Bases standard, élimination et complexité

Marc Giusti
Laboratoire GAGE
GDR de Calcul Formel MEDICIS
&
Centre de Mathématiques
École Polytechnique
giusti@medicis.polytechnique.fr

12 mai 1997

Table des matières

"The purpose of computing is insight, not numbers."

Richard W. HAMMING, *Numerical Methods for Scientists and Engineers*, McGraw-Hill, New-York (1962), p. v.

"The purpose of computing is insight, not formulas."

in *Future Directions for Research in Symbolic Computation*, SIAM Reports on Issues in the Mathematical Sciences, Philadelphia (1990), p. 29.

Étant donné un système d'équations linéaires homogènes à $n+1$ variables, les formules de Cramer permettent de paramétrer les solutions en fonction d'un certain nombre de variables que l'on peut choisir arbitrairement.

Nous nous proposons d'établir un résultat analogue pour des systèmes d'équations non linéaires : il s'agit du lemme de normalisation de Noether. Nous allons nous poser à son sujet des questions d'algorithmique et de complexité. Tout ce qui suit provient essentiellement des deux articles [Giusti, 1988], [Giusti-Heintz, 1993].

Première partie

Le lemme de normalisation de Noether

1 La situation linéaire

Soient $f_1, \dots, f_s$ des formes linéaires homogènes à $n+1$ variables $x_0, \dots, x_n$, à coefficients dans un corps k :

$$f_i(x_0, \dots, x_n) = \sum_{j=0}^{n} f_{ij} x_j \quad i = 1, \dots, s.$$

1.1 Point de vue de l'algèbre

Si la $s \times (n+1)$ matrice F qui leur est associée est de rang $n-r$, il existe un sous-mineur M non nul d'ordre $n-r$. Après changement de variables (en fait une renumérotation), nous pouvons supposer qu'il est bâti sur les dernières colonnes $r+1, \dots, n$, et après une autre renumérotation des indices des formes, que ce sont les $n-r$ premières qui sont linéairement indépendantes. Soient M_j $(j = r+1, \dots, n)$ les mineurs obtenus en substituant à la colonne j de M la colonne formée par les $-\sum_{j=0}^{r} f_{ij} x_j$ $(i = 1, \dots, n-r)$. Ce sont des formes linéaires homogènes en $x_0, \dots, x_r$. Les solutions du système linéaire homogène associé se paramètrent alors par les formules de Cramer :

$$M x_j = M_j(x_0, \dots, x_r) \quad j = r+1, \dots, n$$

qui donnent les $n-r$ dernières coordonnées (variables *liées*) en fonction des $r+1$ premières arbitrairement choisies (variables *libres*). L'espace vectoriel des solutions devient ainsi le graphe d'une application linéaire $k^{r+1} \to k^{n-r}$.

1.2 Point de vue de la géométrie

Rappelons que l'*espace projectif* $\mathbf{P}_k^n$ (ou plus simplement $\mathbf{P}^n$) est l'ensemble des classes d'équivalence des $(n+1)$-uples $(a_0, \ldots, a_n)$ d'éléments de k, non tous nuls, pour la relation d'équivalence identifiant les points d'une même droite de k^{n+1} passant par l'origine. Nous appellerons encore les éléments de $\mathbf{P}^n$ des *points*.

Une *sous-variété linéaire* de $\mathbf{P}^n$ est définie par un système d'équations linéaires homogènes. Si le rang de ce dernier est $n-r$, sa *dimension* est par définition r.

Soient L_{i+1} et B^i deux sous-variétés linéaires de $\mathbf{P}^n$, respectivement de codimension $i+1$ et de dimension i, qui ne se coupent pas. A tout point qui n'est pas dans L_{i+1}, on peut successivement associer la sous-variété linéaire de codimension i qu'il engendre avec L_{i+1}, puis l'unique point d'intersection de cette dernière avec la sous-variété B^i. L'application ainsi définie est *la projection linéaire* de centre L_{i+1} sur B^i.

L'interprétation géométrique des formules de Cramer est alors la suivante : si le rang est $n-r$, nous pouvons partitionner l'ensemble des variables en deux paquets, après renumérotation $x_0, \ldots, x_r$ (variables libres) et $x_{r+1}, \ldots, x_n$ (variables liées). Définissons les deux sous-variétés linéaires L_{r+1} d'équations $x_0 = \cdots = x_r = 0$ et B^r d'équations $x_{r+1} = \cdots = x_n = 0$. La sous-variété linéaire d'équations $f_1 = \cdots = f_s = 0$ ne coupe pas L_{r+1}, et la projection de centre L_{r+1} l'envoie surjectivement sur B^r.

1.3 Point de vue de l'algorithmique

Supposons maintenant que nous voulions faire effectuer à une machine le paramétrage ci-dessus. Il faut déjà avoir à faire à un corps *effectif*, c'est-à-dire un corps représentable en machine dont les quatre opérations arithmétiques $+, -, *, /$ sont réalisables par des algorithmes, sans oublier le test d'égalité. Par exemple, nous apprenons tous à l'école primaire comment représenter les entiers par leur écriture décimale, et des algorithmes d'addition, soustraction, multiplication et division (réfléchissons un peu au cas de cette dernière ...) ; quant au test d'égalité, il se révèle trivial sur cette écriture unique. Après extensions, le corps des rationnels devient ainsi le premier exemple de corps effectif. Il est néanmoins relativement aisé de rencontrer en calcul formel des corps non effectifs: cf [Richardson].

À partir de la matrice F, l'algorithme du pivot de Gauss permet d'exhiber un mineur non nul de taille maximale, avec un nombre d'opérations arithmétiques polynomial en s, n.

2 La situation générale

Soient $f_1, \ldots, f_s$ des formes homogènes à $n+1$ variables $x_0, \ldots, x_n$, de degrés $d_1, \ldots, d_s$, à coefficients dans un corps k :

$$f_i(x_0, \ldots, x_n) = \sum_{|a|=d_i} f_{ia} x_0^{a_0} \ldots x_n^{a_n} \quad i = 1, \ldots, s$$

où $a = (a_0, \ldots, a_n)$ est un élément de $\mathbf{N}^{n+1}$ de degré $|a| = a_0 + \cdots + a_n$.

2.1 Point de vue de l'algèbre

L'anneau $R = k[x_0, \ldots, x_n]$ peut être muni d'une structure d'anneau gradué par la décomposition canonique $R = \bigoplus_{s \geq 0} R_s$ où R_s est l'ensemble des polynômes homogènes de degré s. L'idéal I de R engendré par les formes $f_1, \ldots, f_s$ est *homogène* et respecte la graduation puisque $I = \bigoplus_{s \geq 0} I \cap R_s$.

Version algébrique du lemme de normalisation de Noether: *Après changement linéaire de variables, que nous noterons encore $x_0, \ldots, x_n$, il existe un indice r tel que la composée :*

$$0 \to k[x_0, \ldots, x_r] \to k[x_0, \ldots, x_n] \to k[x_0, \ldots, x_n]/I \to 0$$

de l'injection et de la surjection canoniques soit encore injective et réalise une extension entière d'anneaux.

Dit autrement, nous pouvons après changement de variables partitionner ce dernières en deux paquets : les $r+1$ premières seront dites *libres* et les $n-r$ dernières *liées*, telles que :

- il n'existe pas dans l'idéal I de polynôme ne dépendant que des variables libres ;
- il existe des polynômes $p_{r+1}, \ldots, p_n$ de $k[x_0, \ldots, x_r][t]$, unitaires en t, tels que $p_{r+1}(x_0, \ldots, x_r)(x_{r+1}), \ldots, p_n(x_0, \ldots, x_r)(x_n)$ appartiennent à l'idéal I (relations de dépendance intégrale).

2.2 Point de vue de la géométrie

Étant donné une extension K de k, un zéro dans $\mathbf{P}^n_K$ d'un polynôme homogène est un point qui l'annule, et cette notion est bien définie. Dorénavant nous supposerons quand nous parlerons de géométrie que l'extension est suffisamment grosse ; pour simplifier définitivement que k est algébriquement clos et nous noterons le projectif $\mathbf{P}^n$.

L'ensemble des zéros de l'idéal homogène I est l'ensemble des zéros des éléments homogènes de I, ou ce qui revient au même, l'ensemble des zéros des générateurs de I :

$$Z(I) = \{a \in \mathbf{P}^n \mid f(a) = 0 \ \ \forall f \in I\}.$$

Un sous-ensemble de $\mathbf{P}^n$ est *algébrique* s'il existe un idéal homogène tel qu'il en soit l'ensemble des zéros. L'intersection de toute famille d'ensembles algébriques $Z(I_\alpha)$ est encore algébrique, puisque c'est $Z(\sum_\alpha I_\alpha)$. On dit que deux ensembles algébriques s'évitent (resp. se coupent) si leur intersection est vide (resp. n'est pas vide). Les sous-variétés linéaires définies ci-dessus sont les premiers exemples d'ensembles algébriques.

La version algébrique implique alors :

Version géométrique du lemme de normalisation de Noether : *Il existe deux sous-variétés linéaires L_{r+1} de codimension $r+1$ et B^r de dimension r telles que :*

- *les deux ensembles $Z(I)$ et L_{r+1} ne se coupent pas ;*
- *la restriction à $Z(I)$ de la projection π de centre L_{r+1} et de base B^r est surjective et finie, c'est-à-dire que pour tout point b de B^r, la fibre $\pi^{-1}(b)$ est constitué d'un nombre fini non nul de points.*

En fait cette assertion même affaiblie par la suppression de l'hypothèse de finitude implique en retour la version algébrique.

2.3 Point de vue de l'algorithmique

Afin d'exhiber un algorithme qui rend à partir d'un système de générateurs de l'idéal I les objets promis par le lemme de normalisation, il faut d'abord étendre à l'algèbre de polynômes $R = k[x_0, \ldots, x_n]$ l'effectivité des opérations possibles et le test d'égalité, ce qui s'effectue sans difficulté particulière en développant sur la base des monômes.

Les ennuis commencent avec la structure quotient : la question de l'effectivité de l'anneau quotient bute sur le test de nullité. Si additionner ou multiplier des classes se résoud immédiatement par la pensée, ce n'est plus le cas pour le problème de l'appartenance à un idéal.

Le but du premier chapitre est d'y répondre ; les outils introduits seront même assez puissants pour résoudre totalement la question de l'effectivisation du lemme.

Deuxième partie

Du côté de l'écriture

Passons en revue quelques cas particuliers du problème d'appartenance à un idéal. Dans le cas principal des idéaux (non nécessairement homogènes) de $k[x]$, le vénérable algorithme d'Euclide exhibe un plus grand commun diviseur de la famille, et la question de l'appartenance se réduit au test de nullité du reste de la division par ce PGCD.

L'algèbre linéaire nous permet de conclure quand le degré des générateurs (toujours non nécessairement homogènes) est au plus 1.

Dans les deux cas, observons que nous avons implicitement considéré que les polynômes étaient représentés par leur *écriture* sur la base des monômes, introduit un *ordre total* sur les monômes et fabriqué des règles de *réécriture*, que nous avons appliquées à un polynôme candidat à l'appartenance : et celle-ci est réalisée si et seulement si le processus de réécriture aboutit au polynôme nul, qui est facile à reconnaître ... avec cette représentation.

Précisons les choses. Dans le premier cas, un polynôme est représenté par le vecteur de ses coefficients, les monômes sont rangés par ordre décroissant. Nous considérons tout polynôme non nul de l'idéal, de degré d, écrit (congru à) $x^d - r$, où r est de degré strictement inférieur à d. Diviser par ce polynôme n'est pas autre chose qu'appliquer récursivement et autant de fois qu'il est possible aux monômes du dividende la règle de réécriture $x^d \to r$. Le processus s'arrête sur le reste de la division euclidienne.

Dans le deuxième cas, un polynôme est toujours représenté par le vecteur de ses coefficients. S'il existe parmi les données une constante non nulle, l'idéal est trivial. Sinon, nous considérons un générateur de l'idéal, de degré au plus 1 mais non constant, après renumérotation des variables écrit (congru à) $x_n - l(x_1, \ldots, x_{n-1})$. L'application répétée de la règle de réécriture $x_n \to l$ permet de se ramener à une situation avec une variable de moins. À la réflexion, ceci correspond à choisir un ordre lexicographique pour ordonner les monômes.

Résumons nous : dans les deux cas, nous avons choisi un ordre total sur les monômes, permettant de réécrire le monôme dominant en un polynôme formé de monômes dominés. Vient d'abord une phase de préparation ou *compilation* de l'idéal : en combinant ces règles entre elles, nous avons abouti à un système particulier de générateurs, promus diviseurs : le critère d'appartenance est la nullité du reste par une *division*.

Cette construction va se généraliser à tout idéal engendré par des générateurs non nécessairement linéaires.

3 Bases standard

Nous retournons ici à l'algèbre des polynômes $R = k[x_0, x_1, \ldots, x_n]$ graduée par le degré total. Pour étudier ses idéaux, l'idée de considérer un ordre total sur les monômes de R_d remonte au moins à [Macaulay].

Par monôme on entend ici le produit de puissances. L'ensemble des monômes de $k[x_0, \ldots, x_n]$ est muni d'une structure de monoïde multiplicatif. Il est parfois commode de considérer le monoïde additif $\mathbf{N}^{n+1}$ isomorphe via $x_0^{a_0} \cdots x_n^{a_n} \mapsto (a_0, \ldots, a_n)$.

Un ordre total sur les monômes est dit *admissible* ou *compatible* s'il respecte la structure du monoïde, c'est-à-dire si l'ordre d'une paire ordonnée de monômes ne change pas en multipliant par un troisième. En fait, il faut aussi indiquer dans quel sens utiliser l'ordre pour élire le monôme dominant d'un polynôme.

Il existe un théorème de classification des ordres totaux compatibles. Mais les exemples fondamentaux suivants, admettant une interprétation géométrique, suffiront à nos besoins.

3.1 Définition : ordre lexicographique inférieur (resp. supérieur)

Un point $a = (a_0, \ldots, a_n)$ of $\mathbf{N}^{n+1}$ sera dit plus petit qu'un point $b = (b_0, \ldots, b_n)$ pour l'ordre lexicographique inférieur (resp. plus grand pour l'ordre lexicographique supérieur) si et seulement s'il existe un indice i $(0 \leq i \leq n)$ tel que :

$$a_0 = b_0, \ldots,\ a_{i-1} = b_{i-1},\ a_i < b_i$$

(resp.

$$a_n = b_n, \ldots,\ a_{i+1} = b_{i+1},\ a_i > b_i)$$

3.2 Définition : filtration lexicographique inférieure (resp. supérieure)

À tout polynôme homogène non nul :

$$f = \sum_{a \in \mathbf{N}^{n+1}} f_a\, x^a$$

est associé son support $\{a \in \mathbf{N}^{n+1} \mid f_a \neq 0\}$ dans $\mathbf{N}^{n+1}$. Le plus petit (resp. plus grand) élément du support de f pour l'ordre lexicographique inférieur (resp. supérieur) est appelé son *monôme dominant* $exp(f)$. La *forme dominante* ou *initiale* $in(f)$ est le terme

$$f_{exp(f)}\, x^{exp(f)}$$

Ainsi nous parlerons désormais de la filtration lexicographique inférieure (resp. supérieure) de R.

3.3 Définition : parties stables

Étant donné un idéal homogène I non réduit à (0), l'ensemble $E(I)$ de tous les monômes dominants de tous ses éléments non nuls forment une partie dite *stable* de $\mathbf{N}^{n+1}$, c'est-à-dire :

$$a \in E(I) \Longrightarrow a + \mathbf{N}^{n+1} \subseteq E(I)$$

Par convention, l'ensemble vide (resp. $\mathbf{N}^{n+1}$ tout entier) est associé à l'idéal trivial (0) (resp. R tout entier).

3.4 Lemme de Dickson

Toute partie stable E de $\mathbf{N}^{n+1}$ est finiment engendrée, c'est-à-dire il existe une famille unique minimale $a^{(1)}, \ldots, a^{(p)}$ telle que :

$$E = \bigcup_{i=1}^{p} (a^{(i)} + \mathbf{N}^{n+1})$$

La démonstration de cette *noethérianité* de $\mathbf{N}^{n+1}$ se fait par récurrence sur n. L'assertion est immédiate pour $n = 0$. Ensuite soit $\pi : \mathbf{N}^{n+1} \to \mathbf{N}^n$ la projection canonique sur $\mathbf{N}^n$ (identifié à $\mathbf{N}^n \times \{0\}$). $\pi(E)$ est alors une partie stable de $\mathbf{N}^n$, engendrée par hypothèse de récurrence par une famille finie $a^{(1)}, \ldots, a^{(p)}$. Pour tout i $(1 \leq i \leq p)$ il existe donc un entier $a_{n+1}^{(i)}$ tel que $(a_1^{(i)}, \ldots, a_n^{(i)}, a_{n+1}^{(i)})$ appartienne à E. Posons $m = Sup_{1 \leq i \leq p}(a_{n+1}^{(i)})$. Maintenant chacune des sections E_j de E par l'hyperplan de coordonnées $x_{n+1} = j$ s'identifie par π à une partie stable de $\mathbf{N}^n$, engendrée par une famille finie. Les $\pi(E_j)$ forment une suite croissante de parties stables qui stationnent, égales à $\pi(E)$, pour j assez grand (en fait pour $j \geq m$). On en déduit l'existence d'une famille finie de générateurs de E.

3.5 Définition : bases standard

Soit I un idéal homogène de R. D'après le lemme de Dickson, $E(I)$ est minimalement engendré. Suivant la terminologie d'[Hironaka], nous appelons *base standard* de I une famille d'éléments de I dont les monômes dominants forment cette famille génératrice minimale.
Si E est une partie stable de $\mathbf{N}^{n+1}$, nous noterons $D(E)$ le degré maximum des éléments engendrant minimalement E.

3.6 Théorème de division d'Hironaka

Soit I un polynôme homogène de R. Tout polynôme de R est congru module I à un unique polynôme appelé reste de la division par l'idéal, soit nul soit dont le support est extérieur à $E(I)$.

Démonstration : Si le polynôme dividende f est nul, le reste est nul. Sinon, il est de degré d et possède un monôme dominant. Si ce dernier appartient à $E(I)$, c'est qu'il est divisible par le monôme dominant d'un élément de I, disons g. Le polynôme de départ f est alors congru à $f - (in(f)/in(g))g$, qui est soit nul soit de monôme dominant strictement dominé par celui de f. Comme il n'y a qu'un nombre fini de monômes en degré d, ce processus s'arrête sur un polynôme soit nul soit à monôme dominant extérieur à $E(I)$; auquel cas il suffit de le priver de son terme dominant et d'appliquer récursivement la même procédure pour conclure. L'unicité provient trivialement de la partition de $\mathbf{N}^{n+1}$ en $E(I)$ et son complémentaire.

3.7 Corollaire : noethérianité de l'anneau des polynômes

Toute base standard d'un idéal l'engendre.

Démonstration : En fait, le reste de la division d'un élément de l'idéal par une base standard ne peut être que nul puisque sinon, son monôme dominant devrait être à la fois à l'extérieur de $E(I)$ (par construction du reste) et dans $E(I)$ (par définition de ce dernier). Ce corollaire établit la noethérianité de l'anneau de polynômes.

3.8 Corollaire : décomposition du quotient

En tant que k-espace vectoriel, le quotient R/I est isomorphe à la somme directe :

$$R/I = \bigoplus_{a \notin E(I)} kx^a$$

4 Fonction et polynôme de Hilbert

Le *degré* d'un point $a = (a_0, \ldots, a_n)$ de $\mathbf{N}^{n+1}$ est l'entier $|a| = a_0 + \cdots + a_n$.

4.1 Définition : fonction de Hilbert

Soit E une partie stable de $\mathbf{N}^{n+1}$; la fonction HF_E, qui associe à tout entier u le nombre de points de degré u n'appartenant pas à E, est appelé *fonction de Hilbert* du complémentaire de E :

$$HF_E(u) = \#\{a \in \mathbf{N}^{n+1} \mid a \notin E, |a| = u\}$$

4.2 Théorème : polynôme de Hilbert

C'est un théorème de Hilbert que d'affirmer que, pour u assez grand, la fonction HF_E est égale à un polynôme HP_E (dit de Hilbert). De plus, il existe des entiers $c_0, \ldots, c_d$ tels que :

$$HP_E(u) = \sum_{i=0}^{d} c_i \binom{u}{d-i}$$

où $\binom{u}{r} = u(u-1)(\cdots)(u-r+1)/r!$ est la fonction binomiale. Par définition, d est la *dimension* du complémentaire de E, et c_0 son *degré*. Finalement nous attribuerons par convention le degré -1 au polynôme nul.

4.3 Définition : régularité de la fonction de Hilbert

La *régularité* $H(E)$ de la fonction de Hilbert est le plus petit entier à partir duquel la fonction de Hilbert coïncide avec le polynôme de Hilbert. Nous noterons $D(E)$ le degré maximum des éléments engendrant minimalement E.

4.4 Démonstration du théorème et d'une borne supérieure de la régularité :

$$H(E) \leq (n+1)(D(E)-1) + 1$$

Démonstration : par récurrence sur n. L'assertion est claire pour $n = 0$. Puis d'après le lemme de Dickson, la section E_i de E par l'hyperplan $\{x_{n+1} = i\}$ est constant dès que l'indice i dépasse un certain entier disons e et pas auparavant. Considérons alors le développement suivant de la fonction de Hilbert :

$$HF_E(u) = \sum_{i=0}^{u} HF_{E_i}(u-i)$$

qui se casse en trois morceaux dès que u est assez grand :

$$\begin{aligned} HF_E(u) &= \sum_{0\le i\le e-1} HF_{E_i}(u-i) + \sum_{e\le i\le u-H(E_e)} HF_{E_e}(u-i) + \sum_{u-H(E_e)+1\le i\le u} HF_{E_e}(u-i) \\ &= \sum_{0\le i\le e-1} HF_{E_i}(u-i) + \sum_{H(E_e)\le i\le u-e} HF_{E_e}(i) + \sum_{0\le i\le H(E_e)-1} HF_{E_e}(i) \end{aligned}$$

Pour u suffisamment grand la fonction devient :

$$HF_E(u) = \sum_{0\le i\le e-1} HP_{E_i}(u-i) + \sum_{H(E_e)\le i\le u-e} HP_{E_e}(i) + \sum_{0\le i\le H(E_e)-1} HF_{E_e}(i)$$

qui n'est autre que le polynôme de Hilbert HP_E puisque $\sum_{H(E_e)\le i\le u-e} HP_{E_e}(i)$ est effectivement un polynôme en u, d'après le lemme classique :

Si P est un polynôme à une variable de degré d à coefficients rationnels. Étant donnés deux entiers r et s, $\sum_{r\le i\le s} P(i)$ est un polynôme de degré $d+1$, à coefficients entiers si c'était le cas pour P.
La démonstration est immédiate sur la base binomiale $\binom{i}{d}$.

Plus précisément cette expression est vrai dès que u dépasse $\max\{i + H(E_i) \mid 0 \le i \le e\}$, ce qui est une conséquence de l'hypothèse de récurrence dès que u dépasse $(n+1)(D(E)-1)+1$.

4.5 Exemple

Étant donnés $n+1$ entiers positifs $a_0, \dots, a_n$, considérons l'idéal $(x_0^{a_0}, \dots, x_n^{a_n})$, dont ces générateurs monomiaux forment évidemment une base standard. La partie stable associée E est le complément d'un parallélépipède dont l'élément de degré maximal est $(a_0-1, \dots, a_n-1)$. La régularité est donc $1 + \sum_{i=0}^{n}(a_i - 1)$; dans le cas où tous les a_i sont égaux, ceci prouve que la borne ci-dessus peut être atteinte.

4.6 Remarque historique

Si I est un idéal homogène de R, la fonction de Hilbert de Hilbert de $E(I)$ est indépendante de l'ordre par 3.8 et on l'appelle la fonction de Hilbert associée à l'idéal. Hilbert avait en fait introduit historiquement la fonction $u \mapsto \dim_k I \cap R_u$ (« nombre de formes homogènes de degré u linéairement indépendantes »), complémentaire au polynôme $\binom{u+n}{n} = \binom{u+n}{u}$ de celle étudiée ci-dessus.

5 Syzygies et algorithmes de construction

L'algèbre linéaire permet de calculer a priori la fonction de Hilbert en étudiant l'application k-linéaire $R_{u-d_1} \times \cdots \times R_{u-d_s} \to R_u$ induite en degrés adéquats par $(g_1, \dots, g_s) \to \sum_i g_i f_i$. Le même algorithme de triangulation permet en grimpant de degré en degré de construire une base standard. Le processus s'arrête par noethérianité, mais pour transformer cette idée en algorithme il faut assurer effectivement la terminaison par une borne supérieure a priori du degré maximal $D(E)$ à atteindre.

Ce qui précède consiste à considérer la structure k-vectorielle de I. Du point de vue R-module, le conoyau de la même application $R^s \to R$ est R/I et son noyau est par définition le *module* *des relations* entre $f_1, \ldots, f_s$, ou premier *module de syzygie*, qu'on peut par le même algorithme de triangulation construire en degré donné.

Il se trouve que le module des relations entre les éléments d'une base standard se construit facilement ; en retour ceci nous conduira à un algorithme de construction d'une base standard à partir d'un système donné de générateurs.

5.1 Définition : polynôme de syzygie

Soit $(f_1, \ldots, f_s)$ une base standard de I. Pour i différent de j, formons le polynôme (dit de *syzygie*) :

$$S(f_i, f_j) = (in(f_j)f_i - in(f_i)f_j)/m_{ij}$$

où m_{ij} est le monôme plus grand commun diviseur des monômes dominants de f_i et f_j. Divisant $S(f_i, f_j)$ par $(f_1, \ldots, f_s)$, on obtient un reste nul et donc une relation entre les polynômes de la base standard ; ce que nous conviendrons d'appeler *relation bilatérale évidente.*
L'ensemble de celles-ci n'est pas aussi particulier qu'on pourrait le penser, à cause du théorème suivant :

5.2 Théorème de Spears-Schreyer

Les relations bilatérales évidentes engendrent le module des relations entre les éléments d'une base standard.

Démonstration: Donnons-nous une relation entre les générateurs : $\sum_{i=1}^{p} g_i f_i = 0$. Posons $a_i = exp(g_i f_i)$, a le dominant des $\{a_i\}$, la tête T comme l'ensemble des indices i tels que a_i soit égal à a, et $t = Sup(T)$. Remarquons que la tête ne peut pas être réduite au seul élément t. Soit donc s un autre élément de T différent de t ; x^a est un multiple commun de $exp(f_s)$ et $exp(f_t)$, donc à l'aide de la la relation bilatérale évidente entre f_s et f_t on peut réécrire la relation initiale en une nouvelle où soit t n'intervient plus dans plus dans la tête soit celle-ci est nouvelle, et on conclut.

5.3 L'algorithme de construction de Buchberger

Inspiré par ce qui précède, on peut imaginer un algorithme de construction d'une base standard de I, à partir d'un système donné F de générateurs, basé par adjonctions successives de restes de divisions non nulles de polynômes de syzygie. Mais cet idée revient historiquement à [Buchberger, 1965] qui l'a introduite pour d'autres raisons et exprimé dans le cas affine, en appellant le résultat *base de Gröbner* :

Algorithme de Buchberger :

Entrée : un système de générateurs F.
Sortie : une base de Gröbner G.

$G \leftarrow F$
RÉPÉTER
  $G' \leftarrow G$

POUR toute paire p, q $(p \neq q)$ de G' FAIRE
Diviser $S(p, q)$ par G'
SI le reste r est non nul ALORS $G \leftarrow G \cup \{r\}$
JUSQU'À $G = G'$.

Formulation et preuve : voir [Cox-Little-O'Shea], page 59 ; mais c'est essentiellement la même que ci-dessus.

6 Théorie de la dimension

Examinons d'abord les interprétations géométriques des filtrations introduites ci-dessus.

6.1 Proposition : section par une sous-variété linéaire

Soit p un indice entre 0 et $n-1$. Soit $f_1, \ldots, f_s$ une base standard de I pour la filtration lexicographique inférieure. Alors les f_i dont les monômes dominants ne dépendent pas de $x_0, \ldots, x_p$, auxquels on ajoute $x_0, \ldots, x_p$, forment une base standard de $I + (x_0, \ldots, x_p)$ pour la même filtration. Ceci correspond à couper $Z(I)$ par la sous-variété $x_0 = \cdots = x_p = 0$.

Démonstration : elle découle de la remarque que si x_0 divise le monôme dominant d'un polynôme, il divise ce dernier ; et d'une récurrence triviale.

6.2 Proposition : projection sur une sous-variété linéaire

Soit p un indice entre 0 et $n-1$. Soit $f_1, \ldots, f_s$ une base standard de I pour la filtration lexicographique supérieure. Alors les f_i dont le monôme dominant dépend uniquement des variables $x_0, \ldots, x_p$ forment une base standard de $I \cap k[x_0, \ldots, x_p]$ relativement à la même filtration.
Si la variété linéaire définie par $x_0, \ldots, x_p$ ne coupe pas $Z(I)$, ces polynômes définissent la projection de $Z(I)$ sur la sous-variété $x_{p+1} = \cdots = x_n = 0$.

Esquisse de preuve : Pour $p = n-1$, observons que si un polynôme possède un monôme dominant qui ne dépend pas de x_n, lui non plus. Maintenant soit π la restriction à $Z(I)$ de la projection de centre le point $(0, \ldots, 0, 1)$ sur l'hyperplan $x_n = 0$. Le Nullstellensatz permet de d'affirmer que l'adhérence de Zariski de $\pi(Z(I))$ est défini par l'idéal $I \cap k[x_0, \ldots, x_{n-1}]$ et en situation projective un argument de propreté permet de conclure (voir [Hartshorne] I.2 et 4.9). Le cas général suit par récurrence.

6.3 Différentes notions de dimension

D'abord une définition *algébrique* : la *dimension de Hilbert δ* est le degré du polynôme de Hilbert associé à R/I.

Puis deux définitions *géométriques* : la *dimension de section* est le plus petit entier σ tel qu'il existe une sous-variété linéaire de codimension $\sigma + 1$ évitant $Z(I)$; la *dimension de projection* est le plus grand entier π tel qu'il existe une projection envoyant surjectivement $Z(I)$ sur une base de dimension π.

Ces trois notions coïncident classiquement, ce que nous allons prouver via leur égalité avec deux autres notions qui se lisent sur les bases standard.

6.4 Définitions : dimension lexicographique inférieure (resp. supérieure)

Soit x un système de coordonnées de $\mathbf{P}^n$. Nous appellerons $linf_x$ (resp. $lsup_x$) le plus petit (resp. le plus grand) entier e tel que $E_x(I)$ relativement à la filtration lexicographique inférieure (resp. supérieure) rencontre les derniers $n-e$ axes de coordonnées de $\mathbf{N}^{n+1}$ (resp. ne rencontre pas le plan des $e+1$ premières coordonnées).

Le minimum $linf$ des $linf_x$ (resp. le maximum $lsup$ des $lsup_x$) pris sur tous les systèmes de coordonnées est appelé la dimension lexicographique inférieure (resp. supérieure).

6.5 Théorème de la dimension et lemme de normalisation

Les cinq notions ci-dessus coïncident ; ceci établit la version géométrique du lemme de normalisation de Noether.

Preuve : par cinq inégalités successives.

6.5.1 $\delta \geq lsup$

Supposons qu'il existe des coordonnées de $\mathbf{P}^n$ pour lesquelles, relativement à un ordre compatible, par exemple le lexicograhique supérieur, $E(I)$ ne rencontre pas le plan des $e+1$ premières coordonnées. Ainsi la fonction de Hilbert $HF(u)$ est minorée par le nombre de monômes de degré u sur $e+1$ lettres, qui est un $O(u^e)$ quand u tend vers l'infini. Donc δ est minoré par $lsup$.

6.5.2 $lsup \geq \pi$

Supposons que $Z(I)$ puisse être projeté surjectivement sur un plan P de dimension p. Nous pouvons choisir des coordonnées telles que ce plan soit défini par les équations $x_{p+1} = \cdots = x_n = 0$. Ainsi l'idéal $I \cap k[x_0, \ldots, x_p]$ se réduit à 0 ; sinon il existerait un polynôme non nul $f(x_0, \ldots, x_p)$ dans I qui ne peut s'annuler sur tout le plan, et l'ensemble algébrique $Z(I)$ ne peut se projeter surjectivement. Considérons par rapport à de telles coordonnées la partie stable $E(I)$ relativement à la filtration lexicographique supérieure : elle ne peut rencontrer le plan des $p+1$ premières variables d'après 6.2.

6.5.3 $\pi \geq \sigma$

Par définition de σ, il existe une sous-variété linéaire L de codimension $\sigma+1$ évitant $Z(I)$. Par ailleurs nous pouvons choisir une sous-variété linéaire B de dimension σ évitant L. La projection de centre L envoie surjectivement $Z(I)$ sur B, puisque σ est minimal ; car si b est un point de B, la sous-variété linéaire qu'il engendre avec L est de codimension σ, donc coupe $Z(I)$ en au moins un point qui se projette sur b.

6.5.4 $\sigma \geq linf$

Par définition de σ, il existe une sous-variété linéaire L de codimension $\sigma+1$ évitant $Z(I)$. Nous pouvons choisir des coordonnées telles que L soit définie par les équations $x_0 = \cdots = x_\sigma = 0$. L'idéal $J = I + (x_0, \ldots, x_\sigma)$ définit la variété vide, donc d'après le Nullstellensatz contient une puissance de l'idéal maximal $(x_0, \ldots, x_n)$ ([Hartshorne] Ex. 2.1). Quelque soit l'ordre, en particulier l'ordre lexicographique inférieur, $E(J)$ coupe tous les axes de coordonnées. Considérons un polynôme dont le monôme dominant est sur un des axes $x_{\sigma+1}, \ldots, x_n$; il est congru modulo

$(x_0, \ldots, x_\sigma)$ à un polynôme de I, non nul et de même monôme dominant. C'est donc que la section de $E(I)$ par le plan des $n - \sigma$ dernières coordonnées recoupe tous les axes.

6.5.5 $linf \geq \delta$

Supposons qu'il y ait des coordonnées de $\mathbf{P}^n$ telles que, relativement à l'ordre lexicographique inférieur, $E(I)$ coupe les derniers $n - linf$ axes. En degré u suffisamment grand, le complémentaire de $E(I)$ ne contient que des monômes dont les $n - linf$ derniers exposants sont majorés par un un entier fixé ; à une constante multiplicative près, la fonction de Hilbert $HF(u)$ est donc majorée par le nombre de monômes sur $linf + 1$ lettres, soit un $O(u^{linf})$ quand u tend vers l'infini.

6.6 Remarque sur la calculabilité de la dimension

Soit I un idéal engendré par des polynômes de degré inférieur à d. Une fois construite une base standard, on peut calculer la dimension de Hilbert. Mais il existe une famille d'idéaux, donnés par des gén'erateurs de degré au plus d, dont le degré des éléments d'une base standard est minoré par Cd^{a^n}, $C > 0$, $a > 1$ (exemple de [Mayr-Meyer], voir aussi [Demazure]).

Il est proposé dans [Giusti, 1988] un algorithme de mise en position de Noether géométrique, avec un nombre d'opérations arithmétiques polynomial en d^{n^2}, toujours basé sur des constructions de bases standard mais tronqués en degré. Pour faire mieux il faut s'y prendre autrement …

Troisième partie
Du côté de l'évaluation

Soient $f_1, \ldots, f_s$ une famille de polynômes homogènes de $k[x_0, x_1, \ldots, x_n]$), de degré d au moins égal à n. Ecrits dans la représentation dense, ils peuvent donc être décrits par un vecteur dont les coordonnées sont dans l'anneau de base k. La taille de cette entrée est la place mémoire nécessaire pour les stocker, que nous pouvons estimer. En effet le nombre de monômes sur $n+1$ lettres de degré d est le coefficient binomial $(d+n)!/d!\,n!$ quantité majorée par ed^n, qui est donc un $O(d^n)$ (n fixé, d tendant vers l'infini). Comme nous convenons de coder les polynômes d'entrée par leurs coefficients dans la représentation dense, il faut stocker $O(sd^n)$ coefficients.

7 Description des modèles d'algorithmes et de complexité

7.1 Modèles d'algorithmes

Les algorithmes que nous allons utiliser ou introduire seront décrits par un *réseau arithmétique* à entrées dans k, représenté par un graphe orienté acyclique [von zur Gathen, 1986]. A chaque sommet interne correspond un processeur qui effectue une opération élémentaire de l'anneau de base k, et chaque arête indique l'envoi d'une sortie d'un processeur comme entrée du second.

Un algorithme admet un déroulement séquentiel ou parallèle. La *complexité séquentielle* (ou temps séquentiel) est la taille du réseau, c'est-à-dire le nombre de processeurs ou sommets du graphe. La *complexité parallèle* (ou temps parallèle) est la profondeur du réseau, c'est-à-dire la longueur du plus long chemin dans le graphe orienté. Pour une discussion plus approndie de ce modèle de complexité, nous renvoyons à [von zur Gathen, 1986] et [Fitchas-Galligo-Morgenstern, 1990].

Il existe des réseaux arithmétiques particuliers spécialement intéressants : ce sont ceux qui ne font intervenir ni tests d'égalité ni branchements. Nous les appellerons *calculs d'évaluation* (généralement sans divisions) ou *circuits arithmétiques* (*straight line programs* en basic english). Nous renvoyons à [Strassen, 1972], [von zur Gathen, 1986], [Stoss, 1989] ou [Heintz, 1989] pour plus de précisions sur ces réseaux particuliers. La *complexité séquentielle* ou *longueur* d'un tel calcul d'évaluation sera le nombre d'opérations arithmétiques qu'il contient. Ils peuvent servir à coder des polynômes à plusieurs variables, calculant leur valeur en un point.

7.2 Définition de bonnes classes de complexité

Dans le cadre défini ci-dessus, nous dirons qu'un algorithme est de complexité séquentielle *polynomiale en la taille de l'entrée* si le réseau correspondant de paramètres (d, n, s) admet une complexité séquentielle $s^{O(1)}d^{O(n)}$.
Cette terminologie est justifiée quand on considère la taille $O(sd^n)$ de notre entrée $f_1, \ldots, f_s$ pour la structure de données choisie (la représentation dense des polynômes), puisqu'un polynôme en $O(sd^n)$ est bien un $s^{O(1)}\,d^{O(n)}$.

Nous dirons que l'algorithme est *bien parallélisable* si la profondeur du réseau est en $O(n^2 \log^2(sd))$. Ceci signifie bien, conformément au sens général, que la complexité parallèle est d'ordre le carré du logarithme de la complexité séquentielle.

La complexité d'un algorithme peut aussi être mesurée *par rapport à la taille de la sortie*. Si celle-ci consiste par exemple en s polynômes en n variables de degré d^n (comme c'est souvent le cas), donnés par leur écriture dans une représentation dense, la taille de la sortie pour la représentation choisie est un $O(sd^{n^2})$. Un algorithme de complexité séquentielle $s^{O(1)}d^{O(n^2)}$ et parallèle $O(n^4 \log^2 sd)$ est alors à juste titre polynomial en la taille de la sortie et bien parallélisable.

8 Des outils plus sophistiqués

Dans l'étude algorithmique des sous-variétés algébriques apparaissent systématiquement des polynômes intermédiaires ou des sorties dont le meilleur majorant de leur degré qu'on puisse avoir est un $d^{O(n)}$ ou $sd^{O(n)}$. Nos algorithmes ne font pas exception, et c'est sans doute de toute façon inévitable, par exemple, dès lors qu'un dévissage par projection est utilisé.

L'usage de la représentation dense ne peut alors que conduire à des complexités polynomiales en la taille de la sortie. Mais il serait évidemment si agréable de rester dans la meilleure des bonnes classes de complexités, à savoir polynomiales par rapport à la taille de l'entrée ! La solution ne peut alors que passer par un changement de la structure de données choisie pour représenter polynômes intermédiaires et sorties.

8.1 Extensions de l'anneau de base

L'idée principale consiste à introduire des paramètres auxiliaires sous forme de nouvelles indéterminées, par exemple $T_1, \ldots, T_n$. Nous remplacerons alors provisoirement l'anneau de base k par $k[T_1, \ldots, T_n]$. Les résultats intermédiaires représentent des polynômes considérés comme dépendant de variables principales à coefficients eux-mêmes des polynômes en les paramètres $T_1, \ldots, T_n$. Par rapport aux variables principales les polynômes sont codés par leur écriture dans la représentation dense, mais les polynômes coefficients sont eux-mêmes représentés par des calculs d'évaluation dans $k[T_1, \ldots, T_n]$.

Nos algorithmes exécutent alors des opérations arithmétiques (en général sans divisions) et des comparaisons dans $k[T_1, \ldots, T_n]$. Le point essentiel pour la complexité de cette nouvelle arithmétique va résider dans ces comparaisons, et plus exactement les tests de non-nullité. Par exemple, si des paramètres auxiliaires différents des variables d'origine $x_0, x_1, \ldots, x_n$ apparaissent encore dans les polynômes finaux, ils devront être éliminés par spécialisation en des valeurs appropriées de k, mais bien sûr sans donner lieu à des annulations. Ainsi, tous les algorithmes pourront être réalisés par des réseaux sur l'anneau k (voir aussi [Heintz-Sieveking, 1981] et [Kaltofen, 1988] pour l'utilisation de cette représentation des polynômes en calcul formel).

Voyons maintenant comment traiter la question cruciale des comparaisons.

8.2 Un test de nullité et ses conséquences pour la complexité

Nous utiliserons de manière essentielle un théorème de [Heintz-Schnorr, 1982, Theorem 4.4]), dont nous rappelons l'énoncé par commodité pour le lecteur :

Théorème : *Considérons l'ensemble $W(D,n,v)$ des polynômes de $k[T_1,\ldots,T_n]$, de degré au plus D et qui peuvent être évalués par un calcul de longueur au plus v. Soit Γ un sous-ensemble de k de cardinal $2v(1+D)^2$. Alors il existe un sous-ensemble $Q(D,n,v,\Gamma)=\{\gamma_1,\ldots,\gamma_m\}$ de Γ^n (où $m=6(v+n)(v+n+1)$), vérifiant la propriété suivante : tout polynôme de $W(D,n,v)$ s'y s'annulant est identiquement nul.*

Suivant une jolie terminologie introduite par [Henry-Merle, 1987, 7.2] dans une situation du même type, nous appellerons *questeur* un tel ensemble, terme qui traduit avantageusement "correct test sequence".

Appliqué au cadre du paragraphe précédent où D sera toujours en $sd^{O(n)}$ ou $d^{O(n)}$, et v en $s^{O(1)}\,d^{O(n)}$ (sans divisions), ceci nous permettra d'exécuter les comparaisons nécessaires d'éléments de $k[T_1,\ldots,T_n]$ en effectuant seulement $s^{O(1)}\,d^{O(n)}$ opérations arithmétiques dans k, puisque le cardinal de Γ et de l'ensemble questeur sont en $s^{O(1)}\,d^{O(n)}$.

La question du choix de l'ensemble questeur dans Γ^n est essentielle pour l'évaluation de complexité. Bien sûr, il peut se faire au coup par coup algorithmiquement, mais à un coût élevé qui dépend surtout du paramètre n. Il serait dommage de ne pas tirer parti du fait qu'il ne dépend que des paramètres d, s et n mais ni de t ni des coefficients d'une entrée particulière $f_1,\ldots,f_s$. Pourquoi ne pas décider de rejeter ce coût dans les ténèbres extérieures, là où il y a des pleurs et des grincements de dents? Pour d, n et s fixés, nous penserons donc que nous l'avons déterminé une fois pour toute par une préparation préalable (*preprocessing*), dont le coût n'a pas à intervenir dans un calcul particulier. En quelque sorte, nous considérons qu'il est réparti sur toutes les entrées possibles. Autrement dit, pour chaque triplet d, s, n, nous construisons un réseau arithmétique qui résoud une certaine tâche en temps séquentiel $s^{O(1)}\,d^{O(n)}$ et en temps parallèle $O(n^2\log^2 sd)$, mais le coût lui-même de cette construction n'est pas compté. En ce sens, nous dirons que nos algorithmes ne sont pas *uniformes*.

Pour être exhaustif, revenons au traitement algorithmique complet. Le choix des ensembles questeurs peut se faire de manière aléatoire, selon [Heintz-Schnorr, 1982, Theorem 4.4]. Le temps séquentiel de déroulement de nos algorithmes est alors une variable aléatoire dont l'espérance est en $s^{O(1)}\,d^{O(n)}$. Enfin la borne supérieure de complexité, celle obtenue dans le pire des cas (*worst case complexity*) atteint $s^{O(1)}\,d^{O(n^2)}$.

8.3 Algèbre linéaire effective à la Berkowitz-Mulmuley

Les questions d'arithmétique étant réglées, nos résultats sont basés sur des techniques d'algèbre linéaire effective qui utilisent des algorithmes bien parallélisables et sans divisions. L'ingrédient fondamental est l'algorithme de [Berkowitz, 1984] qui calcule en temps polynomial tous les coefficients du polynôme caractéristique d'une matrice carrée à coefficients dans un anneau intègre. Ces coefficients sont représentés par un calcul d'évaluation *sans divisions*.

Pour calculer le rang d'une matrice quelconque nous combinons l'algorithme de Berkowitz avec un résultat de [Mulmuley, 1986] qui exprime ce rang comme valuation du polynôme caractéristique d'une matrice carrée auxiliaire. Ainsi, nous pouvons décider en temps polynomial par un algorithme bien parallélisable et sans effectuer de divisions si un système d'équations linéaires admet des solutions et, en cas de réponse positive, les calculer en ne faisant appel qu'à une seule division par un élément précalculé.

9 Calcul de la dimension et mise en position de Noether

Le but de cette partie est de conforter les conjectures suivant lesquelles, une variété algébrique étant donnée par équations, le calcul d'une mise en position de Noether et donc le calcul de sa dimension peuvent se faire en temps polynomial par rapport à l'entrée, et ce de manière uniforme.

Nous résolvons ici ces questions par des algorithmes bien parallélisables de complexité séquentielle en $s^{O(1)}\, d^{O(n)}$, à condition que le degré maximum des équations ne soit pas trop bas ($d \geq n$ et que ces équations soient données par une écriture dans la représentation dense. Le point est que nos algorithmes *ne sont pas uniformes par rapport à n*, puisqu'ils dépendent du choix d'un ensemble questeur, ce qui aboutit à un coût élevé par rapport à la classe de complexité $s^{O(1)}\, d^{O(n)}$.

Néanmoins, tous nos algorithmes possèdent une version uniforme et bien parallélisable dont la complexité séquentielle est $s^{O(1)}\, d^{O(n^2)}$. Cette borne de complexité uniforme est déjà connue pour les problèmes considérés ici (voir [Dickenstein-Fitchas-Giusti-Sessa, 1991], où cette borne a été obtenue directement).
Enfin, un choix aléatoire des ensembles questeurs ne change pas le caractère déterministe de nos algorithmes et les rend uniformes. Comme nous l'avons déjà dit, la complexité séquentielle devient une variable aléatoire d'espérance un $s^{O(1)}\, d^{O(n)}$, alors que la complexité dans le pire des cas est un $s^{O(1)}\, d^{O(n^2)}$, ce qui correspond à la complexité uniforme.

Du point de vue pratique, notre méthode nous semble prometteuse. La version probabiliste et uniforme de notre algorithme calculant la dimension est de type aléatoire (*randomized*). C'est surtout la complexité qui devient aléatoire, avec une espérance en $s^{O(1)}\, d^{O(n)}$ polynomiale en la taille de l'entrée. Un premier résultat dans cet esprit est contenu dans [Lakshman-Lazard, 1991].

Cependant, nos algorithmes souffrent encore d'un inconvénient pratique et théorique : ils reposent sur le codage des polynômes d'entrée par leur écriture en principe dans la représentation dense. C'est d'ailleurs le plus grave des défauts présentés par la plupart des algorithmes actuels implantés en calcul formel.
Nous noterons V l'ensemble algébrique défini par $f_1, \ldots, f_s$.

Dans toute la suite, z sera une nouvelle indéterminée qui nous servira de variable d'homogénéisation. Du point de vue géométrique, nous l'utiliserons pour effectuer des éclatements.

Soient $\lambda = (\lambda_0, \ldots, \lambda_m)$, $\lambda_0 \leq \ldots \leq \lambda_m$ et $\overline{\lambda} = (\lambda_{m+1}, \ldots, \lambda_n)$, $\lambda_{m+1} \leq \ldots \leq \lambda_n$ deux familles complémentaires d'indices entre 0 et n (c'est-à-dire $\{\lambda_0, \ldots, \lambda_m\} \cup \{\lambda_{m+1}, \ldots, \lambda_n\} = \{0, \ldots, n\}$ et $\{\lambda_0, \ldots, \lambda_m\} \cap \{\lambda_{m+1}, \ldots, \lambda_n\} = \emptyset$). Nous utilisons les notations suivantes, à comparer avec [Giusti-Heintz, 1991, 3.2] :
$x^\lambda := (x_{\lambda_0}, \ldots, x_{\lambda_m})$, $x^{\overline{\lambda}} := (x_{\lambda_{m+1}}, \ldots, x_{\lambda_n})$, $R^{(\lambda)} := k[x^\lambda]$ et $K^{(\lambda)} := k'(x^\lambda)$.
Fixons aussi une clôture algébrique $\overline{K^{(\lambda)}}$ de $K^{(\lambda)}$. Notons que $R^{(\lambda)}$ est un anneau de polynômes à coefficients dans k et que $K^{(\lambda)}$ est son corps de fractions.
Les anneaux $R^{(\lambda)}[z, x^{\overline{\lambda}}] = k[z, x_0, \ldots, x_n]$ et $K^{(\lambda)}[z, x^{\overline{\lambda}}] = k'(x^\lambda)[z, x^{\overline{\lambda}}]$ sont des anneaux (gradués) de polynômes en les variables $z, x_{\lambda_{m+1}}, \ldots, x_{\lambda_n}$ et à coefficients dans $R^{(\lambda)}$ et $K^{(\lambda)}$. Les variables $x_{\lambda_0}, \ldots, x_{\lambda_m}$ seront considérées comme des paramètres.

Soit f un polynôme homogène de $k[x_0, \dots, x_n]$. Nous notons $f^{(\lambda)}$ le polynôme de $R^{(\lambda)}[z, \overline{x^{\lambda}}]$ que nous obtenons en substituant dans f les variables $x_{\lambda_0}, \dots, x_{\lambda_m}$ par $zx_{\lambda_0}, \dots, zx_{\lambda_m}$, ou autrement dit $f^{(\lambda)} := f(zx_{\lambda_0}, \dots, zx_{\lambda_m}, x_{\lambda_{m+1}}, \dots, x_{\lambda_n})$. Observons que $f^{(\lambda)}$ est homogène de degré $\deg f$ en les variables $z, x_{\lambda_{m+1}}, \dots, x_{\lambda_n}$. Par rapport à ces variables, nous représentons $f^{(\lambda)}$ par son écriture dense, comme vecteur de ses coefficients qui sont des éléments de $R^{(\lambda)}$. Nous représentons ceux-ci, qui sont des polynômes de $k[x^{\lambda}]$, par un calcul d'évaluation bien parallélisable (et sans divisions) dans $k[x^{\lambda}]$. Observons aussi que f est le déshomogénéisé de $f^{(\lambda)}$ par rapport à la variable z.

Appelons respectivement I et J les idéaux engendrés par $f_1, \dots, f_s$ dans $k[x_0, \dots, x_n]$ et $k'[x_0, \dots, x_n]$, tandis que $I^{(\lambda)}$ et $J^{(\lambda)}$ seront ceux engendrés par $f_1^{(\lambda)}, \dots, f_s^{(\lambda)}$ dans $R^{(\lambda)}[z, \overline{x^{\lambda}}]$ et $K^{(\lambda)}[z, \overline{x^{\lambda}}]$. Nous dirons que x_{λ} (ou le système des variables $x_{\lambda_0}, \dots, x_{\lambda_m}$) est *dépendant* par rapport à V, s'il existe un polynôme homogène non constant g de $k[x^{\lambda}]$ qui s'annule sur V (ce qui revient à dire que l'intersection $k[x^{\lambda}] \cap I$ ne se réduit pas à (0)). Si x^{λ} n'est pas dépendant par rapport à V, nous l'appellerons *indépendant.*

Enfin, nous dirons que la variable $y := x_{\lambda_i}$ $(m < i \leq n)$ est en position de Noether par rapport à x^{λ} et V s'il existe un polynôme homogène de $k[x^{\lambda}, y]$ qui soit unitaire en y et qui s'annule sur V. Ceci équivaut à dire que l'intersection $k[x^{\lambda}, y] \cap I$ contient un polynôme unitaire en y. Si x^{λ} est un système maximal indépendant et si toutes les variables x_{λ_i} $(m < i \leq n)$ sont en position de Noether par rapport à V, nous dirons que le système de variables $x_0, \dots, x_n$ est lui-même en position de Noether par rapport à V.

Notre algorithme de mise en position de Noether pour les variétés projectives est basé sur le critère géométrique suivant (comparer aussi à [Giusti, 1988] et [Giusti-Heintz, 1991]) :

9.1 Le critère du centre de projection

Soit W la sous-variété projective de $\mathbf{P}^{n-m}(\overline{K^{(\lambda)}})$ définie par les polynômes $f_1^{(\lambda)}, \dots, f_s^{(\lambda)}$. Supposons que les variables $x_{\lambda_{m+1}}, \dots, x_{\lambda_n}$ soient en position de Noether par rapport à x^{λ} et V. Alors nous avons le critère suivant :

Le système des variables x^{λ} est dépendant par rapport à V si et seulement si la sous-variété W est vide.

Avant de commencer la démonstration du critère, explicitons-en la signification géométrique. A la famille $x^{\lambda} = (x_{\lambda_0}, \dots, x_{\lambda_m})$ correspond une application rationnelle $\pi : \mathbf{P}^n \longrightarrow \mathbf{P}^m$ qu'on appelle *projection* de $\mathbf{P}^n$ sur $\mathbf{P}^m$ de centre $\{x_{\lambda_0} = \dots = x_{\lambda_m} = 0\}$. Elle induit une application rationnelle $\phi : V \longrightarrow \mathbf{P}^m$. Le fait que les variables $x_{\lambda_{m+1}}, \dots, x_{\lambda_n}$ soient en position de Noether par rapport à x^{λ} et V garantit que les équations $f_1^{(\lambda)}, \dots, f_s^{(\lambda)}$ décrivent la fibre générique de ϕ, d'où le critère (comparer à [Giusti-Heintz, 1991]).

Démonstration : Supposons que la famille x^{λ} soit dépendante par rapport à V. Il existe alors un polynôme non constant g de $k[x^{\lambda}]$ et des polynômes $p_1, \dots, p_s$ de $k[x_0, \dots, x_n]$ tels que l'équation

$$g = \sum_{1 \leq i \leq s} p_i f_i$$

soit satisfaite. Nous en déduisons immédiatement une deuxième équation

$$(*) \qquad g^{(\lambda)} = \sum_{1 \leq i \leq s} p_i^{(\lambda)} f_i^{(\lambda)}$$

dans l'anneau $R^{(\lambda)}[z, \overline{x^\lambda}]$. Observons que $g^{(\lambda)}$ est égal à $z^{\deg g} g$ et que g est un élément non nul et de degré strictement positif de $R^{(\lambda)}$.
L'identité (*) implique que W est inclus dans l'hyperplan $\{z = 0\}$ de $\mathbf{P}^{n-m}(\overline{K^{(\lambda)}})$. Soit $m < i \leq n$ et $y := x_{\lambda_i}$. Comme y est en position de Noether par rapport à x^λ et V, il existe un polynôme homogène q de $k[x^\lambda, y] \cap I$ qui soit unitaire en y. Comme précédemment, nous obtenons que $q^{(\lambda)}$ appartient à $I^{(\lambda)}$, donc s'annule sur $W^{(\lambda)}$. Ce polynôme de $R^{(\lambda)}[z, y]$ est unitaire en y. Comme W est contenu dans l'hyperplan à l'infini, nous en concluons qu'il est aussi dans l'hyperplan $\{y = 0\}$ de $\mathbf{P}^{n-m}(\overline{K^{(\lambda)}})$. De cette manière, nous en déduisons que W est dans l'intersection de tous les hyperplans $\{z = 0\}$, $\{x_{\lambda_{m+1}} = 0\}$, $\ldots$, $\{x_{\lambda_n} = 0\}$, qui est vide.

Réciproquement, supposons maintenant que W soit vide. Ceci veut dire que $z, x_{\lambda_{m+1}}, \ldots, x_{\lambda_n}$ appartiennent au radical de l'idéal $J^{(\lambda)}$ engendré par $f_1^{(\lambda)}, \ldots, f_s^{(\lambda)}$ dans $K^{(\lambda)}[z, \overline{x^\lambda}]$. Il existe donc un élément non nul g de $R^{(\lambda)} = k[x^\lambda]$, un entier $N \geq 1$ et des polynômes $p_1', \ldots, p_s'$ de $R^{(\lambda)}[z, x^\lambda]$ tels que l'équation

$$(**) \qquad g z^N = \sum_{1 \leq i \leq s} p_i' f_i^{(\lambda)}$$

soit satisfaite.

En déshomogénéisant (**) par la substitution de 1 à z, les polynômes p_i' $(1 \leq i \leq s)$ se spécialisent en des polynômes p_i de $k[x_0, \ldots, x_n]$ et les $f_i^{(\lambda)}$ en f_i. Le polynôme g ne change pas et nous pouvons le supposer constant et homogène. Quant à l'équation (**), elle se transforme en

$$g = \sum_{1 \leq i \leq s} p_i f_i$$

Comme g appartient à $k[x_\lambda]$, ceci implique que $k[x^\lambda] \cap I \neq 0$. Le système de variables x^λ est donc dépendant par rapport à V. Nous allons maintenant transformer notre critère géométrique en algorithme.

9.2 Une bonne équation satisfaite par la projection

Conservons l'hypothèse que les variables $x_{\lambda_{m+1}}, \ldots, x_{\lambda_n}$ sont en position de Noether par rapport à x^λ et à V.

Au prix d'une préparation préalable, nous pouvons décider en temps $s^{O(1)} d^{O(n)}$ par un algorithme bien parallélisable et sans divisions si les variables $x_{\lambda_0}, \ldots, x_{\lambda_m}$ sont dépendantes par rapport à V. Si c'est le cas, l'algorithme calcule un polynôme homogène non constant g de $k[x^\lambda]$ qui s'annule sur la variété V. Son degré est un $d^{O(n)}$. Le polynôme g est représenté par un calcul d'évaluation bien parallélisable sans divisions de longueur $s^{O(1)} d^{O(n)}$.

Démonstration : D'après le critère 9.1 et le Nullstellensatz projectif effectif [Lazard, 1977] (voir aussi [Briançon, 1983]) les assertions suivantes sont équivalentes :

(1) les variables $x_{\lambda_0}, \ldots, x_{\lambda_m}$ sont dépendantes par rapport à V.

(2) les variables $z, x_{\lambda_{m+1}}, \ldots, x_{\lambda_n}$ appartiennent au radical de l'idéal $J^{(\lambda)}$ engendré par $f_1^{(\lambda)}, \ldots, f_s^{(\lambda)}$ dans $K^{(\lambda)}[z, x^{\overline{\lambda}}]$.

(3) tous les monômes en $z, x_{\lambda_{m+1}}, \ldots, x_{\lambda_n}$ de degré $N := nd$ appartiennent à $J^{(\lambda)}$.

Soit Q la matrice à coefficients dans $R^{(\lambda)}$, de l'application linéaire qui à $(h_1, \ldots, h_s)$ associe $h_1 f_1 + \cdots + h_s f_s$ (h_i étant un polynôme de $k[z, x^{\overline{\lambda}}]$ de degré $N - \deg f_i$, $1 \leq i \leq s$). C'est une matrice rectangulaire à $O(sN^n) = sd^{O(n)}$ lignes et $O(N^n) = d^{O(n)}$ colonnes. La condition (3) est équivalente à :

(4) la matrice Q est de rang maximal.

En utilisant les techniques d'algèbre linéaire effective rappelées dans 8.3, nous pouvons calculer le rang de Q par un algorithme bien parallélisable et sans divisions, en effectuant $s^{O(1)}\, d^{O(n)}$ opérations arithmétiques et comparaisons dans $R^{(\lambda)}$. De cette manière, nous pouvons vérifier si la condition (4) est satisfaite, et si c'est le cas, l'algorithme calcule le déterminant g' d'une sous-matrice carrée de Q de rang maximal. Ce déterminant est un polynôme de $k[x^\lambda]$ de degré $d^{O(n)}$, donné par un calcul d'évaluation bien parallélisable et sans divisions de longueur $s^{O(1)}\, d^{O(n)}$. Il se décompose en une somme de polynômes homogènes non nuls ; soit g l'un d'entre eux. Nous voyons immédiatement que g est un polynôme homogène de $k[x^\lambda]$ de degré $d^{O(n)}$, s'annule sur V et est donné d'après [Strassen, 1973] par un calcul d'évaluation bien parallélisable et sans divisions de longueur $s^{O(1)}\, d^{O(n)}$. En utilisant un ensemble questeur $(\gamma_1, \ldots, \gamma_l)$ de $l = s^{O(1)}\, d^{O(n)}$ points appropriés de k^{m+1}, nous transformons l'algorithme de détermination du rang de Q qui se déroule en principe dans $R^{(\lambda)}$ par un algorithme qui s'exécute dans k. Il ne contient pas de divisions, et bien parallélisable et reste de complexité $s^{O(1)}\, d^{O(n)}$.

9.3 Mise en position de Noether effective pour les variétés projectives

Soit r la dimension de V.

Théorème (comparer [Giusti, 1988, 5.6]) *Au prix d'une préparation préalable, nous pouvons déterminer la dimension r de V en temps $s^{O(1)}\, d^{O(n)}$ par un algorithme bien parallélisable et sans divisions. De plus, nous pouvons trouver une $(n+1) \times (n+1)$-matrice non singulière à coefficients dans k telle que si $y_0, \ldots, y_n$ sont par définition de nouvelles variables $M(x_0, \ldots, x_n)$, les $r+1$ premières d'entre elles $y_0, \ldots, y_r$ sont indépendantes par rapport à V. Les nouvelles variables $y_0, \ldots, y_n$ sont en position de Noether par rapport à V.*

Démonstration : Nous construisons M par récurrence.
Comme f_1 est non constant, nous pouvons le supposer unitaire en x_n au prix d'une première transformation linéaire sur les variables $x_0, \ldots, x_n$. Ceci signifie que la variable x_n est en position de Noether par rapport à $x_0, \ldots, x_{n-1}$ et à V. Cette transformation de variables peut être réalisée par un algorithme bien parallélisable en temps $O(sd^n)$.

Supposons maintenant par hypothèse de récurrence que pour un indice m $(0 \leq m < n)$ tel que $x_{m+1}, \ldots, x_n$ soient en position de Noether par rapport à $x_0, \ldots, x_m$ et à V. Testons à l'aide du lemme 4.3 en temps séquentiel $s^{O(1)}\, d^{O(n)}$ et parallèle $O(n^2 \log^2 sd)$ si les variables $x_0, \ldots, x_m$ sont indépendantes par rapport à V.

Si c'est le cas, il nous suffit de prendre la matrice identité pour M. Les variables $x_0, \ldots, x_n$ sont en position de Noether par rapport à V et la dimension de V est m.

Dans le cas contraire, supposons que les variables $x_0, \ldots, x_m$ soient dépendantes par rapport à V. L'algorithme du lemme 4.3 calcule un polynôme homogène non constant g de $k[x_0, \ldots, x_m]$ qui s'annule sur V. Il est de degré d^{cm} pour une constante c approprié et s'évalue par un algorithme bien parallélisable et sans divisions en $v = s^{O(1)}\, d^{O(n)}$ opérations arithmétiques.

Soit $(\gamma_1, \ldots, \gamma_l)$ un ensemble questeur de $l = 6(v+m+1)(v+m+2) = s^{O(1)}\, d^{O(n)}$ points appropriés de k^{m+1}. D'après [Heintz-Schnorr, 1982, Theorem 4.4], il existe un point $\gamma_i = (\gamma_0^{(i)}, \ldots, \gamma_m^{(i)})$ $(1 \leq i \leq l)$ de cet ensemble qui n'annule pas g. Nous pouvons trouver un tel point en évaluant g en tous les points de l'ensemble questeur, ce qui nécessite un temps séquentiel en $s^{O(1)}\, d^{O(n)}$ et un temps parallèle en $O(n^2 \log^2 sd)$. Il suffit maintenant de transformer les variables $x_0, \ldots, x_m$ à l'aide des coordonnées de γ_i en nouvelles variables $y_0, \ldots, y_m$ telles que g, qui est un polynôme de $k[x_0, \ldots, x_m] = k[y_0, \ldots, y_m]$ devienne unitaire en y_m. Posons $y_{m+1} := x_{m+1}, \ldots, y_n := x_n$. Nous obtenons ainsi en temps séquentiel $s^{O(1)}\, d^{O(n)}$ par un algorithme bien parallélisable et sans divisions une $(n+1) \times (n+1)$-matrice non singulière à coefficients dans k qui décrit la transformation de variables recherchée. Par construction, les nouvelles variables $y_m, \ldots, y_n$ sont en position de Noether par rapport à $y_0, \ldots, y_{m-1}$ et V.

L'itération du processus précédent nous conduit au résultat.

REFERENCES

[Bayer-Stillman, 1987]

D. Bayer, M. Stillman, *A theorem on refining division orders by the reverse lexicographic order*, Duke J. Math. **55**, 321-328.

[Berkowitz, 1984]

S. J. Berkowitz, *On computing the determinant in small parallel time using a small number of processors*, Information Processing Letters **18**, 147-150.

[Briançon, 1983]

J. Briançon, *Sur le degré des relations entre polynômes*, C. R. Académie des Sciences de Paris, Série I Math. (1982), 553-556.

[Buchberger, 1965]

B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, Ph. D. Dissertation, U. Innsbruck, Austria, (1965).

[Buchberger, 1985]

B. Buchberger, *Gröbner Bases: an algorithmic method in polynomial ideal theory*, in: Multidimensional Systems Theory (ed. N. K. Bose), D. Reidel Publishing Comp. (1985), 184-232.

[Cox-Little-O'Shea]

D. Cox, J. Little, D. O'Shea, *Ideals, Varieties and Algorithms*, Undergraduate Texts in Mathematics, Springer Verlag (1992).

[Demazure]

M. Demazure, *Le théorème de complexité de Mayr et Meyer*, Géométrie algébrique et applications, C. R. de la deuxième conférence internationale de la Rábida, Aroca, Sanchez-Giralda, Vicente eds. Travaux en cours 22, Hermann (1987), 35-58.

[Dickenstein-Fitchas-Giusti-Sessa, 1991]

A. Dickenstein, Noaï Fitchas, M. Giusti, C. Sessa, *The membership problem for unmixed polynomial ideals is solvable in single exponential time*, 7th Intern. Conf. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes AAECC 7 (Toulouse 1989), Discrete Applied Math. **33** (1991) 73-94, Special Issue.

[Fitchas-Galligo-Morgenstern, 1990]

Noaï Fitchas, A. Galligo, J. Morgenstern, *Algorithmes rapides en séquentiel et parallèle pour l'élimination des quantificateurs en géométrie élémentaire*, Séminaire sur les structures algébriques ordonnées 1984-87 vol. I, Publications de l'Université Paris VII (F. Delon, M. Dickmann et D. Gondard eds.), **32** (1990), 103-145.

[von zur Gathen, 1986],

J. von zur Gathen, *Parallel arithmetic computations: a survey*, Proc. 13th Symp. MFCS 1986, Springer LN Comput. Sci. **233** (1986), 93-112.

[Giusti, 1988]
M. Giusti, *Combinatorial Dimension Theory of Algebraic Varieties*, special issue of J. Symbolic Computation **6** (1988), 249-265.

[Giusti-Heintz, 1991]
M. Giusti, J. Heintz, *Algorithmes - disons rapides - pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionnelles*, Proc. Effective Methods in Algebraic Geometry, MEGA '90 (T. Mora - C. Traverso eds.), Progress in Mathematics **94**, Birkhäuser (1991), 169-193.

[Giusti-Heintz, 1993]
M. Giusti, J. Heintz, *La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial*, Computational Algebraic Geometry and Commutative Algebra, D. Eisenbud and L. Robbiano (eds.), Symposia Matematica, vol. XXXIV, Cambridge University Press, 216–256.

[Hartshorne]
R. Harthshorne, *Algebraic Geometry*, Graduate Texts in Mathematics **52**, Springer Verlag (1977).

[Heintz, 1983]
J. Heintz, *Definability and fast quantifier elimination over algebraically closed fields*, Theoretical Computer Science **24** (1983), 239-277; Russian translation in Kyberneticeskij Sbornik, Novaja Serija, Mir Moskva **22** (1985), 113-158.

[Heintz, 1989]
J. Heintz, *On the computational complexity of poynomials and bilinear mappings, a survey*, Proc. 5th Intern. Conf. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes AAECC 5, Menorca 1987 (L. Huguet et A. Poli eds.), Springer LN Comput. Sci. **356** (1989), 269-300.

[Heintz-Sieveking, 1981]
J. Heintz, M. Sieveking, *Absolute primality of polynomials is decidable in random polynomial time in the number of variables*, Proc. 8^{th} Int. Coll. Automata, Langages and Programming ICALP '81, Springer LNCS **115** (1981), 16-28.

[Heintz-Schnorr, 1982]
J. Heintz, C. P. Schnorr, *Testing polynomials which are easy to compute*, Logic and Algorithmic, an international Symposium held in honour of Ernst Specker, Monographie **30** de l'Enseignement Mathématique, Genève (1982), 237-254. Aussi dans Proc. 12th Annual ACM Symposium on Computing (1980), 262-268.

[Henry-Merle, 1987]
J. P. Henry, M. Merle, *Conditions de régularité et éclatements*, Annales de l'Institut Fourier, Grenoble, **37**, 3 (1987), 159-190.

[Hironaka, 1964]
H. Hironaka, *Resolution of singularities of an algebraic variety over a field of characteristic zero*, Ann. Math. 79, (1964) 109-326.

[Kaltofen, 1988]
E. Kaltofen, *Greatest common divisors of polynomials given by straight line programs*, Journal ACM **35** No 1 (1988), 231-264.

[Lakshman, 1991]
Y. N. Lakshman, *A single exponential bound of the complexity of computing Gröbner bases of zero-dimensional ideals*, Proc. Effective Methods in Algebraic Geometry, MEGA '90 (T. Mora - C. Traverso eds.), Progress in Mathematics **94**, Birkhäuser (1991), 227-234.

[Lakshman-Lazard, 1991]
Y. N. Lakshman, D. Lazard, *On the complexity of zero-dimensional algebraic systems*, Effective Methods in Algebraic Geometry, MEGA '90 (T. Mora - C. Traverso eds.), Progress in Mathematics **94**, Birkhäuser (1991), 217-225.

[Lazard, 1977]
D. Lazard, *Algèbre linéaire sur* $k[x_1, \ldots, x_n]$ *et élimination*, Bulletin de la Société Mathématique de France **105** (1977), 165-190.

[Macaulay, 1927]
F.S. Macaulay, *Some properties of enumeration in the theory of modular systems*, Proc. London Math. Soc. 26 (1927), 531-555.

[Matsumura, 1989]
H. Matsumura, *Commutative ring theory*, Cambridge Studies in Advanced Mathematics **8**, Cambridge University Press (1989).

[Mayr-Meyer, 1982]
E. Mayr, A. Meyer, *The complexity of the word problem for commutative semi-groups and polynomial ideals*, Adv. in Maths. 46 (1982), 305-329.

[Mulmuley, 1986]
K. Mulmuley, *A fast parallel algorithm to compute the rank of a matrix over an arbitrary field*, Proc. 18^{th} Annual ACM Theory of computing (1986), 338-339.

[Richardson, 1968]
D. Richardson, *Some Unsolvable Problems Involving Elementary Functions of a Real Variable*, J. Symbolic Logic **33** (1968), 511-520.

[Stoss, 1989]
H. J. Stoss, *On the representation of rational functions of bounded complexity*, Theoretical Computer Science **64** (1989), 1-13.

[Strassen, 1972]
V. Strassen, *Berechnung und Programm I*, Acta Inform. **1** (1972), 320-334.

[Strassen, 1973]
V. Strassen, *Vermeidung von Divisionen*, Crelle J. Reine Angew. Math. **264** (1973), 184-202.