mathfrak{p} := 1$ lorsque $e_\mathfrak{p} = d_\mathfrak{p}$).

Mentionnons également que le PGCD des mineurs maximaux de $\mathbf{L}(\phi)_\nu$ peut aussi être exprimé comme le déterminant du complexe $\mathcal{Z}_\bullet$ pris en degré ν, mais ce dernier est peu intéressant d'un point de vue algorithmique (voir par exemple [Demazure, 1984; MacRae, 1965; Northcott, 1976; Jouanolou, 1995] pour un traitement détaillé du sujet, ou bien encore [33] pour en avoir un aperçu dans ce contexte).

Focalisons-nous un instant sur les cas $n = 2$ et $n = 3$ qui sont d'un intérêt tout particulier pour la modélisation géométrique et pour lesquels des algorithmes détaillés sont donnés dans [10].

Le cas des courbes. On peut ici déterminer très simplement l'entier η_0 car T, bien que fini, est supporté en codimension 1 ; plus précisément, il correspond au diviseur de $\mathbb{P}^1$ associé au polynôme $\mathrm{PGCD}(f_1, f_2, f_3) \in k[X_1, X_2]$. On obtient

$$\eta_0 = (d-1) - \deg(\mathrm{PGCD}(f_1, f_2, f_3)).$$

Noter qu'une simple division de chacun des f_i par leur PGCD commun permet de supposer que ϕ est régulière, c'est-à-dire que T est vide, et donc que $\eta_0 = d - 1$ où le d est ici le degré après division par ce PGCD.

Pour tout $\nu \geq \eta_0$, les matrices $\mathbf{L}(\phi)_\nu$ représentent notre courbe sans autre facteur parasite (puisque T est un diviseur). L'autre particularité du cas des courbes est que la matrice $\mathbf{L}(\phi)_{\eta_0}$ est carrée (de taille $d \times d$). C'est une conséquence directe du fait que le module des relations de I est un R-module libre de rang 2. D'ailleurs, on vérifie facilement que l'algèbre symétrique est décrite par deux équations et que la matrice $\mathbf{L}(\phi)_{\eta_0}$ est tout simplement la matrice de Sylvester associée au résultant de ces deux équations.

Le cas des surfaces. Il n'y a pas de particularité notable pour ce cas par rapport au cas général en ce qui concerne la méthode. Par contre, il faut noter que l'hypothèse de finitude sur T n'est pas restrictive dans ce cas. En effet, on peut toujours se ramener au cas où T est de codimension au moins 2 en divisant chacun des f_i, $i = 1, \ldots, 4$ par leur PGCD commun.

Le module des relations de I n'est en général pas un module libre. Par contre, il le devient si on se place dans une carte affine de $\mathbb{P}^2$, par exemple en spécialisant X_3 à 1. Il est alors possible de faire un lien entre les matrices de représentation $\mathbf{L}(\phi)_\nu$, $\nu \geq \eta_0$, et des matrices de résultants. Toutefois, les calculs nécessaires pour réaliser ce lien s'avèrent être compliqués et ne se présentent pas sous une forme suffisamment canonique pour être réellement exploitables d'un point de vue pratique. Nous renvoyons ici à la deuxième partie de [10].

1.5 Digression autour des équations non linéaires de l'algèbre de Rees

Jusqu'ici, les entrées des matrices de représentation que nous avons construites sont des formes linéaires de $k[T_1, \ldots, T_{n+1}]$. Plus précisément, chaque colonne de ces matrices correspond à une certaine

relation (forcément linéaire) de I, c'est-à-dire une relation entre les polynômes $f_1, \ldots, f_{n+1}$. Cependant, plusieurs travaux, citons par exemple [Cox et al., 2000; Cox, 2001] et [4], ont mis en évidence qu'il est possible d'obtenir des représentations matricielles faisant intervenir des relations de I, mais également des relations de I^2, c'est-à-dire des relations entre $f_1^2, f_1f_2, \ldots, f_{n+1}^2$. Dans tous ces travaux, les représentations matricielles obtenues sont des matrices carrées et leur validité est soumise à des hypothèses techniques. Ainsi, dans le travail [4] en collaboration avec D. Cox et C. D'Andrea, nous avons construit des représentations matricielles carrées dans le cas $n = 3$ dont la validité est soumise à pas moins de cinq hypothèses dont quatre peuvent être qualifiées de "techniques".

L'objectif de ce qui suit est d'exposer un cadre plus formel afin de construire des représentations matricielles faisant intervenir des relations de I, de I^2, voire de I^r, $r \in \mathbb{N}$ (notons d'ailleurs qu'une équation implicite de $\mathcal{H}$ est une relation de $I^{\deg(\mathcal{H})}$). Ce travail, en collaboration avec M. Chardin et A. Simis [19], montre que les hypothèses techniques présentes dans les travaux antérieurs sur le sujet disparaissent dès lors que l'on s'autorise à considérer des représentations matricielles non nécessairement carrées.

1.5.1 Torsion de l'algèbre symétrique

Les équations de l'algèbre symétrique $\mathrm{Sym}_R(I)$ sont engendrées par les relations de I ; ce sont des équations linéaires. Par conséquent, si nous voulons construire des représentations matricielles faisant intervenir des équations de degré au moins 2 qui ne soient pas triviales (c'est-à-dire pouvant être obtenues à partir d'équations de degré 1), il faut considérer une autre algèbre que l'on pourrait situer entre $\mathrm{Sym}_R(I)$ et $\mathrm{Rees}_R(I)$. On introduit donc l'algèbre

$$\mathrm{Sym}_R(I)^\star := \mathrm{Sym}_R(I)/H^0_{\mathfrak{m}}(\mathrm{Sym}_R(I))$$

qui consiste à éliminer la $\mathfrak{m}$-torsion de l'algèbre symétrique $\mathrm{Sym}_R(I)$. En faisant cela, on fait apparaître des équations non linéaires et non triviales. D'ailleurs, il faut noter ici que si I est $\mathfrak{m}$-primaire, alors $\mathrm{Sym}_R(I)^\star = \mathrm{Rees}_R(I)$. De plus, il est clair que l'invariant de MacRae et le support de $(\mathrm{Sym}_R(I)^\star)_\nu$ coïncide avec celui de $(\mathrm{Sym}_R(I))_\nu$ pour $\nu \geq \eta_0$ puisque $H^0_{\mathfrak{m}}(\mathrm{Sym}_R(I))_\nu = 0$ pour $\nu \geq \eta_0$. En y regardant d'un peu plus près, on montre que les invariants de MacRae se stabilisent avant le degré η_0, le support étant lui stable pour tout $\nu \in \mathbb{N}$.

Théorème 9 ([19, Proposition 7])**.** *Supposons que T soit fini et qu'il forme localement une presque intersection complète. Alors, pour tout entier*

$$\nu \geq \mu_0 := (n-1)(d-1) - \min\left\{\mathrm{indeg}(H_1(f_1, \ldots, f_{n+1}; R)), \mathrm{indeg}(H^0_{\mathfrak{m}}(H_1(f_1, \ldots, f_{n+1}; R))) - d\right\}$$

on a

$$\mathrm{ann}_{k[T_1,\ldots,T_{n+1}]}((\mathrm{Sym}_R(I)^\star)_\nu) = \mathrm{ann}_{k[T_1,\ldots,T_{n+1}]}((\mathrm{Sym}_R(I)^\star)_0) = H^0_{\mathfrak{m}}(\mathrm{Sym}_R(I))_0$$

et

$$\mathfrak{S}((\mathrm{Sym}_R(I)^\star)_\nu) = \mathfrak{S}((\mathrm{Sym}_R(I)^\star)_{\mu_0}) = \mathfrak{S}(\mathrm{Sym}_R(I)_{\eta_0}).$$

Voyons à présent ce que nous gagnons à considérer l'algèbre $\mathrm{Sym}_R(I)^\star$. Pour cela, notons J le noyau du morphisme canonique

$$R[T_1, \ldots, T_{n+1}] \to \mathrm{Sym}_R(I)^\star : T_i \mapsto f_i.$$

Pour tout entier $\ell \in \mathbb{N}$, nous noterons $J\langle\ell\rangle$ l'idéal de $R[T_1, \ldots, T_{n+1}]$ qui est engendré par les éléments de J de degré au plus ℓ en les variables $T_1, \ldots, T_{n+1}$. Ainsi, nous avons par exemple $J\langle 0\rangle = 0$ et $\mathrm{Sym}_R(I) \simeq R[T_1, \ldots, T_{n+1}]/J\langle 1\rangle$. En outre, nous avons le résultat suivant, point clé de l'intérêt de l'algèbre $\mathrm{Sym}_R(I)^\star$ dans notre contexte.

Théorème 10 ([19, Theorem 1])**.** *Supposons que T soit fini et qu'il forme localement une presque intersection complète. Alors, pour tout entier $\nu \geq \mu_0$ et tout entier $\ell \geq 2$, le $k[T_1, \ldots, T_{n+1}]$-module $(J\langle\ell\rangle/J\langle\ell-1\rangle)_\nu$ est libre de rang*

$$\begin{cases} \dim_k(H^0_{\mathfrak{m}}(H_1))_{\nu+2d} & \text{si } \ell = 2 \\ \dim_k(H^0_{\mathfrak{m}}(H_1))_{\nu+\ell d} + \dim_k(R/(I : \mathfrak{m}^\infty))_{(n+1-\ell)d-n-\nu} & \text{si } \ell \geq 3 \end{cases}$$

Le fait que les modules $(J\langle\ell\rangle/J\langle\ell-1\rangle)_\nu$ soient libres est tout à fait remarquable. Il permet, en adjoignant le morphisme canonique

$$\oplus_{\ell=2}^{n}(J\langle\ell\rangle/J\langle\ell-1\rangle)_\nu \to R_\mu \otimes_k k[T_1,\ldots,T_{n+1}]$$

au complexe d'approximation $(\mathcal{Z}_\bullet)_\nu$ qui est acyclique sous les hypothèse du théorème ci-dessus, de construire une résolution de $(\mathrm{Sym}_R(I)^\star)_\nu$. Plus précisément, on a le

Corollaire 11 ([19, Corollary 1])**.** *Supposons que T soit fini et qu'il forme localement une presque intersection complète. Alors, pour tout entier $\nu \geq \mu_0$ le $k[T_1,\ldots,T_{n+1}]$-module $(\mathrm{Sym}_R(I)^\star)_\nu$ admet une résolution libre et minimale de la forme*

$$\cdots \to (\mathcal{Z}_i)_\nu \to \cdots \to (\mathcal{Z}_2)_\nu \to (\mathcal{Z}_1)_\nu \oplus_{\ell=2}^{n} (J\langle\ell\rangle/J\langle\ell-1\rangle)_\nu \to (\mathcal{Z}_0)_\nu = R_\nu \otimes_k k[T_1,\ldots,T_{n+1}]. \quad (1.7)$$

Enfin, mentionnons l'encadrement suivant de l'entier "seuil" μ_0 en termes de n et d.

Proposition 12 ([19, Proposition 6])**.** *Supposons que T soit fini et qu'il forme localement une presque intersection complète. Alors,*

$$\left\lfloor \frac{(n-2)(d-1)-1}{2} \right\rfloor \leq \mu_0 \leq \eta_0 \leq (n-1)(d-1).$$

1.5.2 Matrices de représentations à coefficients des formes non linéaires

Du corollaire 11 on peut extraire une nouvelle famille de matrices à coefficients dans $k[T_1,\ldots,T_{n+1}]$. Pour tout $\nu \in \mathbb{N}$ on définit la matrice $\mathbf{M}(\phi)_\nu$ comme étant une matrice de l'application

$$(\mathcal{Z}_1)_\nu \oplus_{\ell=2}^{n} (J\langle\ell\rangle/J\langle\ell-1\rangle)_\nu \to (\mathcal{Z}_0)_\nu = R_\nu \otimes_k k[T_1,\ldots,T_{n+1}]$$

extraite du complexe (1.7). Au vu du théorème 9, pour tout $\nu \geq \mu_0$ ces matrices peuvent être qualifiées de matrices de représentation de ϕ puisqu'elles possèdent les mêmes propriétés que la famille de matrices $\mathbf{L}(\phi)_\nu$, $\nu \geq \eta_0$.

L'intérêt de cette nouvelle famille réside principalement dans les matrices $\mathbf{M}(\phi)_\nu$ pour $\mu_0 \leq \nu < \eta_0$. Effet, pour tout $\nu \geq \eta_0$ les matrices $\mathbf{M}(\phi)_\nu$ et $\mathbf{L}(\phi)_\nu$ fournissent une présentation du même module puisque $H^0_{\mathfrak{m}}(\mathrm{Sym}_R(I))_\nu = 0$ pour $\nu \geq \eta_0$ et donc le corollaire 11 entraîne immédiatement que $\mathbf{M}(\phi)_\nu$ et $\mathbf{L}(\phi)_\nu$ coïncident pour $\nu \geq \eta_0$. Ainsi, on s'aperçoit que cette méthode permet, pour tout $\mu_0 \leq \nu < \eta_0$, de compléter la matrice $\mathbf{L}(\phi)_\nu$ par un bloc construit à partir d'éléments non linéaires de J, de telle sorte que cette matrice conserve ses propriétés de représentation matricielle de ϕ. On obtient ainsi des matrices dont la taille est plus petite et surtout dont le rang générique est plus petit. Par contre, ces matrices sont un peu plus compliquées à construire puisqu'il va falloir calculer des équations non linéaires de I. Il faut cependant noter que cela reste des calculs d'algèbre linéaire puisque l'on travaille toujours au degré fixé ν.

Illustrons notre propos avec l'exemple suivant tiré de [4] et [19], pour lequel tous les calculs ont été faits avec le logiciel Macaulay2 [Grayson and Stillman] :

$$f_1 = X_1X_3^2,\ f_2 = X_2^2(X_1+X_3),\ f_3 = X_1X_2(X_1+X_3),\ f_4 = X_2X_3(X_1+X_3).$$

Le schéma T se compose de 2 points de multiplicité 2, qui sont $(0:0:1)$, $(1:0:0)$, et d'un point de multiplicité 3, le point $(0:1:0)$. Il se trouve que le saturé de I par rapport à $\mathfrak{m}$ est l'intersection complète $(X_1X_2+X_2X_3, X_1X_3^2)$ dont on déduit que $\eta_0 = 2\times(3-1)-2 = 2$. On peut alors calculer, par exemple, la matrice

$$\mathbf{L}(\phi)_2 = \begin{pmatrix} T_1 & 0 & 0 & 0 & 0 & T_3 & 0 & 0 & 0 \\ -T_2 & T_1 & 0 & 0 & 0 & 0 & T_3 & 0 & T_0 \\ 0 & 0 & T_1 & 0 & 0 & -T_2 & 0 & T_3 & 0 \\ 0 & -T_2 & 0 & T_3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -T_2 & -T_1 & T_3 & 0 & -T_2 & 0 & T_0 \\ 0 & 0 & 0 & 0 & -T_1 & 0 & 0 & -T_2 & -T_2 \end{pmatrix}.$$

Maintenant, calculons l'entier μ_0 : nous avons $\mathrm{indeg}(H_1) = \mathrm{indeg}(H^0_{\mathfrak{m}}(H_1)) - d = 4$ et donc $\mu_0 = 0$. Ainsi, bien que $\mathbf{L}(\phi)_0$ et $\mathbf{L}(\phi)_1$ ne fournissent pas une représentation matricielle de ϕ, la méthode exposée ci-dessus permet de les compléter en les matrices $\mathbf{M}(\phi)_0$ et $\mathbf{M}(\phi)_1$ afin de récupérer cette propriété de représentation en ces deux degrés.

Le calcul montre que $H^0_{\mathfrak{m}}(H_1)$ est concentré en degré 7. On déduit alors que $\mathbf{M}(\phi)_0$ est une matrice 1×1 dont l'unique entrée est une équation implicite de $\mathcal{H}$ qui est de degré 3 ;

$$\mathbf{M}(\phi)_0 = \left(T_1T_2T_3 + T_1T_2T_4 - T_3T_4^2\right).$$

Plus intéressant est le cas $\mu = 1$; le calcul donne $\dim(Z_1)_{1+d} = 3$ équations linéaires et $\dim H^0_{\mathfrak{m}}(H_1)_{1+3d} = 1$ équations quadratiques de J puisque $\dim(R/I^{sat})_{-1} = 0$. On trouve ainsi

$$\mathbf{M}(\phi)_1 = \begin{pmatrix} T_2 & 0 & T_4 & -T_4^2 \\ -T_3 & T_4 & 0 & T_1T_3 + T_1T_4 \\ 0 & -T_2 & -T_4 & 0 \end{pmatrix}.$$

Dans le travail [4] en collaboration avec D. Cox et C. D'Andrea, nous cherchions à construire des matrices de représentation de ϕ faisant intervenir des équations linéaires et quadratiques qui soient carrées. L'exemple ci-dessus était un exemple où la méthode exposée dans [4] échouait. Le travail [19] en collaboration avec M. Chardin et A. Simis, met en évidence que les limites techniques apparaissant dans [4] sont uniquement dues au fait que nous nous focalisions sur des matrices carrées.

1.5.3 Le cas où I est $\mathfrak{m}$-primaire

Sous l'hypothèse que le schéma projectif T est vide, on peut préciser quelques points de la méthode précédente. Tout d'abord, nous avons $H^1_{\mathfrak{m}}(H_1) = 0$, $H^0_{\mathfrak{m}}(H_1) = 0$ et

$$\mu_0 = n(d-1) - \mathrm{indeg}(H_1) + 1.$$

Il est d'ailleurs possible d'affiner l'encadrement de μ_0 comme suit.

Proposition 13 ([19, Corollary 3])**.** *Supposons que $T = \emptyset$, alors*

$$\left\lfloor \frac{(n-1)(d-1)}{2} \right\rfloor \leq \mu_0 \leq \eta_0 = (n-1)(d-1).$$

De plus, l'inégalité à gauche devient une égalité si le corps k est de caractéristique nulle et les polynômes $f_1, \ldots, f_{n+1}$ sont suffisamment généraux.

Revenant sur la famille de matrices $\mathbf{M}(\phi)_\nu$, $\nu \geq \mu_0$, il est également possible de préciser leur construction. En premier lieu, on montre que toute équation non linéaire de J intervenant dans une des matrices $\mathbf{M}(\phi)_\nu$ peut être obtenue en appliquant un morphisme, appelé "downgrading", à une équation linéaire de J. En effet, on montre que les coefficients d'une telle forme linéaire sont des éléments qui appartiennent à une certaine puissance de I. Pour préciser, on montre [19, §3.3] que pour tout $\nu \geq \mu_0$ et tout entier $p \geq 2$ l'application (bien définie) graduée

$$\begin{array}{rcl} (J\langle p\rangle / J\langle p-1\rangle)_\nu & \to & (J\langle p-1\rangle / J\langle p-2\rangle)_{\nu+d} \\ \displaystyle\sum_{1\leq i_1,\ldots,i_p\leq n+1} c_{i_1,\ldots,i_p} T_{i_1}\ldots T_{i_p} & \mapsto & \displaystyle\sum_{1\leq i_1,\ldots,i_p\leq n+1} c_{i_1,\ldots,i_p} f_{i_1} T_{i_2}\ldots T_{i_p} \end{array}$$

est un isomorphisme.

Enfin, il est également possible de décrire un peu plus explicitement le degré des éléments de J qui apparaissent dans une matrice de représentation $\mathbf{M}(\phi)_\nu$. On a le résultat suivant.

Proposition 14 ([19, §3.2])**.** *Supposons que $T = \emptyset$. Pour tout $\ell \in \mathbb{N}$, la matrice $\mathbf{M}(\phi)_\nu$ ne contient que des équations de J de degré au plus ℓ si*

$$\nu \geq \max\left\{(n-\ell)(d-1) - (\ell-1), \mu_0\right\}.$$

De plus, pour tout $\nu \geq \mu_0$, toute équation de degré ℓ de J qui apparaît dans la construction de la matrice $\mathbf{M}(\phi)_\nu$ est telle que

$$\ell \leq \left\lceil \frac{\mathrm{indeg}(H_1)}{d} \right\rceil \leq \left\lceil \frac{n+1}{2} \right\rceil.$$

On peut noter par exemple que la matrice $\mathbf{M}(\phi)_\nu$ ne fait intervenir que des équations linéaires et quadratiques de J si $\nu \geq \max\{(n-2)(d-1)-1, \mu_0\}$. On en déduit que dans le cas $n=3$ les matrices $\mathbf{M}(\phi)_\nu$, $\nu \geq \mu_0$, ne font intervenir que des équations linéaires ou quadratiques de J, et rien d'autre, puisque dans ce cas on a nécessairement $\mu \geq d-1$ par la proposition 13. D'ailleurs, il est à noter que, toujours dans ce cas $n=3$, on retrouve les résultat de [Cox et al., 2000] (ces résultats correspondent au cas $\mu = d-1$, voir [19] pour plus de détails) et on les améliore en montrant que les conditions techniques disparaissent ici aussi en considérant des matrices non nécessairement carrées.

1.6 Application au problème d'intersection courbe/surface

Dans ce qui précède, nous avons construit une famille de matrices $\mathbf{M}(\phi)_\nu$, $\nu \geq \mu_0$, qui permet de représenter l'hypersurface $\mathcal{H}$ obtenue comme l'image fermée de la paramétrisation ϕ. On parle de représentation matricielle, terminologie que l'on justifie par les propriétés suivantes : pour tout $\nu \geq \mu_0$,

- les coefficients de $\mathbf{M}(\phi)_\nu$ sont des formes homogènes dans $k[T_1, \ldots, T_{n+1}]$; ce sont des formes linéaires dès lors que $\nu \geq \eta_0$, par exemple dès que $\nu \geq (n-1)(d-1)$,
- le rang de $\mathbf{M}(\phi)_\nu$ est génériquement $\binom{n-1+\nu}{n-1}$, c'est-à-dire le nombre de lignes de $\mathbf{M}(\phi)_\nu$, et il chute exactement sur l'hypersurface $\mathcal{H} \subset \mathbb{P}^n$,
- le PGCD des mineurs d'ordre $\binom{n-1+\nu}{n-1}$ de $\mathbf{M}(\phi)_\nu$ est égal au produit

$$H(T_1, \ldots, T_{n+1})^{\deg(\phi)} \prod_{\mathfrak{p} \in T} L_{\mathfrak{p}}(T_1, \ldots, T_{n+1})^{e_{\mathfrak{p}} - d_{\mathfrak{p}}}$$

(avec la convention $L_{\mathfrak{p}} := 1$ lorsque $e_{\mathfrak{p}} = d_{\mathfrak{p}}$).

Les coefficients des matrices $\mathbf{M}(\phi)_\nu$ sont des formes homogènes dans $k[T_1, \ldots, T_{n+1}]$ dont le degré est constant par colonne. Par conséquent la notion de rang de $\mathbf{M}(\phi)_\nu$ en un point de $\mathbb{P}^n$ a du sens. Et par propriété de la matrice $\mathbf{M}(\phi)_\nu$, il est clair que pour tout point $P \in \mathbb{P}^n$, on a

$$P \in \mathcal{H} \subset \mathbb{P}^n \Leftrightarrow \text{rang } (\mathbf{M}(\phi)_\nu(P)) < \binom{n-1+\nu}{n-1}. \tag{1.8}$$

La notation $\mathbf{M}(\phi)_\nu(P)$ signifie que l'on a évalué la matrice $\mathbf{M}(\phi)_\nu$ au point P, coefficient par coefficient. Il faut également noter que la quantité $\binom{n-1+\nu}{n-1}$ correspond au rang générique de la matrice $\mathbf{M}(\phi)_\nu$, donc qu'un point P appartient à l'hypersurface $\mathcal{H}$ si et seulement si le rang de $\mathbf{M}(\phi)_\nu$ chute en ce point.

La propriété (1.8) peut être vue comme un problème d'intersection point/surface. Les représentations matricielles permettent de le résoudre par un simple calcul de rang. Dans ce qui suit, nous allons montrer comment ces représentations peuvent aussi se substituer à des représentations plus classiques dans la résolution du problème d'intersection courbe/surface, problème important en modélisation géométrique. Rappelons que ce type de représentations matricielles a déjà été étudié mais uniquement dans le cas où ces matrices sont carrées (voir par exemple [Manocha and Canny, 1991]). Notre objectif est de montrer que l'on peut aussi utiliser des représentations matricielles non carrées.

À partir de maintenant, nous allons nous concentrer sur le cas $n=3$ car c'est le cas pertinent pour la modélisation géométrique. Les hypothèses d'existence de la matrice $\mathbf{M}(\phi)_\nu$ y sont d'ailleurs tout à fait raisonnables. Noter que dans le cas $n=2$ il existe toujours une représentation matricielle carrée et que ce cas est donc plus ou moins déjà traité dans la littérature existante.

Dans la suite, pour simplifier le texte nous nous restreindrons au cas où T est fini et qu'il forme localement une intersection complète, de telle sorte que $\mathbf{M}(\phi)_\nu$, $\nu \geq \mu_0$, représente exactement $\mathcal{H}$ sans autre facteur parasite. Aussi, k sera supposé être un corps algébriquement clos.

1.6.1 Intersection avec une courbe

On suppose donnée une courbe rationnelle $\mathcal{C}$ qui est représentée par la paramétrisation

$$\Psi : \mathbb{P}^1 \to \mathbb{P}^3 : (s:t) \mapsto (x(s,t) : y(s,t) : z(s,t) : w(s,t))$$

où $x(s,t), y(s,t), z(s,t), w(s,t)$ sont des polynômes homogènes dans $k[s,t]$ sans facteur commun et de même degré. On suppose en outre que l'intersection $\mathcal{C} \cap \mathcal{H}$ est finie, ce qui revient à supposer que $\mathcal{C}$ n'est pas contenue dans $\mathcal{H}$.

Afin de déterminer l'ensemble d'intersection $\mathcal{C} \cap \mathcal{H}$, une procédure classique consiste à déterminer les racines du polynôme homogène

$$H(x(s,t), y(s,t), z(s,t), w(s,t)) \in k[s,t]$$

puisque ces dernières sont en correspondance avec l'ensemble $\mathcal{C} \cap \mathcal{H}$ par Ψ. Dans le cadre de la thèse T. Luu Ba, et en collaboration avec B. Mourrain, nous avons proposé [27] une méthode alternative basée sur l'utilisation des matrices de représentation, évitant ainsi le calcul du polynôme $H(T_1, \ldots, T_4)$. Nous la décrivons maintenant brièvement.

Soit $\mathbf{M}(\phi)_\nu$, $\nu \geq \eta_0$, une matrice de représentation de ϕ. En substituant les polynômes $x(s,t)$, $y(s,t)$, $z(s,t)$, $w(s,t)$ aux variables $T_1, \ldots, T_4$ dans cette matrice, nous obtenons une nouvelle matrice, que nous noterons

$$M(s,t) := \mathbf{M}(\phi)_\nu(x(s,t), y(s,t), z(s,t), w(s,t)),$$

dont les entrées sont des polynômes homogènes dans $k[s,t]$. Puisque Ψ est supposée régulière, par propriété d'une matrice de représentation nous avons que pour tout point $(s_0 : t_0) \in \mathbb{P}^1$, le rang de la matrice $M(s_0, t_0)$ chute si et seulement si le point $\Psi(s_0, t_0)$ appartient à l'ensemble $\mathcal{C} \cap \mathcal{H}$. Par conséquent, l'ensemble $\mathcal{C} \cap \mathcal{H}$ est en correspondance avec les points de $\mathbb{P}^1$ où le rang de la matrice $M(s,t)$ chute, plus précisément où le rang de $M(s,t)$ n'est pas égal à son nombre de lignes.

À ce stade, un calcul de forme de Smith sur la matrice $M(1,t)$ permet de ramener le problème ci-dessus à la résolution d'un polynôme univarié. Cependant, le calcul d'une forme de Smith peut s'avérer algorithmiquement parlant très coûteux. Dans ce qui suit, nous présentons une approche alternative, ainsi que les ingrédients nécessaires de l'algèbre linéaire ; le lecteur intéressé est renvoyé à [27] pour plus de détails.

1.6.2 Linéarisation d'une matrice polynomiale

Étant donnée une matrice $M(t) = (a_{i,j}(t))$ de taille $m \times n$ à coefficients dans $k[t]$, on peut l'écrire sous la forme

$$M(t) = M_d t^d + M_{d-1} t^{d-1} + \ldots + M_0$$

où $d = \max_{i,j}\{\deg(a_{i,j}(t))\}$ et M_i, $i = 1, \ldots, d$, est une matrice de taille $m \times n$ à coefficients dans k. On définit alors les *matrices compagnes généralisées*, que nous noterons A et B, par

$$A = \begin{pmatrix} 0 & I_m & 0 & \cdots & 0 \\ 0 & 0 & I_m & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & I_m \\ {}^tM_0 & {}^tM_1 & \cdots & {}^tM_{d-2} & {}^tM_{d-1} \end{pmatrix}, \quad B = \begin{pmatrix} I_m & 0 & 0 & \cdots & 0 \\ 0 & I_m & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & I_m & 0 \\ 0 & \cdots & 0 & 0 & -{}^tM_d \end{pmatrix}$$

où I_r désigne la matrice identité de taille r et où la notation ${}^t-$ désigne l'opération de transposition d'une matrice. Ce sont deux matrices de taille $((d-1)m+n) \times dm$ à coefficients dans k. Elles permettent de *linéariser* la matrice polynomiale $M(t)$ au sens où il existe deux matrices unimodulaires $E(t)$ et $F(t)$ à coefficients dans $k[t]$ et de taille respective dm et $(d-1)m+n$ telles que

$$E(t)\,(A - tB)\,F(t) = \left(\begin{array}{c|c} {}^tM(t) & 0 \\ \hline 0 & I_{d(m-1)} \end{array}\right). \tag{1.9}$$

Ainsi, les valeurs de $t \in k$ pour lesquelles le rang de $M(t)$ chute sont en correspondance avec les valeurs de $t \in k$ pour lesquelles le rang de $A - tB$ chute. On les appelle les valeurs propres généralisées du pinceau de matrices $A - tB$. Si les matrices A et B sont des matrices carrées et que B est une matrice inversible alors les valeurs propres généralisées du pinceau $A - tB$ se calculent directement à l'aide de l'algorithme dit "QZ" [Golub and Van Loan, 1996]. Dans le cas contraire, il faut réduire le pinceau.

1.6.3 Extraction de la partie régulière d'un pinceau de matrices

Pour tout pinceau de matrices $A - tB$, il existe des matrices constantes et inversibles P et Q telles que le pinceau de matrices $P(A - tB)Q = PAQ - tPBQ$ est diagonal par blocs de la forme

$$\mathrm{diag}\{L_{i_1}, ..., L_{i_s}, L^t_{j_1}, ..., L^t_{j_u}, \Omega_{k_1}, ..., \Omega_{k_v}, A' - tB'\} \tag{1.10}$$

où les matrices A' et B' sont carrées, la matrice B' est inversible et où pour tout entier $k \geq 1$ les matrices $L_k(t)$, de taille $k \times (k+1)$, et $\Omega_k(t)$, de taille $k \times k$, sont définies par

$$L_k(t) = \begin{pmatrix} 1 & t & 0 & \dots & 0 \\ 0 & 1 & t & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 1 & t & 0 \\ 0 & 0 & \dots & 1 & t \end{pmatrix}, \quad \Omega_k(t) = \begin{pmatrix} 1 & t & 0 & \dots & 0 \\ 0 & 1 & t & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & \dots & 1 & t \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}.$$

On parle de la forme de Kronecker du pinceau $A - tB$ (voir par exemple [Gantmacher, 1966, p. 31-34] ou bien [Dieudonné, 1946]).

Le bloc $A' - tB'$ est la partie régulière du pinceau $A - tB$. Dans notre contexte du problème d'intersection, il est très intéressant car il contient toute l'information sur les valeurs propres généralisées (à distance finie) du pinceau $A - tB$ et car l'on sait calculer ses valeurs propres généralisées par un algorithme QZ puisque c'est un bloc carré. Avec B. Mourrain et T. Luu Ba, nous avons donc proposé dans [27] un algorithme permettant d'extraire la partie régulière $A' - tB'$ d'un pinceau de matrice $A - tB$. Cet algorithme est essentiellement basé sur les idées développées dans [Beelen and Van Dooren, 1988] et les méthodes de réduction exposées dans [Mourrain, 1998, 2005]. Nous renvoyons à nouveau le lecteur à [27] pour plus de détails.

1.6.4 Retour sur l'intersection courbe/surface

Nous avons maintenant tous les éléments pour énoncer un algorithme permettant de calculer, de manière approchée, l'intersection entre une surface rationnelle et une courbe rationnelle lorsque cette dernière n'est pas contenue dans la première. Cet algorithme a été implémenté par Thang Luu Ba dans le cadre de son travail de thèse.

Entrées : une matrice de représentation, notée $M(T_1, \dots, T_4)$, de la surface $\mathcal{H}$ et une paramétrisation Ψ de la courbe rationnelle $\mathcal{C}$.
Sortie : les coordonnées des points de $\mathcal{H} \cap \mathcal{C}$ (à distance finie).
Description :

1. On forme la matrice $M(\Psi(t))$.
2. On forme les matrices compagnes A, B de la matrice $M(\Psi(t))$.
3. On calcule la partie régulière $A' - tB'$ du pinceau $A - tB$.
4. On calcule l'ensemble des valeurs propres (généralisées) $\{t_1, \dots, t_r\}$ du pinceau $A' - tB'$.
5. On renvoie l'ensemble de points $\{\Psi(t_1), \dots, \Psi(t_r)\}$.

Mentionnons que de l'algorithme ci-dessus on peut également tirer des informations sur la multiplicité d'intersection d'un point. Supposons pour simplifier que $\mathcal{H}$ et $\mathcal{C}$ sont toutes les deux données initialement par des paramétrisations birationnelles, bien qu'il soit possible de discuter le cas général de manière comparable. Toute valeur propre généralisée, disons t_1, obtenue à l'étape 4 de l'algorithme ci-dessus vient avec sa multiplicité, en tant que valeur propre, que nous noterons m_{t_1}. Des équations (1.9), (1.10) et des propriétés classiques des matrices polynomiales sur un anneau principal on déduit aisément que m_{t_1} est la valuation d'un générateur de l'idéal (principal) des mineurs maximaux de $M(t)$ en t_1 :

$$m_{t_1} := \mathrm{val}_{t_1} \det_{\max}(M(t)).$$

Ceci étant, le point $P := \Psi(t_1)$ est un point appartenant à l'intersection de $\mathcal{H}$ et de $\mathcal{C}$. Comme tel, on peut lui associer une multiplicité d'intersection, que nous noterons I_P, et que l'on peut définir par la formule (supposant que $\Psi(\infty) \neq P$)

$$I_P = \sum_{t_i \text{ tel que } \Psi(t_i) = P} \mathrm{val}_{t_i} H(\Psi(t)).$$

On a alors envie d'en déduire directement la formule suivante qui relie les deux notions de multiplicités en tant que point d'intersection et valeur propre généralisée :

$$I_P = \sum_{t_i \text{ tel que } \Psi(t_i)=P} m_{t_i}. \tag{1.11}$$

Cette formule n'est malheureusement pas toujours vraie, bien qu'elle le soit dans la plupart des cas. En effet, en toute généralité, le polynôme $H(\Psi(t))$ n'est qu'un diviseur d'un générateur de l'idéal $\det_{\max}(M(t))$. Cela provient du fait que les idéaux (H) et $\det_{\max}(M)$ de $k[T_1, \ldots, T_4]$ ne définissent pas les mêmes schémas, mais définissent les mêmes variétés algébriques. L'idéal $\det_{\max}(M)$ décrit ici la surface $\mathcal{H}$ et d'éventuelles composantes immergées. Ce sont ces composantes qui peuvent faire augmenter la multiplicité en tant que valeur propre. En fait, l'égalité (1.11) est vraie si I_P désigne la multiplicité d'intersection de $\mathcal{C}$ avec le schéma défini par l'idéal $\det_{\max}(M)$, et non pas la surface $\mathcal{H}$. On a donc, en toute généralité, uniquement l'inégalité

$$I_P \leq \sum_{t_i \text{ tel que } \Psi(t_i)=P} m_{t_i}.$$

Notons toutefois que pour un choix générale de la courbe $\mathcal{C}$, celle-ci évite les composantes immergées sur $\mathcal{H}$ du schéma défini par l'idéal $\det_{\max}(M) \subset k[T_1, \ldots, T_4]$.

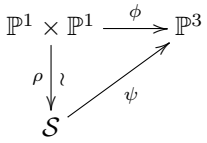
1.7 Une note sur les paramétrisations bi-graduées de surfaces.

Dans le cadre de la thèse de Marc Dohm [Dohm, 2008], nous avons proposé une première extension à la méthode d'implicitation décrite aux paragraphes 1.3 et 1.4 pour pouvoir traiter le cas des surfaces paramétrées par le produit de deux droites projectives sans contorsion. En effet, ce type de surfaces est très utilisé en modélisation géométrique et il est donc intéressant de prendre en compte leur structure plutôt que de devoir compactifier au plan projectif avec le risque d'introduire des points base en nombre et qualité indésirables. Nous expliquons très succinctement ici l'idée principale de notre approche et renvoyons le lecteur à [26] pour plus de détails et une description algorithmique de la méthode en Macaulay2 [Grayson and Stillman].

Soit une surface $\mathcal{H}$ donnée par la paramétrisation

$$\begin{array}{rcl} \mathbb{P}^1 \times \mathbb{P}^1 & \xrightarrow{\phi} & \mathbb{P}^3 \\ (s:u) \times (t:v) & \mapsto & (f_1 : f_2 : f_3 : f_4)(s,u,t,v) \end{array}$$

où chaque polynôme f_1, f_2, f_3, f_4 est bi-homogène par rapport aux deux couples de variables $(s:u)$ et $(t:v)$. En outre, pour des raisons techniques qui vont rapidement apparaître, nous supposerons que f_1, f_2, f_3, f_4 sont de bi-degré (d,d), d étant un entier positif non nul. L'approche développée dans [26] consiste à reparamétrer $\mathcal{H}$ afin de ramener la bi-graduation de ϕ à une graduation simple, c'est-à-dire au cadre algébrique qui a été développé précédemment pour les surfaces paramétrées par un espace projectif. Une telle reparamétrisation peut se faire au travers du plongement de Segre $\rho : \mathbb{P}^1 \times \mathbb{P}^1 \xrightarrow{\sim} \mathcal{S} \subset \mathbb{P}^3$ qui fournit le diagramme commutatif



D'un point de vue algébrique, $\mathcal{S} = \mathrm{Proj}(A)$ où A est l'anneau gradué $k[X_1, X_2, X_3, X_4]/(X_1X_4 - X_2X_3)$ et $\mathbb{P}^1 \times \mathbb{P}^1$ peut être vu comme le spectre homogène de l'anneau gradué $\bigoplus_{n\in\mathbb{N}} (k[s,u]_n \otimes_k k[t,v]_n)$. Il s'en suit que l'isomorphisme ρ est induit par l'isomorphisme gradué d'anneaux

$$\begin{array}{rcl} A = k[X_1, X_2, X_3, X_4]/(X_1X_4 - X_2X_3) & \xrightarrow{\sim} & \displaystyle\bigoplus_{n\in\mathbb{N}} (k[s,u]_n \otimes_k k[t,v]_n) \\ X_1 & \mapsto & st \\ X_2 & \mapsto & sv \\ X_3 & \mapsto & ut \\ X_4 & \mapsto & uv. \end{array}$$

Ainsi, il apparaît que la paramétrisation ψ est induite par le morphisme

$$\begin{array}{rcl} k[T_1, T_2, T_3, T_4] & \stackrel{h}{\to} & A \\ T_i & \mapsto & g_i(X_1, X_2, X_3, X_4) \end{array}$$

où $g_1, \ldots, g_4$ sont des polynômes homogènes de degré d tels que $g_i(st, sv, ut, uv) = f_i(s, u; t, v)$. Partant de là, on peut reprendre tout le cheminement de la méthode exposée au début de ce chapitre, car bien que l'anneau A ne soit plus un anneau de polynômes, il possède la propriété Gorenstein qui demeure suffisante (cf. [26]).

Suite à ces travaux, Marc Dohm a continué l'étude de cette approche au cas des surfaces paramétrées par une variété torique, en collaboration avec Nicolàs Botbol et Alicia Dickenstein [Botbol et al., 2009], toujours en utilisant un plongement (d'une variété torique cette fois). Plus récemment, Nicolàs Botbol a donné dans son travail de thèse [Botbol, 2010c,a] une extension directe de la méthode décrite aux paragraphes 1.3 et 1.4 sans considérer de plongement, mais en travaillant directement sur l'anneau de Cox associé à une variété torique. Mentionnons pour finir que [Botbol et al., 2009] et [Botbol, 2010a] ont donné lieu à des implémentations en Macaulay2 [Grayson and Stillman] par leurs auteurs, respectivement [Botbol and Dohm, 2010] et [Botbol, 2010b].

Chapitre 2

Étude des courbes algébriques rationnelles pour la modélisation géométrique

Les courbes algébriques qui sont utilisées en modélisation géométrique sont souvent données sous une forme paramétrée. Ces courbes sont dites rationnelles et constituent une classe particulière des courbes algébriques. Pour de nombreuses applications, il s'avère très utile de pouvoir changer la représentation paramétrée de ces courbes pour une représentation implicite ; c'est le problème d'implicitation.

Le cas des courbes planes a été très largement traité dans la littérature et peut être considéré comme bien compris (voir par exemple le chapitre précédent). Par contre, le cas des courbes rationnelles dans un espace projectif de dimension au moins 3 est beaucoup plus compliqué. La raison principale est qu'une unique équation implicite ne suffit plus pour décrire cette courbe, il en faut forcément plusieurs. La détermination de telles équations, en nombre et format raisonnables est alors un problème difficile (cf. par exemple [Fortuna et al., 2009], [Song and Goldman, 2009] et [Jia et al., 2010]).

Mes travaux sur ce sujet ont porté sur la recherche d'une représentation matricielle implicite simple. Les premiers résultats ont été obtenus en collaboration avec A. Galligo [22] dans le cadre d'une nouvelle représentation des surfaces que nous avions introduite et baptisée *semi-implicite* [9]. L'idée sous-jacente était d'exploiter la structure déterminantielle de certaines familles de courbes pour aboutir à une représentation implicite matricielle basée sur le résultant déterminantiel [7]. Toutefois, cette méthode possède le défaut de rigidifier énormément la classe des objets algébriques pour laquelle elle s'applique [23]. Par la suite, je me suis aussi intéressé, en collaboration avec M. Elkadi et A. Galligo, au cas des surfaces réglées utilisées en modélisation géométrique, surfaces qui peuvent s'interpréter à l'aide d'une certaine courbe rationnelle dans un espace projectif de plus grande dimension [15].

Plus récemment, dans le cadre de la thèse de Thang Luu Ba, nous avons proposé une nouvelle représentation implicite des courbes rationnelles [20] qui possède l'avantage de représenter la courbe à l'aide d'une *unique* matrice, alors qu'une représentation par un ensemble d'équations en nécessite forcément plusieurs. L'idée de cette nouvelle représentation est simple : plutôt que de chercher une structure particulière à notre problème, nous forçons une telle structure en introduisant une approximation de notre courbe par une courbe déterminantielle. Le terme d'approximation signifie ici que nous introduisons une nouvelle courbe algébrique, en général non rationnelle, qui possède le même support que notre courbe originale mais qui peut présenter des composantes immergées.

Nous commençons ce chapitre en introduisant cette nouvelle représentation implicite des courbes rationnelles [20]. Ensuite, nous montrons sa pertinence pour traiter un problème important en modélisation géométrique : la détection d'intersection entre deux courbes. Nous expliquons comment cette nouvelle représentation matricielle implicite permet de traiter ce problème en restant au niveau des matrices et en n'utilisant que des outils standards d'algèbre linéaire (numérique), de manière très similaire à ce que nous avons fait au chapitre précédent pour le problème d'intersection courbe/surface. Ces développements sont en fait une généralisation de techniques déjà bien connues pour le cas des courbes planes (cf. [25]). Enfin, nous illustrons aussi la pertinence de ces représentations pour détecter le lieu singulier d'une courbe rationnelle. Notons que de tels problèmes pour les courbes rationnelles ont été récemment traités dans [Song and Goldman, 2009], [Wang et al., 2009] et [Jia et al., 2010] à l'aide de méthodes basées sur des

représentations implicites polynomiales des courbes rationnelles. Notre approche permet de gommer les limitations de ces dernières en termes de degré des courbes et de multiplicités des points singuliers.

La dernière partie de ce chapitre est dédiée à des résultats que j'ai obtenus autour des courbes planes rationnelles, à savoir [17] puis [31] en collaboration avec C. D'Andrea. Ces travaux ont été motivés par plusieurs conjectures autour des équations de l'algèbre de Rees associée à une paramétrisation d'une courbe algébrique plane, notamment une conjecture de D. Cox autour d'un lien entre ces équations et des pinceaux de courbes adjointes.

Pour simplifier l'exposition, dans la suite k désignera un corps algébriquement clos.

2.1 Représentations implicites matricielles

Supposons donnée une paramétrisation régulière d'une courbe algébrique rationnelle $\mathcal{C}$

$$\begin{array}{rcl} \mathbb{P}^1 & \xrightarrow{\phi} & \mathbb{P}^n \\ (s:t) & \mapsto & (f_0 : f_1 : \cdots : f_n)(s,t). \end{array}$$

où $f_0, f_1, \ldots, f_n$ sont $n+1$ polynômes homogènes dans $k[s,t]$ de même degré $d \geq 1$ tels que leur plus grand diviseur commun est un élément non nul dans k. Le degré de $\mathcal{C}$, le degré de ϕ et l'entier d sont alors liés par la relation $\deg(\mathcal{C})\deg(\phi) = d$.

2.1.1 L'idéal de définition

La paramétrisation ϕ est une représentation très pratique de la courbe $\mathcal{C}$, représentation qui est largement utilisée en modélisation géométrique. Cependant, pour résoudre certains problèmes, notamment des problèmes d'intersection, une représentation implicite de $\mathcal{C}$, c'est-à-dire en termes des coordonnées de $\mathbb{P}^n$, est souhaitable. En outre, nous noterons $(x_0 : \cdots : x_n)$ les coordonnées homogènes de $\mathbb{P}^n$.

La représentation implicite de $\mathcal{C}$ la plus répandue est son idéal de définition, que nous noterons $\mathfrak{I}_\mathcal{C}$ et qui est, par définition, le noyau du morphisme d'anneaux

$$\begin{array}{rcll} h : k[x_0, \ldots, x_n] & \to & k[s,t] & \\ x_i & \mapsto & f_i(s,t) & i = 0, \ldots, n. \end{array}$$

En d'autres termes, $\mathfrak{I}_\mathcal{C}$ est l'ensemble des polynômes $P(x_0, \ldots, x_n) \in k[x_0, \ldots, x_n]$ satisfaisant à l'égalité $P(f_0, \ldots, f_n) \equiv 0$. C'est un idéal premier (donc radical) gradué de $k[x_0, \ldots, x_n]$. D'un point de vue géométrique, on a

$$V(\mathfrak{I}_\mathcal{C}) = \{(x_0 : \cdots : x_n) \in \mathbb{P}^n \ : \ P(x_0, \ldots, x_n) = 0 \text{ pour tout } P \in \mathfrak{I}_\mathcal{C}\} = \mathcal{C}.$$

Un système fini de générateurs de $\mathfrak{I}_\mathcal{C}$ fournit donc une représentation implicite de la courbe $\mathcal{C}$. Cependant, une telle représentation peut s'avérer difficile à obtenir et à manipuler (cf. par exemple [Garrity and Warren, 1989; Fortuna et al., 2009] pour le cas $n = 3$). Dans le cadre de la thèse de Thang Luu Ba, nous avons proposé une représentation implicite alternative [20] que nous décrivons dans ce qui suit.

2.1.2 La notion de μ-base d'une courbe rationnelle

Elle a été introduite par D. Cox, T. Sederberg, F. Chen [Cox et al., 1998] et peut s'interpréter comme un pont entre les deux représentations paramétrique ϕ et implicite $\mathfrak{I}_\mathcal{C}$ de la courbe $\mathcal{C}$.

Considérons l'ensemble des relations de $\mathbf{f} := (f_0, \ldots, f_n)$

$$\mathrm{Syz}(\mathbf{f}) := \left\{ (g_0(s,t), \ldots, g_n(s,t)) \ : \ \sum_{i=0}^{n} g_i(s,t) f_i(s,t) = 0 \right\} \subset \bigoplus_{i=0}^{n} k[s,t].$$

C'est un $k[s,t]$-module libre et gradué de rang n. De plus, il existe des entiers positifs $\mu_1, \ldots, \mu_n$ et n vecteurs de polynômes

$$(u_{i,0}(s,t), u_{i,1}(s,t), \ldots, u_{i,n}(s,t)) \in \mathrm{Syz}(\mathbf{f}) \subset k[s,t]^{\oplus n+1}, \quad i = 1, \ldots, n \tag{2.1}$$

tels que :

– Pour tout $i \in \{1, \ldots, n\}$ et $j \in \{0, \ldots, n\}$, $u_{i,j}(s,t)$ est un polynôme homogène de degré $\mu_i \geq 0$,
– Les n vecteurs (2.1) forment une $k[s,t]$-base des relations de $\mathbf{f}$,
– $\sum_{i=1}^{n} \mu_i = d$,
– Pour tout $j \in \{0, \ldots, n\}$, le déterminant de la matrice obtenue en supprimant la colonne $(u_{i,j})_{i=1,\ldots,n}$ de la matrice

$$M(s,t) := \begin{pmatrix} u_{1,0}(s,t) & u_{1,1}(s,t) & \ldots & u_{1,n}(s,t) \\ u_{2,0}(s,t) & u_{2,1}(s,t) & \ldots & u_{2,n}(s,t) \\ \ldots & \ldots & \ldots & \ldots \\ u_{n,0}(s,t) & u_{n,1}(s,t) & \ldots & u_{n,n}(s,t) \end{pmatrix}$$

est égal à la quantité $(-1)^j c\, f_j(s,t) \in k[s,t]$ où $c \in k \setminus \{0\}$.

Tout cela est une conséquence directe d'un théorème classique de structure connu sous le nom du théorème de Hilbert-Burch (cf. par exemple [Eisenbud, 1995, §20.4]). Une collection de vecteurs (2.1) satisfaisant aux propriétés ci-dessus est appelée une μ-base de la paramétrisation ϕ. Il faut noter qu'une μ-base est évidemment loin d'être unique, mais la suite d'entiers $(\mu_1, \mu_2, \ldots, \mu_n)$ est unique pour peu qu'on l'ordonne. Ainsi, dans la suite nous supposerons toujours pour une μ-base que $0 \leq \mu_1 \leq \mu_2 \leq \cdots \leq \mu_n$.

Une conséquence immédiate des propriétés d'une μ-base et des règles de Cramer pour la résolution des systèmes linéaires fournit le résultat suivant d'importance notable pour construire une représentation implicite matricielle de $\mathcal{C}$.

Lemme 15. *Pour tout point $(s_0 : t_0) \in \mathbb{P}^1$, le vecteur non nul*

$$< f_0(s_0,t_0), f_1(s_0,t_0), \ldots, f_n(s_0,t_0) > \in k^{n+1}$$

engendre le noyau de la matrice $M(s_0,t_0)$. En particulier, la matrice $M(s_0,t_0)$ est de rang (maximum) n pour tout point $(s_0 : t_0) \in \mathbb{P}^1_k$.

2.1.3 Projection du graphe de la paramétrisation ϕ

Pour tout entier $i = 1, \ldots, n$, posons

$$u_i(s,t,x_0,x_1,\ldots,x_n) = \sum_{j=0}^{n} u_{i,j}(s,t)x_j \in k[s,t,x_0,\ldots,x_n]. \tag{2.2}$$

Le lemme 15 entraîne directement que la variété algébrique

$$W := \{(s:t) \times (x_0 : \cdots : x_n) \ : \ u_1 = u_2 = \cdots = u_n = 0\} \subset \mathbb{P}^1 \times \mathbb{P}^n$$

est exactement le graphe de la paramétrisation ϕ. Par suite, $\pi(W) = \mathcal{C}$ où π désigne la projection canonique

$$\pi : \mathbb{P}^1 \times \mathbb{P}^n \to \mathbb{P}^n : (s:t) \times (x_0 : \cdots : x_n) \mapsto (x_0 : \cdots : x_n).$$

Mais la situation est encore plus favorable puisque cette égalité est également vraie en termes de schémas. Afin de préciser ce point, il nous faut introduire de nouvelles notations.

Soit A l'anneau de polynômes $k[x_0, \ldots, x_n]$, de telle sorte que $k[s,t,x_0,\ldots,x_n] = A[s,t]$, soit I l'idéal $I := (u_1, \ldots, u_n)$ de $A[s,t]$ et considérons l'*idéal résultant* $\mathfrak{A}$ de I par rapport à l'idéal $\mathfrak{m} = (s,t) \subset A[s,t]$. Ainsi, par définition,

$$\mathfrak{A} = (I : \mathfrak{m}^\infty) \cap A = \{P \in A \text{ tel que } \exists\, \nu \in \mathbb{N} \ : \ \mathfrak{m}^\nu P \subset I\} \subset A.$$

Proposition 16 ([5, Corollary 3.8])**.** *Avec les notations précédentes, $\mathfrak{A} = \mathfrak{I}_\mathcal{C} \subset A$.*

Comme nous l'avons fait dans le premier chapitre pour produire des représentations matricielles de la courbe $\mathcal{C}$, nous allons exploiter le lien entre les idéaux résultants et certains annulateurs. Plus précisément, définissons l'anneau quotient $B := A[s,t]/I$ qui hérite d'une structure graduée de la graduation canonique de l'anneau $C := A[s,t]$ et de l'idéal homogène I : $\deg(s) = \deg(t) = 1$ et $\deg(a) = 0$ pour tout $a \in A$. Posons également

$$\nu_0 := \max_{i \neq j}\{\mu_i + \mu_j\} - 1 = \mu_n + \mu_{n-1} - 1$$

et pour tout entier $\nu \in \mathbb{N}$ considérons

$$\mathrm{ann}_A(B_\nu) = \{P \in A \text{ tel que } P.B_\nu = 0\} \subset A.$$

On obtient alors le résultat suivant dont la preuve est essentiellement basée sur les techniques développées dans [Jouanolou, 1980, §2.10].

Corollaire 17 ([20, Corollary 3]). *Pour tout entier $\nu \geq \nu_0$, $\mathrm{ann}_A(B_\nu) = \mathfrak{A} = \mathfrak{I}_\mathcal{C} \subset A$.*

Puis, utilisant l'idéal de Fitting initial $\mathfrak{F}(B_\nu)$ comme approximation de $\mathrm{ann}_A(B_\nu)$, on déduit le

Théorème 18. *Pour tout entier $\nu \geq \nu_0$, $V(\mathfrak{F}(B_\nu)) = \mathcal{C} \subset \mathbb{P}^n$.*

2.1.4 Représentations matricielles d'une courbe rationnelle

L'anneau quotient B est, par définition, le conoyau du morphisme gradué

$$\oplus_{i=1}^n C(-\mu_i) \xrightarrow{u_1,\ldots,u_n} C : (g_1, \ldots, g_n) \mapsto \sum_{i=1}^n u_i g_i. \tag{2.3}$$

Ainsi, en prenant les parties graduées pour tout entier $\nu \in \mathbb{N}$, le conoyau de l'application A-linéaire

$$\oplus_{i=1}^n C_{\nu-\mu_i} \xrightarrow{u_1,\ldots,u_n} C_\nu : (g_1, \ldots, g_n) \mapsto \sum_{i=1}^n u_i g_i \tag{2.4}$$

est exactement le A-module B_ν.

Pour tout entier $\nu \geq \nu_0$ nous noterons $\mathtt{M}(\phi)_\nu$ la matrice de l'application A-linéaire (2.4). Bien sûr, $\mathtt{M}(\phi)_\nu$ dépend aussi bien du choix de la μ-base de ϕ que des choix des A-bases de C_ν et $C_{\nu-\mu_i}$, $i = 1, \ldots, n$.

Le théorème 18 montre qu'un point $P \in \mathbb{P}^n$ appartient à la courbe $\mathcal{C}$ si et seulement si tous les mineurs d'ordre $\nu + 1$ de $\mathtt{M}(\phi)_\nu$ (qui forment un système de générateurs de l'idéal $\mathfrak{F}(B_\nu)$) s'annulent en ce point, et donc si et seulement si le rang de la matrice $\mathtt{M}(\phi)_\nu$ évaluée au point P n'est pas égal à $\nu + 1$ (sa valeur maximale). Par conséquent, nous avons construit une famille de matrices indexée par $\nu \in \mathbb{N}$ telle que, pour tout $\nu \geq \nu_0$

(i) $\mathtt{M}(\phi)_\nu$ est génériquement de rang maximum, c'est-à-dire de rang $\nu + 1$,

(ii) le rang de $\mathtt{M}(\phi)_\nu$ chute exactement sur la courbe $\mathcal{C}$.

Ces deux propriétés suggèrent que toute matrice $\mathtt{M}(\phi)_\nu$, $\nu \geq \nu_0$, peut être considérer comme une *représentation implicite* de la courbe $\mathcal{C}$.

Définition 1. Pour tout $\nu \geq \nu_0$, la matrice $\mathtt{M}(\phi)_\nu$ est appelée une matrice de représentation de la courbe $\mathcal{C}$, ou plus rigoureusement une matrice de représentation de la paramétrisation ϕ.

D'un point de vue ensembliste, la représentation implicite de $\mathcal{C}$ comme lieu d'annulation de plusieurs équations polynomiales (par exemple un système générateur de l'idéal de définition de $\mathcal{C}$) est remplacée par la chute du rang d'une *unique* matrice.

Il faut noter qu'en général, étant donné un entier $\nu \geq \nu_0$, l'idéal $\mathfrak{F}(B_\nu)$ n'est pas égal à l'idéal de définition $\mathfrak{I}_\mathcal{C}$ de la courbe rationnelle $\mathcal{C}$ (cf. [20, Example 7]). Néanmoins, $\mathfrak{F}(B_\nu)$ est presque partout algébriquement fidèle à la paramétrisation ϕ au sens suivant :

Théorème 19 ([20]). *Pour tout entier $\nu \geq \nu_0$,*

$$\mathfrak{F}(B_\nu)_{\mathfrak{I}_\mathcal{C}} = {\mathfrak{I}_\mathcal{C}}^{\deg(\phi)} A_{\mathfrak{I}_\mathcal{C}}$$

où $A_{\mathfrak{I}_\mathcal{C}}$ désigne la localisation de l'anneau A par l'idéal premier $\mathfrak{I}_\mathcal{C}$. En d'autres mots, les idéaux $\mathfrak{F}(B_\nu)$ et ${\mathfrak{I}_\mathcal{C}}^{\deg(\phi)}$ sont égaux en tous les points de la courbe $\mathcal{C}$ excepté pour un nombre fini, eventuellement nul, d'entre eux.

En corollaire, on voit que l'idéal $\mathfrak{F}(B_\nu)$ est égal à l'idéal ${\mathfrak{I}_\mathcal{C}}^{\deg(\phi)}$ auquel il faut éventuellement ajouter un nombre fini de composantes immergées et isolées.

Pour finir ce paragraphe, mentionnons que dans le cas $n = 2$, les deux familles de matrices construites dans ce chapitre et dans le chapitre précédent coïncident. D'ailleurs, dans ce cas la matrice $\mathtt{M}(\phi)_{d-1}$, qui n'est rien d'autre que la matrice de Sylvester associée à une μ-base u_1, u_2, est une matrice carrée dont le déterminant est une équation implicite de $\mathcal{C}$ élevée à la puissance $\deg(\phi)$.

2.2 Le problème d'intersection courbe/courbe

Étant données deux courbes rationnelles représentées par leur paramétrisation, nous décrivons l'approche développée dans [20] pour déterminer leur intersection, approche basée sur l'utilisation d'une représentation matricielle d'une des deux courbes. Soient donc une courbe $\mathcal{C}_1$ paramétrée par l'application

$$\mathbb{P}^1 \xrightarrow{\phi_1} \mathbb{P}^n : (s:t) \mapsto (f_0 : \cdots : f_n)(s,t) \tag{2.5}$$

et une autre courbe $\mathcal{C}_2$ paramétrée par l'application *régulière*

$$\mathbb{P}^1 \xrightarrow{\phi_2} \mathbb{P}^n : (s:t) \mapsto (g_0 : \cdots : g_n)(s,t). \tag{2.6}$$

Notant $\mathtt{M}(\phi_1)_\nu$ une matrice de représentation de la courbe $\mathcal{C}_1$ pour un entier ν approprié, la substitution des variables $x_0, \ldots, x_n$ par la paramétrisation homogène de $\mathcal{C}_2$ dans cette matrice conduit à une nouvelle matrice

$$\mathtt{M}(\phi_1, \phi_2)_\nu(s,t) := \mathtt{M}(\phi_1)_\nu(g_0(s,t), \ldots, g_n(s,t)).$$

Le résultat suivant est une conséquence directe des propriétés d'une matrice de représentation.

Lemme 20. *Soit* $(s_0 : t_0) \in \mathbb{P}^1$*, alors*

$$\text{rang } \mathtt{M}_\nu(\phi_1, \phi_2)(s_0, t_0) < \nu + 1 \Leftrightarrow \phi_2(s_0, t_0) \in \mathcal{C}_1 \cap \mathcal{C}_2.$$

L'ensemble $\mathcal{C}_1 \cap \mathcal{C}_2$ est ainsi en correspondance avec les points de $\mathbb{P}^1$ où le rang de la matrice $\mathtt{M}(\phi_1, \phi_2)_\nu(s,t)$ chute. En substituant $t = 1$, la détermination des valeurs de s telles que le rang de $\mathtt{M}(\phi_1, \phi_2)_\nu(s,1)$ chute peut être traitée au niveau des matrices en utilisant des techniques de linéarisation comme celles présentées dans le chapitre précédent. On obtient l'algorithme suivant (cf. [20,§6]) qui a été implémenté par Thang Luu Ba dans le cadre de son travail de thèse :

Entrées : deux courbes paramétrées $\mathcal{C}_1$ et $\mathcal{C}_2$ définies par (2.5) et (2.6).
Sortie : les coordonnées des points de $\mathcal{C}_1 \cap \mathcal{C}_2$ (à distance finie).
Description :

1. On forme la matrice de représentation $\mathtt{M}(\phi_1)_\nu$ de $\mathcal{C}_1$ pour un entier ν adapté.
2. On forme les matrices compagnes A, B de la matrice $\mathtt{M}(\phi_1, \phi_2)_\nu$.
3. On calcule la partie régulière $A' - sB'$ du pinceau $A - sB$.
4. On calcule l'ensemble des valeurs propres (généralisées) $\{s_1, \ldots, s_r\}$ du pinceau $A' - sB'$.
5. On renvoie l'ensemble de points $\{\phi_2(s_1), \ldots, \phi_2(s_r)\}$.

2.3 Singularités

Dans ce paragraphe, nous nous intéressons à la détermination des singularités d'une courbe rationnelle. Dans [Wang et al., 2009], les auteurs dérivent une correspondance entre les singularités d'une courbe rationnelle et une de ses μ-bases. Ils fournissent également des algorithmes pour déterminer toutes les singularités d'une courbe rationnelle de bas degré. Dans [20], une autre approche pour le calcul des singularités d'une courbe rationnelle, basée sur l'utilisation des matrices de représentations, est proposée. Cette méthode permet de surmonter les limitations de [Wang et al., 2009] et revient pour l'essentiel à faire un calcul d'auto-intersection suivant la méthode d'intersection courbe/courbe énoncée plus haut. On est alors en mesure de définir des *facteurs singuliers*, généralisant ainsi la notion de facteurs singuliers pour les courbes planes introduite dans [Chen et al., 2008] (voir aussi [31]) sur laquelle nous reviendrons un peu plus loin.

2.3.1 Rang d'une matrice de représentation en un point de la droite projective

Soit $\mathcal{C}$ une courbe rationnelle dans $\mathbb{P}^n$ de degré $d \geq 1$, que nous supposons paramétrée par l'application régulière

$$\begin{array}{ccc} \mathbb{P}^1 & \xrightarrow{\phi} & \mathbb{P}^n \\ (s:t) & \mapsto & (f_0 : f_1 : \cdots : f_n)(s,t). \end{array}$$

où $f_0, f_1, \ldots, f_n$ sont $n+1$ polynômes homogènes dans $k[s,t]$ du même degré d tels que leur plus grand commun diviseur est un élément non nul dans k.

Soit à présent P un point de $\mathcal{C}$. Il existe au moins une pré-image de P par ϕ, c'est-à-dire un point $(s_1 : t_1) \in \mathbb{P}^1$ tel que $P = \phi(s_1 : t_1)$. Soit $\mathcal{H}$ un hyperplan dans $\mathbb{P}^3$ passant par P et ne contenant pas $\mathcal{C}$. Si $H(x_0, \ldots, x_n)$ désigne une équation (donc une forme linéaire de $\mathbb{K}[x_0, \ldots, x_n]$) de $\mathcal{H}$, alors on peut former le polynôme homogène de degré d dans $k[s,t]$

$$H(f_0(s,t), f_1(s,t), \ldots, f_n(s,t)) = \prod_{i=1}^{d} (t_i s - s_i t) \tag{2.7}$$

où les points $(s_i : t_i) \in \mathbb{P}^1$, $i = 1, \ldots, d$, ne sont pas nécessairement distincts. On définit alors la multiplicité d'intersection de $\mathcal{C}$ avec $\mathcal{H}$ au point P, notée $i_P(\mathcal{C}, \mathcal{H})$, comme le nombre de points $(s_i : t_i)_{i=1,\ldots,d}$ tels que $\phi(s_i : t_i) = P$.

Définition 2. La multiplicité $m_P(\mathcal{C})$ d'un point P de $\mathcal{C}$ est définie comme le minimum de l'ensemble des multiplicités d'intersection $i_P(\mathcal{C}, \mathcal{H})$ lorsque $\mathcal{H}$ parcourt tous les plans ne contenant pas $\mathcal{C}$ et passant par le point $P \in \mathcal{C}$, minimum qui est atteint pour un choix suffisamment général de $\mathcal{H}$.

Définition 3. Un *polynôme d'inversion* du point P sur $\mathcal{C}$ est un polynôme homogène $h_P(s,t) \in k[s,t]$ de degré $m_p(\mathcal{C})$ qui divise (2.7) pour tout plan $\mathcal{H}$ passant par P. Il est défini à multiplication près par un élément non nul de k.

Étant donnée une μ-base de la paramétrisation ϕ, on définit comme en (2.2) les polynômes

$$u_i(s,t,x_0,x_1,\ldots,x_n) = \sum_{j=0}^{n} u_{i,j}(s,t)x_j \in k[s,t,x_0,\ldots,x_n], \quad i = 1,\ldots,n,$$

de degré respectif $\mu_1 \leq \mu_2 \leq \ldots \leq \mu_n$. On peut alors calculer une polynôme d'inversion pour un point donné $P \in \mathbb{P}^3$ à l'aide du résultat suivant qui est apparu pour la première fois dans [Wang et al., 2009], et pour lequel une preuve plus courte est donnée dans [20, Lemma 12].

Lemme 21. *Pour tout point P de $\mathcal{C}$, le plus grand commun diviseur des polynômes homogènes $u_1(s,t;P)$, $u_2(s,t;P)$, ..., $u_n(s,t;P)$ dans $k[s,t]$ est un polynôme d'inversion pour P.*

Comme nous l'avons vu précédemment, pour tout entier $\nu \geq \nu_0 := \mu_n + \mu_{n-1} - 1$ il existe une matrice de représentation $\mathtt{M}(\phi)_\nu$ de la courbe $\mathcal{C}$ qui est construite à l'aide d'une μ-base. Ses entrées sont des formes linéaires de $k[x_0, \ldots, x_n]$.

Théorème 22 ([20, Theorem 6])**.** *Soit un point $P \in \mathbb{P}^n$. Pour tout entier $\nu \geq \nu_0$ on a*

$$\operatorname{rang} \mathtt{M}(\phi)_\nu(P) = \nu + 1 - m_P(\mathcal{C}),$$

ou de manière équivalente $\operatorname{corang} \mathtt{M}(\phi)_\nu(P) = m_P(\mathcal{C})$.

Ce résultat montre que l'on peut stratifier les points de $\mathbb{P}^n$ par rapport à la courbe $\mathcal{C}$. En effet, on observe que :

- Si P est tel que $\operatorname{rang} \mathtt{M}(\phi)_\nu(P) = \nu + 1$ alors $P \notin \mathcal{C}$,
- Si P est tel que $\operatorname{rang} \mathtt{M}(\phi)_\nu(P) = \nu$ alors P est un point lisse (i.e. de multiplicité 1) de $\mathcal{C}$,
- Si P est tel que $\operatorname{rang} \mathtt{M}(\phi)_\nu(P) = \nu - 1$ alors P est un point singulier de multiplicité 2 de $\mathcal{C}$,
- etc.

2.3.2 Inversion d'un point lisse sur $\mathcal{C}$

Supposons donné un point P sur notre courbe $\mathcal{C} \subset \mathbb{P}^n$ paramétrée par ϕ et notons $\mathtt{M}(\phi)_\nu$ une matrice de représentation pour un entier ν approprié. Comme nous venons tout juste de l'énoncer, par propriété d'une matrice de représentation nous avons le test d'appartenance suivant :

$$\operatorname{rang} \left(\mathtt{M}(\phi)_\nu(P)\right) < \nu + 1 \text{ si et seulement si } P \in \mathcal{C}.$$

Un problème classique en modélisation géométrique consiste à déterminer une pré-image du point P lorsque ce dernier est un point lisse ; on parle du problème d'*inversion*. Ainsi, dans [Song and Goldman, 2009] ce problème est traité à l'aide de calculs de PGCD à partir d'une μ-base. Dans [20], nous avons proposé une nouvelle approche au problème d'inversion basée sur l'utilisation d'un matrice de représentation.

Supposons donc que $m_P(\mathcal{C}) = 1$ de telle sorte que P possède une unique pré-image $(s_1 : t_1)$ par ϕ. Puisque $\operatorname{rang} \mathtt{M}(\phi)_\nu(P) = \operatorname{rang} \mathtt{M}(\phi)_\nu - 1 = \nu$, le noyau de la transposée de la matrice $\mathtt{M}(\phi)_\nu(P)$ est engendré par un vecteur non nul, disons $W_P = (w_0, \ldots, w_\nu) \in k^{\nu+1}$. Maintenant, notons $b_0(s,t), \ldots, b_\nu(s,t)$ la base de C_ν qui a été choisie pour former la matrice $\mathtt{M}(\phi)_\nu$. Alors, il est clair qu'il existe $\lambda \in k \setminus \{0\}$ tel que

$$W_P = \lambda \left(b_0(s_1, t_1), \ldots, b_\nu(s_1, t_1) \right).$$

Par suite, on en déduit (s_1, t_1). Par exemple, si $b_i(s,t) = s^i t^{\nu-i}$, $i = 0, \ldots, \nu$ (la base monomiale usuelle), alors $(s_1 : t_1) = (w_1 : w_0)$ si $w_0 \neq 0$, et sinon $(s_1 : t_1) = (1 : 0)$.

Lorsque le point P n'est plus un point lisse, i.e. $m_P(\mathcal{C}) > 1$, le noyau que nous avons considéré est de dimension strictement plus grande que 1 et il est par conséquent délicat d'en extraire les pré-images directement. Afin de surmonter cette difficulté, et obtenir un traitement plus général du problème d'inversion, nous allons nous intéresser à l'auto-intersection de la courbe $\mathcal{C}$.

2.3.3 Facteurs singuliers

Cette notion a été introduite pour les courbes rationnelles planes dans [Chen et al., 2008], cas pour lequel il existe une matrice de représentation carrée ; nous y reviendrons d'ailleurs dans le prochain paragraphe. Dans [20], nous avons étendu, grâce au théorème 22, cette notion au cas des courbes rationnelles dans un espace projectif de dimension arbitraire ; nous en donnons ici les grandes lignes.

On suppose toujours donné un entier $\nu \geq \nu_0$ et une matrice de représentation $\mathtt{M}(\phi)_\nu$ de la courbe $\mathcal{C}$ construite à partir d'une μ-base $u_1, u_2, \ldots, u_n$ de degré $\mu_1 \leq \mu_2 \leq \ldots \leq \mu_n$ respectivement. Nous noterons $\mathtt{M}(\phi)_\nu(s,t)$ la matrice $\mathtt{M}(\phi)_\nu$ dans laquelle on a substitué $x_0, \ldots, x_n$ par $f_0(s,t), f_1(s,t), \ldots, f_n(s,t)$ respectivement (noter qu'avec les notations adoptées plus haut pour le problème d'intersection, c'est la matrice $\mathtt{M}(\phi, \phi)_\nu$) Ainsi, il est clair que $\operatorname{rang} \mathtt{M}(\phi)_\nu(s,t) < \nu + 1$ pour tout point $(s : t) \in \mathbb{P}^1$.

Définition 4 ([20])**.** Une collection de polynômes homogènes $d_1(s,t), \ldots, d_{\nu+1}(s,t)$ dans $\mathbb{K}[s,t]$ telle que pour tout entier $i = 1, \ldots, \nu + 1$ le produit

$$d_{\nu+1}(s,t)^{\nu+1-i+1} d_\nu(s,t)^{\nu+1-i} \cdots d_{i+1}(s,t)^2 d_i(s,t)$$

est égal au plus grand commun diviseur des mineurs d'ordre $(\nu + 2 - i)$ de $\mathtt{M}(\phi)_\nu(s,t)$ est appelée une collection de facteurs singuliers de la paramétrisation ϕ.

Il faut noter que ces facteurs singuliers sont définis à multiplication près par un élément non nul de k. De plus, leur existence est garantie par le fait que l'on est au-dessus de $\mathbb{P}^1$: ils s'obtiennent en homogénéisant avec précaution les facteurs invariants de la matrice $\mathtt{M}(\phi)_\nu(s,1)$, $k[s]$ étant un anneau principal.

Théorème 23 ([20, Theorem 15])**.** *On a $d_{\nu+1}(s,t) = d_\nu(s,t) = \cdots = d_{\mu_n+1}(s,t) = 1$ et $d_1(s,t) = 0$. De plus, pour tout point singulier $P \in \mathcal{C}$, le polynôme d'inversion $h_P(s,t)$ divise $d_{m_P(\mathcal{C})}(s,t)$ et est premier avec chacun des polynômes $d_k(s,t)$ pour tout $k > m_P(\mathcal{C})$.*

De ce théorème découlent deux résultats qui permettent de caractériser la multiplicité d'un point singulier et de calculer les points singuliers.

Corollaire 24 ([20, Corollary 16])**.** *Soit $P = \phi(s_1 : t_1)$ un point de $\mathcal{C}$, alors $d_{m_P(\mathcal{C})}(s_1 : t_1) = 0$ et $d_k(s_1 : t_1) \neq 0$ pour tout $k > m_P(\mathcal{C})$. En particulier, la multiplicité de P est le plus grand entier k tel que $d_k(s_1 : t_1) = 0$.*

Corollaire 25 ([20, Corollary 17])**.** *Pour tout entier k tel que $2 \leq k \leq \mu_n$, le produit*

$$\prod_{P \in \mathcal{C} \,:\, m_P(\mathcal{C}) = k} h_p(s,t)$$

divise le facteur singulier $d_k(s,t)$.

2.3.4 Aspects effectifs.

On peut déterminer les facteurs singuliers par le calcul d'une forme de Smith puisque la matrice $\mathtt{M}(\phi)_\nu(s,1)$ a ses coefficients dans un anneau principal. Ainsi, $\mathtt{M}(\phi)_\nu(s,1)$ est équivalente à la matrice diagonale

$$\begin{pmatrix} d_{\nu+1}(s,1) & & & & & & \\ & d_{\nu+1}d_\nu(s,1) & & & & & \\ & & d_{\nu+1}d_\nu d_{\nu-1}(s,1) & & & & \\ & & & \ddots & & & \\ & & & & d_{\nu+1}\cdots d_3(s,1) & & \\ & & & & & d_{\nu+1}\cdots d_3 d_2(s,1) & \\ & & & & & & 0 \end{pmatrix}.$$

Le calcul de cette forme de Smith fournit donc l'évaluation des facteurs singuliers en $t = 1$. Par conséquent, si le point $\phi(1:0)$ n'est pas singulier, alors les singularités de $\mathcal{C}$ se déduisent de cette unique forme de Smith. Sinon, il est nécessaire de calculer la forme de Smith de $\mathtt{M}(\phi)_\nu(1,t)$, ou bien d'obtenir toute l'information sur le point singulier $\phi(1:0)$ en calculant un plus grand commun diviseur comme dans le lemme 21. Noter que d'un point de vue de la complexité du calcul, il peut s'avérer intéressant d'exploiter la suite des sous-résultants associés à la μ-base, mais nous n'entrerons pas dans ces détails ici.

2.4 Singularités : le cas des courbes planes

La littérature des courbes algébriques planes est abondante et riche, notamment car la géométrie des courbes planes est beaucoup plus contrainte que celle des courbes dans un espace projectif de dimension plus grande que 3. Par exemple, pour toute courbe plane $\mathcal{C}$ de degré n, nous avons l'égalité, appelée formule du genre,

$$(n-1)(n-2) = \sum_{P\in \mathrm{Sing}(\mathcal{C})} m_P(\mathcal{C})(m_P(\mathcal{C})-1)$$

où $\mathrm{Sing}(\mathcal{C})$ désigne les points singuliers, propres ou infiniment voisins, de la courbe $\mathcal{C}$ et $m_P(\mathcal{C})$ désigne la multiplicité du point singulier P de $\mathcal{C}$. Il n'y a pas d'équivalent à cette formule pour une courbe non plane.

Dans ce qui suit, reprenant la situation du paragraphe précédent, nous allons entre autres décrire complètement les facteurs singuliers d'une courbe rationnelle plane en termes de ses singularités. Ces travaux sont publiés dans les articles [17] et [31]. Dans toute la suite, nous supposerons que $k = \mathbb{C}$ et que $\mathcal{C}$ est une courbe plane rationnelle de degré $n \geq 3$, puisque toute courbe rationnelle de degré plus petit que 2 est lisse, paramétrée par l'application régulière

$$\begin{array}{ccc} \mathbb{P}^1 & \xrightarrow{\phi} & \mathbb{P}^2 \\ (s:t) & \mapsto & (f_0:f_1:f_2)(s,t) \end{array}$$

où f_0, f_1, f_2 sont 3 polynômes homogènes de degré $n \geq 3$. Nous supposons en outre que ϕ est birationnelle sur $\mathcal{C}$. Enfin, nous désignerons par (p,q) une μ-base de ϕ de degré $1 \leq \mu \leq n-\mu$ respectivement.

2.4.1 Facteurs singuliers

Afin d'énoncer le résultat principal, il nous faut introduire quelques notations à propos de la résolution des singularités de $\mathcal{C}$ (voir par exemple [Brieskorn and Knörrer, 1986]). Soient $\{P_1,\ldots,P_r\}$ les points singuliers propres de $\mathcal{C}$, c'est-à-dire les points singuliers usuels de $\mathcal{C}$ dans le plan projectif de coordonnées $(x_0:x_1:x_2)$. Pour tout entier $i = 1,\ldots,r$ nous noterons

- $\mathfrak{z}^i_j$, $j \in I_i$, les branches irréductibles de $\mathcal{C}$ au point P_i,
- $(s_{i,j}:s_{i,j})$, $j \in I_i$, le point de $\mathbb{P}^1$ tel que $\mathfrak{z}^i_j(s_{i,j}:t_{i,j}) = P_i$,
- $(P^i_{j,h})_{0\leq h}$ la suite de points infiniment voisins de $\mathfrak{z}^i_j$ au point P_i,
- $(m^i_{j,h})_{0\leq h}$ la suite des multiplicités de $\mathfrak{z}^i_j$ au point P_i,
- $(\sim_h)_{0\leq h}$ les relations d'équivalences du graphe des multiplicités de $\mathcal{C}$.

Ainsi, la multiplicité d'un point virtuel $P^i_{j,h}$ de $\mathcal{C}$ est donnée par la formule $m_{P^i_{j,h}}(\mathcal{C}) = \sum_{j' \sim_h j} m^i_{j',h}$.

Le résultat qui suit, obtenu en collaboration avec Carlos D'Andrea dans [31], démontre et précise deux conjectures qui ont été énoncées dans [Chen et al., 2008]. À partir de maintenant, on suppose que la matrice de représentation de $\mathcal{C}$ utilisée implicitement dans ce qui suit est la matrice $M(\phi)_{n-1}$; c'est la matrice la plus petite possible et elle est de surcroît carrée.

Théorème 26 ([31,Theorem 1.1])**.** *Soient $d_n(s,t), \ldots, d_2(s,t)$ une collection de facteurs singuliers de ϕ. Alors,*

$$d_{n-\mu+1}(s,t) = \cdots = d_n(s,t) = 1,$$

et pour tout $k = 2, \ldots, n-\mu$

$$d_k(s,t) = \prod_{i=1,\ldots,r,\ j \in I_i} (t_{i,j}s - s_{i,j}t)^{\epsilon^k_{i,j}}$$

où

$$\epsilon^k_{i,j} = \sum_{h \text{ such that } m_{P^i_{j,h}}(\mathcal{C})=k} m^i_{j,h}$$

La preuve de ce résultat repose en partie sur des travaux connexes, d'intérêts indépendants et qui sont publiés dans [17]. Aussi, nous les présentons brièvement dans ce qui suit avant d'indiquer les grandes lignes de la preuve du théorème 26.

2.4.2 Équations de l'algèbre de Rees associée à ϕ

Toute μ-base de ϕ engendre les équations de l'algèbre symétrique de $I \subset R$. Une question naturelle est alors de s'interroger sur les équations d'une autre algèbre d'éclatement : l'algèbre de Rees de $I := (f_0, f_1, f_2) \subset R := \mathbb{C}[s,t]$. La question de la détermination des équations d'une algèbre de Rees est bien connue en algèbre commutative et possède de très nombreux développements (voir par exemple le livre [Vasconcelos, 1994] et ses références). Dans le contexte qui nous intéresse ici, la question de la détermination des équations de $\mathrm{Rees}_R(I)$ apparaît entre autres dans [Cox et al., 2008; Cox, 2008; Hong et al., 2008; Kustin et al., 2008; Cortadellas Benítez and D'Andrea, 2010] où des réponses sont apportées dans certains cas particuliers (correspondant pour l'essentiel au cas $\mu = 1$ pour les courbes planes). Dans la première partie de l'article [17], je retrouve ces résultats et donne un système complet d'équations de $\mathrm{Rees}_R(I)$ pour de nouvelles classes de courbes. Plus généralement, j'identifie explicitement des équations de l'algèbre $\mathrm{Rees}_R(I)$ qui ne forment cependant pas toujours un système complet d'équations.

L'approche utilisée dans [17] est basée sur le fait suivant. Identifions la μ-base $p = (p_1, p_2, p_3), q = (q_1, q_2, q_3)$ de la paramétrisation ϕ aux deux formes linéaires en x_0, x_1, x_2 :

$$\begin{aligned} p(s,t,x_0,x_1,x_2) &= p_1(s,t)x_0 + p_2(s,t)x_1 + p_3(s,t)x_2 \\ &= u_0(x_0,x_1,x_2)s^\mu + u_1(x_0,x_1,x_2)s^{\mu-1}t + \cdots + u_\mu(x_0,x_1,x_2)t^\mu, \\ q(s,t,x_0,x_1,x_2) &= p_1(s,t)x_0 + p_2(s,t)x_1 + p_3(s,t)x_2 \\ &= v_0(x_0,x_1,x_2)s^{n-\mu} + v_1(x_0,x_1,x_2)s^{n-\mu-1}t + \cdots + v_\mu(x_0,x_1,x_2)t^{n-\mu}. \end{aligned} \tag{2.8}$$

Il n'est pas difficile de montrer que la suite (p,q) est régulière dans $\mathbb{C}[s,t,x_0,x_1,x_2]$ et que les équations de $\mathrm{Rees}_R(I)$ sont données par l'idéal saturé $(p,q) : (s,t)^\infty \subset \mathbb{C}[s,t,x_0,x_1,x_2]$. Ainsi, les équations de $\mathrm{Rees}_R(I)$ apparaissent comme l'idéal des *formes d'inerties* de (p,q) par rapport à l'idéal (s,t). Mettant à profit cette remarque, j'ai pu construire des équations explicites de $\mathrm{Rees}_R(I)$ et montrer dans certains cas que ces équations suffisaient à engendrer toutes les équations de $\mathrm{Rees}_R(I)$. Plus précisément, un système explicite de générateurs de $\mathrm{Rees}_R(I)$ est obtenu pour $\mu = 1$, $\mu = 2$ et $n = 4$, $\mu = 2$ et $n > 4$ sous la condition que la courbe $\mathcal{C}$ ne possède pas de point singulier de multiplicité $n-2$ (valeur maximale pour la multiplicité d'un point singulier d'une telle courbe $\mathcal{C}$). Lorsque $\mu \geq 3$, les équations décrites dans [17] ne permettent pas d'engendrer toutes les équations de $\mathrm{Rees}_R(I)$. Nous renvoyons le lecteur à [17, §3] pour plus de détails. Notons cependant que le cas $\mu = 1$ a été également démontré dans [Cox et al., 2008, théorème 2.3] (voir aussi [Kustin et al., 2008]) et que le cas $\mu = 2$, mais uniquement pour $n = 4$ et $n = 5$, apparaît dans [Hong et al., 2008, propositions 4.2 et 4.5].

2.4.3 Courbes adjointes

Commençons par rappeler quelques définitions.

Définition 5. Une courbe algébrique plane $\mathcal{D}$ est dite adjointe à $\mathcal{C}$ si elle passe en tout point singulier $\mathfrak{p}$ de $\mathcal{C}$, propre ou infiniment voisin, avec la multiplicité virtuelle $m_{\mathfrak{p}}(\mathcal{C}) - 1$.

Les notions de *multiplicité virtuelle* et de *passer par un point avec une multiplicité virtuelle donnée* sont assez subtiles, mais essentielles pour formuler une définition correcte des courbes adjointes [Casas-Alvero, 2000, Sections 4.1 and 4.8]. Mentionnons simplement que si $\mathfrak{p}$ est un point singulier propre de $\mathcal{C}$ de multiplicité $m_{\mathfrak{p}}$, alors la courbe $\mathcal{D}$ passe par $\mathfrak{p}$ avec la multiplicité virtuelle $m_{\mathfrak{p}} - 1$ si elle est de multiplicité au moins $m_{\mathfrak{p}} - 1$ au point $\mathfrak{p}$. Observons d'ailleurs qu'une telle condition imposée en tous les points singuliers, propres aussi bien qu'infiniment voisins, est parfois utilisée pour définir une courbe adjointe, comme par exemple dans [Abhyankar, 1990].

Notre courbe $\mathcal{C}$ étant supposée rationnelle, on montre qu'il n'existe pas de courbe adjointe à $\mathcal{C}$ de degré $\leq n-3$. Par contre, on montre qu'il existe toujours des courbes adjointes de degré $\geq n-2$. Évidemment, ce sont les courbes adjointes de degré $n-2$ et $n-1$ qui sont particulièrement intéressantes (puisque $\mathcal{C}$ est adjointe à elle-même par définition).

Un *pinceau de courbes adjointes* à $\mathcal{C}$ de degré m est une famille de courbes au-dessus d'une droite telle que chaque courbe de la famille est adjointe à $\mathcal{C}$ et de degré m. Il est donc de la forme

$$sD_1(x_0, x_1, x_2) + tD_2(x_0, x_1, x_2)$$

où D_1, D_2 sont deux polynômes homogènes dans $\mathbb{K}[x_0, x_1, x_2]$ de degré m. Dans son article [Cox, 2008], D. Cox a observé que les équations de $\mathrm{Rees}_R(I)$ de degré $n-2$ (resp. $n-1$) qui sont linéaires en s, t fournissent parfois des pinceaux de courbes adjointes à $\mathcal{C}$. Cette remarque a donné lieu à une conjecture de D. Cox [Cox, 2008, Conjecture 3.8] (voir aussi [Cox, 2008, Remark 3.9]). Dans [17], je démontre le résultat suivant :

Théorème 27 ([17])**.** *Parmi les équations de* $\mathrm{Rees}_R(I)$ *de degré* $n-2$ *ou* $n-1$ *qui sont linéaires en* s *et* t*, on trouve toujours des pinceaux de courbes adjointes à* $\mathcal{C}$*.*

D'après ce que nous avons expliqué dans le paragraphe précédent, ce résultat se démontre en analysant les éléments de $H^0_{\mathfrak{m}}(B)_1$, où $A = \mathbb{K}[x_0, x_1, x_2]$, $B = A[s,t]/(p,q)$ et $\mathfrak{m} = (s,t)$, qui sont homogènes de degré $n-2$ et $n-1$ en les variables x_0, x_1, x_2. C'est d'ailleurs cette analyse qui a motivé l'étude des équations de l'algèbre $\mathrm{Rees}_R(I)$. En particulier si nous n'avons donné un système de générateurs explicites pour les équations de $\mathrm{Rees}_R(I)$ que dans certains cas (essentiellement $\mu = 1, 2$), nous donnons un système de générateurs explicites de $H^0_{\mathfrak{m}}(B)_1$ dans presque tous les cas. Pour être un peu plus précis, introduisons la notation suivante.

Définition 6. Étant donnés deux polynômes homogènes

$$f(s,t) = a_0 s^{d_1} + \cdots + a_{d_1} t^{d_1}, \quad g(s,t) = b_0 s^{d_2} + \cdots + b_{d_2} t^{d_2},$$

telles que $d_1 \geq 2$ et $d_2 \geq 2$, on appellera *sous-résultants* (du premier ordre) de f et g les mineurs d'ordre $d_1 + d_2 - 2$ de la matrice de Sylvester de f et g. Plus précisément, on a l'égalité

$$\begin{vmatrix} a_0 & & 0 & b_0 & & 0 & T_0 \\ & \ddots & & & \ddots & & \vdots \\ \vdots & & a_0 & \vdots & & b_0 & \\ & & & & & & \\ a_{d_1} & & \vdots & b_{d_2} & & \vdots & \vdots \\ & \ddots & & & \ddots & & \\ 0 & & a_{d_1} & 0 & & b_{d_2} & T_\delta \end{vmatrix} = \sum_{i=0}^{\delta} \mathrm{SRes}_{\delta - i}(f,g)\, T_i$$

(les $d_2 - 1$ premières colonnes de a's, les $d_1 - 1$ suivantes de b's)

et l'élément $\mathrm{SRes}_0(f,g)$ est parfois qualifié de sous-résultant *principal*.

Dans [17], je démontre d'une part que si $\mu = 1$ alors $H^0_{\mathfrak{m}}(B)_1$ est engendré par un unique déterminant, et d'autre part que les $n-2$ éléments

$$X_1 \mathrm{SRes}_i(p,q) - X_2 \mathrm{SRes}_{i+1}(p,q), \quad i = 0, \ldots, n-3 \tag{2.9}$$

appartiennent toujours à $H^0_{\mathfrak{m}}(B)_1$ et l'engendrent dans les cas suivants :

- Si $\mu = 2$ and $n = 4$,
- Si $\mu = 2$, $n \geq 5$ et $V(u_0, u_1, u_2) = \emptyset \subset \mathbb{P}^2$ (cf. la notation (2.8)),
- Si $\mu \geq 3$ et

$$\mathrm{prof}_A \det_{n-4} \underbrace{\begin{pmatrix} U_0 & & 0 & V_0 & & 0 \\ & \ddots & & & \ddots & \\ \vdots & & U_0 & \vdots & & V_0 \\ & & & & & \\ U_\mu & & \vdots & V_{n-\mu} & & \vdots \\ & \ddots & & & \ddots & \\ 0 & & U_\mu & 0 & & V_{n-\mu} \end{pmatrix}}_{n-\mu-2 \qquad\qquad \mu-2} \geq 3,$$

(noter que cette matrice est de taille $(n-2) \times (n-4)$).

La simplicité des équations (2.9) est tout à fait remarquable. Une autre propriété tout aussi surprenante est la suivante :

Théorème 28 ([17, théorème 4.8])**.** *Supposons $\mu \geq 2$ et $n \geq 4$. Pour tout entier $i = 0, \ldots, n-2$ l'équation $\mathrm{SRes}_i(p,q) = 0$ définit une courbe plane qui est adjointe à $\mathcal{C}$.*

À partir de là, on déduit facilement le théorème 27. En fait, on montre un peu plus. Hormis le cas $\mu = 1$ qui se traite séparément mais qui ne pose pas de difficulté, on obtient que toute équation de l'algèbre $\mathrm{Rees}_R(I)$ de degré $n-2$ ou $n-1$ qui est linéaire en s, t est un pinceau de courbes adjointes à $\mathcal{C}$ sous les conditions, énoncées ci-dessus, permettant de montrer que (2.9) engendrent $H^0_{\mathfrak{m}}(B)_1$. Nous renvoyons le lecteur à [17, §4] pour plus de détails.

2.4.4 Généralisation d'un théorème d'Abhyankar

Dans la lecture 19 de son livre [Abhyankar, 1990], Abhyankar définit le résultant de Taylor de deux polynômes $f(s), g(s) \in k[s]$ comme le résultant éliminant la variable t des polynômes

$$\frac{f(s) - f(t)}{s-t} = f'(s) + \frac{f''(s)}{2!}t + \frac{f'''(s)}{3!}t^2 + \cdots,$$
$$\frac{g(s) - g(t)}{s-t} = g'(s) + \frac{g''(s)}{2!}t + \frac{g'''(s)}{3!}t^2 + \cdots.$$

Comme il l'énonce dans son théorème page 153, sans toutefois le démontrer, ce résultant de Taylor, que nous noterons $\Delta(s) \in k[s]$, est un générateur du conducteur de $k[f(s), g(s)]$ dans $k[s]$. En particulier, supposant que $(f(s), g(s))$ est une paramétrisation d'une courbe plane $\mathcal{C}$, il fournit les singularités de $\mathcal{C}$ au sens suivant :

$$\Delta(s) = \gamma \prod_{j=1}^{l} (s - \gamma_j)^{\epsilon_j}$$

où $0 \neq \gamma \in k$, $\gamma_1, \ldots, \gamma_l$ sont des éléments distincts dans k et $\epsilon_1, \ldots, \epsilon_l$ sont des entiers qui vérifient les trois propriétés suivantes :

(P1) $P = (\alpha, \beta) \in \mathcal{C}$ est un point singulier (propre) de $\mathcal{C}$ si et seulement si $(\alpha, \beta) = (f(\gamma_j), g(\gamma_j))$ pour un certain $j \in \{1, \ldots, l\}$

(P2) Si $P = (\alpha, \beta) \in \mathcal{C}$ est un point singulier (propre) de $\mathcal{C}$ alors

$$\sum\nolimits^{(\alpha,\beta)} \epsilon_j = \sum\nolimits^{P} \nu_i(\nu_i - 1)$$

où $\sum^{(\alpha,\beta)}$ est la somme sur les indices j tels que $(\alpha, \beta) = (p(\gamma_j), q(\gamma_j))$, et $\sum^P$ est la somme sur les indices i tels que le point T_i est soit P, soit infiniment voisin à P et de multiplicité ν_i.

(P3) $\deg(\Delta(s)) = (\deg(\mathcal{C})-1)(\deg(\mathcal{C})-2)$ si tous les points singuliers de $\mathcal{C}$ sont à distance finie.

Ce théorème d'Abhyankar est partiellement démontré dans [van den Essen and Yu, 1997] et interprété en termes de sous-résultants dans [El Kahoui, 2005]. Il ne traite cependant que des courbes rationnelles admettant des paramétrisations polynomiales. Il est donc tout naturel de se poser la question de sa généralisation au cas des courbes rationnelles générales, c'est-à-dire au cas où $f(s)$ et $g(s)$ sont des fractions rationnelles dans $k(s)$. L'article [Gutierrez et al., 2002] propose une généralisation partielle du théorème d'Abhyankar. Si $f = f_n/f_d$ et $g = g_n/g_d$, les auteurs définissent le résultant de Taylor comme le résultant éliminant la variable t des polynômes

$$\frac{f_n(s)f_d(t) - f_d(s)f_n(t)}{s-t},\ \frac{g_n(s)g_d(t) - g_d(s)g_n(t)}{s-t}. \tag{2.10}$$

Si cette généralisation, somme toute assez naturelle, du résultant de Taylor permet de décider si $k(s) = k(f(s), g(s))$ ou bien si $k[s] = k[f(s), g(s)]$, elle ne permet pas de retrouver exactement les points singuliers de la courbe paramétrée par $x = f(s), y = g(s)$ (voir [Gutierrez et al., 2002, Theorem 3.1]). Le principal problème vient du fait que la formulation (2.10) introduit une symétrie qui confond les courbes paramétrées par $x = f(s)^{\pm 1}, y = g(s)^{\pm 1}$.

En fait, reprenant les notations des paragraphes précédents, je montre dans [17] que le polynôme

$$\Delta(s) = \mathrm{SRes}_0(p,q)(f_0(s,1), f_1(s,1), f_2(s,1)) \in \mathbb{K}[s] \tag{2.11}$$

fournit une bonne généralisation du résultant de Taylor au cas rationnel car il satisfait aux propriétés (P1), (P2), (P3) ci-dessus. Plus précisément, reprenant les notations du graphe des multiplicités de $\mathcal{C}$ introduites au §2.4.1, on a le

Théorème 29 ([17])**.**

$$\Delta(s,t) := \mathrm{SRes}_0(p,q)(f_0(s,t), f_1(s,t), f_2(s,t)) = \gamma \prod_{\substack{i=1,\dots,r \\ j\in I_i}} (t_{i,j}s - s_{i,j}t)^{\epsilon_{i,j}} \tag{2.12}$$

où $0 \neq \gamma \in \mathbb{C}$ *et pour tout entiers* $i = 1, \dots, r$ *et* $j \in I_i$

$$\epsilon_{i,j} = \sum_{h\geq 0} m^i_{j,h}(m_{P^h_{j,h}}(\mathcal{C}) - 1).$$

En particulier,

$$\deg(\Delta(s,t)) = (\deg(\mathcal{C})-1)(\deg(\mathcal{C})-2) = (n-1)(n-2) = \sum_{P\in \mathrm{Sing}(\mathcal{C})} m_P(\mathcal{C})(m_P(\mathcal{C})-1).$$

2.4.5 Idée de la preuve du théorème 26

La preuve que nous avons donnée dans [31], en collaboration avec Carlos D'Andrea, du théorème 26 se fait par récurrence sur la longueur minimale d'une résolution de la courbe $\mathcal{C}$, disons $N \geq 0$. Bien que cette preuve soit assez technique, il est possible d'en donner les grandes lignes de manière assez concise.

Commençons par justifier que le théorème 26 est vrai pour $N = 0$. Supposons donc que la courbe $\mathcal{C}$ ne possède que des singularités ordinaires. Nous avons déjà noté au corollaire 25 que pour tout entier k tel que $2 \leq k \leq n-\mu$, le produit $\prod_{P\in\mathcal{C}:m_P(\mathcal{C})=k} h_P(s,t)$ divise le facteur singulier $d_k(s,t)$. Il s'en suit que

$$\prod_{P\in\mathcal{C}\ :\ m_P(\mathcal{C})\geq 1} h_P(s,t)^{m_P(\mathcal{C})-1} \text{ divise } d_{n-\mu}(s,t)^{n-\mu-1} d_{n-\mu-1}(s,t)^{n-\mu-2} \cdots d_2(s,t).$$

Or, de part notre hypothèse et la formule du genre, le polynôme de gauche est de degré

$$\sum_{P\in\mathcal{C}} m_P(\mathcal{C})(m_P(\mathcal{C})-1) = (n-1)(n-2)$$

tout comme le polynôme de droite par le théorème 29. On en déduit ainsi que le théorème 26 est vrai pour $N = 0$, autrement dit que pour tout entier k tel que $2 \leq k \leq n - \mu$, on a l'égalité (à multiplication près par une constante non nulle)

$$d_k(s,t) = \prod_{P \in \mathcal{C} : m_P(\mathcal{C}) = k} h_P(s,t)$$

si la courbe $\mathcal{C}$ ne possède que des singularités ordinaires (on précise donc ici le corollaire 25 pour une courbe rationnelle à singularités ordinaires).

Supposons à présent que la courbe $\mathcal{C}$ possède une résolution minimale de longueur N :

$$\mathcal{C} = \mathcal{C}_0 \leftarrow \tilde{\mathcal{C}} = \mathcal{C}_1 \leftarrow \mathcal{C}_2 \leftarrow \cdots \leftarrow \mathcal{C}_{N-1} \leftarrow \mathcal{C}_N.$$

Chaque flèche correspond à un éclatement d'un point singulier et la courbe $\mathcal{C}_N$ ne possède que des singularités ordinaires. Il est clair que la courbe $\tilde{\mathcal{C}}$ peut être résolue par une suite de $N - 1$ éclatements et donc qu'elle satisfait au théorème 26 par hypothèse de récurrence.

On commence par identifier les facteurs singuliers aux idéaux de Fitting du conoyau, disons M, de la matrice $M(\phi)_{n-1}$ qui n'est autre que la matrice de Sylvester d'une μ-base de la paramétrisation ϕ. Les idéaux de Fitting étant stables par changement de base, il suffit de montrer le résultat annoncé localement en chaque premier de $\mathbb{C}[s]$.

Par un changement suffisamment général de cordonnées, on se ramène à supposer que $\tilde{\mathcal{C}}$ est obtenu par éclatement de $\mathcal{C}$ au point singulier $P = (0 : 0 : 1) \in \mathbb{P}^2$ et que $\mathcal{C}$ est paramétrée birationnellement en coordonnées affines par

$$\mathbb{A}^1_{\mathbb{C}} \xrightarrow{\phi} \mathbb{A}^2_{\mathbb{C}} : s_0 \mapsto \left(\frac{f_0(s_0,1)}{f_2(s_0,1)}, \frac{f_1(s_0,1)}{f_2(s_0,1)} \right)$$

où $f_0(s,1) = h(s)\tilde{f}_0(s)$, $f_1(s,1) = h(s)\tilde{f}_1(s)$, $\gcd(\tilde{f}_0, \tilde{f}_1) = 1$ et $h(s) = h_P(s,1) = \prod_{i=1}^{i_P}(t - t_i)^{\nu_i}$ avec $m = \sum_{i=1}^{i_P} \nu_i$. Aussi, nous pouvons supposer que la courbe $\tilde{\mathcal{C}}$ est de degré $2n - \nu$ et birationnellement paramétrée par

$$\mathbb{A}^1_{\mathbb{C}} \xrightarrow{\tilde{\phi}} \mathbb{A}^2_{\mathbb{C}} : s_0 \mapsto \left(\frac{f_0(s_0,1)}{f_2(s_0,1)}, \frac{\tilde{f}_1(s_0)}{\tilde{f}_0(s_0)} \right) = \left(\frac{f_0(s_0,1)\tilde{f}_0(s_0)}{\tilde{f}_0(s_0)f_2(s_0,1)}, \frac{f_2(s_0,1)\tilde{f}_1(s_0)}{f_2(s_0,1)\tilde{f}_0(s_0)} \right).$$

À partir de là, il n'est pas difficile de constater que les deux polynômes

$$\begin{array}{rcl} \tilde{p} & = & \tilde{f_0}^{\,h}(s,t)x_1 - \tilde{f_1}^{\,h}(s,t)x_2, \\ \tilde{q} & = & f_2(s,t)x_0 - f_0(s,t)x_2, \end{array}$$

où $\tilde{f_0}^{\,h}$ et $\tilde{f_1}^{\,h}$ désignent respectivement les homogénéisés de $\tilde{f}_0$ et $\tilde{f}_1$ au degré $n - \nu$, forment une μ-base de la paramétrisation $\tilde{\phi}$, elle aussi homogénéisée.

On montre alors que, d'une part M peut être localement identifié au conoyau de la matrice de multiplication par $f(s,t) := f_1(s,1)f_2(t,1) - f_1(t,1)f_2(s,1)$ dans l'anneau quotient

$$B := \mathbb{C}[t][s] / \big(f_0(s,1)f_2(t,1) - f_0(t,1)f_2(s,1) \big)$$

(matrice que l'on associe souvent à la formule dite de Poisson), et d'autre part que pour tout premier $\mathfrak{p}$ de $\mathbb{C}[t]$ tel que $\tilde{f}_0(t) \notin \mathfrak{p}$, on a le diagramme commutatif, où $\tilde{f}(s,t) := \big(\tilde{f}_1(s)f_2(t,1)\tilde{f}_0(t) - \tilde{f}_0(s)f_2(t,1)\tilde{f}_1(t) \big)$,

$$\begin{array}{ccc} B_{\mathfrak{p}} & \xrightarrow{\times f(s,t)} & B_{\mathfrak{p}} \\ & {\scriptstyle \times h(s)} \searrow \quad \nearrow {\scriptstyle \times \tilde{f}(s,t)} & \\ & B_{\mathfrak{p}} & \end{array}$$

On peut d'ailleurs interpréter ce diagramme comme la transcription matricielle du processus classique d'éclatement où l'on fait sortir le diviseur exceptionnel dont le rôle est ici joué par la multiplication par $h(s)$.

On peut maintenant observer que les facteurs invariants de la multiplication par $f(s,t)$, respectivement $\tilde{f}(s,t)$, correspondent aux facteurs singuliers de la courbe $\mathcal{C}$, respectivement de la courbe $\tilde{\mathcal{C}}$. De plus, les facteurs invariants de la multiplication par $h(s)$ sont faciles à calculer. Utilisant un résultat de Thompson [Thompson, 1982], on montre alors que plusieurs produits de facteurs invariants de la multiplication par $h(s)$ et de la multiplication par $\tilde{f}(s,t)$ divisent d'autres produits de facteurs invariants de la multiplication par $f(s,t)$. Les premiers étant connus, essentiellement par hypothèse de récurrence, on déduit que chaque facteur singulier de $\mathcal{C}$ est divisible par le polynôme attendu donné dans le théorème 26. Ensuite, on conclut comme pour le cas $N = 0$, en observant que le produit de ces polynôme attendus a le même degré que le produit des facteurs singuliers par le théorème 29 ; c'est en fait ce dernier théorème qui fournit un argument global permettant de "recoller" toutes les propriétés locales précédentes.

Chapitre 3

Sur un test d'irréductibilité absolue pour une hypersurface

Il est bien connu que l'on peut tester la lissité d'une courbe algébrique plane, ou bien d'une hypersurface, à l'aide d'une matrice d'élimination qui correspond au calcul de son discriminant. Tester si cette même courbe est absolument irréductible est un problème plus délicat. Dans ce chapitre, on revient sur une méthode proposant un tel test qui a été introduite par W. Ruppert [Ruppert, 1986]. En effet, en collaboration avec G. Chèze, nous nous sommes penchés sur cette méthode dans le but de l'appliquer à l'étude du spectre d'une fonction rationnelle [18,30].

Soient k un corps, $\overline{k}$ sa clôture algébrique et deux polynômes non constants et premiers entre eux $f, g \in k[X_1, \ldots, X_n]$, $n \geq 2$. Le spectre de la fraction rationnelle $r := f/g \in k(X_1, \ldots, X_n)$ est l'ensemble

$$\sigma(f,g) := \{(\lambda : \mu) \in \mathbb{P}^1_k \text{ tel que } \mu f + \lambda g \text{ est réductible dans } \overline{k}[X_1, \ldots, X_n] \text{ ou } \deg(\mu f + \lambda g) < \max(\deg(f), \deg(g))\}.$$

En des termes plus géométrique, $\sigma(f,g)$ dénombre les hypersurfaces réductibles dans le pinceau d'hypersurfaces $\mu f + \lambda g = 0$ après homogénéisation.

Dans [18], on montre que la réduction modulo p du spectre de r coïncide avec le spectre de la réduction modulo p de r si p est un nombre premier supérieur ou égal à une quantité explicite. Cette quantité s'exprime en termes du degré de r, c'est-à-dire $\max(\deg(f), \deg(g))$, de sa hauteur et du nombre de variables n. Dans [30], on étudie l'ordre total de réductibilité de r, quantité associée au spectre lorsque celui-ci est fini et qui consiste à sommer les éléments du spectre en leur associant une certaine multiplicité. C'est essentiellement ce deuxième travail que nous avons choisi de présenter ci-après, car il met en avant une formulation matricielle, fil conducteur de ce mémoire, du test d'absolue irréductibilité de W. Ruppert.

3.1 La matrice de Ruppert

Étant donné un polynôme $f(X,Y) \in \mathbb{Z}[X,Y]$ absolument irréductible, c'est-à-dire irréductible dans $\overline{\mathbb{Q}}[X,Y]$, il est bien connu que la réduction de f modulo p est aussi absolument irréductible pour tout premier p suffisamment grand. Ce résultat, connu sous le nom de théorème d'Ostrowski, se déduit d'un test effectif d'irréductibilité absolue. Considérant les coefficients du polynôme comme des indéterminées, les polynômes absolument réductibles forment une variété algébrique de l'espace de ces coefficients. Un système d'équations définissant cette variété est appelée un système de formes de Noether [Noether, 1922]. Bien évidemment, un tel système n'est pas unique, et plusieurs travaux ont eu pour but de produire des systèmes les plus simples possibles, surtout en termes de degré des équations et de hauteur des coefficients de ces équations (voir par exemple [Schmidt, 1976; Schinzel, 2000; Kaltofen, 1995; Zannier, 1997]).

Dans son remarquable papier [Ruppert, 1986], W. Ruppert a introduit une nouvelle technique pour décider de l'irréductibilité absolue d'une courbe algébrique plane. Plus précisément, il donne un nouveau système de formes de Noether qui est à ce jour le résultat le plus fin en termes de degré et de hauteur des équations. Son approche est basée sur le calcul du premier groupe de cohomologie de De Rahm du

complémentaire d'une courbe algébrique plane. De ce fait, elle n'est valide que pour un corps de base algébriquement clos de caractéristique nulle. Ainsi, dans toute la suite nous supposerons désormais que le corps de base k est algébriquement clos et de caractéristique nulle.

3.1.1 Définition et résultat principal

Nous présentons ici le résultat principal de [Ruppert, 1986] sous une formulation matricielle et dans un contexte homogène, ce qui permet de mettre en évidence le caractère universel de la méthode.

Soit $f(X,Y,Z) \in k[X,Y,Z]$ un polynôme homogène de degré $d \geq 1$ et considérons le k-espace vectoriel

$$E := \{(G,H) \in k[X,Y,Z]_{d-1} \times k[X,Y,Z]_{d-1} \text{ tel que } Z | XG + YH\}.$$

On peut facilement vérifier que E est de dimension $d^2 - 1$ et un calcul [30, Lemma 4] montre que pour tout couple $(G,H) \in E$, le polynôme

$$f^2 \left(\partial_Y \left(\frac{G}{f} \right) - \partial_X \left(\frac{H}{f} \right) \right) = \begin{vmatrix} f & \partial_Y f \\ G & \partial_Y G \end{vmatrix} - \begin{vmatrix} f & \partial_X f \\ H & \partial_X H \end{vmatrix}$$

est divisible par Z.

Définition 7. Soit $f(X,Y,Z) \in k[X,Y,Z]$ un polynôme homogène non nul de degré $d \geq 1$, l'application

$$\begin{array}{rccc} \mathcal{R}(f): & E & \longrightarrow & k[X,Y,Z]_{2d-3} \\ & (G,H) & \mapsto & \frac{1}{Z} f^2 \left(\partial_Y \left(\frac{G}{f} \right) - \partial_X \left(\frac{H}{f} \right) \right) \end{array}$$

est appelée *application de Ruppert*. Toute matrice de cette application est appelée (par abus de langage) *matrice de Ruppert*.

Il est intéressant de noter que l'opérateur $\mathcal{R}(-)$ est k-linéaire, c'est-à-dire que pour tout couple $(f,g) \in k[X,Y,Z]_d$ et tout couple $(u,v) \in k^2$, on a

$$\mathcal{R}(uf + vg) = u\mathcal{R}(f) + v\mathcal{R}(g).$$

En fait, on pourrait définir $\mathcal{R}(-)$ formellement pour tout polynôme homogène $f(X,Y,Z) \in A[X,Y,Z]$ où A est un anneau commutatif arbitraire. Si A est l'anneau universel des coefficients de f, on obtient alors une opérateur universel qui commute à la spécialisation (des coefficients).

Le résultat principal obtenu par W. Ruppert dans [Ruppert, 1986] est le suivant : $f(X,Y,Z) \in k[X,Y,Z]$ est irréductible si et seulement si $\dim_k \ker \mathcal{R}(f) = 0$. Il fournit donc un test d'irréductibilité absolue. Par ailleurs, suite au travail de S. Gao [Gao, 2003] basé sur [Ruppert, 1986, 1999], ce résultat a également permis des avancées significatives sur l'efficacité des algorithmes de factorisation absolue (voir par exemple [Chèze and Lecerf, 2007; Lecerf, 2007]).

En collaboration avec G. Chèze, nous nous sommes intéressés à cette méthode et avons eu besoin d'approfondir l'étude du noyau de la matrice de Ruppert. Ainsi, un des résultats principaux de [30] est le suivant.

Théorème 30 ([30, Theorem 8])**.** *Soit $f(X,Y,Z) \in k[X,Y,Z]$ un polynôme homogène non nul de degré d et supposons en outre que $f = f_1^{e_1} \cdots f_r^{e_r}$ où chaque polynôme $f_i(X,Y,Z)$ est irréductible et homogène de degré d_i. Alors*

$$\dim_k \ker \mathcal{R}(f) = r - 2 + \binom{2 + \sum_{i=1}^r d_i(e_i - 1)}{2}.$$

En particulier, $f(X,Y,Z)$ est irréductible si et seulement si $\dim_k \ker \mathcal{R}(f) = 0$.

Lorsque f est un polynôme sans facteur carré, c'est-à-dire lorsque $e_i = 1$ pour tout $i = 1, \ldots, r$, on obtient que $\dim_k \ker \mathcal{R}(f) = r - 1$. De plus, on montre que les $r-1$ éléments

$$\left(-d_i \frac{f}{f_1} \partial_X f_1 + d_1 \frac{f}{f_i} \partial_X f_i, -d_i \frac{f}{f_1} \partial_Y f_1 + d_1 \frac{f}{f_i} \partial_Y f_i \right), \quad i = 2, \ldots, r$$

forment une k-base du noyau de $\mathcal{R}(f)$. Il est également possible de décrire une base explicite de ce noyau lorsque $e_1 \geq 1$ et $e_2 = \ldots = e_r = 1$ (résultat non publié obtenu avec G. Chèze), mais on ne connaît pas de base explicite de ce noyau en toute généralité.

3.1.2 Quelques éléments de preuve

Donnons à présent les grandes lignes de la preuve du théorème 30 donnée dans [30], afin notamment d'expliquer le lien entre l'application de Ruppert $\mathcal{R}(f)$ et la cohomologie de De Rahm du complémentaire de la courbe algébrique définie par l'équation $f = 0$.

Pour tout entier ν et tout polynôme non nul $f(X,Y) \in k[X,Y]$ de degré $d \leq \nu$, on définit l'application k-linéaire

$$\begin{array}{rcl} \mathcal{G}_\nu(f) : k[X,Y]_{\leq \nu-1} \times k[X,Y]_{\leq \nu-1} & \longrightarrow & k[X,Y]_{\leq \nu+d-2} \\ (G,H) & \mapsto & f^2\left(\partial_Y\left(\frac{G}{f}\right) - \partial_X\left(\frac{H}{f}\right)\right) = \left|\begin{array}{cc} f & \partial_Y f \\ G & \partial_Y G \end{array}\right| - \left|\begin{array}{cc} f & \partial_X f \\ H & \partial_X H \end{array}\right|. \end{array}$$

En outre, supposons que $f = f_1^{e_1} \cdots f_r^{e_r}$ est une factorisation de f où chaque polynôme f_i est irréductible et désignons par $\mathcal{C} \subset \mathbb{A}_k^2$ la courbe algébrique d'équation $f = 0$. Le premier groupe de cohomologie de De Rahm $H^1(\mathbb{A}_k^2 \setminus \mathcal{C})$ est, par définition, le quotient des 1-formes différentielles fermées $w \in \Omega_{k[X,Y]_f/k}$ de $k[X,Y]_f$ sur k par les 1-formes exactes.

Au vu de la définition de l'application $\mathcal{G}_\nu(f)$, on constate qu'un couple $(G,H) \in k[X,Y]_{\leq \nu-1} \times k[X,Y]_{\leq \nu-1}$ appartient au noyau de $\mathcal{G}_\nu(f)$ si et seulement si la 1-forme $\frac{1}{f}(G\mathbf{d}X + H\mathbf{d}Y)$ est fermée. Par conséquent, le noyau de $\mathcal{G}_\nu(f)$ est en correspondance avec les 1-formes différentielles fermées $w \in \Omega_{k[X,Y]_f/k}$ qui peuvent s'écrire sous la forme $w = \frac{1}{f}(G\mathbf{d}X + H\mathbf{d}Y)$ où G et H sont des polynômes de degré inférieur ou égal à $\nu - 1$. Il se trouve que ces 1-formes fermées sont suffisantes pour fournir un représentant de n'importe quel élément du $H^1(\mathbb{A}_k^2 \setminus \mathcal{C})$, c'est-à-dire que l'application canonique

$$\ker \mathcal{G}_\nu(f) \to H^1(\mathbb{A}_k^2 \setminus \mathcal{C})$$

est surjective. Ce point est démontré de manière assez élémentaire dans [Ruppert, 1986] (voir aussi [Scheiblechner, 2007, Theorem 8.3]), mais il découle plus généralement du fait que les 1-formes fermées $\frac{\mathbf{d}f_1}{f_1}, \ldots, \frac{\mathbf{d}f_r}{f_r}$ constituent une base du $H^1(\mathbb{A}_k^2 \setminus \mathcal{C})$ (voir loc. cit. ou par exemple [Dimca, 1992, Chapter 6]).

Par suite,

$$H^1(\mathbb{A}_k^2 \setminus \mathcal{C}) \simeq \ker \mathcal{G}_\nu(f)/B_\nu \tag{3.1}$$

où B_ν désigne l'ensemble des 1-formes dans $\ker \mathcal{G}_\nu(f)$ qui sont exactes. En général, les éléments de B_ν sont de la forme $d\left(\frac{P}{f^s}\right)$ où $P \in k[X,Y]$ et $s \in \mathbb{N}$. Cependant, on montre [30, Lemma 1 et 2] que

$$B_\nu = \left\{ w = \frac{1}{f}(G\mathbf{d}X + H\mathbf{d}Y), (G,H) \in k[X,Y]_{\leq \nu-1} \times k[X,Y]_{\leq \nu-1} \right. \\ \left. \text{tel que } \exists P \in K[X,Y]_{\leq \nu} \text{ avec } \mathbf{d}\left(\frac{P}{f}\right) = w \right\}. \tag{3.2}$$

À partir de cette description, on peut calculer $\dim_k B_\nu$. De plus, on sait que $\dim_k(H^1(\mathbb{A}_k^2 \setminus \mathcal{C})) = r$ et (3.1) fournit l'égalité

$$\dim_k(\ker \mathcal{G}_\nu(f)) = \dim_k(H^1(\mathbb{A}_k^2 \setminus \mathcal{C})) + \dim_k B_\nu = r + \dim_k B_\nu.$$

On en déduit la

Proposition 31 ([30, Proposition 3])**.** *Soit $f(X,Y) \in k[X,Y]$ un polynôme de degré d tel que $f = f_1^{e_1} \cdots f_r^{e_r}$ est une factorisation de f où chaque polynôme f_i est irréductible de degré d_i. Alors, pour tout $\nu \geq d$ on a*

$$\dim_k \ker \mathcal{G}_\nu(f) = r - 1 + \binom{2 + \nu - d + \sum_{i=1}^r d_i(e_i - 1)}{2}.$$

À présent, introduisons une nouvelle application k-linéaire qui est identique à $\mathcal{G}_\nu(f)$ mais dont nous réduisons la source afin de nous rapprocher de la matrice de Ruppert. Pour tout entier ν, on considère le k-espace vectoriel

$$E_\nu = \{(G,H) \in k[X,Y]_{\leq \nu-1} \times k[X,Y]_{\leq \nu-1} \text{ tel que } \deg(XG + YH) \leq \nu - 1\}$$

qui est de dimension ν^2-1. Soit $f \in k[X,Y]$ un polynôme de degré $d \geq 1$. Il n'est pas difficile de vérifier que pour tout couple $(G,H) \in E_\nu$, le polynôme

$$f^2\left(\partial_Y\left(\frac{G}{f}\right) - \partial_X\left(\frac{H}{f}\right)\right)$$

est de degré au plus $\nu+d-3$. Par conséquent, l'application k-linéaire suivante est bien définie :

$$\mathcal{R}_\nu(f) : E \longrightarrow k[X,Y]_{\leq \nu+d-3} : (G,H) \mapsto f^2\left(\partial_Y\left(\frac{G}{f}\right) - \partial_X\left(\frac{H}{f}\right)\right).$$

Avec cette définition, on peut alors montrer [30, preuve du théorème 8] la propriété suivante. Soit $f(X,Y,Z) \in k[X,Y,Z]$ un polynôme homogène de degré $d \geq 1$ et posons $\tilde{f}(X,Y) := f(X,Y,1) \in k[X,Y]$, alors on a

$$\ker \mathcal{R}(f) \simeq \ker \mathcal{R}_d(\tilde{f}).$$

Suivant que $d = \deg(\tilde{f})$ ou $d > \deg(\tilde{f})$, on peut calculer $\dim_k \mathcal{R}_d(\tilde{f})$, et ainsi conclure la preuve du théorème 30, grâce au résultat suivant.

Proposition 32 ([30, Proposition 5])**.** *Soit $f(X,Y) \in k[X,Y]$ un polynôme de degré $d \geq 1$. On a*

$$\dim_k \ker \mathcal{R}_d(f) = \dim_k \ker \mathcal{G}_d(f) - 1$$

et pour tout $\nu > d$

$$\dim_k \ker \mathcal{R}_\nu(f) = \dim_k \ker \mathcal{G}_{\nu-1}(f).$$

3.2 Ordre total de réductibilité d'un pinceau d'hypersurfaces

Dans ce paragraphe, étant donné un pinceau de courbes algébriques planes dont une courbe générale est irréductible, on s'intéresse à borner supérieurement le nombre de courbes réductibles (qui sont en nombre fini) dans ce pinceau. Cette question a été largement abordée dans la littérature existante et nous commençons par en donner les principaux résultats.

3.2.1 Définition et historique

Soit $r(X,Y) = f(X,Y)/g(X,Y)$ une fraction rationnelle dans $k(X,Y)$, où le corps k est toujours supposé algébriquement clos. Il est d'usage de dire que r est *non-composée* si elle ne peut pas s'écrire $r = u \circ h$ avec $h(X,Y) \in k(X,Y)$ et $u \in k(T)$ telle que $\deg(u) \geq 2$. En outre, on rappelle que le degré d'une fraction rationnelle est par définition le maximum entre le degré de son numérateur et le degré de son dénominateur lorsque ces deux derniers sont premiers entre eux (on dit dans ce cas que r est réduite). Posant $d := \deg(r) = \max(\deg(f), \deg(g))$, on définit les deux polynômes homogènes dans $k[X,Y,Z]$ de même degré d :

$$f^\sharp(X,Y,Z) := Z^d f\left(\frac{X}{Z}, \frac{Y}{Z}\right), \quad g^\sharp(X,Y,Z) = Z^d g\left(\frac{X}{Z}, \frac{Y}{Z}\right).$$

L'ensemble

$$\sigma(f,g) = \{(\mu:\lambda) \in \mathbb{P}^1_k \text{ tel que } \mu f^\sharp + \lambda g^\sharp \text{ est réductible dans } k[X,Y,Z]\} \subset \mathbb{P}^1_k$$

est appelé le *spectre* de r. Un théorème classique de Bertini et Krull montre que le cardinal du spectre de r est un ensemble fini si r est non-composée. Plus précisément, on montre (cf. [Jouanolou, 1979, Chapitre 2, Théorème 3.4.6] ou [Bodin, 2008, Theorem 2.2]) que $\sigma(f,g)$ est fini si et seulement si r est non-composée et si et seulement si le pinceau de courbes planes $\mu f^\sharp + \lambda g^\sharp = 0$, $(\mu:\lambda) \in \mathbb{P}^1_k$, possède un élément général irréductible. L'étude de $\sigma(f,g)$ étant triviale lorsque $d = 1$, nous supposerons désormais que $d \geq 2$.

Choisissons à présent un élément $(\mu:\lambda)$ dans $\sigma(f,g)$ et considérons une factorisation complète du polynôme $\mu f^\sharp + \lambda g^\sharp$:

$$\mu f^\sharp + \lambda g^\sharp = \prod_{i=1}^{n(\mu:\lambda)} P_{(\mu:\lambda),i}^{e_{(\mu:\lambda),i}}, \tag{3.3}$$

chaque polynôme $P_{(\mu:\lambda),i}$ étant irréductible et homogène dans $k[X,Y,Z]$. Lorsque $\sigma(f,g)$ est fini, on définit l'*ordre total de réductibilité* de r, que l'on note $\rho(f,g)$, par

$$\rho(f,g) = \sum_{(\mu:\lambda)\in\mathbb{P}^1_k} \big(n(\mu:\lambda)-1\big).$$

Il est à noter que la somme ci-dessus est finie puisque $n(\mu:\lambda)\neq 1$ entraîne que $(\mu:\lambda)\in\sigma(f,g)$.

Le premier résultat en relation avec le spectre d'une fraction rationnelle semble être dû à Poincaré qui montre dans [Poincaré, 1891] que

$$|\sigma(f,g)| \leq (2d-1)^2 + 2d + 2.$$

Cette borne n'a été améliorée que plus récemment par Ruppert [Ruppert, 1986] qui montre pour sa part, en utilisant le critère d'irréductibilité que nous avons rappelé dans le paragraphe précédent, que $|\sigma(f,g)| \leq d^2-1$. Un peu plus tard, Stein s'est penché sur une question un peu moins générale, mais a donné un résultat plus fort [Stein, 1989] : il a démontré que si $g=1$ alors $\rho(f,1)\leq d-1$. Son approche, basée sur l'étude du groupe multiplicatif de tous les diviseurs des courbes réductibles du pinceau, est complètement différente de celle de Ruppert.

Par la suite, le résultat de Stein a été généralisé par S. Kaliman [Kaliman, 1992], puis plusieurs travaux [Lorenzini, 1993; Vistoli, 1993; Abhyankar et al., 2003; Bodin, 2008] ont développé des techniques similaires pour traiter le cas général $\rho(f,g)$. Tous ont obtenu la borne $\rho(f,g)\leq d^2-1$ mais chacun avec une extension particulière : dans [Lorenzini, 1993], la borne est montrée en toute caractéristique, dans [Bodin, 2008] il est démontré qu'une généralisation directe de la méthode de Stein fournit $\rho(f,g)\leq d^2+d-1$, dans [Vistoli, 1993] le résultat est généralisé à une variété de base très générale et finalement, dans [Abhyankar et al., 2003] les auteurs se sont intéressés à l'ordre total de réductibilité sur un corps non nécessairement algébriquement clos.

3.2.2 Où l'on compte les multiplicités des fibres réductibles

Dans [30], en collaboration avec G. Chèze, nous nous sommes penchés sur l'approche utilisée par W. Ruppert dans son papier [Ruppert, 1986] où il montre que $|\sigma(f,g)|\leq d^2-1$. Nous avons interprété sa méthode en des termes matriciels puis étudié les noyaux des matrices ainsi obtenues ; c'est le contenu du paragraphe précédent. Cela nous a permit de retrouver de manière assez élémentaire la borne $\rho(f,g)\leq d^2-1$, mais surtout d'améliorer cette inégalité en comptant chacune des courbes réductibles du pinceau avec multiplicité. Notre approche consiste pour l'essentiel à transformer un pinceau de courbes en un pinceau de matrices puis d'en déduire une inégalité à partir de calculs de rang de matrices. Il n'est d'ailleurs pas inutile de noter d'ores et déjà que la quantité d^2-1 n'est autre que la dimension du k-espace vectoriel E qui apparaît dans la source de l'application de Ruppert. Mais soyons un peu plus précis.

Soit $r=f/g\in k(X,Y)$ une fraction rationnelle non-composée de degré $d\geq 2$. Pour tout $(\mu:\lambda)\in\sigma(f,g)$, on pose

$$m(\mu:\lambda) := \sum_{i=1}^{n(\mu:\lambda)} e_{(\mu:\lambda),i}$$

où les quantités $n(\mu:\lambda)$ et $e_{(\mu:\lambda)}$ sont définies par (3.3). C'est le nombre de facteurs irréductibles de la courbe $\mu f^\sharp+\lambda g^\sharp=0$ où chaque facteur est compté avec multiplicité. Il est clair que $n(\mu:\lambda)\leq m(\mu:\lambda)$. On appelle alors *ordre total de réductibilité avec multiplicités* de la fraction rationnelle r l'entier

$$m(f,g) = \sum_{(\mu:\lambda)\in\mathbb{P}^1_k} \big(m(\mu:\lambda)-1\big) = \sum_{(\mu:\lambda)\in\mathbb{P}^1_k} \left(\left(\sum_{i=1}^{n(\mu:\lambda)} e_{(\mu:\lambda),i}\right)-1\right).$$

Évidemment, on a que $0\leq\rho(f,g)\leq m(f,g)$. De plus, contrairement à $\rho(f,g)$, $m(f,g)$ compte les courbes du pinceau qui sont géométriquement irréductibles mais non réduites (d'un point de vue schématique). Cependant, il faut nuancer ce point car un pinceau contient au plus 4 telles courbes (cf. [30, paragraphe suivant le lemme 9]).

Avant de pouvoir énoncer le résultat principal, il nous faut introduire deux autres quantités attachées à la fraction rationnelle r. La première consiste à pondérer la multiplicité de chaque facteur irréductible d'une courbe réductible du pinceau par son degré. Plus précisément, pour tout $(\mu : \lambda) \in \sigma(f, g)$, on pose

$$\omega(\mu : \lambda) = \sum_{i=1}^{n(\mu:\lambda)} \deg(P_{(\mu:\lambda),i}) \left(e_{(\mu:\lambda),i} - 1\right) \geq \sum_{i=1}^{n(\mu:\lambda)} \left(e_{(\mu:\lambda),i} - 1\right)$$

puis on définit l'entier

$$\omega(f, g) = \sum_{(\mu:\lambda)\in\mathbb{P}^1_k} \omega(\mu : \lambda).$$

Cette quantité semble être apparue pour la première fois dans les travaux de Darboux [Darboux, 1878] et Poincaré [Poincaré, 1891] où ils traitaient tous les deux de l'étude qualitative des équations différentielles du premier ordre. En particulier, ils avaient noté que $\omega(f, g) \leq 2d - 2$ (cf. [Jouanolou, 1979, Chapitre 2, Corollaire 3.5.6] pour une preuve).

La deuxième quantité que nous introduisons est purement technique, nous ne lui avons pas trouvé de signification particulière. Pour tout $(\mu : \lambda) \in \sigma(f, g)$, on pose

$$\theta(\mu, \lambda) = \binom{\omega(\mu : \lambda) + 1}{2} - \sum_{i=1}^{n(\mu:\lambda)} (e_{(\mu:\lambda),i} - 1) \geq 0$$

puis on définit

$$\theta(f, g) = \sum_{(\mu:\lambda)\in\mathbb{P}^1_k} \theta(\mu : \lambda).$$

On peut ici préciser que la quantité $\theta(\mu, \lambda)$ est définie de telle sorte que l'on ait

$$m(\mu : \lambda) - 1 + \omega(\mu : \lambda) + \theta(\mu : \lambda) = \dim \ker \mathcal{R}(\mu f^\sharp + \lambda g^\sharp) \tag{3.4}$$

où le membre de droite se calcule grâce au théorème 30.

Nous pouvons maintenant donner le résultat principal, ainsi que sa preuve dans le but de souligner son caractère élémentaire.

Théorème 33 ([30, Theorem 10])**.** *Soit $r = f/g \in k(X, Y)$ une fraction rationnelle non-composée et telle que $d = \deg(r) = \max(\deg(f), \deg(g))$. Alors, on a*

$$0 \leq \rho(f, g) \leq m(f, g) + \omega(f, g) + \theta(f, g) \leq d^2 - 1$$

Démonstration. Pour tout $(\mu : \lambda) \in \mathbb{P}^1_k$, considérons l'application linéaire

$$\mathcal{R}(\mu f^\sharp + \lambda g^\sharp) = \mu \mathcal{R}(f^\sharp) + \lambda \mathcal{R}(g^\sharp)$$

et, choisissant des bases pour les k-espaces vectoriels E et $k[X, Y, Z]_{2d-3}$, considérons les matrices correspondantes

$$\mathrm{M}(\mu f^\sharp + \lambda g^\sharp) = \mu \mathrm{M}(f^\sharp) + \lambda \mathrm{M}(g^\sharp).$$

Elles forment un pinceau de matrices de taille $\binom{2d-1}{2} \times (d^2 - 1)$; noter que $d^2 - 1 \leq \binom{2d-1}{2}$.

Soit $\mathrm{Spect}(U, V) \in k[U, V]$ un plus grand diviseur commun à tous les mineurs d'ordre $d^2 - 1$ de la matrice

$$U\mathrm{M}(f^\sharp) + V\mathrm{M}(g^\sharp). \tag{3.5}$$

C'est un polynôme homogène de degré inférieur ou égal à $d^2 - 1$ puisque les entrées de (3.5) sont des formes linéaires dans $k[U, V]$. On remarque tout d'abord que $\mathrm{Spect}(U, V)$ est non nul. En effet, puisque la fraction rationnelle $r = f/g$ est supposée réduite et non-composée, le spectre $\sigma(f, g)$ est fini et donc il existe $(\mu : \lambda) \notin \sigma(f, g)$. Par le théorème 30, on déduit que $\ker \mathrm{M}(\mu f^\sharp + \lambda g^\sharp) = \{0\}$ et par conséquent qu'au moins un des mineurs d'ordre $d^2 - 1$ de (3.5) est non nul puisqu'il est non nul au point (μ, λ).

Maintenant, soit $(\mu : \lambda) \in \sigma(f, g)$. Le théorème 30 montre que

$$\dim \ker \mathrm{M}(\mu f^\sharp + \lambda g^\sharp) = m(\mu : \lambda) - 1 + \omega(\mu : \lambda) + \theta(\mu : \lambda) > 0 \tag{3.6}$$

Par suite, $(\mu : \lambda)$ est une racine de $\mathrm{Spect}(U, V)$. De plus, par propriété des polynômes caractéristiques, $(\mu : \lambda)$ est une racine de $\mathrm{Spect}(U, V)$ de multiplicité au moins (3.6). En sommant toutes ces multiplicités sur tous les éléments du spectre $\sigma(f, g)$, on obtient la quantité $m(f, g) + \omega(f, g) + \theta(f, g)$ qui est donc bornée supérieurement par $d^2 - 1$ car $\mathrm{Spect}(U, V)$ est un polynôme dont le degré est également borné supérieurement par $d^2 - 1$. □

Faisons quelques commentaires à propos de ce théorème :
– Il est remarquable d'observer que le terme $m(f, g) + \omega(f, g) + \theta(f, g)$ ne dépend que quadratiquement des degrés et des multiplicités des composantes irréductibles des courbes réductibles du pinceau $\mu f^\sharp + \lambda g^\sharp$, ce qui est à comparer avec la borne $d^2 - 1$, quadratique en le degré total du pinceau.
– Comme nous l'avons déjà dit, l'inégalité $\rho(f, g) \leq d^2 - 1$ est démontrée dans [Lorenzini, 1993; Vistoli, 1993]. On sait que cette borne est atteinte pour $d = 1, 2, 3$ mais on ne sait pas si elle l'est pour un degré d arbitraire. Cette question a d'ailleurs déjà été mentionnée dans [Abhyankar et al., 2003, Question 1, p. 79] et [Vistoli, 1993, top of p. 254]. Concernant la quantité $m(f, g)$, les conclusions sont identiques. Néanmoins, une conséquence du théorème 33 est que si $\rho(f, g) = d^2 - 1$ alors nécessairement $\omega(f, g) = 0$ (et $\theta(f, g) = 0$). Autrement dit, tout pinceau de courbes dont l'ordre total de réductibilité vaut $d^2 - 1$ satisfait à la propriété que toutes ses courbes réductibles sont réduites.
– Étant donné un polynôme $f \in k[X, Y]$ de degré d, on peut se demander s'il existe une borne plus fine pour $m(f, 1)$ que $d^2 - 1$. En effet, on sait [Stein, 1989] que $\rho(f, 1) \leq d - 1$ et que cette borne est atteinte pour tout degré d. En fait, la combinaison de cette dernière inégalité combinée avec la propriété que $\omega(f, g) \leq 2d - 2$ fournit l'inégalité $m(f, 1) \leq 3d - 3$.

Avant de refermer ce paragraphe, justifions-en le titre qui parlait de pinceaux d'hypersurfaces alors que nous n'avons traité jusqu'ici que de pinceaux de courbes planes. Cette justification provient d'un résultat bien connu sous le nom de théorème de Bertini que nous énonçons ici dans une forme appropriée à notre problème.

Lemme 34 ([Kaltofen, 1995, lemma 7])**.** *Soit*

$$f = \sum_{|\underline{e}| \leq d} c_{e_1,\ldots,e_n} X_1^{e_1} \ldots X_n^{e_n} \in k[X_1, \ldots, X_n]$$

et posons $|\underline{e}| = e_1 + \cdots + e_n$ *et*

$$\mathbb{L} := k(U_1, \ldots, U_n, V_1, \ldots, V_n, W_1, \ldots, W_n)$$

où $U_1, \ldots, U_n, V_1, \ldots, V_n, W_1, \ldots, W_n$ *sont des indéterminées. Alors, le polynôme bivarié*

$$\tilde{f}(X, Y) = f(U_1 X + V_1 Y + W_1, \ldots, U_n X + V_n Y + W_n) \in \mathbb{L}[X, Y]$$

est irréductible dans $\overline{\mathbb{L}}[X, Y]$ *si et seulement si* f *est irréductible dans* $k[X_1, \ldots, X_n]$.

Dans le théorème qui suit, les quantités $m(f, g)$, $\omega(f, g)$ et $\theta(f, g)$ que nous avons définies pour une fraction rationnelle en deux variables X, Y sont naturellement étendues aux fractions rationnelles en n variables $X_1, \ldots, X_n$.

Théorème 35. *Soit* $r = f/g \in k(X_1, \ldots, X_n)$ *une fraction rationnelle réduite non-composée de degré* $d \geq 2$. *On a*

$$m(f, g) + \omega(f, g) + \theta(f, g) \leq d^2 - 1$$

Démonstration. Soit $(\mu : \lambda) \in \mathbb{P}^1_k$. Le lemme 34 implique que

$$\mu f^\sharp + \lambda g^\sharp = \prod_{i=1}^{n(\mu:\lambda)} P_{(\mu:\lambda),i}^{e_{(\mu:\lambda),i}}$$

avec $P_{(\mu:\lambda),i}$ homogène et irréductible dans $k[X_0, X_1, \ldots, X_n]$, si et seulement si

$$\mu \tilde{f}^\sharp + \lambda \tilde{g}^\sharp = \prod_{i=1}^{n(\mu:\lambda)} \tilde{P}_{(\mu:\lambda),i}^{e_{(\mu:\lambda),i}}$$

avec $\tilde{P}_{(\mu:\lambda),i}$ homogène et irréductible dans $\overline{\mathbb{L}}[X, Y, Z]$. Par conséquent, $m(f, g) = m(\tilde{f}, \tilde{g})$, $\omega(f, g) = \omega(\tilde{f}, \tilde{g})$ et $\theta(f, g) = \theta(\tilde{f}, \tilde{g})$. L'inégalité annoncée se déduit alors du théorème 33 appliqué à la fraction rationnelle $r = \tilde{f}/\tilde{g} \in k(X, Y)$. □

Publications de l'auteur

Thèse de doctorat

[1] Laurent Busé, *Étude du résultant sur une variété algébrique*, thèse de l'université de Nice, soutenue le 19 décembre 2001, 130 pages.

Textes publiés dans des revues internationales avec comité de lecture

[2] Laurent Busé, Mohamed Elkadi et Bernard Mourrain, Generalized resultants for unirational algebraic varieties, *Journal of Symbolic Computation*, 59 :515-526, 2000.

[3] Laurent Busé, Mohamed Elkadi et Bernard Mourrain, Resultant over the residual of a complete intersection, *Journal of Pure and Applied Algebra*, 164 (1-2) :35-57,2001.

[4] Laurent Busé, David Cox et Carlos D'Andrea, Implicitization of surfaces in $\mathbb{P}^3$ in the presence of base points, *Journal of Algebra and its Applications*, 2 (2) :189-214, 2003.

[5] Laurent Busé et Jean-Pierre Jouanolou, On the closed image of a rational map and the implicitization problem, *Journal of Algebra*, 265 :312-357, 2003.

[6] Laurent Busé, Mohamed Elkadi et Bernard Mourrain, Using projection operators in Computer Aided Geometric Design, Topics in Algebraic Geometry and Geometric Modeling, *Contemporary Mathematics* 334 :321-342, 2003.

[7] Laurent Busé, Resultants of determinantal varieties, *Journal of Pure and Applied Algebra*, 193 :71-97, 2004.

[8] Laurent Busé et Carlos D'Andrea, On the irreducibility of multivariate subresultants, *C. R. Acad. Sci. Paris, Ser. I* 338 :287-290, 2004.

[9] Laurent Busé et André Galligo, Semi-implicit representations of surfaces in $\mathbb{P}^3$, resultants and applications, *Journal of Symbolic Computation*, 39 :317-329, 2005.

[10] Laurent Busé et Marc Chardin, Implicitizing rational hypersurfaces using approximation complexes, *Journal of Symbolic Computation*, 40 :1150-1168, 2005.

[11] Laurent Busé et Carlos D'Andrea, A matrix-based approach to properness and inversion problems for rational surfaces, *Applicable Algebra in Engineering, Communication and Computing*, 17(6) :393–407, 2006.

[12] Laurent Busé, Mohamed Elkadi et André Galligo, Intersection and self-intersection of surfaces by means of Bezoutian matrices, *Computer Aided Geometric Design*, 25(2) :53–68, 2008.

[13] Laurent Busé et Ron Goldman, Division Algorithms for Bernstein Polynomials, *Computer Aided Geometric Design*, 25(9) :850-865, 2008.

[14] Laurent Busé et Bernard Mourrain, Explicit factors of some iterated resultants and discriminants, *Mathematics of Computations*, 78(265) :345–386, 2009.

[15] Laurent Busé, Mohamed Elkadi et André Galligo, A computational study of rational ruled surfaces, *Journal of Symbolic Computation*, 44(3) :232–241, 2009.

[16] Laurent Busé, Marc Chardin et Jean-Pierre Jouanolou, Torsion of the symmetric algebra and implicitization, *Proceedings of the American Mathematical Society*, 137(6) :1855–1865, 2009.

[17] Laurent Busé, On the equations of the moving curve ideal, *Journal of Algebra*, 321(8) :2317–2344, 2009.

[18] Laurent Busé, Guillaume Chèze et Salah Najib, Noether's forms for the study of non-composite rational functions and their spectrum, *Acta Arithmetica*, à paraître.

[19] Laurent Busé, Marc Chardin et Aron Simis, avec une appendice de Joseph Oesterlé, Elimination and nonlinear equations of Rees Algebras, *Journal of Algebra*, 324(6) :1314–1333, 2010.

[20] Laurent Busé et Thang Luu Ba, Matrix-based implicit representations of rational algebraic curves and applications, *Computer Aided Geometric Design*, 27(9) :681–699, 2010.

Actes de congrès internationaux avec comité de lecture

[21] Laurent Busé, Residual resultant over the projective plane and the implicitization problem, *Proceedings ACM of the International Symposium on Symbolic and Algebraic Computation 2001* (London, Ontario), ACM Press., New-York, pages 48-55, 2001.

[22] Laurent Busé et André Galligo, A resultant approach to detect intersecting curves in $\mathbb{P}^3$, *Proceedings of the International MEGA conference 2003* (electronique), 2003.

[23] Laurent Busé et André Galligo, Using semi-implicit representation of algebraic surfaces, *Proceedings IEEE Computer Society of the International Shape Modeling and Applications Conference 2004*, pp. 342-345, 2004.

[24] Laurent Busé et Carlos D'Andrea, Inversion of parameterized hypersurfaces by means of subresultants, *Proceedings ACM of the International Symposium on Symbolic and Algebraic Computation 2004* (Santander, Spain), ACM Press., New-York, pages 65-71, 2004.

[25] Laurent Busé, Houssam Khalil et Bernard Mourrain, Resultant-based methods for plane curves intersection problems, Proceedings of the CASC 2005 conference (Kalamata, Greece), *Lecture Notes in Computer Sciences*, 3718 :75-92, 2005.

[26] Laurent Busé et Marc Dohm, Implicitization of Bihomogeneous Parametrizations of Algebraic Surfaces via Linear Syzygies, *Proceedings ACM of the International Symposium on Symbolic and Algebraic Computation 2007* (Waterloo, Ontario, Canada), ACM Press., New-York, pages 69–76, 2007.

[27] Thang Luu Ba, Laurent Busé et Bernard Mourrain, Curve/surface intersection problem by means of matrix representations, *Proceedings ACM of the International Symposium on Symbolic and Numerical Computation 2009* (Kyoto, Japan), ACM Press., New-York, pages 71–78, 2009.

Chapitre de Livre

[28] Stefanie Hahmann, Alexander Belyaev, Laurent Busé, Gershon Elber, Bernard Mourrain et Christian Roessl, *Shape interrogation*, Shape Analysis and Structuring, Leila De Floriani, Michela Spagnuolo (Ed.), Springer, series *Mathematics and Visualization*, pages 1–57, 2007.

Travail éditorial

[29] Laurent Busé, Mohamed Elkadi et Bernard Mourrain, éditeurs invités, Computational Algebraic Geometry and Applications, *Theoretical Computer Science*, 392(1-3) :1–178, 2008.

Textes soumis pour publication dans des revues internationales avec comité de lecture

[30] Laurent Busé et Guillaume Chèze, On the total order of reducibility of a pencil of algebraic plane curves.

[31] Laurent Busé et Carlos D'Andrea, Singular factors of rational plane curves.

Notes de cours

[32] Laurent Busé, Résultant univarié et courbes algébriques planes, 38 pages, 2006-2008. Cours de Master2.

[33] Laurent Busé, Elimination theory in codimension one and applications, 47 pages, 2006. Cours dans le cadre de l'école CIMPA-UNESCO-IRAN à Zanjan, Iran, 9-22 Juillet 2005.

[34] Laurent Busé, Géométrie différentielle et applications, 25 pages, 2004. Cours de Master1.

Bibliographie

S. S. Abhyankar. *Algebraic geometry for scientists and engineers*, volume 35 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1990. ISBN 0-8218-1535-0.

S. S. Abhyankar, W. J. Heinzer, and A. Sathaye. Translates of polynomials. In *A tribute to C. S. Seshadri (Chennai, 2002)*, Trends Math., pages 51–124. Birkhäuser, Basel, 2003.

T. Beelen and P. Van Dooren. An improved algorithm for the computation of Kronecker's canonical form of a singular pencil. *Linear Algebra Appl.*, 105 :9–65, 1988.

A. Bodin. Reducibility of rational functions in several variables. *Israel J. Math.*, 164 :333–347, 2008.

N. Botbol. Implicit equation of multigraded hypersurfaces. Preprint arXiv : 1007.3690, 2010a.

N. Botbol. An algorithm for computing implicit equations of bigraded rational surfaces. Preprint arXiv : 1007.3690, 2010b.

N. Botbol. *Implicitization of rational maps*. PhD thesis, Université Pierre et Marie Curie, Paris, 2010c.

N. Botbol and M. Dohm. A package for computing implicit equations of parametrizations from toric surfaces. Preprint arXiv : 1001.1126, 2010.

N. Botbol, A. Dickenstein, and M. Dohm. Matrix representations for toric parametrizations. *Comput. Aided Geom. Design*, 26(7) :757–771, 2009.

E. Brieskorn and H. Knörrer. *Plane algebraic curves*. Birkhäuser Verlag, Basel, 1986. ISBN 3-7643-1769-8. Translated from the German by John Stillwell.

W. Bruns and J. Herzog. *Cohen-Macaulay rings*, volume 39 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993. ISBN 0-521-41068-1.

P. Cartier and J. Tate. A simple proof of the main theorem of elimination theory in algebraic geometry. *Enseign. Math. (2)*, 24(3-4) :311–317, 1978.

E. Casas-Alvero. *Singularities of plane curves*, volume 276 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2000. ISBN 0-521-78959-1.

M. Chardin. In *Algebraic geometry and geometric modeling*, Math. Vis., pages 23–35. Springer, Berlin, 2006.

F. Chen, W. Wang, and Y. Liu. Computing singular points of plane rational curves. *J. Symbolic Comput.*, 43(2) :92–117, 2008.

G. Chèze and G. Lecerf. Lifting and recombination techniques for absolute factorization. *J. Complexity*, 23(3) :380–420, 2007.

T. Cortadellas Benítez and C. D'Andrea. Minimal generators of the defining ideal of the rees algebra associated to monoid parametrizations. *Computer Aided Geometric Design*, 27(6) :461–473, 2010.

D. Cox, R. Goldman, and M. Zhang. On the validity of implicitization by moving quadrics of rational surfaces with no base points. *J. Symbolic Comput.*, 29(3) :419–440, 2000.

D. Cox, J. W. Hoffman, and H. Wang. Syzygies and the Rees algebra. *J. Pure Appl. Algebra*, 212(7) : 1787–1796, 2008.

D. A. Cox. Equations of parametric curves and surfaces via syzygies. In *Symbolic computation : solving equations in algebra, geometry, and engineering (South Hadley, MA, 2000)*, volume 286 of *Contemp. Math.*, pages 1–20. Amer. Math. Soc., Providence, RI, 2001.

D. A. Cox. The moving curve ideal and the Rees algebra. *Theoret. Comput. Sci.*, 392(1-3) :23–36, 2008.

D. A. Cox, T. W. Sederberg, and F. Chen. The moving line ideal basis of planar rational curves. *Comput. Aided Geom. Design*, 15(8) :803–827, 1998.

G. Darboux. Mémoire sur les équations différentielles algébriques du premier ordre et du premier degré (Mélanges). *Bull. Sci. Math. 2ème série*, 2 :60–96 ; 123–144 ; 151–200, 1878.

M. Demazure. Une définition constructive du résultant. Preprint of the "Notes Informelles de Calcul Formel", `http://www.gage.polytechnique.fr/notes/1984-1994.html`, may 1984.

J. Dieudonné. Sur la réduction canonique des couples de matrices. *Bull. Soc. Math. France*, 74 :130–146, 1946.

A. Dimca. *Singularities and topology of hypersurfaces*. Universitext. Springer-Verlag, New York, 1992. ISBN 0-387-97709-0.

M. Dohm. *Implicitization of rational algebraic surfaces with syzygy-based methods*. PhD thesis, Université de Nice Sophia Antipolis, Nice, 2008.

D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. ISBN 0-387-94268-8 ; 0-387-94269-6. With a view toward algebraic geometry.

D. Eisenbud and J. Harris. *The geometry of schemes*, volume 197 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

D. Eisenbud, F.-O. Schreyer, and J. Weyman. Resultants and Chow forms via exterior syzygies. *J. Amer. Math. Soc.*, 16(3) :537–579, 2003.

M. El Kahoui. D-resultant and subresultants. *Proc. Amer. Math. Soc.*, 133(8) :2193–2199 (electronic), 2005.

E. Fortuna, P. Gianni, and B. Trager. Generators of the ideal of an algebraic space curve. *J. Symbolic Comput.*, 44(9) :1234–1254, 2009.

F. R. Gantmacher. *Théorie des matrices. Tome 2 : Questions spéciales et applications*. Traduit du Russe par Ch. Sarthou. Collection Universitaire de Mathématiques, No. 19. Dunod, Paris, 1966.

S. Gao. Factoring multivariate polynomials via partial differential equations. *Math. Comp.*, 72(242) : 801–822 (electronic), 2003.

T. Garrity and J. Warren. On computing the intersection of a pair of algebraic surfaces. *Comput. Aided Geom. Design*, 6(2) :137–153, 1989.

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.

G. H. Golub and C. F. Van Loan. *Matrix computations*. Johns Hopkins Studies in the Mathematical Sciences. Johns Hopkins University Press, Baltimore, MD, third edition, 1996. ISBN 0-8018-5413-X ; 0-8018-5414-8.

D. R. Grayson and M. E. Stillman. Macaulay2, a software system for research in algebraic geometry. Available at http ://www.math.uiuc.edu/Macaulay2/.

J. Gutierrez, R. Rubio, and J.-T. Yu. *D*-resultant for rational functions. *Proc. Amer. Math. Soc.*, 130 (8) :2237–2246 (electronic), 2002.

R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. ISBN 0-387-90244-9. Graduate Texts in Mathematics, No. 52.

O. Henrici. On certain formulæ concerning the theory of discriminants. *Proc. of London Math. Soc.*, pages 104–116, Nov. 12th 1868.

O. Henrici. On the singularities of curves envelopes. *Proc. of London Math. Soc.*, pages 177–195, May 13th 1869.

J. Herzog, A. Simis, and W. V. Vasconcelos. Approximation complexes of blowing-up rings. *J. Algebra*, 74(2) :466–493, 1982.

J. Herzog, A. Simis, and W. V. Vasconcelos. Approximation complexes of blowing-up rings. II. *J. Algebra*, 82(1) :53–83, 1983a.

J. Herzog, A. Simis, and W. V. Vasconcelos. Koszul homology and blowing-up rings. In *Commutative algebra (Trento, 1981)*, volume 84 of *Lecture Notes in Pure and Appl. Math.*, pages 79–169. Dekker, New York, 1983b.

J. Hong, A. Simis, and W. V. Vasconcelos. On the homology of two-dimensional elimination. *J. Symbolic Comput.*, 43(4) :275–292, 2008.

X. Jia, H. Wang, and R. Goldman. Set-theoretic generators of rational space curves. *Journal of Symbolic Computation*, 45(4) :414 – 433, 2010.

J. P. Jouanolou. Singularités rationnelles du résultant. In *Algebraic geometry (Proc. Summer Meeting, Univ. Copenhagen, Copenhagen, 1978)*, volume 732 of *Lecture Notes in Math.*, pages 183–213. Springer, Berlin, 1979.

J. P. Jouanolou. Idéaux résultants. *Adv. in Math.*, 37(3) :212–238, 1980.

J.-P. Jouanolou. Aspects invariants de l'élimination. *Adv. Math.*, 114(1) :1–174, 1995.

S. Kaliman. Two remarks on polynomials in two variables. *Pacific J. Math.*, 154(2) :285–295, 1992.

E. Kaltofen. Effective Noether irreducibility forms and applications. *J. Comput. System Sci.*, 50(2) : 274–295, 1995. 23rd Symposium on the Theory of Computing (New Orleans, LA, 1991).

A. Kustin, C. Polini, and B. Ulrich. Rational normal scrolls and the defining equations of rees algebras. Preprint arXiv :0812.4963, 2008.

G. Lecerf. Improved dense multivariate polynomial factorization algorithms. *J. Symbolic Comput.*, 42 (4) :477–494, 2007.

D. Lorenzini. Reducibility of polynomials in two variables. *J. Algebra*, 156(1) :65–75, 1993.

R. E. MacRae. On an application of the Fitting invariants. *J. Algebra*, 2 :153–169, 1965.

D. Manocha and J. Canny. A new approach for surface intersection. In *Proceedings of the first ACM symposium on Solid modeling foundations and CAD/CAM applications*, pages 209–219, Austin, Texas, United States, 1991. ACM. ISBN 0-89791-427-9.

B. Mourrain. Computing isolated polynomial roots by matrix methods. *J. of Symbolic Computation, Special Issue on Symbolic-Numeric Algebra for Polynomials*, 26(6) :715–738, Dec. 1998.

B. Mourrain. Bezoutian and quotient ring structure. *J. of Symbolic Computation*, 39(3) :397–415, 2005.

E. Noether. Ein algebraisches Kriterium für absolute Irreduzibilität. *Math. Ann.*, 85(1) :26–40, 1922.

D. G. Northcott. *Finite free resolutions*. Cambridge University Press, Cambridge, 1976. Cambridge Tracts in Mathematics, No. 71.

H. Poincaré. Sur l'intégration algébrique des équations différentielles du premier ordre. *Rendiconti des Circulo Matematico di Palermo*, 5 :161–191, 1891.

W. Ruppert. Reduzibilität Ebener Kurven. *J. Reine Angew. Math.*, 369 :167–191, 1986.

W. M. Ruppert. Reducibility of polynomials $f(x, y)$ modulo p. *J. Number Theory*, 77(1) :62–70, 1999.

P. Scheiblechner. *On the complexity of counting irreducible components and computing betti numbers of algebraic variety*. PhD thesis, University of Paderborn, 2007.

A. Schinzel. *Polynomials with special regard to reducibility*, volume 77 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2000. ISBN 0-521-66225-7. With an appendix by Umberto Zannier.

W. M. Schmidt. *Equations over finite fields. An elementary approach*. Springer-Verlag, Berlin, 1976. Lecture Notes in Mathematics, Vol. 536.

A. Simis and W. V. Vasconcelos. The syzygies of the conormal module. *Amer. J. Math.*, 103(2) :203–224, 1981.

N. Song and R. Goldman. μ-bases for polynomial systems in one variable. *Comput. Aided Geom. Design*, 26(2) :217–230, 2009.

Y. Stein. The total reducibility order of a polynomial in two variables. *Israel J. Math.*, 68(1) :109–122, 1989.

R. C. Thompson. An inequality for invariant factors. *Proc. Amer. Math. Soc.*, 86(1) :9–11, 1982.

A. van den Essen and J.-T. Yu. The D-resultant, singularities and the degree of unfaithfulness. *Proc. Amer. Math. Soc.*, 125(3) :689–695, 1997.

W. V. Vasconcelos. *Arithmetic of blowup algebras*, volume 195 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1994. ISBN 0-521-45484-0.

A. Vistoli. The number of reducible hypersurfaces in a pencil. *Invent. Math.*, 112(2) :247–262, 1993.

H. Wang, X. Jia, and R. Goldman. Axial moving planes and singularities of rational space curves. *Comput. Aided Geom. Design*, 26(3) :300–316, 2009.

H. Whitney. On singularities of mappings of euclidean spaces. i. mapping of the plane into the plane. *Annals of Mathematics*, 62(3) :374–410, 1955.

U. Zannier. On the reduction modulo p of an absolutely irreducible polynomial $f(x, y)$. *Arch. Math. (Basel)*, 68(2) :129–138, 1997.

Résumé

Ce mémoire d'habilitation présente des travaux qui développent une approche matricielle de la théorie de l'élimination et l'illustrent au travers d'applications à la modélisation géométrique. Cette approche matricielle, qui correspond essentiellement à un changement de représentation, permet de livrer des problèmes géométriques à la puissance des algorithmes d'algèbre linéaire numérique. Le premier chapitre traite de la représentation matricielle implicite d'une hypersurface rationnelle dans un espace projectif et propose une nouvelle méthode pour traiter le problème d'intersection entre une courbe et une surface rationnelles dans l'espace projectif de dimension trois. Le deuxième chapitre propose une représentation matricielle implicite d'une courbe rationnelle dans un espace projectif de dimension arbitraire, représentation qui est illustrée par un algorithme répondant au problème d'intersection entre deux courbes rationnelles. Le dernier chapitre est dédié à une approche matricielle du test d'irréductibilité de Ruppert qui conduit au raffinement du dénombrement des fibres réductibles dans un pinceau d'hypersurfaces algébriques génériquement irréductible.

Mots clés : théorie de l'élimination, géométrie algébrique effective, algèbres de Rees et symétriques, courbes et surfaces rationnelles, implicitation.

Abstract

In this habilitation thesis, a matrix-based approach of elimination theory is described and illustrated through applications in algebraic modeling. This matrix-based approach allows to build a bridge between geometry and numerical linear algebra, so that some geometric problems can be given to the powerful numerical linear algebra tools. The first chapter deals with matrix-based implicit representations of rational hypersurfaces in a projective space and a new method to address the computation of the intersection locus between a rational curve and a rational surface is exposed. The second chapter contains a matrix-based implicit representation of a rational curve in a projective space of arbitrary dimension. Then, the usefulness of such a representation is illustrated with an algorithm to treat the intersection problem between two rational curves. In last chapter, a matrix-based approach to Ruppert's irreducibility criterion is given and used to improve the counting of reducible fibers in a pencil of algebraic hypersurfaces whose general member is irreducible.

Key words : elimination theory, computational algebraic geometry, Rees and symmetric algebras, rational curves and surfaces, implicitization.

Université de Nice - Sophia Antipolis