Algorithmes - disons rapides - pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionnelles

MARC GIUSTI* JOOS HEINTZ

Résumé. Nous décrivons dans cet article deux algorithmes qui construisent les décompositions irréductible et équidimensionnelle d'une variété algébrique affine (ou projective), définie par un ensemble fini de polynômes. Le premier calcule les composantes irréductibles, donc dépend d'un algorithme de factorisation, et en conséquence ne peut se paralléliser que partiellement, du moins à notre connaissance. Le second correspond aux composantes équidimensionelles, et est susceptible d'une parallélisation totale. Comme applications, le lecteur trouvera en appendice un calcul de la forme de Chow d'une variété projective quelconque, dû à T. Krick et P. Solerno, et un calcul du degré d'une variété affine.

Ces algorithmes sont décrits par des réseaux arithmétiques, ce qui permet un déroulement séquentiel ou parallèle (avec la restriction concernant la factorisation). En séquentiel, leurs complexités admettent une borne supérieure simplement exponentielle en la taille des polynômes d'entrée (quantité, degré, nombre de variables et éventuellement taille arithmétique). En parallèle, la complexité du deuxième algorithme devient polynomiale en cette taille.

1 Introduction

Pour l'ensemble de ce travail, nous allons fixer les notations.

1.1 Notations de base

Soient k un corps commutatif, parfait et infini, et $\bar{k}$ une clôture algébrique. Afin de traiter simultanément les situations affine et projective, nous allons considérer des espaces ambiants de même dimension n: l'espace affine $\mathbf{A}_{\bar{k}}{}^n$ (resp. l'espace projectif $\mathbf{P}_{\bar{k}}{}^n$), munis de la topologie de Zariski, et notés plus simplement $\mathbf{A}^n$ et $\mathbf{P}^n$.

*Avec un soutien du GDR G0060 “Calcul Formel, Algorithmes, Langages et Systèmes” et du PRC “Mathématiques et Informatique”.

Nous voulons considérer des sous-variétés vivant dans ces espaces ambiants. Il y a deux points de vue: le premier est *intrinsèque*, et consiste à parler d'une sous-variété sans avoir précisé coordonnées ou équations. Mais ce deuxième point de vue *non intrinsèque* est souvent inévitable et il faut donc en passer par là: soient donc $x_1, \ldots, x_n$ (resp. $x_0, x_1, \ldots, x_n$) des indéterminées sur k, et f un système fini de polynômes $f_1, f_2, \ldots, f_s$ de $k[x_1, \ldots, x_n]$ (resp. des polynômes homogènes de $k[x_0, x_1, \ldots, x_n]$). L'idéal engendré sera noté $I(f_1, \ldots, f_s)$ ou plus simplement $(f_1, \ldots, f_s)$, voire I, et la variété algébrique, au sens classique, affine (resp. projective) définie par f ou I sera notée $V_{\bar{k}}(I)$, ou plus simplement $V(I)$, $V(f)$ ou V quand aucun doute n'est possible.

1.2 Considérations de complexité

Les algorithmes considérés ci-dessous vont admettre comme entrées et sorties des ensembles finis de polynômes. Il nous faut donc d'abord quantifier et mesurer la taille d'un tel ensemble, puis préciser le type d'algorithmes qui vont le manipuler.

1.2.1 Taille des entrées-sorties

Soit $f = f_1, \ldots, f_s$ un ensemble fini de polynômes à n variables (resp. homogènes à $n+1$ variables). Nous supposerons qu'ils sont rangés par degré total décroissant $d_1 \geq \cdots \geq d_s$ et, dans le cas projectif, nous noterons $d(f)$ (ou d pour simplifier) le plus grand d'entre eux, à savoir d_1. Dans le cas affine, nous noterons $d(f)$ le maximum de d_1 et de 3; cette restriction technique est due à l'utilisation d'un Nullstellensatz affine effectif, où elle semble être pour le moment inévitable. Sans restriction de généralité, nous supposerons aussi que la dimension de l'espace ambiant est au moins 2.

Il existe un cas particulier important de corps de base: celui des rationnels. En fait comme aucun des algorithmes n'utilise la division dans le corps de base, nous supposerons les coefficients entiers. Dans ce cas la complexité de notre ensemble doit inclure la *taille arithmétique*, c'est-à-dire le nombre maximal $t(f)$ (ou plus simplement t) de bits qu'il faut pour écrire n'importe quel coefficient des polynômes de f.

Autrement dit, la hauteur de chaque f_i $(i = 1, \ldots, s)$, au sens classique des arithméticiens, qui est le maximum des valeurs absolues de tous ses coefficients, est majoré par 2^t.

Une bonne mesure de la complexité du système f semble donc être le triplet (d, n, s) ou le quadruplet (d, n, s, t) dans le cas entier, ce que nous appellerons la *taille* de f. En effet nous pouvons aisément majorer la place mémoire nécessaire pour stocker f à partir de sa taille. Le nombre de monômes sur n lettres de degré au plus d (resp. sur $n+1$ lettres de degré d) est le coefficient binomial $(d+n)!/d!n!$, quantité majorée par $(d+1)^n$. Si nous convenons de coder un polynôme par le vecteur de ses coefficients dans la représentation dense, il faut stocker au plus $s(d+1)^n$ coefficients, et s'ils sont entiers, cela demande au plus $s(d+1)^n t$ bits.

Par ailleurs, remarquons qu'au prix d'un algorithme standard d'algèbre linéaire nous pouvons supposer que les polynômes $f_1, \ldots, f_s$ sont linéairement indépendants sur le corps de base, et donc que s est majoré par $(d+1)^n$. Le coût de cette préparation n'est pas très élevé, et nous le préciserons au paragraphe suivant. Nous la supposerons donc dorénavant faite systématiquement. Avec cette remarque, il suffirait donc de nous restreindre au couple (d, n) ou au triplet (d, n, t) pour caractériser la complexité de f. Mais nous conserverons s dans les données, car posséder un petit nombre de générateurs constitue pour un idéal une propriété intéressante dont il faut garder trace.

Par contre, nous aurons aussi envie de considérer des quantités intrinsèques caractérisant la complexité de V: ce seront essentiellement sa dimension $r(V)$, majorée par n, et son degré $deg(V)$ majoré par d^n (voir la définition et l'inégalité de Bézout correspondante dans Heintz (1983)).

1.2.2 Algorithmes et leur complexité

Les algorithmes que nous allons utiliser ou introduire seront en principe décrits par un *réseau arithmétique*, représenté par un graphe orienté acyclique (von zur Gathen, 1986). A chaque sommet correspond un processeur élémentaire qui effectue une opération de base du corps de base k, et chaque arête indique l'envoi d'une sortie d'un processeur comme entrée du second. Les opérations de base sont l'addition, la soustraction, la multiplication et un sélecteur associé au test d'égalité. Si la caractéristique est positive, il convient d'y ajouter l'extraction des racines $p^{ièmes}$. Nous parlerons alors de *réseau arithmétique étendu*.

Chaque polynôme est codé par le vecteur de ses coefficients dans la représentation dense. Un algorithme travaille donc sur un vecteur d'éléments du corps de base, et admet un déroulement séquentiel ou parallèle. La *complexité séquentielle* est la taille du réseau, c'est-à-dire le nombre de processeurs ou sommets du graphe. La *complexité parallèle* est la profondeur du réseau, c'est-à-dire la longueur du plus long chemin dans le graphe orienté.

Dans le cas entier chaque processeur arithmétique devient lui-même un réseau booléen dont les processeurs manipulent maintenant les bits. Comme nous ne voulons pas entrer dans des considérations de parallélisation à ce niveau booléen, nous nous restreindrons à l'aspect séquentiel en interprétant le déroulement dans le modèle des machines de Turing. Il faut alors tenir compte de la croissance éventuelle des coefficients des polynômes intermédiaires.

Pour une discussion plus approndie de ce modèle de complexité, nous renvoyons à von zur Gathen (1986) et Fitchas-Galligo-Morgenstern (1987).

Dans ce cadre, nous dirons qu'un algorithme est de complexité *admissible* si pour traiter une entrée de taille (d, n, s) le réseau correspondant admet une complexité séquentielle $(sd)^{n^{O(1)}}$ et parallèle en $(n \log(sd))^{O(1)}$. Le cas échéant nous préciserons la constante $O(1)$ en parlant d'un algorithme *admissible d'exposant a*. Dans le cas entier, nous parlerons de complexité admissible si nous pouvons contrôler la taille des entiers qui apparaissent dans les calculs intermédiaires par des bornes du type $(tsd)^{n^{O(1)}}$. Observons que dans le cas où le résultat est constitué de polynômes, la somme de leurs degrés est au plus $(sd)^{n^{O(1)}}$.

Par exemple, l'algorithme de réduction de s, mentionné à la fin du paragraphe précédent, est admissible. C'est une conséquence immédiate de l'algorithme de Berkowitz (1984), et la borne dépend linéairement de s en séquentiel (resp. de $\log(s)$ en parallèle).

1.3 Enoncé des problèmes et des résultats

Un problème fondamental pour la description de V consiste en la détermination de l'ensemble $\mathcal{C}(V)$ des composantes irréductibles de V. Du point de vue algébrique, ceci peut être évidemment résolu par une décomposition primaire irredondante de I. Mais qu'on utilise l'algorithme originel de Hermann (1926), repris par Seidenberg (1974) ou celui plus récent de Gianni-Trager-Zacharias (1988), on se heurte à l'utilisation massive de résolutions de systèmes linéaires à coefficients polynomiaux ou de constructions de bases standard, ce qui entraîne a fortiori une complexité au moins doublement exponentielle.

Mais si nous ne nous intéressons pas au schéma correspondant à l'idéal donné, mais seulement à l'espace topologique sous-jacent, c'est-à-dire à l'ensemble algébrique constitué par les points à coordonnées dans $\bar{k}$ qui annulent tous les polynômes de l'idéal, la situation s'améliore très nettement: ceci constitue la contribution fondamentale de Chistov-Grigoriev (1983), montrant que la détermination ensembliste des composantes irréducibles d'une variété projective peut se calculer par un algorithme séquentiel admissible d'exposant 2. Malheureusement ce dernier dépend d'un algorithme de factorisation, et se parallélise donc mal (il n'en reste pas moins que le reste de leur algorithme peut, lui, fort bien se paralléliser).

Nous nous proposons dans cet article de nous libérer de cette contrainte en exposant un algorithme qui calcule la décomposition équidimensionnelle d'une variété V, c'est-à-dire partant des équations définissantes rend, pour chaque dimension intermédiaire i, $(0 \leq i \leq r(V))$ un ensemble fini de polynômes définissant la réunion des composantes irréductibles ensemblistes de dimension i. Cet algorithme se parallélise totalement car il n'utilise que des sous-algorithmes d'algèbre linéaire sur k.

Chemin faisant, nous redémontrerons dans le cas entier par une méthode originale une version un peu plus faible du théorème de Chistov-

Grigoriev, en calculant les composantes irréductibles sur Q sans entrer dans des questions d'extensions algébriques, en fait en renonçant à la factorisation absolue.

Du point de vue du coût, les complexités sont admissibles, et nous pouvons préciser l'exposant pour la détermination des composantes irréductibles et équidimensionnelles (2, comme chez Chistov-Grigoriev): en séquentiel $s^5 d^{O(n^2)}$ et en parallèle $O(n^4 \log^2 sd)$).

Nous avons appris pendant la préparation de cet article que P. Hintenhaus (1989) avait également traité d'une version du résultat de Chistov-Grigoriev.

L'algorithme de décomposition équidimensionnelle permet de ramener la considération d'une variété arbitraire au cas d'une variété équidimensionnelle. Par exemple, signalons le calcul en temps admissible de la forme de Cayley (ou forme de Chow) d'une variété projective en utilisant l'algorithme d'élimination des quantificateurs de la théorie élémentaire de $\bar{k}$ (Fitchas-Galligo-Morgenstern, 1989, ou Krick, 1990). Ce travail est rassemblé dans un appendice.

Une méthode plus directe pour calculer la forme de Chow d'un idéal équidimensionnel est donné dans Caniglia (1989). Remarquons aussi que découle du même algorithme le calcul du degré de la variété (au sens donné par Heintz (1983), à savoir la somme des degrés de toutes les composantes irréductibles ensemblistes). Ceci découle de Caniglia-Galligo-Heintz (1989, Theorem 19) ou de notre méthode de calcul du polynôme de Chow.

Terminons enfin cette introduction par une remarque technique. Ce qui suit utilise de manière essentielle et constante les divers Nullstellensätze effectifs. Dans le cas projectif, il s'agit d'un résultat de D. Lazard (1977), bien plus facile à établir que son homologue affine. La première version de ce résultat affine a été obtenue par Brownawell (1987), et a été suivie par des extensions de Caniglia-Galligo-Heintz, Kollár, Berenstein-Yger, Philippon, et bien d'autres ... Une bibliographie sur ce sujet se trouve dans la revue de Teissier (1989) au séminaire Bourbaki. Pour ce qui nous concerne ici, nous emploierons principalement la version "à la Hentzelt" (voir par exemple Fitchas-Galligo, 1988 Théorème 10) ou la version locale de Caniglia-Guccione-Guccione (1990).

Une partie de la rédaction de cet article a été effectuée pendant la tenue à Bonn d'un "workshop on algebraic and geometric complexity". Il nous est agréable de remercier ici Marek Karpinski de son invitation.

2 Mise en position générique

Il se peut que les données sur la variété V à décomposer soient très mal conditionnées. Comment est définie V au départ? Dans le cas affine par exemple, comme fibre au dessus de 0 d'une application polynomiale de $\mathbf{A}^n$ dans $\mathbf{A}^s$. Nous allons être amenés à opérer des changements linéaires de coordonnées à la source. Dans le cas projectif, il faudra également changer de coordonnées à la source, mais comme f ne donne pas naturellement naissance à une application projective, la préparation sur les générateurs de l'idéal est un peu plus compliqué qu'un changement de coordonnées.

2.1 Définition des variables normales et générales

Le but est de préparer notre situation, au besoin à l'aide d'un changement linéaire des variables, de manière à ce que la variété étudiée se projette de la façon la plus agréable possible, sur une sous-variété linéaire de même dimension, puis de dimension un de plus.
Le premier pas correspond au lemme algébrique de normalisation de Noether, le second est plus subtil car de nature géométrique: après projection, il s'agit de pouvoir continuer à séparer les composantes irréductibles.

Afin d'alléger les notations, nous allons noter r la dimension $r(V)$ de V.

Précisons ce qui a été indiqué ci-dessus. Etant donné un système de coordonnées $x_1, \ldots, x_n$ de l'espace affine $\mathbf{A}^n$, nous considérerons les projections $\pi_0 : \mathbf{A}^n \to \mathbf{A}^r$ et $\pi : \mathbf{A}^n \to \mathbf{A}^{r+1}$ définies par $\pi_0(x_1, \ldots, x_n) = (x_1, \ldots, x_r)$ et $\pi(x_1, \ldots, x_n) = (x_1, \ldots, x_{r+1})$.

Dans la situation projective, il faut éviter les sous-variétés linéaires $V(x_0, x_1, \ldots, x_r)$ ou $V(x_0, x_1, \ldots, x_{r+1})$ centres de projection. Etant donné un système de coordonnées $x_0, x_1, \ldots, x_n$ de l'espace projectif $\mathbf{P}^n$, nous considérerons les projections $\pi_0 : \mathbf{P}^n - \mathbf{P}^{n-r-1} \to \mathbf{P}^r$ et $\pi : \mathbf{P}^n - \mathbf{P}^{n-r-2} \to \mathbf{P}^{r+1}$ définies par $\pi_0(x_0, x_1, \ldots, x_n) = (x_0, x_1, \ldots, x_r)$ et $\pi(x_0, x_1, \ldots, x_n) = (x_0, x_1, \ldots, x_{r+1})$.

En l'honneur de Max Noether et de son lemme de normalisation, nous dirons que les variables $x_1, \ldots, x_n$ sont en position *normale* par rapport à V si la restriction $\pi_0|_V$ de π_0 à V est un morphisme fini et surjectif de variétés. Ceci revient à dire que l'homorphisme canonique $k[x_1, \ldots, x_r] \to k[x_1, \ldots, x_n]/(f_1, \ldots, f_s)$ est injectif et correspond à une extension entière d'anneaux.

Nous dirons que les variables $x_1, \ldots, x_n$ sont en position *générale* par rapport à V si elles sont en position normale par rapport à la variété et si de plus π sépare les composantes de V, c'est-à-dire que $\pi(C)$ n'est pas contenu dans $\pi(C')$ pour tout couple de composantes distintes C et C' de $\mathcal{C}(V)$.

2.2 Méthode brutale

La mise en position générique peut s'obtenir par une extension trancendante brutale du corps de base k, obtenue en adjoignant un certain nombre de lettres. Décrivons la dans le cas affine.
Soient A la $n \times n$-matrice carrée à coefficients génériques a_{ij} $(i, j = 1, \ldots, n)$, et B la $(n+1) \times s$-matrice à coefficients génériques b_{ij} $(i = 1, \ldots, n+1$, $j = 1, \ldots, s)$. Si x et f sont respectivement les vecteurs colonnes des

$x_1, \dots, x_n$ et des $f_1, \dots, f_s$, on change linéairement de coordonnées à la source et au but en introduisant $y = Ax$ et $g = Bf$.

Dans le cas projectif, la matrice carrée de changement de base à la source doit être d'ordre $n+1$. En ce qui concerne le but, afin de conserver le caractère homogène des générateurs, il faut d'abord les multiplier par des polynômes ad hoc de degré $d_1 - d_i$ avant d'effectuer des combinaisons linéaires à coefficients constants.

En considérant que le nouveau corps de base est $K = k(A, B)$, et que k est infini, les lemmes d'évitement classiques assurent la mise en position générique. Le lecteur peut également se référer au paragraphe suivant.

Il est clair que la méthode précédente n'est pas très bonne du point de vue de la complexité. Cependant si un algorithme est de complexité admissible sur K, il le reste sur k, essentiellement parce que le nombre de monômes de degré $d^{n^{(O(1)}}$ sur n lettres reste du même ordre. [S'il faut changer de générateurs, il est nécessaire d'éviter que s grimpe en exposant, ce que nous pourrons faire en utilisant Heintz-Schnorr (1980, Theorem 4.4), mais nous n'en aurons pas besoin ici.]

2.3 Méthodes raffinées de mise en position générique

Cependant si nous voulons de meilleures bornes, il faut un peu plus travailler.

2.3.1 Mise en position normale

Dans le cas affine, comme k est infini nous pouvons appliquer l'algorithme de normalisation décrit dans Dickenstein-Fitchas-Giusti-Sessa (1989, 1.15) ou dans Logar (1988, A.4). Celui-ci calcule un changement k-linéaire de variables, telles que les nouvelles variables soient en position normale par rapport à V, avec une complexité séquentielle $s^5 d^{O(n^2)}$ et parallèle $O(n^4 \log^2(sd))$. L'algorithme mentionné se base sur une version effective du Nullstellensatz affine (Fitchas-Galligo, 1988, Théorème 10). Dans le cas projectif, nous pouvons nous servir de l'algorithme de normalisation homogène donné par Giusti (1988, Théorème 5.6.2), qui utilise la version effective du Nullstellensatz projectif démontrée par Lazard (1977). Ces deux algorithmes incluent le calcul de la dimension.

Il nous faut maintenant passer à la mise en position générale, que nous allons traiter dans le cas affine. L'extension au cas projectif est laissée (pour le moment !) au lecteur. La clef est de disposer d'un lemme d'évitement très précis, et en fait la dimension 0 suffit. L'idée de ce lemme est due à Chistov-Grigoriev (1983) et repose sur la propriété bien connue des déterminants de Vandermonde.

2.3.2 Définition: les formes x_γ et les projections associées

Si γ est un élément du corps de base, notons x_γ la forme linéaire sur $\mathbf{A}^n$ (resp. $\mathbf{P}^n$) définie par: $x_\gamma(x_1, \ldots, x_n) = x_1 + \gamma x_2 + \cdots + \gamma^{n-1} x_n$ (resp. $x_\gamma(x_0, \ldots, x_n) = x_0 + \gamma x_1 + \cdots + \gamma^n x_n$). Remarquons qu'un ensemble d'éléments distincts deux à deux donne naissance à des formes linéairement indépendantes, pourvu bien sûr qu'elles ne soient pas en nombre trop grand.

Nous aurons aussi à considérer le morphisme d'espaces affines défini par $\pi_\gamma(x) := (x_1, \ldots, x_r, x_\gamma(x))$ où $x = (x_1, \ldots, x_n)$ est un point de $\mathbf{A}^n$.

2.3.3 Un lemme d'évitement en dimension zéro affine

Lemme. *Soit Γ un ensemble fini de c éléments du corps de base k. Soit m un entier vérifiant l'inégalité $(n-1)m < c$. Pour tout sous-ensemble fini M de $\mathbf{A}^n$, ne contenant pas l'origine, et de cardinal au plus m, il existe un élément γ dans Γ tel que la forme linéaire x_γ ne s'annule pas sur M.*

Preuve: Soit t une nouvelle indéterminée, et considérons le polynôme non identiquement nul $w := \prod_{(x_1,\ldots,x_n)\in M}(x_1 + \cdots + x_n t^{n-1})$. Le degré de w ne dépasse pas $(n-1)m$. Comme le cardinal de Γ est strictement supérieur à cette quantité, w ne peut pas s'annuler sur tous les points de Γ: soit γ un point le contredisant. Mais $w(\gamma)$, non nul, n'est pas autre chose que $\prod_{x\in N} x_\gamma(x)$. Il s'ensuit que la forme x_γ ne s'annule pas sur M.

Corollaire 2.3.4 *Soit Γ un ensemble fini de c éléments du corps de base k. Soit m un entier vérifiant l'inégalité $(n-1)m(m-1)/2 < c$. Pour tout sous-ensemble fini M de $\mathbf{A}^n$, de cardinal au plus m, il existe un élément γ dans Γ tel que la forme linéaire x_γ sépare les points de M, c'est-à-dire prenne des valeurs distinctes $x_\gamma(x) \neq x_\gamma(x')$ pour tout couple de points distincts $x \neq x'$ de M.*

Preuve: Formons l'ensemble $N = \{x - x' \mid x, x' \in M, x \neq x'\}$, de cardinal au plus $m(m-1)/2$, et qui ne contient pas zéro par construction. Il suffit de démontrer qu'il existe un point γ de Γ tel que la forme x_γ ne s'annule pas sur l'ensemble N. Mais c'est clair par 2.3.3.

2.3.5 Algorithme non déterministe de calcul de variables générales

Lemme. *Supposons les variables $x_1, \ldots, x_n$ en position normale par rapport à V et la dimension $r(V)$ non triviale, c'est-à-dire $r(V) < n$. Alors si Γ est un ensemble de valeurs de k, de cardinal au moins $n(deg(V))^4$,* *il existe un point γ de Γ tel que les variables $x_1, \ldots, x_r, x_\gamma, x_{r+2}, \ldots, x_n$ soient en position générale par rapport à V.*

Preuve: Choisissons pour chaque composante C de V un point x_C qui n'appartienne à aucune autre composante C' du moment qu'elle soit distincte de C. La définition du degré que nous avons choisie (Heintz, 1983) implique que le nombre de composantes est majoré par le degré de la variété. Comme $\pi_0 \mid_V$ est un morphisme fini, la fibre $\pi_0^{-1}(\pi_0(x_C)) \cap V$ n'est constituée que de points en nombre fini majoré par $deg(V)$, d'après l'inégalité de Bézout affine (Heintz, 1983, Théorème 1). Le cardinal de la réunion de tous ces points, $M := \cup_{C \in \mathcal{C}(V)} \pi_0^{-1}(\pi_0(x_C)) \cap V$ est donc au plus $(deg(V))^2$. Pour chaque élément γ de Γ, considérons le morphisme π_γ introduit en 2.3.2. Observons que $\pi_\gamma \mid_C$ est aussi un morphisme fini pour toute composante C de V. D'après le corollaire 2.3.4, il existe un γ tel que π_γ sépare les points de M. Soient C et C' deux composantes distinctes de V. Alors $\pi_\gamma(x_C)$ ne peut pas appartenir à la projection de C' par π_γ (voir Heintz, 1983, preuve de Lemma 3, pour détails). Ceci implique évidemment que $\pi_\gamma(C)$ n'est pas contenue dans $\pi_\gamma(C')$.

Certes il est désagréable de ne pouvoir déterminer cet élément γ algorithmiquement par un réseau arithmétique, mais la cardinalité admissible de l'ensemble d'où nous le tirons suffira pour nos calculs de complexité.

Une dernière remarque de convention: par abus de notation, nous considérerons toujours être revenu dans les anciennes variables $x_1, \ldots, x_r$, $x_{r+1}, \ldots, x_n$ en n'écrivant jamais le changement de variables correspondant.

3 Trouver une équation de petit degré pour la projection

Dorénavant, nous allons supposer que les variables $x_1, \ldots, x_n$ sont normales pour la variété V à décomposer, et que sa dimension est strictement inférieure à n.

Groupons les composantes de V en deux sous-variétés: d'abord la réunion $T(V)$ des composantes de plus grande dimension. Nous nous référerons de manière imagée à la *tête* de la variété. Il reste éventuellement la réunion $Q(V)$ des autres composantes de plus petite dimension, que nous appellerons le *croupion* de la variété. Nous remercions Jacques Morgenstern de nous avoir dissuadé d'utiliser un autre mot (qui semblait pourtant s'imposer phonétiquement), et donc de sa contribution décisive en faveur de cette terminologie. [1]

[1] "...we take the occasion to stress that English is strongly recommended for the final version (at least the Program Committee suggests that an English translation of "croupion" is provided to help readers not very familiar with French!)" *The MEGA 90 Program Committee.*

D'après le *Petit Robert* (Paul Robert, 1970, traduction anglaise de notre

3.1 Cas affine

Nous allons définir de deux manières différentes la projection de la tête de la variété sur une sous-variété linéaire de dimension 1 de plus en position générale.

3.1.1 Le polynôme minimal

Observons que comme le système de coordonnées est en position normale, la restriction de π à la variété est un morphisme fini de V sur son image. La tête $T(V)$ étant une variété équidimensionnelle définissable sur k, $\pi(T(V))$ l'est aussi. Donc cette dernière est une hypersurface de $\mathbf{A}^{r+1}$, et soit $h(V)$ un polynôme de degré minimal qui la définit. Comme k est parfait par hypothèse, nous en déduisons que $h(V)$ est sans carrés ("quadratfrei !", comme aime à le rappeler le théoricien des nombres Maurice Mignotte, qui possède une solide culture germanique), et que son degré est majoré par celui de la tête (voir Heintz, 1983, Lemma 2), donc par celui de la variété, et en dernier ressort par d^n d'après l'inégalité de Bézout.

3.1.2 Le polynôme calculable

Posons maintenant $D = D(V) := d^n(d^n + 1)$, et analysons le k-espace vectoriel $E(V)$ formé des polynômes de I ne dépendant que des $r+1$ premières variables, et tels que leur écriture sur la base des générateurs donnés $f_1, \ldots, f_s$ se réalise en degré au plus D:

$$E(V) = \{f \in k[x_1, \ldots, x_{r+1}] \mid \exists\, p_1, \ldots, p_s \in k[x_1, \ldots, x_n]$$
$$avec\ \ f = \sum_{1 \leq i \leq s} p_i f_i \ \ et\ \ Max\ \{deg(p_i f_i) \leq D \mid i = 1, \ldots s\}\}$$

Comme D a été choisi suffisamment grand, $E(V)$ n'est pas réduit à 0 (voir Dickenstein-Fitchas-Giusti-Sessa, 1989, Proposition 1.11), et sa dimension est au plus $(D+1)^n$, lui-même majoré par $d^{O(n^2)}$. Soit $g(V)$ (ou g pour simplifier) le plus grand commun diviseur d'une base de $E(V)$: il est évidemment de degré au plus D.

Nous pouvons décrire les coefficients de f et des p_i qui interviennent dans la définition de $E(V)$ par un système d'équations linéaires, donné par

---

cru):

CROUPION. n. m. (v. 1460); de *croupe.* **1°** Extrémité postérieure du corps de l'oiseau, composée des dernières vertèbres dorsales et supportant les plumes de la queue (V. Uropygial) (**rump**). *Morceau délicat au-dessus du croupion d'une volaille.* V. Sot-l'y-laisse. (**parson's, pope's nose**). **2°** *Plaisant.* Le derrière humain. *V. Croupe.* (**rump**) **3°** *Hist.* (trad. angl.). *Le Parlement Croupion:* convoqué par Charles I[er] en 1640, dissous par Cromwell en 1653 et rappelé à deux reprises (**The Rump**).

une matrice d'ordre au plus $(D+1)^n \times (s+1)(D+1)^n$ dont les entrées sont formées des coefficients des f_i. Une base de cet espace vectoriel se calcule par un réseau arithmétique, en temps séquentiel $s^5 d^{O(n^2)}$ et parallèle $O(n^2 \log^2 sD) = O(n^4 \log^2 sd)$. Le calcul du pgcd se ramène à des des techniques d'algèbre linéaire sur k et s'effectue avec les mêmes bornes de complexité (voir Brown, 1971 et von zur Gathen, 1986).

Lemme 3.1.3 *Les variétés définies dans $\mathbf{A}^n$ par h et g coïncident.*

Quoique les polynômes h et g ne dépendent que des $r+1$ premières variables, nous les considérerons comme éléments de $k[x_1, \ldots, x_n]$ sauf mention explicite du contraire. En ce sens la tête de la variété est bien contenue dans le lieu des zéros de h et de g.

Preuve: Comme tout polynôme de E appartient à $I \cap k[x_1, \ldots, x_{r+1}]$, il s'annule évidemment sur $\pi(T(V))$. Mais le polynôme minimal h qui définit cette dernière variété dans l'espace ambiant $\mathbf{A}^{r+1}$ étant libre de carrés, il divise tous les polynômes de E, donc leur pgcd g. Ceci implique donc que $V(h)$ est contenu dans $V(g)$.

Montrons maintenant l'inclusion dans l'autre sens. Comme $\pi(Q(V))$ est une variété définissable sur k, de dimension strictement inférieure à celle de V et de degré au plus celui du croupion de V, nous en déduisons par des arguments analogues à ceux utilisés dans Heintz (1983, Proposition 3) qu'il existe des polynômes q_1 et q_2 de $k[x_1, \ldots, x_{r+1}]$, sans facteurs communs et de degré au plus $deg(Q(V))$, qui s'annulent sur $\pi(Q(V))$ donc sur $Q(V)$. Comme par ailleurs h s'annule sur la tête, hq_1 et hq_2 s'annulent sur la variété V. Maintenant le degré de chaque hq_i est majoré par $deg(V)$:

$$deg(hq_i) = deg(h) + deg(q_i) \leq deg(T(V)) + deg(Q(V)) = deg(V)$$

Appliquons à cette situation Dickenstein-Fitchas-Giusti-Sessa 1989, Remark 1.7: hq_1 et hq_2, élevés à une puissance convenable (d^n) tombent dans $E(V)$. Donc $g(V)$ divise une puissance de h, et $V(g)$ est contenue dans $V(h)$.

3.1.4 Définition: les polynômes minimaux $h_\gamma(V)$ et les polynômes calculables $g_\gamma(V)$

Il est clair d'après ce qui précède que les polynômes minimaux $h(V)$ et calculables $g(V)$ dépendent fortement des coordonnées. Afin de rendre cette dépendance plus explicite, dans le cas où la necessité de travailler avec des variables générales conduit à introduire des formes x_γ (voir 2.3.2), nous noterons $h_\gamma(V)$ le polynôme minimal défini en 3.1.1 et $g_\gamma(V)$ le polynôme calculable défini en 3.1.2 quand les coordonnées sont constituées de $x_1, \ldots, x_r, x_\gamma, x_{r+2}, \ldots, x_n$. Conformément à ce que nous avons dit dans 2.3.5, ces polynômes sont considérés comme éléments de $k[x_1, \ldots, x_n]$.

3.2 Cas projectif

Nous pourrions évidemment brutalement appliquer ce que nous avons dit dans le cas affine ci-dessus. Mais il n'est pas inintéressant de traiter à part le cas projectif dans la mesure où nous pouvons remplacer le Nullstellensatz affine effectif par sa version projective beaucoup plus facile à établir. Nous allons donc seulement en esquisser les grandes lignes.

Comme nous sommes en position normale, l'idéal $I \cap k[x_0, \ldots, x_r]$ se réduit à (0), alors que $I \cap k[x_0, \ldots, x_{r+1}]$ n'est pas trivial et définit $\pi(V)$ (voir par exemple Giusti, 1988, 2.12). De plus tous ses éléments sont divisibles par un polynôme non trivial, qui définit $\pi(T(V))$ puisque nous sommes en position générale. L'idée consiste à trouver dans $I \cap k[x_0, \ldots, x_{r+1}]$ un polynôme $p(V)$ de degré $d^{O(n)}$, en étudiant une certaine base standard.

3.2.1 Le morphisme fondamental

Nous définissons l'application ϕ_0 suivante:

$$\begin{array}{ccc} k[x_0, \ldots, x_n] & \longrightarrow & K[t, x_{r+1}, \ldots, x_n] \\ f(x_0, \ldots, x_n) & \longmapsto & f(tx_0, \ldots, tx_r, x_{r+1}, \ldots, x_n) \end{array}$$

où K est le corps $k(x_0, \ldots, x_r)$.

C'est un morphisme de k-algèbres qui conserve le caractère homogène des polynômes, et le degré. Autrement dit, il s'agit d'un morphisme d'algèbres graduées de poids 0.

Maintenant si I est un idéal homogène de $k[x_0, \ldots, x_n]$, son image par ϕ_0 n'est malheureusement plus un idéal de $K[t, x_{r+1}, \ldots, x_n]$, et ce pour une raison stupide de non-surjectivité (x_0 n'admet pas de contre-image !). Nous allons donc caractériser l'image de ϕ_0.

3.2.2 L'image du morphisme fondamental

La sous-algèbre $k[x_0, \ldots, x_r][t, x_{r+1}, \ldots, x_n]$ de $K[t, x_{r+1}, \ldots, x_n]$ constituée des éléments à coefficients dans $k[x_0, \ldots, x_r]$ admet une double graduation par le degré partiel en $t, x_{r+1}, \ldots, x_n$ et le degré partiel en $x_0, \ldots, x_r, x_{r+1}, \ldots, x_n$. L'image de ϕ_0 est évidemment composée des polynômes dont les deux degrés partiels ci-dessus sont égaux.

Qui plus est, il n'est pas difficile de voir en utilisant cette bigraduation que l'image de l'idéal I par ϕ_0 est exactement l'intersection de l'idéal J engendré par $\phi_0(I)$ et de l'image de ϕ_0.

3.2.3 La fibre générique

L'idéal J définit une variété de dimension zéro, qui n'est autre que la fibre générique de $\pi_0 |_{V(I)}$, de degré égal à celui de la tête de V. Nous pouvons alors utiliser les résultats connus sur les bases standard en dimension 0 (voir Giusti, 1989 et 1990). En choisissant un ordre total à la Bayer-Stillman sur les monômes de $K[t, x_{r+1}, \ldots, x_n]$, séparant t et x_{r+1} des autres variables, nous voyons qu'il existe dans cette base standard un polynôme en t et x_{r+1} de degré au plus $H(J)^{O(n)} Sup(deg(V(J)), H(J))$, où $H(J)$ est la régularité de la fonction de Hilbert de J. De plus, comme les variables sont normales, son monôme dominant est une puissance pure de x_{r+1}.

Proposition 3.2.4 *Il existe dans $I \cap k[x_0, \ldots, x_{r+1}]$ un polynôme p de degré majoré par une expression ne faisant intervenir que des quantités intrinsèques, au plus $d^{O(n)}$ au vu des majorations standard.*

Notons pour simplifier $\delta(J) = Sup(deg(V(J)), H(J))$. Une fois obtenu le polynôme du paragraphe précédent, le problème vient de la remontée. Mais ses coefficients, qui sont des polynômes en $x_0, \ldots, x_r$, s'obtiennent en triangulant une matrice d'ordre au plus $(H(J + (t, x_{r+1})^n \delta(J))^{O(1)}$, ce qui donne la puissance maximale de t par laquelle multiplier le dit polynôme pour tomber dans l'image de ϕ_0.

3.2.5 Corollaire: une version faible du théorème de Chistov-Grigoriev

Là encore nous nous contenterons d'esquisser l'algorithme, le résultat de complexité étant connu.

L'intérêt de la proposition ci-dessus réside en ce que la majoration du degré de $p(V)$ n'implique que des quantités intrinsèques. C'est ce qui va permettre d'itérer la construction sans aboutir à l'explosion doublement exponentielle de la complexité.

Plaçons nous dans le cas entier, et factorisons $p(V)$ sur $\mathbf{Q}$: $p = \prod_i p_i$, ce qui peut se faire polynomialement en taille et degré (algorithme de Lenstra-Lenstra-Lovascz) (répétons que nous ne voulons pas entrer dans des considérations d'extensions algébriques, et donc nous nous contenterons d'irréductibilité sur $\mathbf{Q}$). Il s'agit de réitérer la construction précédente sur $I + (p_i)$, un simple calcul de dimension séparant composantes de la tête et du croupion.

4 Décomposition équidimensionnelle

Nous sommes maintenant arrivés au point suivant: après mise en position normale, et application de 2.3.5, il existe un point γ dans un ensemble de cardinal au moins $n(deg(V))^4$ tel que les variables $x_1, \ldots, x_r, x_\gamma, x_{r+2}, \ldots, x_n$ soient en position générale par rapport à V. Pour simplifier les notations dans les raisonnements non algorithmiques qui suivent, nous poserons $x_{r+1} := x_\gamma$.

4.1 Détermination de la tête

Supposons que V ne soit pas équidimensionnelle, c'est-à dire que dans la décomposition $V = T(V) \cup Q(V)$ le croupion $Q(V)$ ne soit pas vide. Rappelons que nous avons introduit un polynôme $h = h(V)$ qui définit la projection de la tête de V. Pour récupérer la tête, une idée naturelle consiste alors à couper la décomposition tête-croupion par le lieu des zéros de h: comme h s'annule sur $T(V)$, la tête ne bouge pas, par contre comme les variables sont générales, le croupion doit être coupé proprement. C'est ce que va confirmer le lemme suivant.

Définissons donc $V' := V \cap V(h)$. D'après l'inégalité de Bézout, nous avons $deg(V') \leq deg(V)deg(h) \leq (deg(V))^2$.

Lemme 4.1.1 *La dimension de $Q(V')$ est strictement inférieure à celle de $Q(V)$.*

Preuve: Soit C' une composante de $Q(V')$. Choisissons une composante C de V tel que C' soit une composante irréductible de $C \cap V(h)$: C est nécessairement une composante du croupion, par définition de h. Nous disons que C est coupée proprement par $V(h)$, car les variables étant en position générale, $\pi(C)$ n'est pas contenue dans $\pi(T(V))$ et par conséquent h ne s'annule pas sur $\pi(C)$. Par conséquent C' a une dimension inférieure à celle de C, cqfd.

Choisissons un ensemble Γ de valeurs de k de cardinal au moins nd^{4n^2}. D'après 2.3.5, il existe alors un point γ' dedans, tel que les variables $x'_1 := x_1, \ldots, x'_r := x_r, x'_{r+1} := x_{\gamma'}, x'_{r+2} := x_{r+2}, \ldots, x'_n := x_n$ soient en position générale par rapport à V', et nous pouvons définir les polynômes $h(V')$ et $g(V')$ d'après 3.1.

Théorème 4.1.2 (algorithme de calcul de la tête et sa complexité) *Soit V une variété définie par $f_1, \ldots, f_s$, avec les notations de base 1.1, et Γ un ensemble de valeurs de k de cardinal au moins nd^{4n^2}. Pour chaque point γ de Γ, suivant 3.1.4 calculons le polynôme $g_\gamma(V)$ de $k[x_1, \ldots, x_r, x_\gamma]$. Alors $T(V)$ est défini par l'idéal $(f_1, \ldots, f_s, g_\gamma; \gamma \in \Gamma)$. La complexité séquentielle est d'ordre $s^5 d^{O(n^2)}$ et la complexité parallèle d'ordre $O(n^4 \log^2 sd)$.*

Démonstration: Comme g_γ s'annule sur la tête de V, nous obtenons une inclusion dans un sens. Pour démontrer l'inclusion dans l'autre sens, l'idée consiste à introduire une suite de variétés démarrant par V et aboutissant à $T(V)$, définie par récurrence comme suit:

Soit $V_0 = V$; il existe alors par 2.3.5 un élément γ_0 dans Γ autorisant la mise en position générale de V, et soit h_{γ_0} le polynôme minimal correspondant (3.1.1). Nous définissons par récurrence $V_i = V_{i-1} \cap V(h_{\gamma_{i-1}}(V_{i-1}))$ $(i = 1, \ldots, q)$. Ces variétés ont toutes la même tête que V (donc les degreś des polynômes $h(V_i)$ restent majorés par $deg(V)$) et les dimensions de leurs croupions forment une suite strictement décroissante d'après le lemme 4.1.1, aboutissant au croupion de V_q qui est vide. Par suite V_q est équidimensionnelle et égale à la tête de V, et q est majoré par $r(V)$. Remarquons que le degré de chaque V_i reste majoré par d^{n^2} puisque $deg(V_i) \leq deg(V_0)deg(h(V_0))\ldots deg(h(V_{i-1})) \leq (deg(V))^{q+1} \leq d^{n^2}$. En conséquence nous pouvons utiliser le même ensemble Γ de cardinal au moins nd^{4n^2} pour les mises en positions générales successives. Enfin pour chaque $i = 0, \ldots, q-1$ calculons par 3.1.4 le polynôme g_{γ_i} correspondant. Le lemme 3.1.3 implique que g_{γ_i} et h_{γ_i} définissent la même variété, et donc:

$$T(V) = V_q = V \cap V(g_{\gamma_0}) \ldots \cap V(g_{\gamma_{q-1}}) = V(f_1, \ldots, f_s, g_{\gamma_0}, \ldots, g_{\gamma_{q-1}})$$

Le degré de chaque g_γ est majoré par $D(V) = d^{O(n)}$, et nous pouvons définir la tête avec au plus $s + \mid \Gamma \mid = s + d^{O(n^2)}$ équations. Par conséquent du point de vue coût, il faut répéter $\mid \Gamma \mid = d^{O(n^2)}$ fois l'algorithme décrit dans 3.1.2, ce qui conserve le même ordre de borne que pour en calculer un seul.

4.2 Détermination des parties équidimensionnelles de dimension non maximale

Pour la détermination de la tête $T(V)$ en temps séquentiel $s^5 d^{O(n^2)}$ et parallèle $O(n^4 \log^2 sd)$ nous avons pu nous contenter des polynômes calculables $g(V)$ pour définir les projections de la tête. Ces polynômes ont un degré d'ordre $d^{O(n)}$: en itérant naïvement ce processus du calcul de la tête pour décomposer V en parties équidimensionelles, cette majoration du degré conduirait à une complexité doublement exponentielle.

En étant plus subtil, il est possible de conserver une complexité admissible et de borner par $d^{O(n^2)}$ le degré de tous les polynômes qui interviennent dans les calculs intermédiaires.

Mais pour conserver le même type de bornes, c'est-à-dire une complexité séquentielle d'ordre $s^5 d^{O(n^2)}$, parallèle $O(n^4 \log^2 sd)$ et des polynômes d'ordre $d^{O(n)}$ en degré, nous serons amenés à calculer le polynôme $h(V)$, dont le degré est majoré par la quantité intrinsèque $deg(V)$. Pour ce faire, nous demanderons donc à disposer d'une opération arithmétique additionelle (qui ne sera en fait utile que dans le cas où le corps de base k est de caractéristique positive p): l'extraction des racines $p^{ièmes}$. Nous appellerons les réseaux arithmétiques qui disposent d'une telle opération des *réseaux arithmétiques étendus.*

Lemme 4.2.1 (calcul du polynôme $h(V)$). *Le polynôme $h(V)$ se calcule à partir de $f_1, \ldots, f_s$ par un réseau arithmétique étendu avec une complexité admissible d'exposant 2.*

Reprenons la démonstration du lemme 3.1.3: g est à une constante près une puissance de h, et ce dernier est sans facteur carré.

En caractéristique nulle, comme les variables sont en position normale, le polynôme g dépend effectivement de la variable x_{r+1}, et donc $\frac{\partial g}{\partial x_{r+1}} \neq 0$. Pour récupérer le polynôme sans facteur carré h, il suffit de prendre $g/\frac{\partial g}{\partial x_{r+1}}$. Et ce calcul s'effectue avec les mêmes bornes de complexité qu'en 3.1.3.

Supposons maintenant la caractéristique p positive. Comme k est parfait et h sans carré, il existe une variable, disons x_{r+1}, qui apparait à une puissance non divisible par p dans h, et $\frac{\partial h}{\partial x_{r+1}} \neq 0$. Sans restriction de généralité on peut supposer $g = h^{p^a b}$, avec a et b entiers, et b non divisible par la caractéristique. Des inégalités $p^a \leq deg(g) \leq D = d^n(d^n + 1)$ nous déduisons que a est un $O(n \log d)$. Par ailleurs il se détermine aisément par inspection des monômes qui apparaissent dans g.

Nous commençons donc à calculer h^b à partir de g en extrayant consécutivement a fois la racine $p^{ième}$ des coefficients de g et en réduisant les monômes correspondants, puis h à partir de h^b sans problème par la formule:

$$h = \frac{h^b}{pgcd(h^b, \frac{\partial h^b}{\partial x_n})}$$

tout à fait licite puisque b non divisible par la caractéristique implique que $\frac{\partial h^b}{\partial x_n}$ est non nul.

4.2.2 Une amélioration de l'algorithme de calcul de la tête

Comme nous l'avions annoncé, voici une version du calcul de la tête qui consiste à remplacer les polynômes calculables g_γ par les polynômes minimaux h_γ.

Proposition. *Soit V une variété définie par $f_1, \ldots, f_s$, avec les notations de base 1.1, et Γ un ensemble de valeurs de k de cardinal au moins nd^{4n^2}. Pour chaque point γ de Γ, suivant 3.1.4 et 4.2.1 calculons le polynôme $h_\gamma(V)$ de $k[x_1, \ldots, x_r, x_\gamma]$. Alors $T(V)$ est défini par l'idéal $(h_\gamma; \gamma \in \Gamma)$. La complexité séquentielle est d'ordre $s^5 d^{O(n^2)}$ et la complexité parallèle d'ordre $O(n^4 \log^2 sd)$.*

Démonstration: il nous suffit de reprendre celle de 4.1.2 en utilisant le calcul des h_γ effectuée en 4.2.1. Enfin il est inutile de conserver les générateurs initiaux, en modifiant légèrement les démonstrations données dans (Heintz, 1983, Lemma 3 et Proposition 3), voir aussi 2.3.5.

4.2.3 Stratégie de calcul des composantes équidimensionnelles

Pour tout entier m $(0 \leq m \leq n)$, soient $T_m(V)$ la réunion des composantes de V de dimension m et $Q_m(V)$ la réunion des composantes de V de dimension strictement inférieure à m. Par exemple, si m est strictement supérieur à la dimension r de V, $T_m(V)$ est vide mais $Q_m(V)$ est V tout entier.

Observons que le résultat 4.2.2 nous donne un idéal définissant la tête $T_r(V)$: notons le $J_r(V)$ ou J_r s'il n'y a pas d'ambiguité. Notre but va être de fabriquer successivement des idéaux J_m définissant les composantes équidimensionnelles T_m $(r \geq m)$.

Une fois la tête calculée via l'idéal J_r, la première idée qui vient à l'esprit consiste à itérer le processus en recommençant avec l'idéal quotient $(I : J_r)$ qui définit ensemblistement le croupion. En effet, rappelons le résultat élémentaire classique qui affirme que étant donné deux idéaux I et J, l'idéal quotient $(I : J)$ définit la réunion des composantes irréductibles de $V(I)$ non contenues dans $V(J)$, qui est encore la clôture de Zariski de la différence $V(I) - V(J)$. Malheureusement, les degrés des générateurs d'un tel idéal quotient sont beaucoup trop grands a priori pour sauvegarder une complexité admissible. Il faut donc être un peu plus rusé.

4.2.4 Définition et notations utiles à la récurrence descendante

Soit W une variété définie par des polynômes $g_1, \ldots, g_t$ de degré borné par d^n. Nous allons maintenant introduire de manière un peu analogue à 3.1.2 un k-espace vectoriel $E(V, W)$ comme suit: choisissons un entier $D := d^n(2d^n + 1)$ (légèrement plus grand que celui de 3.1.2), et considérons:

$$\begin{aligned} &E(V, W) = \\ &\quad \{f \in k[x_1, \ldots, x_{r+1}] \mid \forall j\,,\ 1 \leq j \leq t\ \ \exists\, p_1{}^{(j)}, \ldots, p_s{}^{(j)} \in k[x_1, \ldots, x_n] \\ &\quad avec\ \ f g_j{}^{d^n} = \textstyle\sum_{1 \leq i \leq s} p_i{}^{(j)} f_i\ \ et\ \ Max\, \{deg(p_i{}^{(j)} f_i)\} \leq D \mid\ i = 1, \ldots, s\} \end{aligned}$$

Comme $E(V)$, cet espace vectoriel dépend en fait des générateurs f et g des idéaux $I = (f_1, \ldots, f_s)$ et $J = (g_1, \ldots, g_t)$ plutôt que des idéaux ou des variétés. Cependant, le k-espace vectoriel $E(V)$ (de dimension finie) représentait une troncature (par le degré) de l'idéal définissant une projection de V, considéré comme k-espace vectoriel de dimension infinie. Cette troncature était suffisamment haute pour que le lieu des zéros d'une base de $E(V)$ définisse effectivement cette projection. De la même manière, le k-espace vectoriel de dimension finie $E(V, W)$ consistue une troncature (par le degré) d'une sorte d'idéal quotient. Cette troncature serait-elle suffisamment haute pour définir la projection de la clôture de Zariski de la différence $V - W$, autrement dit la réunion des composantes de V non contenues dans W?

Avant de parler de projection, il nous faut d'abord étudier ce qui se passe en haut. Introduisons l'espace vectoriel auxiliaire:

$$\begin{aligned} &E'(V, W) = \\ &\quad \{f \in k[x_1, \ldots, x_n] \mid \forall j\,,\ 1 \leq j \leq t\ \ \exists\, p_1{}^{(j)}, \ldots, p_s{}^{(j)} \in k[x_1, \ldots, x_n] \\ &\quad avec\ \ f g_j{}^{d^n} = \textstyle\sum_{1 \leq i \leq s} p_i{}^{(j)} f_i\ \ et\ \ Max\, \{deg(p_i{}^{(j)} f_i)\} \leq D \mid\ i = 1, \ldots, s\} \end{aligned}$$

4.2.5 Une version locale du Nullstellensatz effectif

Cette version est due à L. Caniglia. Nous reproduisons ici son énoncé pour la commodité du lecteur (Caniglia, 1989, Corollario 2.3, et Caniglia, Guccione, Guccione, 1990, Corollary 3.1).

Lemme. *Soient f un polynôme et J un idéal de $k[x_1, \ldots, x_n]$. Supposons qu'il existe un entier $N \geq 0$ tel que $f\,J^N$ soit inclus dans $I = (f_1, \ldots, f_s)$ avec les notations de base 1.1. Pour tout g appartenant à J^{d^n}, il existe des polynômes $p_1, \ldots, p_s$ tels que:*

$$\begin{aligned} f\,g &= \sum_{i=1}^{s} p_i f_i \\ Max\{deg(p_i f_i) \mid i = 1, \ldots, s\} &\leq deg(f) + deg(g) + d^n \end{aligned}$$

Proposition 4.2.6 *Les polynômes de $E'(V, W)$ définissent la clôture de Zariski de $V - W$.*

Démonstration: Soit f un élément de $E'(V, W)$ et soit C une composante irréductible de V non contenue dans W. Nous allons démontrer que f s'annule sur C. Si ce n'était pas le cas, il existerait un ouvert de Zariski non vide U de C où f ne s'annulerait pas. Mais C n'étant pas contenue dans W, il existe un polynôme g_j $(1 \leq j \leq t)$ et un ouvert de Zariski non vide U' de C tels que g_j ne s'annule pas sur U'. Donc le produit $f{g_j}^{d^n}$ ne s'annule pas non plus sur l'ouvert non vide $U \cap U'$ de C. Ceci contredit l'hypothèse de l'appartenance de f à E'.

Réciproquement, d'après Heintz (1983, Proposition 3 and Theorem 3) la variété $\overline{V - W}$ peut être définie par $n + 1$ polynômes $f'_1, \ldots, f'_{n+1}$ de degré au plus son propre degré, majoré par le degré de V, lui-même majoré par d^n. Pour tout l $(1 \leq n + 1)$ et tout j $(1 \leq j \leq t)$, le produit $f'_l g_j$ s'annule sur V, donc appartient au radical de $(f_1, \ldots, f_s)$. En appliquant une version adaptée du Nullstellensatz effectif (voir par exemple 4.2.5 ou Fitchas-Galligo, 1988, Théorème 10), nous obtenons que $(f'_l g_j)^{d^n}$ appartient à l'idéal $(f_1, \ldots, f_s)$. Il s'ensuit qu'il existe un entier N tel que ${f'_l}^{d^n} J^N$ soit inclus dans I; nous sommes donc dans les conditions d'application de 4.2.5, pour conclure finalement que ${f'_l}^{d^n}$ appartient à E', puisque $deg({f'_l}^{d^n}) + deg({g_j}^{d^n}) + d^n$ est majoré par D.

Corollaire 4.2.7 (fabrication descendante des composantes équidimensionnelles). *Soit m un entier $(0 \leq m < r)$. Supposons que pour tout entier $l = r, r-1, \ldots, m+1$ nous ayons construit des idéaux $J_l = (h_1^{(l)}, \ldots, h_{t_l}^{(l)})$ (définissant comme précisé en 4.2.3 $T_l(V)$), dont les générateurs sont de degré majoré par $degT_l$.*

Supposons de plus que nous ayons aussi construit un sous-ensemble K_{m+1} de $\{h_{j_r}^{(r)} \dots h_{j_{m+1}}^{(m+1)} \mid 1 \leq j_r \leq t_r, \dots, 1 \leq j_{m+1} \leq t_{m+1}\}$ de cardinal $d^{O(n^2)}$ dont les éléments engendrent l'idéal $J_r \dots J_{m+1}$.

Alors il existe un réseau arithmétique étendu qui construit en temps séquentiel $s^5 d^{O(n^2)}$ et parallèle $O(n^4 \log^2 sd)$ un idéal $J_m = (h_1^{(m)}, \dots, h_{t_m}^{(m)})$, définissant $T_m(V)$, engendré par des polynômes en nombre $t_m = d^{O(n^2)}$ et de degré majoré par $degT_m(V)$.

De plus le réseau construit un sous-ensemble K_m de $\{h_{j_r}^{(r)} \dots h_{j_m}^{(m)} \mid 1 \leq j_r \leq t_r, \dots, 1 \leq j_m \leq t_m\}$ de cardinal $d^{O(n^2)}$ dont les éléments engendrent l'idéal $J_r \dots J_m$.

Esquisse de la démonstration: Reprenons les notations de 4.2.4 et appliquons la proposition 4.2.6 à la variété W définie par l'ensemble K_{m+1}, puisque les polynômes constituant celui-ci sont de degré au plus $degT_r + \dots + degT_{m+1} \leq degV \leq d^n$. Les polynômes contenus dans $E'(V, W)$ définissent bien $Q_{m+1}(V)$.

Il va nous suffire maintenant de généraliser *mutatis mutandis* les sections de 2.3.1 à 2.3.5 , 3.1, 4.1.2 et 4.2.2. L'idée consiste à ne faire que des opérations d'algèbre linéaire sur $E'(V, W)$, ce qui conserve une complexité séquentielle d'ordre $s^5 d^{O(n^2)}$ et parallèle d'ordre $O(n^4 \log^2 sd)$ des algorithmes.

C'est ainsi que nous pouvons modifier l'algorithme 1.15 de Dickenstein-Fitchas-Giusti-Sessa (1989) pour obtenir en temps séquentiel $s^5 d^{O(n^2)}$ et parallèle $O(n^4 \log^2 sd)$ des variables en position normale par rapport à $Q_{m+1}(V)$. L'algorithme détermine aussi sa dimension r', si bien que nous pouvons supposer sans restriction de généralité que les variables $x_1, \dots, x_n$ sont en position normale par rapport à $Q_{m+1}(V)$.

Le reste, mise en position générale, projection et détermination de la tête de Q_{m+1} se déroule sans problèmes. Le seul point nouveau consiste en la fabrication de l'ensemble K_m.

Théorème 4.2.8 (décomposition équidimensionnelle et sa complexité). *Soit V une variété affine définie avec les notations de base 1.1. Alors le réseau arithmétique étendu décrit ci-dessus calcule pour chaque entier m $(0 \leq m \leq n)$ la réunion $T_m(V)$ des composantes de V de même dimension m, c'est-à-dire des polynômes $h_1^{(m)}, \dots, h_{t_m}^{(m)}$ en nombre $t_m = d^{O(n^2)}$, de degré majoré par $degT_m(V) \leq d^n$ et tels que leur lieu des zéros soit $T_m(V)$.*

La complexité du réseau est en temps séquentiel $s^5 d^{O(n^2)}$ et parallèle $O(n^4 \log^2 sd)$.

Si nous nous limitons aux réseaux arithmétiques non étendus, nous pouvons obtenir en modifiant de façon ad hoc ce qui précède un algorithme de décomposition équidimensionnelle de complexité légèrement supérieure mais qui reste néanmoins admissible:

Remarque 4.2.9 *Soit V une variété affine définie avec les notations de base 1.1. Alors il existe un réseau arithmétique (non étendu) qui calcule pour chaque entier m $(0 \leq m \leq n)$ la réunion $T_m(V)$ des composantes de V de même dimension m, c'est-à-dire des polynômes $h_1^{(m)}, \ldots, h_{t_m}^{(m)}$ en nombre $t_m = d^{O(n^3)}$, de degré d'ordre $d^{O(n^2)}$ et tels que leur lieu des zéros soit $T_m(V)$. La complexité du réseau est en temps séquentiel $s^5 d^{O(n^3)}$ et parallèle $O(n^6 \log^2 sd)$.*

5 Appendice: application au calcul de la forme de Chow et du degré

Nous allons montrer que la forme de Chow d'une variété équidimensionnelle se calcule par un algorithme parallélisable de complexité admissible. D'après ce qui précède, ce résultat s'étendra donc à une variété arbitraire. Comme corollaire, le degré s'obtient de la même manière. Puis nous donnerons une meilleure méthode, plus directe, pour obtenir ce dernier invariant.

5.1 Rappel de la notion de forme de Chow

Dans tout ce qui suit, nous identifierons un point du dual $\check{\mathbf{P}}^n$ de l'espace projectif avec l'hyperplan lieu des zéros de la forme linéaire qu'il définit.
Soit V une sous-variété équidimensionnelle, fermée et de dimension r de l'espace projectif $\mathbf{P}^n$. Considérons le sous-ensemble fermé Ω de $(\check{\mathbf{P}}^n)^{r+1} \times V$ défini par:

$$\Omega = \{(y^{(0)}, \ldots, y^{(r)}, x) \in (\check{\mathbf{P}}^n)^{r+1} \times V \mid x \in y^{(j)}\ 0 \leq j \leq r\}$$

Soit π la projection canonique $(\check{\mathbf{P}}^n)^{r+1} \times V \longrightarrow (\check{\mathbf{P}}^n)^{r+1}$. Alors $\pi(\Omega)$ est une hypersurface de $(\check{\mathbf{P}}^n)^{r+1}$ dont le polynôme minimal F_V est appelé la *forme de Chow* de V (voir par exemple comme référence Shafarevitch (1972) ou Nesterenko (1977). Elle possède les deux propriétés suivantes:

(i) $deg(F_V) = deg(V)$

(ii) $V = \bigcap_{j=0}^{r} \{y^{(j)} \mid F_V(y^{(0)}, \ldots, y^{(r)}) = 0\}$

Si V est une sous-variété fermée arbitraire de l'espace projectif, la forme de Chow F_V est définie comme le produit des formes de Chow de toutes les composantes équidimensionnelles de V:

$$F_V = \prod_{j=0}^{r(V)} \{F_{T_j(V)} \mid T_j(V) \neq \emptyset\}$$

Ces rappels effectués, nous remercions T. Krick de nous avoir communiqué l'application suivante de l'algorithme de complexité admissible de décomposition équidimensionnelle:

Théorème 5.2 (Krick, 1990) *Soit V une variété projective définie par des polynômes homogènes $f_1, \ldots, f_s$ de $k[x_0, \ldots, x_n]$, avec les notations de base 1.1. Alors la forme de Chow F_V est calculable par un réseau arithmétique étendu de complexité admissible.*

Esquisse de la démonstration: en utilisant la version projective du théorème 4.2.8, nous nous ramenons d'abord au cas où V est équidimensionnelle de dimension r.

Soient $y_0^{(0)}, \ldots, y_n^{(0)}, \ldots, y_0^{(r)}, \ldots, y_n^{(r)}$ des nouvelles indéterminées et considérons la forme de Chow F_V, que nous noterons désormais F pour simplifier, comme un polynôme de $k[y_l^{(j)} \ ; \ 0 \leq j \leq r \ , \ 0 \leq l \leq n]$. Puisque k est parfait, F est sans facteur carré. Pour tout indice j $(0 \leq j \leq r)$ soit $L^{(j)}$ la forme linéaire en $x_0, \ldots, x_n$, définie par $L^{(j)}(x_0, \ldots, x_n) = y_0^{(j)}x_0 + \cdots + y_n^{(j)}x_n$, et W l'hypersurface $\{w \in \mathbf{A}^{(n+1)(r+1)} \mid F(w) = 0\}$. En tenant compte de la propriété (ii) des formes de Chow, nous voyons que l'ensemble W est définissable par une formule élémentaire Φ du langage des corps algébriquement clos contenant k, et est de la forme:

$$
\begin{aligned}
(\exists x_0)\ (\exists x_n)\ (f_1(x_0, \ldots, x_n) = 0) \wedge \ldots \wedge (f_s(x_0, \ldots, x_n) = 0) \wedge \\
(L^{(0)}(y_0^{(0)}, \ldots, y_n^{(0)}, x_0, \ldots, x_n) = 0) \wedge \ldots \wedge \\
(L^{(r)}(y_0^{(r)}, \ldots, y_n^{(r)}, x_0, \ldots, x_n) = 0)
\end{aligned}
$$

et contient $(n+1)(r+2)$ variables, dont $y_0^{(0)}, \ldots, y_n^{(0)}, \ldots, y_0^{(r)}, \ldots, y_n^{(r)}$ sont libres et $x_0, \ldots, x_n$ liées, et $s+r+1$ polynômes de degré au plus d et un seul bloc de quantificateurs. Appliquons maintenant à Φ la procédure efficace d'élimination des quantificateurs décrite dans Fitchas-Galligo-Morgenstern (1987, 1989) ou dans Krick (1990). En temps admissible nous obtenons une formule équivalente Ψ sans quantificateurs qui est une disjonction de conjonctions où apparaissent des polynômes $G_1, \ldots, G_Q$ de $k[y_l^{(j)} \mid 0 \leq j \leq r,\ 0 \leq l \leq n]$ qui satisfont la borne suivante:

$$\sum_{q=1}^{Q} deg(G_q) = (sd)^{n^{O(1)}}$$

Sans restriction de généralité, nous pouvons supposer que Ψ est une disjonction de $M = (sd)^{n^{O(1)}}$ conjonctions Ψ_m de la forme:

$$(G_{q_1} = 0) \wedge \ldots \wedge (G_{q_m} = 0) \wedge (G_{q_m+1} \neq 0)$$

qui définit un sous-ensemble localement fermé non vide W_m de $\mathbf{A}^{(n+1)(r+1)}$. Nous pouvons déterminer la dimension de chaque W_m $(1 \leq m \leq M)$ (voir Caniglia-Galligo-Heintz (AAECC 6), 1989, Theorem 19 ou Dickenstein-Fitchas-Giusti-Sessa, 1989, Corollary 1.9.1).

Notons $N := (n+1)(r+1)$ et $S := \{m \in \mathbf{N} \mid 1 \leq m \leq M,\ dim(W_m) = N-1\}$. Ce dernier ensemble n'est pas vide parce que $W = \bigcup m = 1^M W_m$ est une hypersurface de $\mathbf{A}^N$. Considérons un de ses éléments m, et la conjonction Ψ_m qui peut être supposée sans restriction de généralité de la forme $(G_q = 0) \wedge \ldots \wedge (G_q = 0) \wedge (G_{q+1} \neq 0)$. Puisque l'ensemble W_m défini par Ψ_m a la dimension $r(W_m) = N-1$ et comme W_m est contenue dans W nous voyons que l'entier q est strictement positif et qu'il existe un facteur premier de F qui divise $G_1, \ldots, G_q$ mais pas G_{q+1}.

Soit H_m le polynôme sans facteur carré associé au pgcd de $G_1, \ldots, G_q$; d'après 4.2.1, il est possible de le calculer par un réseau arithmétique étendu en temps admissible. Nous pouvons avec la même complexité calculer le polynôme $P_m := H_m/pgcd(H_m, G_{q+1})$ et P le polynôme sans facteur carré associé à $\prod_{m \in S} P_m$.

Il suffit pour terminer la démonstration de prouver que P et F coïncident. Soit R un polynôme irréductible qui divise F dans $k[y_l^{(j)} \mid 0 \leq j \leq r,\ 0 \leq l \leq n]$. Comme l'hypersurface $V(R) = \{w \in \mathbf{A}^{(n+1)(r+1)} \mid R(w) = 0\}$ est contenue dans $W = V(F)$, il existe un entier m $(1 \leq m \leq M)$ tel que la dimension de $W_m \cap V(R)$ est $N-1$, ce qui implique que m appartient à S et que R divise P_m: par suite R divise aussi P. Comme R était un facteur irréductible arbitraire de F, lui-même sans facteur carré, nous en déduisons que F divise P.

Démontrons maintenant que P divise F. Soit R un facteur irréductible de P. Choisissons un entier m dans S tel que R divise P_m; nous pouvons supposer sans restriction de généralité que Ψ_m est de la forme $(G_1 = 0) \wedge \ldots \wedge (G_q = 0) \wedge (G_{q+1} \neq 0)$. Alors R divise $G_1, \ldots, G_q$ mais pas G_{q+1}, ce qui implique que $V(R)$ est contenu dans la clôture de Zariski de W_m qui est un sous-ensemble de $W = V(P)$: R divise donc F. De la même manière qu'auparavant nous concluons donc que P divise F, c.q.f.d.

5.3 Calcul du degré d'une variété en temps admissible

Le théorème précédent implique que nous pouvons calculer le degré d'une variété projective en temps admissible. En utilisant le fait que la clôture projective d'une variété affine s'obtient en temps admissible (voir Caniglia-Galligo-Heintz (AAECC 7), 1989, Theorem 2.10), nous en déduisons le même résultat algorithmique pour les variétés affines. Ceci généralise Caniglia-Galligo-Heintz (AAECC 6), 1989, Theorem 19, (iii) où un algorithme de complexité admissible était annoncé. En fait, par une méthode plus directe nous allons produire un résultat plus précis:

Proposition 5.3.1 *Le calcul du degré d'une variété affine de V de $\mathbf{A}^n$, définie par des polynômes $f_1, \ldots, f_s$ conformément aux notations de base 1.1, peut s'effectuer par un réseau arithmétique étendu avec une complexité séquentielle en $s^5 d^{O(n^3)}$ et parallèle en $O(n^6 \log^2 sd)$.*

Démonstration: en calculant une décomposition équidimensionnelle de V au moyen du théorème 4.2.8, nous pouvons nous ramener au cas où V est une variété équidimensionnelle de dimension connue, disons r, et définie par $t = d^{O(n^2)}$ polynômes $h_1, \ldots, h_t$ de $k[x_1, \ldots, x_n]$ de degré majoré par d^n.

Introduisons de nouvelles indéterminées ${y_1}^{(1)}, \ldots, {y_n}^{(1)}, \ldots, {y_1}^{(r)}, \ldots, {y_n}^{(r)}$, et $y_1, \ldots, y_n$, en nombre $(r+1)n$. Notons A (respectivement K) l'extension $k[{y_l}^{(j)}, y_j \ ; \ 1 \leq j \leq r, \ 1 \leq l \leq n]$ (respectivement l'extension $k({y_l}^{(j)}, y_j \ ; \ 1 \leq j \leq r, \ 1 \leq l \leq n))$. Pour tout j $(1 \leq j \leq r)$, définissons la forme linéaire $l^{(j)}$ de $A[x_1, \ldots, x_n]$ comme suit: $l^{(j)}(x_1, \ldots, x_n) := y_j + \sum_{l=1}^{n} {y_l}^{(j)} x_l$. L'idéal $J := (h_1, \ldots, h_t, l^{(1)}, \ldots, l^{(r)})$ de $K[x_1, \ldots, x_n]$ définit une variété de dimension zéro.

Fixons un ordre total admissible sur les monômes de $K[x_1, \ldots, x_n]$, et en utilisant un réseau arithmétique sur A, calculons alors en temps séquentiel $s^5 d^{O(n^3)}$ et parallèle $O(n^6 \log^2 sd)$ l'escalier relativement à cet ordre du radical $rad(J)$ de J (voir Krick-Logar, 1990 et Dickenstein-Fitchas-Giusti-Sessa, 1989 pour détails). Sur l'escalier ainsi obtenu nous lisons la dimension du K-espace vectoriel $K[x_1, \ldots, x_n]/rad(J)$ qui n'est autre que $degV$.

Reste à voir quelle est la complexité d'un réseau arithmétique sur le corps de base k qui exécute les opérations arithmétiques sur A nécessaires au calcul de l'escalier du radical de J. En fait, pour obtenir ce dernier, nous n'avons qu'à tester s'il existe des polynômes dans $rad(J)$, de degré borné par d^n et contenant certains monômes. Pour cela, nous utilisons seulement des éléments de A qui comme polynômes en les $(r+1)n$ variables ${y_1}^{(1)}, \ldots, {y_n}^{(1)}, \ldots, {y_1}^{(r)}, \ldots, {y_n}^{(r)}$, et $y_1, \ldots, y_n$, ont un degré majoré par d^{n^2}. Il nous faut tester la nullité ou non de ces polynômes, donnés par nos calculs dans A. D'après Heintz-Schnorr (1980), cela est possible par des évaluations de ces polynômes en $s^5 d^{O(n^3)}$ points choisis à propos dans $k^{(r+1)n}$. Ces évaluations peuvent être effectuées par un réseau arithmétique sur k en en temps séquentiel $s^5 d^{O(n^3)}$ et parallèle $O(n^6 \log^2 sd)$.

REFERENCES

[1] D. Bayer, M. Stillman, *A theorem on refining division orders by the reverse lexicographic order*, Lecture Notes for the meeting on Algebraic Geometry and Computing, 1985, Trento, Italy.

[2] S. J. Berkowitz, *On computing the determinant in small parallel time using a small number of processors*, Information Processing Letters **18** (1984), 147–150.

[3] W. S. Brown, *On Euclid's algorithm and the computation of polynomial greatest common divisors*, J. ACM **18** (1971), 478–504.

[4] D. Brownawell, *Bounds for the degree in the Nullstellensatz*, Ann. Math. **126** (1987), 577–591.

[5] L. Caniglia, *Complejidad de algoritmos en geometria computational*, Thèse, Universidad de Buenos Aires 1989.

[6] L. Caniglia, *How to compute the Chow form of an unmixed polynomial ideal in simple exponential time*, (submitted), Applicable Algebra in Engeneering Communication and Computer Science (1989).

[7] L. Caniglia, A. Galligo, J. Heintz, *Borne simple exponentielle pour les degrés dans le théorème des zéros sur un corps de caractéristique quelconque*, C. R. A. S. Paris **307** (1988), 255–258.

[8] L. Caniglia, A. Galligo, J. Heintz, *Some new effectivity bounds in computational geometry,*, in "Proc. AAECC 6," Springer LNCS **357**, 1989, pp. 131–151.

[9] L. Caniglia, A. Galligo, J. Heintz, *Equations for the projective closure of an affine algebraic variety*, Discrete Appl. Math. Proc. AAECC-7, Toulouse (1989). (to appear)

[10] L. Caniglia, J. A. Guccione, J. J. Guccione, *Local membership problems for polynomial ideals,*, in "Proc. MEGA 90," 1990.

[11] A. L. Chistov, D. Yu. Grigoriev, *Subexponential-time solving systems of algebraic equations I, II*, Steklov Mathematical Institute, Lenigrad department, LOMI Preprints E-9-83, 0E-10-c83 (1983).

[12] A. Dickenstein, N. Fitchas, M. Giusti, C. Sessa, *The membership problem for unmixed polynomial ideals is solvable in subexponential time*, Discrete Appl. Math. Proc. AAECC-7, Toulouse (1989). (to appear)

[13] N. Fitchas, A. Galligo, *Nullstellensatz effectif et conjecture de Serre (Théorème de Quillen-Suslin) pour le calcul formel*, Math. Nachrichten (1988). (à paraître)

[14] Noaï Fitchas, A. Galligo, J. Morgenstern, *Algorithmes rapides en séquentiel et parallèle pour l'élimination des quantificateurs en géométrie élémentaire*, in "Séminaire Structures Algébriques Ordonnées 1986–87," Université Paris VII, 1987. (à paraître)

[15] Noaï Fitchas, A. Galligo, J. Morgenstern, *Precise sequential and*

parallel complexity bounds for quantifier elimination over algebraically closed fields, Journal of Pure and Applied Algebra (1987). (to appear)

[16] J. Von zur Gathen, *Parallel arithmetic computations: a survey,*, in "Proc. 13th Symp. MFCS 1986," Springer Lecture Notes in Computer Science **233**, 1986, pp. 93–112.

[17] P. Gianni, B. Trager, G. Zacharias, *Gröbner bases and primary decomposition of polynomial ideals*, J. Symbolic Computation **6** Computational aspects of commutative algebra (1988), 249–265.

[18] M. Giusti, *Combinatorial Dimension Theory of Algebraic Varieties*, J. Symbolic Computation **6** Computational aspects of commutative algebra (1988), 249–265.

[19] M. Giusti, *Complexity of standard bases in projective dimension zero*, in "Proceedings of EUROCAL 87," (European Conference on Computer Algebra, Leipzig, RDA), Lecture Notes in Computer Science **378**, Springer Verlag, 1989, pp. 333–335.

[20] M. Giusti, *Complexity of standard bases in projective dimension zero II*, in "Proceedings of AAECC," Tokyo, 1990. (to appear)

[21] J. Heintz, *Definability and fast quantifier elimination over algebraically closed fields,*, Theoretical Computer Science **24** (1985), 239–277. Russian translation in Kyberneticeskij Sbornik, Novaja Serija, Mir Moscow **22**, pp. 113–158

[22] J. Heintz, C.P. Schnorr, *Testing polynomials which are easy to compute*, in "Proc. 12th Annual Symposium ACM on computing," 1980, pp. 262–272. also in: "Logic and Algorithmic. An international Symposium held in honour of Ernst Specker" Monographie **30** de l'Enseignement Mathématique, Genève 1982, pp. 237–254

[23] G. Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polinomideale*, Math. Ann. **95** (1926), 736–788.

[24] P. Hintenhaus, *Decomposing and Parameterizing the Solution Set of an Algebraic System*, Ph. D. Thesis, preprint RISC-Linz **89-27**.

[25] T. Krick, *Complejidad para problemas de geometriá elemental*, Thèse, Universidad de Buenos Aires 1990.

[26] T. Krick, A. Logar, *Membership problems, representation problems and the computation of the radical for one-dimensional ideals*, in "Proceedings MEGA-90," (these proceedings), 1990.

[27] T. Krick, P. Solernó, *Calcul effectif du polynôme de Chow d'un idéal homogène ensemblistement équidimensionnel*, Prépublication, Buenos Aires 1989.

[28] D. Lazard, *Algèbre linéaire sur $K[x_1, \ldots, x_n]$ et élimination*, Bull. Soc. Math. France **105** (1977), 165–190.

[29] A. Logar, *A computational proof of the Noether normalization lemma*, in "Proc. AAECC 6," (Roma), Springer LNCS **357**, 1988, pp. 259–273.

[30] Y. V. Nesterenko, *Estimates for the order of zeroes of functions of a cerain class and applications in the theory of transcendantal numbers*,

Izvestija Akad. Nauk. SSR **41** (1977). Translation in: Math. USSR Izvestija **11**

[31] P. Robert, "Dictionnaire alphabétique et analogique de la langue française,," Société du nouveau Littré, Paris, 1970.

[32] A. Seidenberg, *Constructions in algebra*, Trans. Amer. Math. Soc. **197** (1974), 273–313.

[33] I. R. Shafarevich, *Basic Algebraic Geometry*, Nauka, Moscow. English version: Springer, Berlin 1974

[34] B. Teissier, *Résultats récents d'algèbre commutative effective*, in "Séminaire Bourbaki," $42^{ième}$ année, **718**, 1989.

Marc Giusti
SDI CNRS 6176 "Calcul formel, Algèbre et Géométrie algorithmiques"
(associé au Centre de Mathématiques, URA CNRS D.0169)
Laboratoire d'Informatique
Ecole Polytechnique, 91128 Palaiseau Cedex, France
giusti@cmep.polytechnique.fr
cfmagi@frpoly11.BITNET

Joos Heintz
Groupe de travail Noaï Fitchas
Instituto Argentino de Matemática (CONICET)
Viamonte 1636, (1055) Buenos Aires, Argentina
atina!mate!nfitchasuunet.uu.net
nfitchasmate.edu.ar
atina!dcfcen!mate!nfitchas