La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial

Marc Giusti [1]
Centre de Calcul Formel (Laboratoire GAGE)
&
Groupe Aleph et Géode du Centre de Mathématiques (URA 169 du CNRS)
Ecole Polytechnique
91128 Palaiseau Cedex
France
giusti@poly.polytechnique.fr, giusti@frpoly11.bitnet

Joos Heintz [2]
Departamento de Matemáticas, Estadística y Computación
Facultad de Ciencias, Universidad de Cantabria
39071 Santander, Espagne
heintz@ccucvx.unican.es
et
Departamento de Matemáticas
Universidad de Buenos Aires
Argentine

Novembre 1991

[1]Avec un soutien de l'Action Concertée MEDICIS du CNRS (Mathématiques Effectives, Développements Informatiques, Calcul, Ingénierie et Systèmes), du GDR-PRC Mathématiques et Informatique et du projet européen ESPRIT BRA contract 6846 POSSO.
[2]Contre le CONICET.

Sommaire

Abstract

We show that the dimension of an algebraic (affine or projective) variety can be computed by a well parallelizable arithmetical network in non-uniform polynomial sequential time in the size of the input. This input is given by a system of polynomial equations written in dense representation. The coordinates of the ambient space can be put in Noether position with respect to the variety within the same time bounds.
By the way, we consider as an intermediate problem the determination of the isolated points of the given variety, which is of obvious practical interest.
We suppose that the base domain, from where the coefficients of the input polynomials are taken, is infinite and, in the case of an affine variety, that its field of fractions is perfect. If this domain consists of the integers, our algorithms can be realized by boolean networks of the same complexity type (however these networks are not uniform with respect to the number of variables occuring in the input polynomials).
Our results imply an effective version of the affine Nullstellensatz in terms of degrees and straight line programs.

Résumé

Nous considérons la question du calcul de la dimension d'une variété algébrique (affine ou projective), ainsi que plus généralement la mise des variables en position de Noether par rapport à la variété. Chemin faisant, nous examinons comme problème intermédiaire la détermination des points isolés, ce qui présente un intérêt pratique évident. Nous supposons que la variété est donnée par un système d'équations polynomiales écrites en représentation dense.
Nous présentons ici des algorithmes qui résolvent ces problèmes en temps séquentiel polynomial en la taille des entrées, par des réseaux arithmétiques bien parallélisables. Néanmoins ces algorithmes ne sont pas uniformes en le nombre de variables dont dépendent les polynômes d'entrée.
Nous supposons l'anneau de base intègre, infini et dans le cas affine, son corps des fractions parfait. Dans le cas particulier de l'anneau des entiers, nos algorithmes peuvent être réalisés par des réseaux booléens du même type de complexité.
Les résultats impliquent une version effective d'un Nullstellensatz affine en termes de calculs d'évaluation (*straight line programs*) et de degrés de polynômes.

> “ MATHEMATICS *The synthesis of the calculus of n-variables and of n-dimensional geometry is the basis of what Seldon once called “my little algebra of humanity” ...* ”
>
> Isaac ASIMOV, Second Foundation.

1. Définitions et notations

Pour l'ensemble de ce travail, nous allons fixer les notations qui seront essentiellement les mêmes que dans l'article [Giusti-Heintz, 1991]. Nous les reprenons ici par commodité pour le lecteur.

1.1. Notations de base

Soit k un anneau intègre commutatif, infini, et effectif, c'est-à-dire que les opérations arithmétiques de base : addition, soustraction, multiplication, division (si elle a lieu dans k) et test d'égalité sont réalisées par des algorithmes. Soit k' le corps des fractions de k et soit $\bar{k}'$ une clôture algébrique de k'. 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 $\mathbf{P}^n$.
Dans la situation affine et quand la caractéristique de k est positive, il convient de supposer que l'anneau de base est fermé sous l'extraction des racines $p^{\text{ièmes}}$, par conséquent le corps k' sera parfait. Mais nous le supposerons encore effectif, ce qui veut dire que l'extraction des racines $p^{\text{ièmes}}$ sera réalisée par un algorithme.

Nous voulons étudier des sous-variétés vivant dans ces espaces ambiants. Soient $x_1, \ldots, x_n$ (resp. $x_0, x_1, \ldots, x_n$) des indéterminées sur k. Le degré total d'un polynôme f à coefficients dans k' sera noté $\deg f$ et son degré partiel par rapport à la variable x_i par $\deg_{x_i} f$. Un polynôme f est appelé *unitaire* en x_i si son degré partiel par rapport à cette variable coïncide avec son degré total supposé positif.
Dans toute la suite, soit $f_1, f_2, \ldots, f_s$ un système fini de polynômes non constants de $k[x_1, \ldots, x_n]$ (resp. des polynômes homogènes non constants de $k[x_0, x_1, \ldots, x_n]$), et soit d un entier majorant n et le plus grand des degrés totaux des f_i. L'idéal engendré par ces polynômes dans $k[x_1, \ldots, x_n]$ (resp. dans $k[x_0, x_1, \ldots, x_n]$) sera noté $I(f_1, \ldots, f_s)$ ou plus simplement $(f_1, \ldots, f_s)$, voire I. Si aucun doute n'est possible, nous noterons aussi $(f_1, \ldots, f_s)$ l'idéal étendu induit par une extension de l'anneau de base, notamment l'extension de k à k'.
La variété algébrique, au sens classique, affine (resp. projective) définie par $(f_1, \ldots, f_s)$ ou I dans $\mathbf{A}^n$ (resp. $\mathbf{P}^n$) sera notée $V(f_1, \ldots, f_s)$, $V(I)$, ou plus simplement V quand aucun doute n'est possible.

1.2. Structures de données, modèles d'algorithmique et de complexité

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

1.2.1. Représentation naïve des entrées/sorties et leur taille

Soit $f_1, \ldots, f_s$ l'ensemble de polynômes de $k[x_1, \ldots, x_n]$ (resp. de s polynômes homogènes de $k[x_0, x_1, \ldots, x_n]$) introduit dans 1.1. Rappelons que nous supposerons toujours que le maximum de leurs degrés est borné supérieurement par un nombre préfixé 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, et dont la taille dépend des paramètres d, n et s.

Il existe un cas particulier important d'anneau de base : celui des entiers $\mathbf{Z}$. Dans ce cas la taille de notre ensemble peut inclure la *taille arithmétique*, c'est-à-dire le nombre maximal t de bits qu'il faut pour écrire n'importe lequel des coefficients des polynômes f_i. Autrement dit, la hauteur de chaque f_i $(1 \leq i \leq s)$, qui est le maximum des valeurs absolues de tous ses coefficients (au sens classique des arithméticiens), est majorée par 2^t.

La taille de l'entrée $f_1, \ldots, f_s$ est la place mémoire nécessaire pour les stocker, c'est-à-dire celle qu'occupent les coefficients. En effet nous pouvons aisément estimer la place mémoire nécessaire pour stocker $f_1, \ldots, f_s$ à partir des paramètres d, n, s et éventuellement t dans le cas de l'anneau de base des entiers. 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 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, et s'ils sont entiers, cela demande $O(sd^nt)$ bits.

Les sorties pourront être des valeurs booléennes, des entiers compris entre -1 et n (représentés par des vecteurs de valeurs booléennes) et des matrices carrées d'ordre n ou $n+1$ à coefficients dans k. Nous aurons aussi à traiter le cas où les sorties sont encore des polynômes. De la même manière naïve, nous pourrons toujours les coder par leur écriture dans la représentation dense.

Nous aurons aussi à considérer des quantités géométriques intrinsèques liées à $V(f_1, \ldots, f_s)$, essentiellement dimension et degré.
Soit $V = \cup_{1\leq j\leq N} C_j$ la décomposition de V en composantes irréductibles. La dimension dim C_j et le degré deg C_j d'une composante irréductible sont définis comme d'habitude. De même, nous utiliserons la notion usuelle de dimension pour la variété V :
$\dim V := \max \{\dim C_j \ ; 1 \leq j \leq N\}$. Par contre, le degré de la variété sera définie comme la somme des degrés de ses composantes irréductibles : $\deg V := \sum_{1\leq j\leq N} \deg C_j$. Cette notion présente l'avantage sur le degré classique de satisfaire à une inégalité de Bézout sans restrictions sur le type d'intersections à effectuer (voir [Heintz, 1983]).

1.2.2. Les opérations arithmétiques dans l'anneau de base

Tous nos algorithmes s'appuient sur les opérations suivantes, dites arithmétiques, dans l'anneau de base k : choix d'un élément fixe de k (par exemple 0 ou 1) comme opération constante, addition, soustraction, multiplication et éventuellement extraction de racines $p^{i\grave{e}mes}$ dans le cas d'une caractéristique positive p et d'une variété affine. Très exceptionnellement quand k est un corps, nous admettrons aussi les divisions dans k (voir 3.4.6 et 3.6). En dehors de ces opérations arithmétiques, nous utiliserons aussi des sélecteurs associés au test d'égalité (comparaison entre éléments de k). Le réseau peut aussi contenir des processeurs qui exécutent les opérations booléennes correspondant à la logique propositionnelle.

1.2.3. Description des modèles d'algorithmes et de complexité

Les algorithmes que nous allons utiliser ou introduire seront en principe 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.

Si l'anneau de base est celui des entiers, chaque processeur arithmétique devient lui-même un circuit booléen dont les processeurs manipulent maintenant des bits. Il faut alors tenir compte de la croissance éventuelle des coefficients des polynômes intermédiaires. Ceci fait, notre réseau arithmétique se transforme de manière naturelle en réseau booléen, auquel nous pouvons attacher de manière analogue une notion de complexité séquentielle et parallèle.

Pour résumer, nos algorithmes seront donc des familles de réseaux arithmétiques paramétrés par les quantités d, s, n (ou des réseaux booléens paramétrés par d, s, n et t).

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 de $\mathbf{A}^n$ (ou $\mathbf{A}^{n+1}$).

1.3. 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) (resp. (d, n, s, t) dans le cas booléen) admet une complexité séquentielle $s^{O(1)}d^{O(n)}$ (resp. $(st)^{O(1)}d^{O(n)}$).
Cette terminologie est justifiée quand on considère la taille $O(sd^n)$ (resp. $O(std^n)$) de notre entrée $f_1, \ldots, f_s$ pour la structure de données choisie (la représentation dense des polynômes), puisqu'un polynôme en $O(sd^n)$ (resp. en $O(std^n)$) est bien un $s^{O(1)}\, d^{O(n)}$ (resp. un $(st)^{O(1)}\, d^{O(n)}$).

Nous dirons que l'algorithme est *bien parallélisable* si la profondeur du réseau est en $O(n^2 \log^2(sd))$ (resp. en $O(n^2 \log^2(std))$). 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.

2. 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 (voir par exemple 3.4.5, 3.4.7, 3.7.2, ou 4.3). 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.

2.1. Extension de l'anneau de base

L'idée principale de notre travail consiste à introduire des paramètres auxiliaires sous forme de nouvelles indéterminées, par exemple $T_1, \ldots, T_n$ (voir 3.4.5). 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 $x_1, \ldots, x_n$ ou $x_0, x_1, \ldots, x_n$ 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).

Dans la situation affine et dans le cas d'une caractéristique positive p, nous aurons aussi à envisager l'extraction de racines $p^{\text{ièmes}}$ dans $k[T_1, \ldots, T_n]$. Le nombre d'itérations d'extractions est a priori majoré par un entier μ qui sera en $O(n \log d)$ (voir par exemple 3.4.6 et 3.4.7). Sans restriction de généralité nous pouvons supposer que les paramètres $T_1, \ldots, T_n$ sont de la forme $T_i = S_i^{p^\mu}$ $(1 \leq i \leq n)$, où $S_1, \ldots, S_n$ sont de nouvelles indéterminées. Fixons un entier ν compris entre 1 et μ. Afin de pouvoir extraire les racines $(p^\nu)^{\text{ièmes}}$ nécessaires dans $k[T_1, \ldots, T_n]$, nous effectuons nos calculs dans $k[S_1, \ldots, S_n]$ comme suit :

Soit u un polynôme de $k[T_1, \ldots, T_n]$ donné par un calcul d'évaluation β dans $k[T_1, \ldots, T_n]$. Chaque fois qu'une variable T_i est introduite dans β, remplaçons-la par $S_i^{p^{\mu-\nu}}$, tandis que chaque fois qu'un paramètre de k l'est, il est remplacé par sa racine $(p^\nu)^{\text{ième}}$ dans k. Nous obtenons ainsi un calcul d'évaluation β' dans $k[S_1, \ldots, S_n]$, de même longueur que β, qui calcule un polynôme v de $k[S_1, \ldots, S_n]$ tel que $v^{p^\nu} = u$, et donc qui évalue la racine $(p^\nu)^{\text{ième}}$ de u. Dans les cas où l'extraction des racines $p^{\text{ièmes}}$ dans des anneaux de paramètres est nécessaire, nous supposerons dorénavant que ces paramètres sont déjà donnés comme puissances $(p^\mu)^{\text{ièmes}}$.

Voyons maintenant comment traiter la question cruciale des comparaisons.

2.2. 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 $s^{O(1)}\, d^{O(n)}$.

Si l'anneau de base est celui des entiers, il convient de choisir pour Γ la suite des entiers compris entre 0 et $2v(1 + sd^{cn})^2$. Ce choix nous permet d'exécuter nos algorithmes avec une complexité séquentielle binaire en $(st)^{O(1)}\, d^{O(n)}$ de manière bien parallélisable.

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. Nous procédons de manière analogue pour les paramètres d, s, t, n et les réseaux booléens et le cas de l'anneau de base des entiers (voir [von zur Gathen, 1986] pour détails). 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 $s^{O(1)}\, d^{O(n^2)}$.

2.3. 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.
Dans la situation affine, il nous faudra aussi calculer des pgcd de polynômes à une variable et à coefficients dans un anneau intègre (voir 3.4.6 et 3.4.7). Nous renvoyons à [Giusti-Heintz, 1991] en nous appuyant sur des techniques de sous-résultants [Brown, 1971], en combinaison avec l'algorithme de Berkowitz. Si la caractéristique est positive, c'est là où l'extraction de racines $p^{\text{ièmes}}$ risque d'intervenir (voir 2.1).

2.4. Enoncé des résultats

2.4.1. Calcul de la dimension et mise en position de Noether ; le rôle des points isolés

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

Il est à noter que dans le cas d'une variété affine, nous commençons par la détermination des points isolés qui sert de résultat intermédiaire pour le calcul de la dimension, puis nous terminons par la mise en position de Noether. Par contre dans le cas projectif, nous procédons directement à la mise en position de Noether qui inclut bien sûr la détermination de la dimension.

Nous résolvons ici quasiment 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 (voir 3.4.6, 3.4.8, 3.5, 3.7.2 et 4.4). 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.

Tous nos résultats de complexité sont énoncés en termes de réseaux arithmétiques, et à l'exception de 3.6 peuvent être reformulés en termes de réseaux booléens dans le cas de l'anneau de base des entiers.
Malheureusement, c'est là que la non-uniformité ne nous permet pas de reformuler sans pertes nos résultats dans le langage des machines de Turing si l'anneau de base est celui des entiers.

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 tous les algorithmes actuels en calcul formel, et le défi à relever le plus excitant pour les recherches à venir.

2.4.2. Un Nullstellensatz affine effectivement effectif

Notre méthode de calcul de la dimension d'une variété affine via celui de ses points isolés, couplée avec les techniques utilisées dans la preuve de [Caniglia-Galligo-Heintz, 1989] d'un Nullstellensatz affine effectif, sert d'ingrédient fondamental à la démonstration de cette version plus “informatique” :

Théorème (en collaboration avec Juan Sabia, Buenos Aires) :
Soient k un corps infini et parfait, et $f_1, \ldots, f_s$ des polynômes de $k[x_1, \ldots, x_n]$. Au prix d'une préparation préalable, nous pouvons décider en temps $s^{O(1)}\, d^{O(n)}$ par un algorithme bien parallélisable si la constante 1 appartient à l'idéal engendré par $f_1, \ldots, f_s$. Si c'est le cas, nous pouvons trouver des polynômes $p_1, \ldots, p_s$ de degré $d^{O(n^2)}$, représentés par un calcul d'évaluation dans $k(x_1, \ldots, x_n)$ bien parallélisable de longueur $s^{O(1)}\, d^{O(n)}$ (avec divisions), vérifiant l'identité de Bézout $1 = p_1 f_1 + \cdots + p_s f_s$.

Ce résultat est encore imparfait, car on désirerait bien sûr une borne sur les degrés en $d^{O(n)}$ et éviter toute division dans le calcul qui représente les quotients $p_1, \ldots, p_s$. Mais l'avantage sur les Nullstellensätze effectifs connus (dont on pourra trouver des références dans la revue de [Teissier, 1991] ou l'article [Fitchas-Galligo, 1990]) réside dans le gain de complexité qu'apporte la représentation de la sortie $p_1, \ldots, p_s$ dans une structure de donnée de taille $s^{O(1)}\, d^{O(n)}$ au lieu du $s^{O(1)}\, d^{O(n^2)}$ auquel aboutissent les travaux cités. En effet, ces derniers ne considèrent que les degrés et l'écriture dans la représentation dense comme structure de données. Nous aimerions signaler ici que l'approche due à [Berenstein-Yger, 1991] pourrait contenir la possibilité d'un codage court des quotients dans l'identité de Bézout.

Notre nouvelle version du Nullstellensatz a été conjecturée par E. Kaltofen en 1988 (et par bien d'autres sans doute). Elle fera l'objet d'une publication ultérieure ([Giusti-Heintz-Sabia, 1991]).

3. Situation affine

3.1. Préliminaires

Soit k un anneau intègre comme dans 1.1 et k' son corps des fractions. Soient $f_1, \ldots, f_s$ des polynômes non constants de $k[x_1, \ldots, x_n]$, et $g_1, \ldots, g_s$ des polynômes homogènes de $k[x_0, x_1, \ldots, x_n]$, qui pourront être par exemple les homogénéisés des f_i ; dans ce cas, x_0 sera la variable d'homogénéisation. Nous supposerons que les degrés des polynômes $f_1, \ldots, f_s$ et $g_1, \ldots, g_s$ sont majorés par d, avec $d \geq n$.
Nous allons nous intéresser à la variété algébrique affine V définie par l'idéal $I := (f_1, \ldots, f_s)$ (resp. à la variété algébrique projective W définie par l'idéal $J := (g_1, \ldots, g_s)$), dans une clôture algébrique de k'. Dans le cas où les g_i sont les homogénéisés des f_i (éventuellement multipliés par une puissance de x_0), nous pouvons considérer V comme un sous-ensemble de W ; à ce titre, observons que les points isolés de V sont des points isolés de W.

C'est à la détermination de ces derniers que nous allons d'abord nous intéresser. Ce pas nous servira de lemme technique pour la suite, mais son intérêt pratique évident en fait un résultat primordial en soi.

Dans le cadre affine où nous sommes, il faut déformer les équations pour se ramener, d'abord au cas localement intersection complète, puis au cas projectif de dimension zéro.

3.2. Le cas de la dimension projective zéro

Soit $J := (g_1, \ldots, g_s)$ un idéal homogène tel que la variété W qu'il définit ne contienne qu'un nombre fini non nul de points (autrement dit de dimension projective zéro), aucun d'entre eux n'étant contenu dans l'hyperplan $x_0 = 0$ (que nous appellerons par commodité "l'hyperplan à l'infini").

Le lemme suivant reprend les idées et les résultats contenus dans l'article fondamental de D. Lazard ([Lazard, 1981]).

3.2.1. Lemme

Plaçons nous sous les hypothèses ci-dessus. Soit l une forme linéaire indépendante de x_0. Il existe dans l'idéal engendré par $g_1, \ldots, g_s$ dans $k'[x_0, \ldots, x_n]$ un polynôme h ne dépendant que des variables x_0 et l, à coefficients dans k, de degré majoré par $d^n + (n+1)d$, calculable par un algorithme bien parallélisable sans divisions, et ceci en temps séquentiel $s^{O(1)} d^{O(n)}$. De plus, les coefficients de h sont des polynômes de degré $d^{O(n)}$ en les coefficients de $g_1, \ldots, g_s$ sur l'anneau premier de k. Le degré de h en l est strictement positif et borné par d^n.

Démonstration : Observons que le degré (au sens classique défini par le polynôme de Hilbert) de l'idéal engendré par $g_1, \ldots, g_s$ dans $k'[x_0, \ldots, x_n]$ est majoré par d^n (voir par exemple [Fitchas-Galligo, 1990] pour détails). Par ailleurs, la régularité de la fonction de Hilbert est largement majorée par l'entier $N = (n+1)d$ ([Lazard, 1981], [Briançon, 1983]). Soient A l'anneau quotient gradué $k'[x_0, \ldots, x_n]/(g_1, \ldots, g_s)$ et A_ν sa partie homogène de degré ν, qui est un k'-espace vectoriel de dimension finie. Par définition de la régularité, dès que ν dépasse l'entier N, cette dimension est égale au degré de l'idéal, donc au plus d^n.

Notons $\overline{}$ l'homomorphisme canonique surjectif de degré zéro $k'[x_0, \ldots, x_n] \longrightarrow A$, et faisons le raisonnement général suivant :

Soit L une forme linéaire de $k[x_0, \ldots, x_n]$ telle que $\overline{L}$ induise par multiplication une application k'-linéaire bijective $\overline{L}\ : A_N \longrightarrow A_{N+1}$. Soit F une forme homogène à coefficients dans k de degré strictement positif δ. Nous obtenons donc par composition un endomorphisme $\phi\ := \overline{L}^{-\delta} \circ \overline{F}$ de A_N. Pour A_N et $A_{N+\delta}$, nous calculons une base monomiale ainsi que les relations de dépendance k-linéaire entre les monômes, ce qui correspond à trianguler deux matrices d'ordre au plus $O(sN^n)$ et $O(s(N+\delta)^n)$, ce qui peut se faire par un algorithme bien parallélisable en temps séquentiel $s^{O(1)}(N+\delta)^{O(n)}$ sans divisions. Nous pouvons maintenant calculer la matrice de ϕ dans ces bases, puis son polynôme caractéristique $\chi(\phi)$ par l'algorithme de Berkowitz, et ce avec la même complexité. En prémultipliant ϕ par un élément non nul approprié de k, provenant du calcul des bases monomiales de A_N, $A_{N+\delta}$ et des coefficients de L, nous pouvons supposer sans restriction de généralité que les entrées de la matrice ϕ appartiennent à k. Notons que tout ceci se fait sans divisions et que le degré de $\chi(\phi)$ est égal à celui de l'idéal, lui-même majoré par d^n. En homogénéisant $\chi(\phi)$, nous obtenons un polynôme homogène en deux variables Δ, à coefficients dans k et de même degré. Le théorème de Cayley-Hamilton implique alors que $\overline{L}^N \Delta(\overline{L}^\delta, \overline{F})$ est identiquement nul.
Observons aussi que par construction, le polynôme Δ est unitaire en la deuxième variable, et qu'il est calculable avec la même complexité sans divisions. En particulier, nous avons l'appartenance de $L^N \Delta(L^\delta, F)$ à l'idéal $(g_1, \ldots, g_s)$. Nous voyons immédiatement que, par construction, les coefficients de Δ sont des polynômes de degré $(N+\delta)^{O(n)}$ en les coefficients de $g_1, \ldots, g_s$ sur l'anneau premier de k.

Vu l'hypothèse que l'idéal J ne définit pas de points à l'infini, l'idéal $J + (x_0)$ ne définit aucun point du tout ; en lui appliquant le Nullstellensatz projectif effectif ([Lazard, 1977], ou [Briançon, 1983]), nous voyons que la multiplication par x_0 induit une application bijective de A_N dans A_{N+1}. Il nous suffit maintenant de spécialiser le raisonnement général précédent au cas $L = x_0$ et $F = l$ pour obtenir le polynôme h recherché par un algorithme bien parallélisable sans divisions en temps séquentiel $s^{O(1)}\,(N+1)^{O(n)}$, ce qui compte-tenu de l'hypothèse $d \geq n$, est en $s^{O(1)}\,d^{O(n)}$.

3.3. Le cas où les points isolés sont localement intersection complète

3.3.1. Notations

Nous avons donc autant d'équations que d'inconnues ($s = n$). Nous aurons aussi besoin d'une indéterminée supplémentaire ε, qui pourra être considérée soit comme une variable, soit comme un paramètre.

Nous allons établir deux lemmes géométriques permettant de relier la situation affine à la situation projective par une déformation le long de l'axe ε. Plus précisément, celle-ci sera plate au dessus de l'ouvert $\varepsilon \neq 0$.

Cette approche "homotopique" par déformation des équations est bien connue en Analyse Numérique (voir par exemple [Zangwill - Garcia, 1981]). Elle a été introduite par Chistov-Grigoriev dans les études de complexité en géométrie algébrique effective [Chistov-Grigoriev, 1983], puis réutilisée par [Canny, 1988 a, b], [Lakshman, 1991], et [Lakshman-Lazard, 1991].

Soit p_i le produit de l'homogénéisé du polynôme f_i par x_0, et g_i le polynôme $p_i + \varepsilon {x_i}^{1+\deg f_i}$ $(i = 1, \ldots, n)$.

Nous allons considérer la sous-variété V de $\mathbf{A}^n$, lieu des zéros communs aux f_i, comme incluse dans la sous-variété S de $\mathbf{P}^n$, lieu des zéros communs aux p_i, elle-même incluse dans la sous-variété W de $\mathbf{A}^1 \times \mathbf{P}^n$, lieu des zéros communs aux g_i. A ce titre, les points isolés de V restent des points isolés de S.

La restriction à W de la projection canonique de $\mathbf{A}^1 \times \mathbf{P}^n$ sur $\mathbf{A}^1$ sera notée π. Ainsi, S devient la fibre en zéro de π, et tout point isolé de V appartient à une composante irréductible de W et se projette par π sur zéro. Soit C une composante irréductible de W contenant un point de V. Sa projection par π ne peut être que $\mathbf{A}^1$ tout entier ou l'origine.

Quand nous considérerons π comme section globale du faisceau structural de W, nous le noterons par abus de notation encore ε. Ainsi, quand une composante irréductible C de W se projette sur $\mathbf{A}^1$ tout entier, le localisé $C_\varepsilon = \{y \in C \mid \varepsilon(y) \neq 0\}$ est un ouvert de Zariski non vide.

3.3.2. Lemme de localisation

Soit x un point isolé de V, et soit C une composante irréductible de W contenant x. Alors le localisé C_ε est non vide.

Démonstration : Comme W est une sous-variété définie par n équations dans un espace ambiant de dimension $n+1$, toutes ses composantes irréductibles ont une dimension au moins 1. Soit x un point isolé de V, et C une composante irréductible de W passant par lui. Il suffit de démontrer qu'elle se projette sur $\mathbf{A}^1$ tout entier. Si ce n'était pas le cas, elle se projetterait sur l'origine, et donc serait incluse dans S. Sa partie affine dans V serait toujours de dimension au moins 1, et passant par le point x contradirait le fait que ce dernier est isolé.

Dans le lemme précédent, ε était considéré comme une variable. Dans le lemme suivant, il sera considéré comme un paramètre contenu dans une clôture algébrique $\overline{k'(\varepsilon)}$ de $k'(\varepsilon)$. Ainsi, les polynômes g_i seront maintenant des polynômes de $k[\varepsilon][x_0, \ldots, x_n]$.

3.3.3. Lemme de déformation

Avec les remarques précédentes, les g_i $(i = 1, \ldots, n)$ définissent une sous-variété projective de $\mathbf{P}^n(\overline{k'(\varepsilon)})$ de dimension 0.

Pour trancher un peu parmi les démonstrations bien connues de ce lemme très apprécié de nombreux auteurs, nous allons en donner une preuve purement géométrique.

La variété à étudier peut aussi être définie par les polynômes $\frac{1}{\varepsilon}g_i$. Introduisons alors l'indéterminée $t = \frac{1}{\varepsilon}$; la variété devient la fibre générique du morphisme π exprimée dans les nouvelles coordonnées. Mais la fibre en $t = 0$ de ce morphisme étant trivialement de dimension 0, le lemme se déduit immédiatement de la classique semi-continuité de la dimension.

3.3.4. Proposition

Soient $I = (f_1, \ldots, f_n)$ un idéal et l une forme linéaire de $k[x_1, \ldots, x_n]$, suivant les notations de 3.1. Il existe un algorithme bien parallélisable et sans divisions qui calcule en temps $d^{O(n)}$ un polynôme non nul p de $k[l]$, de degré au plus $(d+1)^n$, qui s'annule en tout point isolé de V. De plus, tous les résultats intermédiaires de l'algorithme sont des polynômes de degré $d^{O(n)}$ en les coefficients des entrées $f_1, \ldots, f_n$ sur l'anneau premier de k.

Démonstration : Comme dans 3.3.1, nous construisons des polynômes g_i à partir des f_i. Par abus de notation, nous appellerons encore l le polynôme de $k[x_0, \ldots, x_n]$ homogénéisé du polynôme affine donné l. D'après 3.2.1 et 3.3.3, nous pouvons calculer un polynôme h de $k[\varepsilon][x_0, l]$, homogène en les variables x_0 et l, de degré en l borné par $(d+1)^n$. Il appartient à l'idéal engendré par $g_1, \ldots, g_n$ dans $k'(\varepsilon)[x_0, \ldots, x_n]$ et, considéré comme polynôme en x_0 et l, ses coefficients sont des polynômes de $k[\varepsilon]$ dont l'écriture requiert $d^{O(n)}$ opérations arithmétiques dans l'anneau $k[\varepsilon]$. En effet nous évitons les divisions dans l'anneau intègre $k[\varepsilon]$ en utilisant les algorithmes entiers d'algèbre linéaire bien parallélisable introduits par [Berkowitz, 1984] et [Mulmuley, 1986]. Dans ces calculs n'apparaissent que des coefficients polynômes en ε de degré au plus $d^{O(n)}$. En particulier, le résultat h obéit à cette observation, et tous les calculs peuvent se transférer à l'anneau de base k en $d^{O(n)}$ opérations arithmétiques. Ce polynôme h appartient à l'idéal engendré par $g_1, \ldots, g_n$ dans l'anneau $k'(\varepsilon)[x_0, \ldots, x_n]$, et s'annule donc sur le localisé W_ε de la variété W défini dans 3.3.1. Nous réduisons h en un polynôme h' en le divisant par la plus grande puissance de ε de son contenu. Evidemment, h' s'annule sur le localisé W_ε. Il s'écrit comme somme d'un polynôme h'_0 constant et non nul en ε, et d'un reste divisible par ε. Maintenant soit $x = (x_1, \ldots, x_n)$ un point isolé de V, et soit C une composante irréductible de W passant par x. Pour mettre les points sur les ı, comme le désire le second auteur, ceci veut dire en bon français : $(0, (1 : x_1 : \cdots : x_n)) \in C$. (Que ceux qui ne comprennent pas le français élémentaire arrêtent là la lecture du texte, c'est désespéré). D'après le lemme 3.3.2, C_ε est un ouvert non vide de l'ensemble irréductible C. Le polynôme h' s'y annule, donc aussi sur C tout entier. Ceci implique, toujours en bon français, que $h'_0(1 : x_1 : \cdots : x_n) = 0$. Le déshomogéisé p de h'_0 est le polynôme recherché.

3.4. Le cas général

Jusqu'à maintenant, tous les algorithmes mentionnés étaient uniformes et dans le cas de l'anneau de base des entiers, traduisibles en algorithmes éxécutables par des machines de Turing en temps $(st)^{O(1)}d^{O(n)}$. Dorénavant, nous sommes obligés de considérer également des algorithmes non uniformes.

Si la variété V contient des points isolés, d'après le Hauptidealsatz de Krull, nous devons disposer de plus d'équations que d'inconnues ($s \geq n$).

3.4.1. Lemme de construction d'une famille sécante

Etant donné un élément τ de $\overline{k'}$, nous définissons le polynôme $\hat{f}_\tau$ comme la combinaison linéaire $f_1 + \tau^1 f_2 + \cdots + \tau^{s-1} f_s$.

Choisissons un sous-ensemble Γ de l'anneau de base k, de cardinal $sd^n + 1$. Il existe un point $\gamma = (\gamma_1, \ldots, \gamma_n)$ de Γ^n tel que chaque composante de V est une composante de $\hat{V}$, définie par les *polynômes $\hat{f}_{\gamma_1}, \ldots, \hat{f}_{\gamma_n}$. De plus, les composantes de $\hat{V}$ qui ne sont pas composantes de V sont réduites à un point.*

Démonstration : (voir [Heintz, 1983] et [Giusti-Heintz, 1991]) nous démontrons par récurrence sur i ($1 \leq i \leq n$) qu'il existe dans Γ des points $\gamma_1, \ldots, \gamma_i$ tels que la dimension de toute composante irréductible de $\{\hat{f}_{\gamma_1} = \cdots = \hat{f}_{\gamma_i} = 0\}$ non contenue dans V soit $n - i$.

Le cas $i = 1$ est évident. Pour les valeurs supérieures, supposons que l'assertion soit vraie pour $i - 1$. Dans chaque composante irréductible C de la sous-variété $\hat{f}_{\gamma_1} = \cdots = \hat{f}_{\gamma_{i-1}} = 0$, non contenue dans V, choisissons un point x_C à l'extérieur de V. En conséquence, au moins un des polynômes $f_1, \ldots, f_s$ ne s'annule pas au point x_C. Introduisons alors une nouvelle indéterminée T et le polynôme à une variable $w_C(T) := f_1(x_C) + T f_2(x_C) + \cdots + T^{s-1} f_s(x_C)$ de considéré à coefficients dans la clôture algébrique $\overline{k}'$ de k' ; il n'est pas identiquement nul par construction, ainsi que le produit $\prod_C w_C(T)$ étendu à toutes les composantes de $\hat{f}_{\gamma_1} = \cdots = \hat{f}_{\gamma_{i-1}} = 0$ non contenues dans V. Comme le degré de ce dernier polynôme est au plus sd^n, il ne peut pas s'annuler sur tout l'ensemble Γ qui est de cardinal $sd^n + 1$; soit donc γ_i un élément de Γ qui ne l'annule pas. La combinaison linéaire $\hat{f}_{\gamma_i} = f_1 + {\gamma_i}^1 f_2 + \cdots + \gamma_i^{s-1} f_s$ ne s'annule en aucun des points x_C, pour toute composante C de $\hat{f}_{\gamma_1} = \cdots = \hat{f}_{\gamma_{i-1}} = 0$ non contenue dans V. Une telle composante, de dimension $n - i + 1$ par hypothèse de récurrence, est donc coupée proprement par l'hypersurface $\hat{f}_i = 0$, ce qui démontre notre assertion.

Avec les notations introduites ci-dessus, nous obtenons immédiatement la conséquence suivante :

3.4.2. Corollaire de densité

L'ensemble des points $\gamma = (\gamma_1, \ldots, \gamma_n)$ de k^n, tels que la variété $\hat{V}$, définie par les polynômes $\hat{f}_{\gamma_1}, \ldots, \hat{f}_{\gamma_n}$ consiste en la réunion de V et d'un nombre fini de points, est Zariski-dense dans $\mathbf{A}^n$.

Nous noterons $U(f_1, \ldots, f_s)$, ou plus simplement U, ce sous-ensemble dense de k^n.

3.4.3. La famille sécante générique

Soient $T_1, \ldots, T_n$ n nouvelles indéterminées. Nous noterons π la restriction de la première projection à la sous-variété S de $\mathbf{A}^n \times \mathbf{A}^n$ définie par les polynômes $f_1 + T_i f_2 + \cdots + {T_i}^{s-1} f_s$ ($1 \leq i \leq n$). Pour chaque point t de $\mathbf{A}^n$, la variété $\{t\} \times V$ est incluse dans la fibre $\pi^{-1}(t)$.

Lemme : *Soit x un point isolé de $V = \{f_1 = \cdots = f_s = 0\}$, et d'après le corollaire 3.4.2 soit γ un point $(\gamma_1, \ldots, \gamma_n)$ de k^n tel que toute composante de V soit une composante de $\{\hat{f}_{\gamma_1} = \cdots = \hat{f}_{\gamma_n} = 0\}$. Soit C une composante irréductible de S passant par le point (γ, x). Alors sa dimension est n et le localisé C_G est non vide pour tout polynôme non nul G de $k[T_1, \ldots, T_n]$.*

Démonstration : Comme S est défini par n équations dans un espace ambiant de dimension $2n$, la dimension de chacune de ses composantes est au moins n. Par construction, le point γ appartient à la projection de C, et le point (γ, x) est isolé dans $C \cap \pi^{-1}(\gamma)$. La semi-continuité de la dimension de la fibre implique que $\overline{\pi(C)}$ et C ont même dimension. Comme $\dim C$ est au moins n et $\dim \overline{\pi(C)}$ au plus n, nous obtenons l'égalité $\dim \overline{\pi(C)} = \dim C = n$. En particulier aucun polynôme non nul G de $k[T_1, \ldots, T_n]$ ne s'annule sur $\overline{\pi(C)}$ et donc sur C.

3.4.4. Observation

Avec les notations du lemme 3.4.3, nous avons un morphisme injectif de $k'[T_1,\ldots,T_n]$ dans $k'[C]$. Ce dernier peut être considéré comme module sur le précédent, mais comme ils ont même dimension n, le localisé $k'[C]\otimes_{k'[T_1,\ldots,T_n]} k'(T_1,\ldots,T_n)$ est de dimension zéro. Une composante C de S qui passe par (γ,x) correspond donc à un point isolé de la variété défini par les n polynômes $f_1+T_if_2+\cdots+T_i^{s-1}f_s$ $(1\leq i\leq n)$ dans l'espace affine de dimension n sur la clôture algébrique du corps $k'(T_1,\ldots,T_n)$.

3.4.5. Lemme

Il existe une constante universelle $c>0$ telle que, pour toute forme linéaire l de $k[x_1,\ldots,x_n]$, il existe un polynôme non nul p dans $k[l]$ de degré majoré par d^{cn}, qui s'annule sur tout point isolé x de $V=\{f_1=\cdots=f_s=0\}$.
Au prix d'une préparation préalable, ce polynôme p est calculable par un algorithme sans divisions en temps séquentiel majoré par $(sd^n)^c$, et en temps parallèle majoré par $cn^2\log^2 sd$. De plus, tous les résultats intermédiaires de l'algorithme sont des polynômes de degré au plus d^{cn} en les coefficients des entrées $f_1,\ldots,f_s$ sur un sous-anneau approprié de k de type fini.
Cette préparation préalable dépend seulement des paramètres s,d,n, mais ni des coefficients de $f_1,\ldots,f_s$ ni de la forme l.

Démonstration : Nous utiliserons les notations de 3.4.2 et 3.4.3. Soit x un point isolé de V, s'il existe, et γ un point de U. Observons que l'ensemble irréductible et fermé $\mathbf{A}^n\times\{x\}$ est contenu dans S. Il existe une composante irréductible C de S qui contient $\mathbf{A}^n\times\{x\}$. Comme C contient le point (γ,x), nous pouvons appliquer le lemme 3.4.3. La dimension de C est donc n et l'homomorphisme canonique $k'[T_1,\ldots,T_n]\rightarrow k'[C]$ est injectif. D'après 3.4.4 et 3.3.4, nous pouvons calculer en $ns+d^{O(n)}$ opérations arithmétiques dans l'anneau $k[T_1,\ldots,T_n]$ un polynôme non constant P dans $k[T_1,\ldots,T_n,l]$ tel que P s'annule sur un ouvert non vide de C, donc sur tout C. Comme C contient l'ensemble $\mathbf{A}^n\times\{x\}$, nous en déduisons que $P(\gamma',l(x))$ est nul pour tout γ' dans $\mathbf{A}^n$. Le degré partiel de P en l est un $d^{O(n)}$ et le degré total un $sd^{O(n)}$. En utilisant les méthodes à la Berkowitz-Mulmuley, les coefficients de P, considéré comme polynôme en la variable l à coefficients dans $k[T_1,\ldots,T_n]$, se calculent sans divisions par des calculs d'évaluation dans $k[T_1,\ldots,T_n]$. Soit v la longueur du calcul qui évalue les coefficients de P, qui sont de degré borné par $sd^{c'n}$ pour un c' approprié. Cette longueur v est un $ns+d^{O(n)}$. Choisissons un ensemble Γ dans k, de cardinal $2v(1+sd^{c'n})^2=s^{O(1)}d^{O(n)}$. D'après [Heintz - Schnorr, 1982, Theorem 4.4], il existe un ensemble questeur $(\gamma_1,\ldots,\gamma_m)$ de points de Γ^m où m est égal à $6(v+n)(v+n+1)=s^{O(1)}d^{O(n)}$. Comme P est non nul, il existe un indice j compris entre 1 et m tel que $P(\gamma_j,l)$ soit non nul. Le polynôme de $P(\gamma_j,l)$ est le polynôme p de $k[l]$ recherché ; il est non nul, son degré est un $d^{O(n)}$, et son écriture requiert $s^{O(1)}d^{O(n)}$ opérations arithmétiques dans le corps de base k, et enfin il vérifie :

$$p(l(x))=P(\gamma_j,l(x))=0.$$

De la construction, nous déduisons que les coefficients de p sont des polynômes de degré $d^{O(n)}$ en les coefficients de $f_1,\ldots,f_s$ sur l'anneau $\Omega[\gamma_j]$, où Ω est l'anneau premier de k.

3.4.6. Lemme dit de l'élément primitif

Dans ce paragraphe nous démontrons un résultat technique qui représente une généralisation convenable des versions effectives connues du théorème de l'élément primitif dans la théorie des extensions de corps (voir [Canny, 1988 a, b] et [Heintz-Roy-Solernó, 1990]).

Soit k un corps. Au prix d'une préparation préalable, nous pouvons calculer en temps séquentiel $s^{O(1)}d^{O(n)}$ et en temps parallèle $O(n^3 \log^2 sd)$ une forme linéaire y de $k[x_1, \ldots, x_n]$ et des polynômes $r_1, \ldots, r_n$ de $k[y]$, de degré $d^{O(n)}$, vérifiant : pour tout point isolé $x = (x_1, \ldots, x_n)$ de V, la coordonnée x_i ($1 \leq j \leq n$) est égale à $r_i(y(x))$. Nous dirons que la variable y est en position générale par rapport aux points isolés de V.

Le résultat va être une conséquence immédiate du lemme technique suivant, dont la démonstration va se faire par récurrence.

Fixons nous un ensemble Γ de $d^{4cn}+1$ valeurs non nulles du corps de base k (c est la constante universelle introduite dans 3.4.5). Soit i un indice compris entre 1 et n. Il existe des constantes universelles $C > 0$ et $c'' > 0$ telles qu'au prix d'une préparation préalable, nous pouvons calculer par un algorithme en temps séquentiel $iC(sd^n)^{c''}$ et parallèle $iCn^2 \log^2 sd$, une forme linéaire $y_i = \gamma_1^{(i)}x_1 + \cdots + \gamma_i^{(i)}x_i$ de $k[x_1, \ldots, x_i]$, à coefficients des éléments de Γ, et des polynômes $r_1^{(i)}, \ldots, r_i^{(i)}$ de $k[y_i]$, de degré au plus d^{cn}, vérifiant : pour tout point isolé $x = (x_1, \ldots, x_n)$ de V, la coordonnée x_j ($1 \leq j \leq i$) est égale à $r_j^{(i)}(y_i(x))$.

Démonstration : Supposons sans restriction de généralité que V contienne un point isolé. Au départ, pour i égal à 1, nous prenons $y_1 := x_1$ et $r_1 := x_1$.
Maintenant, soit i un indice au moins égal à 2, et supposons le lemme acquis à l'ordre $i-1$ et la variable y_{i-1} donnée.
D'après le même lemme 3.4.5, nous calculons en temps séquentiel $(sd^n)^c$ et parallèle $cn^2 \log^2 sd$ deux polynômes $p(y_{i-1})$ dans $k[y_{i-1}]$ et $q(x_i)$ dans $k[x_i]$, de degré au plus d^{cn}, qui s'annulent sur tout point isolé de V. Considérons l'idéal de hauteur 2 engendré par p et q dans $k[y_{i-1}, x_i]$, et son radical N. D'après [Krick - Logar, 1991] nous calculons à partir de p et de q des générateurs $\hat{p}, \hat{q}$ de N en temps séquentiel et parallèle au plus $d^{c'n}$ et $c'n^2 \log^2 d$, où $c' \geq 2c$ est suffisamment grand. Notons que l'hypothèse du corps de base parfait est ici indispensable, puisqu'il faut extraire des racines $p^{\text{ième}}$ si la caractéristique est positive. Comme le degré de l'idéal N est au plus d^{2cn}, il existe dans Γ un élément γ_i tel que la forme linéaire $y_i := y_{i-1} + \gamma_i x_i$ sépare les points de $\{\hat{p} = \hat{q} = 0\} \subset \mathbf{A}^2$. Changeons de variables, et considérons $N = (\hat{p}, \hat{q})$ comme idéal de $k[y_{i-1}, y_i]$. Par construction, y_i sépare les points définis par N. Calculons alors une base standard de N à partir des générateurs $\hat{p}$ et $\hat{q}$ relativement à l'ordre lexicographique de $k[y_{i-1}, y_i]$ induit par $y_{i-1} > y_i$. Ceci peut se faire en temps séquentiel et parallèle majoré respectivement par $d^{c'n}$ et $c'n^2 \log^2 d$, la constante c' étant suffisamment grande. Une telle base standard a deux générateurs de la forme $u, y_{i-1} - v$, où u et v sont des polynômes de degré au plus $d^{2cn} \leq d^{c'n}$ ne dépendant que de la variable y_i. Comme x_i est une combinaison k-linéaire de y_{i-1} et y_i, il est congru modulo l'idéal N à un polynôme r de degré au plus $d^{c'n}$ en la seule variable y_i, et le calcul de r à partir de v ne demande qu'un temps constant. Mais d'après le lemme 3.4.5, nous pouvons calculer en temps séquentiel $(sd^n)^c$ et parallèle $cn^2 \log^2 sd$ un polynôme non nul h de $k[y_i]$, de degré au plus d^{cn}, qui s'annule en tout point isolé de V. Le reste de la division de r par h nous fournit le polynôme $r_i^{(i)}$ recherché, qui est de degré au plus d^{cn}, en temps $d^{c'n}$. En effet tout point isolé $x = (x_1, \ldots, x_n)$ annule $p(y_{i-1})$ et $q(x_i)$, donc tous les éléments de N, donc $x_i = r(y_i(x))$ et enfin $x_i = r_i^{(i)}(y_i(x))$.
Pour obtenir les polynômes $r_1^{(i)}, \ldots, r_i^{(i)}$, il suffit de remplacer la variable y_{i-1} par $v(y_i)$ dans les polynômes $r_1^{(i-1)}, \ldots, r_{i-1}^{(i-1)}$, puis de les réduire modulo h. Nous calculons ces polynômes de

degré au plus d^{cn} en temps séquentiel $d^{c'n}$ et parallèle $c'n^2\log^2 d$, à partir de $r_1^{(i-1)},\dots,r_{i-1}^{(i-1)}, v, h$ (la constante c' étant suffisamment grande). Ils conviennent, puisque pour tout point isolé $x = (x_1,\dots,x_n)$ et tout indice j compris entre 1 et $i-1$, nous avons :

$$x_j - r_j^{(i)}(y_i(x)) = x_j - r_j^{(i-1)}(v(y_i(x))) = x_j - r_j^{(i-1)}(y_{i-1}(x)) = 0.$$

Comme par hypothèse de récurrence y_{i-1} et $r_1^{(i-1)},\dots,r_{i-1}^{(i-1)}$ sont calculables en temps séquentiel $(i-1)C(sd^n)^{c''}$ et parallèle $(i-1)Cn^2\log^2 sd$ (où les constantes C et c'' sont encore à choisir de manière appropriée), il existe une constante universelle C_1 (indépendante de d, s, n et i) telle que y_i et $r_1^{(i)},\dots,r_i^{(i)}$ s'obtiennent en temps séquentiel $(i-1)C(sd^n)^{c''}+C_1((sd^n)^c+d^{c'n}) \le (i-1)C(sd^n)^{c''}+2C_1(sd^n)^{\max\{c,c'\}}$. Nous choisissons la constante c'' supérieure ou égale à $\max\{c,c'\}$ et la constante C supérieure ou égale à $2C_1$ pour que $(i-1)C(sd^n)^{c''}+2C_1(sd^n)^{\max\{c,c'\}}$ soit majoré par $iC(sd^n)^{c''}$. De la même manière, nous choisissons la constante C suffisamment grande pour que les polynômes y_i et $r_1^{(i)},\dots,r_i^{(i)}$ s'obtiennent en temps parallèle $iCn^2\log^2 sd$.

3.4.7. Un raffinement du lemme de l'élément primitif

Dans 3.4.6 nous avons démontré que pour un ensemble Γ fixé à l'avance, contenu dans k et de cardinal $d^{O(n)}$, nous pouvons trouver en temps séquentiel $s^{O(1)}d^{O(n)}$ et parallèle $O(n^3\log^3 sd)$ une forme linéaire $y = \gamma_1 x_1 + \cdots + \gamma_n x_n$ $(\gamma_1,\dots,\gamma_n \in \Gamma)$, qui possède la propriété d'élément primitif énoncé dans ce lemme. De plus, notre algorithme faisait appel à des divisions par des éléments de k qui étaient calculables en temps séquentiel $s^{O(1)}d^{O(n)}$ comme polynômes de degré $d^{O(n)}$ en les coefficients de $f_1,\dots,f_s$.
Pour certaines applications du lemme de l'élément primitif, le cardinal en $d^{O(n^2)}$ de Γ^n et l'existence des divisions contenues dans l'algorithme présentent un inconvénient si k est un anneau intègre. De plus, l'algorithme de 3.4.6 n'est pas bien parallélisable au sens défini dans 1.3. Si nous remplaçons dans la démonstration du lemme 3.4.6 les éléments $\gamma_1,\dots,\gamma_n$ de Γ par de nouvelles indéterminées $T_1,\dots,T_n$ servant de paramètres nous pouvons appliquer les arguments de la preuve du lemme 3.4.5 basés sur [Heintz, Schnorr, 1982, Theorem 4.4] et spécialiser $T_1,\dots,T_n$ en des éléments de k convenablement choisis. En multipliant par les dénominateurs adéquats de $k[T_1,\dots,T_n]$ nous évitons les divisions. Les formes linéaires y_i et les polynômes p, q, $\hat{p}$, $\hat{q}$ et h apparaissant dans la preuve du lemme de 3.4.6 sont maintenant calculables à l'avance (pour chaque indice i compris entre 1 et n) ce qui rend notre algorithme bien parallélisable. Ainsi nous obtenons le raffinement suivant du lemme 3.4.6 :

Au prix d'une préparation préalable nous pouvons trouver pour d, s, n fixés un ensemble questeur $\gamma_1,\dots,\gamma_m$ de points de k^n de cardinal $m = s^{O(1)}d^{O(n)}$ possédant la propriété suivante :

Pour chaque variété affine V donnée par des polynômes $f_1,\dots,f_s$ de degré borné par d (où d est au moins égal à n), nous pouvons calculer en temps $s^{O(1)}d^{O(n)}$ par un algorithme bien parallélisable et **sans divisions** *un élément α non nul de k, un élément $\gamma_i = (\gamma_1^{(i)},\dots,\gamma_n^{(i)})$ de l'ensemble questeur, et en posant $y := \gamma_1^{(i)}x_1 + \cdots + \gamma_n^{(i)}x_n$, des polynômes $r_1,\dots,r_n$ de degré $d^{O(n)}$ tels que chaque point isolé x de V satisfasse $\alpha\, x = (r_1(y(x)),\dots,r_n(y(x)))$. Les coordonnées des points questeurs $\gamma_1,\dots,\gamma_m$ peuvent être choisis dans un sous-ensemble Γ de k, fixé à l'avance et de cardinal $s^{O(1)}d^{O(n)}$.*

3.4.8. Observation : reconstruction des points isolés d'une variété affine arbitraire

La mise bout à bout des lemmes 3.4.5 et 3.4.6 explique comment nous pouvons "reconstruire" en temps $s^{O(1)}d^{O(n)}$ tous les points isolés de la variété V. Cette observation a d'abord été faite par J. Canny dans le cas $s = n$ [Canny, 1988 a, b] et a été appliquée au cas réel par [Renegar, 1992].

Remarquons de plus que si nous considérons les polynômes $p_j := f_j(r_1, \ldots, r_n)$ de $k[y]$ $(1 \le j \le s)$, et leur plus grand commun diviseur q, nous voyons que leur degré est un $d^{O(n)}$ et qu'ils sont calculables en temps $s^{O(1)}d^{O(n)}$. De plus, nous obtenons les deux implications suivantes :

1. Si V contient des points isolés, le pgcd q n'est pas constant.
2. Réciproquement, si ce pgcd est non constant, la variété V n'est pas vide.

La démonstration est une conséquence immédiate du lemme 3.4.6. L'algorithme sous-jacent repose sur des techniques d'algèbre linéaire effective dans k (à la Berkowitz-Mulmuley, comparer 3.4.7). Il peut donc être exécuté sans utiliser de divisions. Tous les résultats intermédiaires de cet algorithme sont des polynômes de degré $d^{O(n)}$ en les coefficients de $f_1, \ldots, f_s$ sur un sous-anneau approprié de k de type fini. Ils s'évaluent en temps $s^{O(1)}d^{O(n)}$.

3.5. Calcul de la dimension d'une variété affine

Nous conservons les notations introduites en 3.1.

Théorème : *Au prix d'une préparation préalable, nous pouvons calculer la dimension de la variété affine V en temps $s^{O(1)}d^{O(n)}$ par un algorithme bien parallélisable qui ne contient aucune division.*

Démonstration : Soient T_{ij} et T_i $(1 \le i, j \le n)$ des nouveaux paramètres, R le nouvel anneau de base $k[T_{i,j}, T_i;\ 1 \le i, j \le n]$ et K une clôture algébrique du corps des fractions de R.
Pour tout indice i compris entre 1 et n, définissons la forme affine l_i comme le polynôme $T_{i1}x_1 + \cdots + T_{in}x_n + T_i$ de $R[x_1, \ldots, x_n]$.
Soit r le nombre maximal de formes $l_1, \ldots, l_r$ tels que la sous-variété de l'espace affine $\mathbf{A}^n(K)$ défini par l'idéal $(f_1, \ldots, f_s, l_1, \ldots, l_r)$ de $K[x_1, \ldots, x_n]$ soit non vide. Cette variété ne contient que des points isolés, et r est la dimension de V.
Considérons la suite d'idéaux $(f_1, \ldots, f_s) \subseteq (f_1, \ldots, f_s, l_1) \subseteq \ldots \subseteq (f_1, \ldots, f_s, l_1, \ldots, l_n)$. L' observation 3.4.8 et 3.4.7 impliquent que nous pouvons déterminer r par un algorithme bien parallélisable qui utilise $s^{O(1)}d^{O(n)}$ opérations arithmétiques dans R sans aucune division. Les résultats intermédiaires de cet algorithme sont des éléments de R, c'est-à-dire des polynômes à coefficients dans k en les $n^2 + n$ variables T_{ij}, T_i. D'après 3.4.8 ces polynômes sont de degré $d^{O(n)}$, et sont donnés par un calcul d'évaluation bien parallélisable de complexité séquentielle $s^{O(1)}d^{O(n)}$ qui ne contient aucune division. Pour obtenir r par un réseau arithmétique sur k il suffit de déterminer lesquels de ces polynômes sont non nuls; et pour le tester, nous appliquons encore une fois [Heintz-Schnorr 1982, Theorem 4.4] en utilisant un ensemble questeur de $s^{O(1)}d^{O(n)}$ points de k^{n^2+n} (comparer à la démonstration du lemme 3.4.5). Le coût de cette procédure consiste en $s^{O(1)}d^{O(n)}$ opérations arithmétiques dans k.

Ce dernier théorème peut être raffiné comme suit :

3.5.1. Lemme

Soient k' le corps des fractions de k et r la dimension de V. Nous dirons que les variables $x_1, \ldots, x_r$ sont *libres* par rapport à V si la condition suivante est satisfaite :

$$(i) \quad k[x_1, \ldots, x_r] \cap (f_1, \ldots, f_s) = 0$$

Nous dirons que la variable x_i $(r < i \leq n)$ est *en position de Noether* par rapport à $x_1, \ldots, x_r$ et V s'il existe un polynôme de $k[x_1, \ldots, x_r, x_i]$, unitaire en x_i et qui s'annule sur V.
Maintenant, les variables $x_1, \ldots, x_r$ seront dites en position de Noether par rapport à V si elles satisfont (i) et (ii) : l'homomorphisme canonique

$$k'[x_1, \ldots, x_r] \longrightarrow k'[x_1, \ldots, x_n]/(f_1, \ldots, f_s)$$

est une extension entière d'anneaux.
Si les variables libres sont connues et les conditions (i) et (ii) satisfaites, nous dirons encore que l'ensemble des variables, soit $x_1, \ldots, x_n$, sont en position de Noether par rapport à V.

Le théorème précédent peut alors être raffiné comme suit :

Au prix d'une préparatrion préalable, nous pouvons trouver par un algorithme bien parallélisable en temps $s^{O(1)}d^{O(n)}$ des indices différents $i_1, \ldots, i_r$ de $\{1, \ldots, n\}$ tels que les variables $x_{i_1}, \ldots, x_{i_r}$ sont libres par rapport à V.

Démonstration : Calculons d'abord la dimension r de V en temps $s^{O(1)}d^{O(n)}$ par l'algorithme bien parallélisable du théorème 3.5. Puis effectuons $\binom{n}{r}$ essais afin de choisir les variables $x_{i_1}, \ldots, x_{i_n}$ comme suit. Les variables “candidates” sont traitées comme des paramètres et nous appliquons les méthodes précédentes : nous considérons les $f_1, \ldots, f_s$ comme des polynômes à coefficients dans $k[x_{i_1}, \ldots, x_{i_r}]$ et nous calculons la dimension de la variété qu'ils définissent sur la clôture algébrique de $k(x_{i_1}, \ldots, x_{i_r})$ en appliquant le théorème 3.5 et en tenant compte de l'observation 3.4.8 et de [Heintz-Schnorr, 1982, Theorem 4.4] (les arguments sont similaires à ceux employés dans la démonstration du lemme 3.4.5). Les variables $x_{i_1}, \ldots, x_{i_r}$ sont libres par rapport à V si et seulement si nous trouvons comme dimension 0. Ceci est décidable en temps $s^{O(1)}d^{O(n)}$ par l'algorithme indiqué. Comme par hypothèse d est au moins égal à n (voir 1.2.1), nous trouvons ainsi en temps $s^{O(1)}d^{O(n)}$ un ensemble de r variables libres par rapport à V. Tous nos calculs sont bien parallélisables et ne contiennent aucune division.

3.6. Calcul séquentiel d'une base standard en dimension zéro

Nous conservons les notations introduites en 3.1.
Pour la notion de base standard (ou de Gröbner) d'idéaux polynomiaux et son rôle dans l'algèbre commutative et la géométrie algébrique effectives, nous renvoyons à [Buchberger, 1985]. Précisons que nous appellerons *base standard réduite* d'un idéal l'unique base standard dont les éléments sont des polynômes complètement réduits par rapport à l'idéal.
D'après le théorème 3.5, nous pouvons vérifier en temps $s^{O(1)}\,d^{O(n)}$ par un algorithme bien parallélisable si la dimension de $V(f_1, \ldots, f_s) = V(I)$ est zéro. Nous supposerons alors être dans cette dernière situation tout au long de ce paragraphe. Soit $<$ un ordre total admissible sur sur les monômes de $k[x_1, \ldots, x_n]$. Le résultat principal de ce paragraphe est basé sur l'observation suivante :

3.6.1. Lemme

Supposons que x_1 *soit en position générale par rapport à la variété de dimension zéro* $V = V(I)$ *(voir 3.4.6). L'ordre total admissible choisi est l'ordre lexicographique des variables* $x_1, x_2, \ldots, x_n$*. Alors au prix d'une préparation préalable, nous pouvons calculer en temps* $s^{O(1)}\, d^{O(n)}$ *par un algorithme bien parallélisable sans divisions un élément non nul* α *de* k *et des polynômes* $g_1, \ldots, g_n$ *de* $k[x_1, \ldots, x_n]$ *vérifiant les conditions suivantes :*

(i) $\max\{\deg g_i \mid 1 \le i \le n\} \le \deg V \le d^n$

(ii) $g_1, \ldots, g_n$ forment une suite régulière dans $k'[x_1, \ldots, x_n]$

(iii) $g_1/\alpha, \ldots, g_n/\alpha$ constituent la base standard réduite du radical de l'idéal I' engendré par $f_1, \ldots, f_s$ dans $k'[x_1, \ldots, x_n]$ relativement à l'ordre choisi.

Remarquons que d'après 3.4.7 nous pouvons trouver en temps $s^{O(1)}\, d^{O(n)}$ par un algorithme bien parallélisable sans divisions une transformation linéaire des variables qui mette x_1 en position générale par rapport à V.

Démonstration : C'est une conséquence directe du lemme de l'élément primitif dans sa version 3.4.7. Adoptons les notations de 3.4.7 et 3.4.8 avec $y := x_1$. Sans restriction de généralité nous pouvons supposer que le polynôme q est à coefficients dans k, tout en étant libre de carrés comme polynôme de $k'[x_1]$, et que de plus son coefficient dominant est α. Son degré est majoré par celui de V. Quant au degré des polynômes r_i $(1 \le i \le n)$, il vaut au plus celui de q. Posons alors $g_1 := q, g_2 := \alpha x_2 - r_2, \ldots, g_n := \alpha x_n - r_n$. Ces polynômes sont à coefficients dans k et vérifient (i).
Ils sont calculables en temps $s^{O(1)}\, d^{O(n)}$ par un algorithme bien parallélisable sans divisions. D'après 3.4.7 et 3.4.8 les variétés V, $V(g_1, \ldots, g_n, \alpha x_1 - r_1)$ et $V(g_1, \ldots, g_n)$ coïncident. Les polynômes $g_1, \ldots, g_n$ satisfont donc (ii). Enfin, ils engendrent un idéal J dans $k'[x_1, \ldots, x_n]$ dont ils constituent une base standard par rapport à l'ordre choisi. Comme g_1 est sans carrés et g_i est unitaire et linéaire en x_i $(2 \le i \le n)$, cet idéal J est radical. Ceci implique que J est le radical de I', d'où l'énoncé (iii).

3.6.2. Théorème

Supposons que k *soit un corps et que* $V(I)$ *soit de dimension zéro. Au prix d'une préparation préalable, nous pouvons calculer par un algorithme séquentiel à partir des données* $f_1, \ldots, f_s$ *une base standard réduite de* I *par rapport à l'ordre choisi avec* $s^{O(1)}\, d^{O(n)}$ *opérations arithmétiques dans* k*.*

Démonstration : Au vu de [Faugère-Gianni-Lazard-Mora, 1989] et de 3.4.7, nous pouvons supposer que la variable x_1 est en position générale par rapport à V et que que l'ordre choisi est l'ordre lexicographique des variables $x_1, \ldots, x_n$. Soit J le radical de I. D'après le lemme précédent nous pouvons calculer en temps $s^{O(1)}\, d^{O(n)}$ une base standard réduite $g_1, \ldots, g_n$ de J. Posons $\delta := (n+1)d^n$. Le théorème de Bézout implique que J^δ est contenu dans I et que le degré de I, défini par $\dim_k k[x_1, \ldots, x_n]/I$, est majoré par d^n (voir par exemple [Caniglia-Galligo-Heintz, 1989], Theorem 17).

Soit m l'entier $\lceil \log_2 \delta \rceil$. Pour tout indice k compris entre 0 et m, considérons les idéaux $J_k := I + J^{2^k}$. Au début, J_0 et J_m ne sont autres que J et I, et en général le degré de J_k est majoré par celui de I et a fortiori par d^n. En suivant les idées de [Lakshman, 1991] nous allons construire successivement les bases standard réduites des idéaux J_k. Après $m = O(n \log d)$ pas, nous obtiendrons celle de J_m. Pour k égal à 0, $g_1, \ldots, g_n$ forment déjà une base standard réduite de J_0. Soit donc k un indice strictement positif, et $p_1, \ldots, p_t$ une base standard réduite de J_{k-1}. Appelons M l'ensemble des monômes réduits modulo $p_1, \ldots, p_t$. Observons que $p_1, \ldots, p_t$ contient $t + \#M$ monômes, dont ceux de M, que le cardinal $\#M$ (qui est égal au degré de J_{k-1}) est majoré par d^n, et que t vaut au plus $n\#M$ [Faugère-Gianni-Lazard-Mora, 1989].

Considérons alors un polynôme arbitraire f de $k[x_1, \ldots, x_n]$. En le divisant à la Hironaka par $p_1, \ldots, p_t$ nous en obtenons une première représentation

$$f = h_0 + \sum_{1 \le j \le t} h_j \, p_j.$$

En redivisant $h_0, h_1, \ldots, h_t$ par $p_1, \ldots, p_t$ nous obtenons une deuxième représentation

$$f = r_0 + \sum_{1 \le j \le t} r_j \, p_j + \sum_{1 \le j,l \le t} r_{jl} \, p_j \, p_l.$$

Les polynômes $r_0, \ldots, r_t$ sont uniquement déterminés par la construction précédente et sont réduits modulo $p_1, \ldots, p_t$, donc ne contiennent que des monômes de M. Notons $[f]$ le polynôme $r_0 + \sum_{1 \le j \le t} r_j \, p_j$. Il est congru à f modulo J_{k-1}^2. Soit D l'entier $(t+1)\#M$, qui majore $\deg J_{k-1}^2$ et est un $d^{O(n)}$. Nous représenterons $[f]$ par le vecteur correspondant aux coefficients de $r_0, \ldots, r_t$ dans l'espace vectoriel $E := k^D$. Considérons la base canonique $(e_\lambda)_{1 \le \lambda \le D}$ de E. A chaque élément e_λ de cette base correspond un polynôme unique f_λ vérifiant $[f_\lambda] = f_\lambda$. De manière naturelle f_λ induit une application k-linéaire sur E que nous notons $[e_\lambda]$. A partir de la base standard $p_1, \ldots, p_t$, nous calculons la matrice de $[e_\lambda]$ pour tout λ $(1 \le \lambda \le D)$ en temps $s^{O(1)} \, d^{O(n)}$. De la même manière, nous déterminons ensuite les applications k-linéaires induites par $f_1, \ldots, f_s$ et par les $p_j \, p_l$ $(1 \le j, l \le t)$. Maintenant, calculons une base du sous-espace k-linéaire F de E engendré par les images de ces aplications. Finalement, tout en respectant l'ordre lexicographique des variables, nous obtenons une base de l'espace vectoriel E/F codée par des monômes qui apparaissent dans les polynômes f de $k[x_1, \ldots, x_n]$ vérifiant $[f] = f$. Les espaces vectoriels $k[x_1, \ldots, x_n]/J_k = k[x_1, \ldots, x_n]/I + J_{k-1}^2$ et E/F sont canoniquement isomorphes. La base de E/F que nous venons de déterminer est représentée par des monômes réduits modulo J_k. A partir des matrices des $[e_\lambda]$ $(1 \le \lambda \le D)$ et des bases construites des espaces vectoriels F et E/F, il est maintenant facile de calculer une base standard réduite de l'idéal J_k. Toute cette partie de notre algorithme s'exécute en temps $s^{O(1)} \, d^{O(n)}$. Après $\lceil \log_2 \delta \rceil = O(n \log d)$ pas, nous obtenons une base standard réduite de I avec un coût total de $s^{O(1)} \, d^{O(n)}$ opérations arithmétiques.

A cause de son caractère itératif, l'algorithme n'est pas bien parallélisable. Pour la même raison, la borne de complexité séquentielle obtenue ne peut entrer en compétition avec celle de l'algorithme [Dickenstein-Fitchas-Giusti-Sessa, 1991, Theorem 3.3 (iv)] dans le cas du corps de base des rationnels. En effet, si nous désignons conformément à 1.2.1 par t la taille binaire de l'entrée $f_1, \ldots, f_s$, la complexité de l'algorithme [Dickenstein-Fitchas-Giusti-Sessa, 1991, Theorem 3.3], qui est un $(st)^{O(1)} \, d^{O(n^2)}$ l'emporte sur la complexité binaire séquentielle de l'algorithme du théorème précédent (voir aussi pour cette difficulté [Faugère-Gianni-Lazard-Mora, 1989, Remark 6].

3.7. Mise en position de Noether effective pour les variétés affines

Dans ce paragraphe nous conservons les notations introduites en 3.1. Soient k' le corps des fractions de k et r la dimension de V. D'après le théorème 3.5, nous pouvons calculer la dimension r en temps $s^{O(1)}\, d^{O(n)}$ par un algorithme bien parallélisable, ce que nous supposons fait, ce qui permet de reconnaître le cas où V est non vide et de nous y placer.

3.7.1. Construction effective d'une suite régulière de longueur la codimension contenue dans l'idéal définissant

Proposition : *Au prix d'une préparation préalable nous pouvons trouver par un algorithme bien parallélisable en temps $s^{O(1)}\, d^{O(n)}$ des polynômes $h_1, \ldots, h_{n-r}$ contenus dans $I = (f_1, \ldots, f_s)$ et de degré majoré par d, formant une suite régulière dans $k'[x_1, \ldots, x_n]$.*

Démonstration : Nous utilisons les notations introduites en 3.4.1. Soient $T_1, \ldots, T_{n-r}$ de nouvelles indéterminées, R l'anneau $k[T_1, \ldots, T_{n-r}]$ et K une clôture algébrique de $k(T_1, \ldots, T_{n-r})$. D'après la démonstration du lemme 3.4.1, il existe des points $\mu_1, \ldots, \mu_{n-r}$ de k tels que les polynômes $\hat{f}_{\mu_1}, \ldots, \hat{f}_{\mu_{n-r}}$ forment une famille sécante de $\mathbf{A}^n$ (c'est-à-dire une suite régulière de $k'[x_1, \ldots, x_n]$, ou bien que la dimension de $V(\hat{f}_{\mu_1}, \ldots, \hat{f}_{\mu_{n-r}})$ est égale à r). Ceci implique que $\hat{f}_{T_1}, \ldots, \hat{f}_{T_{n-r}}$ forment aussi une famille sécante de $\mathbf{A}^n(K)$.
En tenant compte de l'observation 3.4.8, nous appliquons l'algorithme 3.5 à la famille $\hat{f}_{T_1}, \ldots, \hat{f}_{T_{n-r}}$ de polynômes de $R[x_1, \ldots, x_n]$, en choisissant un ensemble questeur de points à coordonnées dans k.
Cet algorithme fabrique certains polynômes non nuls de R. Ils sont de degré borné par d^{cn} pour un c approprié et sont donnés par un calcul d'évaluation bien parallélisable de complexité v (égale à $s^{O(1)}\, d^{O(n)}$) qui ne contient aucune division. Sans restriction de généralité, nous pouvons supposer que le produit de ces polynômes est de degré majoré par $(sd^n)^c$ et s'évalue en v opérations arithmétiques. Ces polynômes possèdent la propriété suivante : étant donné un point $(\lambda_1, \ldots, \lambda_{n-r})$ de k^{n-r} qui n'annule aucun de ces polynômes, la famille $\hat{f}_{\lambda_1}, \ldots, \hat{f}_{\lambda_{n-r}}$ est sécante dans $\mathbf{A}^n$.
Choisissons comme dans la preuve de 3.4.5 un ensemble questeur convenable $\gamma_1, \ldots, \gamma_m$ de points de k^{n-r} pour la classe des polynômes à $n-r$ variables, de complexité v et de degré au plus $(sd^n)^c$. Le cardinal m est un $s^{O(1)}\, d^{O(n)}$. Posons $\gamma_i = (\gamma_1^{(i)}, \ldots, \gamma_{n-r}^{(i)})$. Pour chaque indice i compris entre 1 et m nous pouvons calculer la dimension de $V(\hat{f}_{\gamma_1^{(i)}}, \ldots, \hat{f}_{\gamma_{n-r}^{(i)}})$ d'après le théorème 3.5, par un algorithme bien parallélisable en temps $s^{O(1)}\, d^{O(n)}$. Pour au moins un indice i nous trouvons une de ces dimensions égale à r. Donc les polynômes $h_1 := \hat{f}_{\gamma_1^{(i)}}, \ldots, h_{n-r} := \hat{f}_{\gamma_{n-r}^{(i)}})$ forment une famille sécante contenue dans I ; ils sont à coefficients dans k et de degré majoré par d, et constituent une suite régulière de l'algèbre $k'[x_1, \ldots, x_n]$.

3.7.2. Théorème de normalisation effective pour les variétés affines

Au prix d'une préparation préalable, nous pouvons trouver par un algorithme bien parallélisable en temps $s^{O(1)}\, d^{O(n)}$ une $n \times n$-matrice M de changement de variables à coefficients dans k telle que, si $y_1, \ldots, y_n$ sont par définition les nouvelles variables $M(x_1, \ldots, x_n)$, les r premières d'entre elles sont en position de Noether par rapport à V.

Démonstration : Les algorithmes qui vont suivre seront tous bien parallélisables. D'après le lemme 3.5.1, nous pouvons supposer sans restriction de généralité que les variables $x_1, \ldots, x_r$

sont libres par rapport à V. A l'aide de la proposition 3.7.1, nous trouvons en temps $s^{O(1)}\,d^{O(n)}$ des polynômes $h_1, \ldots, h_{n-r}$ dans I de degré majoré par d, formant une suite régulière dans $k'[x_1, \ldots, x_n]$. Appelons J et J^* les idéaux qu'ils engendrent respectivement dans $k'[x_1, \ldots, x_n]$ et $k'(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$. Observons que J est équidimensionnel d'après le théorème de Macaulay (voir [Matsumura, 1989, Theorem 17.7]). Appelons W la variété définie par J dans $\mathbf{A}^n$ et W^* la variété définie par J^* dans $\mathbf{A}^{n-r}(\overline{k'(x_1, \ldots, x_r)})$, où $\overline{k'(x_1, \ldots, x_r)}$ est une clôture algébrique de $k'(x_1, \ldots, x_r)$. La variété W^* est de dimension 0 et les variables $x_1, \ldots, x_r$ sont libres par rapport à W. Soit y une forme linéaire de $k[x_1, \ldots, x_n]$ supposée en position générale par rapport aux points de W^* (voir 3.4.6 et 3.4.7). Au vu de 3.4.7, il suffit d'exhiber un algorithme bien parallélisable de complexité séquentielle $s^{O(1)}\,d^{O(n)}$ produisant une transformation k-linéaire des variables $x_1, \ldots, x_r, y$ en de nouvelles variables $x'_1, \ldots, x'_r, y$ telles que y soit en position de Noether par rapport à $x'_1, \ldots, x'_r$ et W (et donc V). En itérant cette procédure $n - r$ fois, pour des variables y que nous choisissons suivant 3.4.7 suffisamment génériques, nous obtenons l'énoncé du théorème.
D'après la proposition 3.3.4 et l'observation 3.4.8, nous trouvons en temps $s^{O(1)}\,d^{O(n)}$ dans $k[x_1, \ldots, x_r, y]$ un polynôme non constant p qui s'annule sur W^*. Il dépend évidemment de la variable y et appartient au radical de J^*. Son degré est majoré par d^{cn} pour une constante c appropriée et notre algorithme le rend sous forme d'un calcul d'évaluation sans divisions et de longueur v. La complexité séquentielle v est une fonction en principe connue des paramètres d, s et n, d'ordre $s^{O(1)}\,d^{O(n)}$, la complexité parallèle est d'ordre $O(n^2 \log^2 sd)$. Pour un entier N suffisamment grand, p^N appartient à J^*. Il existe donc un élément non nul α de $k[x_1, \ldots, x_r]$ tel que le produit αp^N tombe dans J. Comme l'idéal J est équidimensionnel et que les variables $x_1, \ldots, x_r$ sont libres par rapport à W, c'est p^N lui-même qui appartient à J, et donc s'annule sur la variété W. Soit p' la partie homogène de plus haut degré de p. Nous pouvons supposer p' calculé et de complexité au plus v. Choisissons un ensemble questeur $(\gamma_1, \ldots, \gamma_m)$ de points convenables de k^{r+1} pour la classe des polynômes de complexité v et de degré d^{cn} en $r + 1$ variables. Le cardinal m est un $s^{O(1)}\,d^{O(n)}$. Nous pouvons trouver en temps séquentiel $s^{O(1)}\,d^{O(n)}$ un point γ_i $(1 \leq i \leq m)$ qui n'annule pas p'. A l'aide des coordonnées de ce point, nous transformons par la procédure usuelle les variables $x_1, \ldots, x_r, y$ en de nouvelles variables $x'_1, \ldots, x'_r, y$ de telle manière que le degré partiel de p en y soit le degré total (voir par exemple [Dickenstein-Fitchas-Giusti-Sessa, 1991, 1.15]). Comme p s'annule sur W, cela signifie que y est en position de Noether par rapport à $x'_1, \ldots, x'_r$ et W.

3.7.3. Observation

Conservons les notations précédentes.
Il n'est pas trop difficile de trouver en temps $s^{O(1)}\,d^{O(n)}$ par un algorithme bien parallélisable une transformation de variables, telle que les nouvelles variables, renommées $x_1, \ldots, x_n$ satisfassent les conditions algorithmiques suivantes :

- $x_1, \ldots, x_n$ sont en position de Noether par rapport à V.

- Soit l une forme linéaire de $k[x_1, \ldots, x_n]$. Après une préparation préalable, nous pouvons trouver en temps $s^{O(1)}\,d^{O(n)}$ par un algorithme bien parallélisable des polynômes $\alpha_0, \ldots, \alpha_{m-1}$ de $k[x_1, \ldots, x_r]$ $(1 \leq m \leq d^n)$, représentés par un calcul d'évaluation bien parallélisable de complexité $s^{O(1)}\,d^{O(n)}$ et de degré $d^{O(n)}$, tels que le polynôme $l^m + \alpha_{m-1} l^{m-1} + \cdots + \alpha_0$ appartienne à l'idéal engendré par $f_1, \ldots, f_s$ dans $k'[x_1, \ldots, x_n]$ (voir [Giusti-Heintz-Sabia, 1991] pour détails).

4. Situation projective

4.1. Préliminaires

Nous conservons les notations et hypothèses de 1.1, sans avoir à supposer que le corps des fractions k' soit parfait. Les polynômes d'entrée $f_1, \ldots, f_s$ sont maintenant homogènes non constants. En suivant les idées de [Giusti, 1988] et [Giusti-Heintz, 1991], nous décrirons dans cette section comment mettre les variables homogènes $x_0, x_1, \ldots, x_n$ en position de Noether par rapport à la variété projective $V = V(f_1, \ldots, f_s)$. L'algorithme employé est bien parallélisable de complexité $s^{O(1)}\, d^{O(n)}$, et se révèle considérablement plus direct et plus simple que celui décrit dans 3.7.2 pour le cas affine.

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 certains éclatements qui remplacent dans le cas projectif les déformations utilisées dans le cas affine (notamment en 3.3 et 3.4).

Soient $\lambda = (\lambda_0, \ldots, \lambda_m)$, $\lambda_0 \le \ldots \le \lambda_m$ et $\overline{\lambda} = (\lambda_{m+1}, \ldots, \lambda_n)$, $\lambda_{m+1} \le \ldots \le \lambda_n$ 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 $k[x_0, \ldots, x_n]$. Nous notons $f^{(\lambda)}$ le polynôme de $R^{(\lambda)}[z, x^{\overline{\lambda}}]$ que nous obtenons en substituant dans f les variables $x_{\lambda_0}, \ldots, x_{\lambda_m}$ par $zx_{\lambda_0}, \ldots, zx_{\lambda_m}$, ou autrement dit $f^{(\lambda)} := f(zx_{\lambda_0}, \ldots, zx_{\lambda_m}, x_{\lambda_{m+1}}, \ldots, x_{\lambda_n})$. Observons que $f^{(\lambda)}$ est homogène de degré $\deg f$ en les variables $z, x_{\lambda_{m+1}}, \ldots, x_{\lambda_n}$. 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 $f_1, \ldots, f_s$ dans $k[x_0, \ldots, x_n]$ et $k'[x_0, \ldots, x_n]$, tandis que $I^{(\lambda)}$ et $J^{(\lambda)}$ seront ceux engendrés par $f_1^{(\lambda)}, \ldots, f_s^{(\lambda)}$ dans $R^{(\lambda)}[z, x^{\overline{\lambda}}]$ et $K^{(\lambda)}[z, x^{\overline{\lambda}}]$. Nous dirons que x_λ (ou le système des variables $x_{\lambda_0}, \ldots, x_{\lambda_m}$) 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 $y := x_{\lambda_i}$ $(m < i \le n)$ 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} $(m < i \le n)$ sont en position de Noether par rapport à V, nous dirons que le système de variables $x_0, \ldots, x_n$ 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]) :

4.2. Le critère du centre de projection

Nous conservons les notations de 4.1. Soit W la sous-variété projective de $\mathbf{P}^{n-m}(\overline{K^{(\lambda)}})$ définie par les polynômes $f_1^{(\lambda)}, \ldots, f_s^{(\lambda)}$. Supposons que les variables $x_{\lambda_{m+1}}, \ldots, x_{\lambda_n}$ 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 $x^\lambda = (x_{\lambda_0}, \ldots, x_{\lambda_m})$ 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 $\{x_{\lambda_0} = \cdots = x_{\lambda_m} = 0\}$. Elle induit une application rationnelle $\phi : V \longrightarrow \mathbf{P}^m$. Le fait que les variables $x_{\lambda_{m+1}}, \ldots, x_{\lambda_n}$ soient en position de Noether par rapport à x^λ et V garantit que les équations $f_1^{(\lambda)}, \ldots, f_s^{(\lambda)}$ 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 $p_1, \ldots, p_s$ de $k[x_0, \ldots, x_n]$ tels que l'équation

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

soit satisfaite. Nous en déduisons immédiatement une deuxième équation

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

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 $m < i \le n$ 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 $\{z = 0\}$, $\{x_{\lambda_{m+1}} = 0\}$, …, $\{x_{\lambda_n} = 0\}$, 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 $N \ge 1$ et des polynômes $p'_1, \ldots, p'_s$ de $R^{(\lambda)}[z, x^\lambda]$ tels que l'équation

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

soit satisfaite.
En déshomogénéisant (**) par la substitution de 1 à z, les polynômes p'_i $(1 \le i \le s)$ 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.

4.3. Une bonne équation satisfaite par la projection

Conservons les notations de 4.2 ainsi que 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 4.2 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 2.3, 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 comme dans 3.4.5 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 $s^{O(1)}\, d^{O(n)}$.

4.4. Mise en position de Noether effective pour les variétés projectives

Nous conservons les notations de 4.1. 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 comme dans 3.4.5 $(\gamma_1, \ldots, \gamma_l)$ 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.

Observons finalement que les algorithmes de cette section ne nécessitent aucun calcul de pgcd et se basent exclusivement sur l'algèbre effective à la Berkowitz-Mulmuley (voir 2.3). Donc aucune extraction de racines $p^{\text{ième}}$ n'est nécessaire dans cette section.

REFERENCES

[Berenstein-Yger, 1991]
C.A. Berenstein, A. Yger, *Une formule de Jacobi et ses conséquences*, Ann. scient. Ec. Norm. Sup. 4ième série, t. 24 (1991), 363-377.

[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.

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

[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.

[Canny, 1988 a]
J. Canny, *Some algebraic and geometric computations in PSPACE*, Proc. 20^{th} Ann. ACM Symp. Theory of Computing (1988), 460-467.

[Canny, 1988 b]
J. Canny, *Generalized characteristic polynomials*, Proc. International Symposium on Symbolic and Algebraic Computation ISSAC '88, Springer LN Comput. Sci. **358** (1989), 293-299.

[Caniglia-Galligo-Heintz, 1989]
L. Caniglia, A. Galligo, J. Heintz, *Some new effectivity bounds in computational geometry*, Proc. 6th Intern. Conf. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes AAECC 6, Springer LN Comput. Sci. **357** (1989), 131-151.

[Chistov-Grigoriev, 1983]
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, E-10-83, Leningrad (1983).

[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.

[Faugère-Gianni-Lazard-Mora, 1989]
J. C. FAUGÈRE, P. GIANNI, D. LAZARD, T. MORA, *Efficient computation of zero-dimensional Gröbner bases by change of ordering*, J. Symb. Comput. (to appear).

[Fitchas-Galligo, 1988]
NOAÏ FITCHAS, A. GALLIGO, *Nullstellensatz effectif et conjecture de Serre (Théorème de Quillen-Suslin) pour le calcul formel*, Math. Nachrichten **149** (1990), 231-253.

[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.

[Garcia-Zangwill, 1991]
C. B. GARCIA, W. I. ZANGWILL, *Pathways to Solutions, Fixed Points, and Equilibria*, Prentice-Hall, Englewood Cliffs, N. J. (1981).

[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-Sabia, 1991]
M. GIUSTI, J. HEINTZ, J. SABIA, *On the efficiency of effective Nullstellensätze*, à paraître dans Computational Complexity.

[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-Roy-Solernó, 1980]
J. HEINTZ, M. F. ROY, P. SOLERNÓ, *Sur la complexité du principe de Tarski-Seidenberg*, Bulletin de la Société Mathématique de France **118** (1990), 101-126.

[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.

[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.

[Lazard, 1981]
D. Lazard, *Résolution des systèmes d'équations algébriques*, Theoretical Computer Science **15** (1981), 77-110.

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

[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.

[Renegar, 1992]
J. Renegar, *On the computational complexity and geometry of the first order theory of the reals I*, J. Symb. Comput. **13** (1992) 255-300.

[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.

[Teissier, 1991]
B. Teissier, *Résultats récents d'algèbre commutative effective*, Séminaire Bourbaki $42^{ième}$ année (1989-1990) **718**, Astérisque **189-190** (1991), 107-131.