Abstract

Let k be an infinite and perfect field, $x_1, \ldots, x_n$ indeterminates over k and let $f_1, \ldots, f_s$ be polynomials in $k[x_1, \ldots, x_n]$ given by the array of their coefficients (the so called dense representation). Let d be an upper bound for their degrees, satisfying $d \geq n$.

Thanks to a suitable coding of the output, we prove that the decision and representation problems arising in an effective affine Nullstellensatz can be solved in polynomial time.

More precisely, for arbitrary given parameters d, s, n, there exists an arithmetic network over k of size $s^{O(1)}\ d^{O(n)}$ (i.e. polynomial in the the size $O(sd^n)$ of the input), deciding whether the ideal generated by $f_1, \ldots, f_s$ in $k[x_1, \ldots, x_n]$ is trivial. If so, it produces a straight-line program in $k[x_1, \ldots, x_n]$ of same polynomial length which represents polynomials $p_1, \ldots, p_s$ of $k[x_1, \ldots, x_n]$ of degree $d^{\,O(n)}$ satisfying the Bézout identity

$$1 = p_1 f_1 + \cdots + p_s f_s.$$

Furthermore, this network can be constructed by a probabilistic (randomized) algorithm with same polynomial sequential complexity.

The arithmetic network and its output (the straight-line program) are well parallelizable, i.e. their depth is of order $O(n^2 \log^2 sd)$. The probabilistic randomized algorithm constructing the network can be also parallelized with a slightly higher complexity $O(n^{12} \log^9 sd)$.

Résumé

Soient k un corps infini et parfait, $x_1, \ldots, x_n$ des indéterminées sur k et soient $f_1, \ldots, f_s$ des polynômes de $k[x_1, \ldots, x_n]$ donnés par le vecteur de leurs coefficients. Soit d un majorant de leur degrés, supposé supérieur ou égal à n.

Grâce à un codage approprié des sorties, nous prouvons que les problèmes de décision et de représentation posés par un théorème effectif des zéros affine peuvent être résolus en temps polynomial en la taille de l'entrée.

Plus précisément, étant donnés des paramètres d, s, n, il existe un réseau arithmétique sur k de taille $s^{O(1)}\ d^{O(n)}$ (ce qui est bien un polynôme en la taille $O(sd^n)$ de l'entrée), qui décide si l'idéal engendré par $f_1, \ldots, f_s$ dans $k[x_1, \ldots, x_n]$ est trivial. Si c'est le cas, le réseau produit un calcul d'évaluation dans $k[x_1, \ldots, x_n]$ de taille encore polynomiale qui représente des polynômes $p_1, \ldots, p_s$ de $k[x_1, \ldots, x_n]$ de degré $d^{\,O(n)}$ quotients de l'identité de Bézout

$$1 = p_1 f_1 + \cdots + p_s f_s.$$

De plus, ce réseau peut être construit par un algorithme probabiliste de type aléatoire toujours en temps séquentiel polynomial.

Le réseau arithmétique et sa sortie (le calcul d'évaluation) sont susceptibles d'être bien parallélisés, c'est-à-dire peuvent être executés en temps parallèle $O(n^2 \log^2 sd)$. L'algorithme probabiliste de construction admet aussi un déroulement parallèle en temps $O(n^{12} \log^9 sd)$.

Sur la complexité du théorème des zéros

Noaï FITCHAS [1]
Departamento de Matemáticas, Universidad de Buenos Aires
Ciudad Universitaria Pab. I
1428 Buenos Aires, Argentine
joos@mate.edu.ar
Departamento de Matemáticas, Estadística y Computación
Facultad de Ciencias, Universidad de Cantabria
39071 Santander, Espagne
pardo@ccucvx.unican.es, heintz@ccucvx.unican.es

Marc GIUSTI [2]
Groupe "ALEPH ET GÉODE"
Centre de Mathématiques de l'Ecole Polytechnique
91128 Palaiseau Cedex, France
giusti@ariana.polytechnique.fr

Frédéric SMIETANSKI [2]
Département de Mathématiques
Université de Nice, Parc Valrose
06108 Nice Cedex 2, France

23 Décembre 1993

[1] Groupe de travail à cheval sur les Universités de Buenos Aires (BA) et de Santander (S). Ont collaboré à ce travail Joos HEINTZ (S), Luis Miguel PARDO (S), Juan SABIA (BA), Pablo SOLERNÓ (BA).

[2] Avec un soutien du GDR de Calcul Formel MEDICIS (MATHÉMATIQUES EFFECTIVES, DÉVELOPPEMENTS INFORMATIQUES, CALCUL, INGÉNIERIE ET SYSTÈMES), du PRC/GDR MATHÉMATIQUES ET INFORMATIQUE et du projet européen ESPRIT BRA contract 6846 POSSO.

Sommaire

Alla memoria di Mario Raimondo

1. Introduction et énoncé des résultats

Pour l'ensemble de ce travail, nous allons fixer les notations qui seront essentiellement les mêmes que dans les articles [Gi-He 91] et [Gi-He-Sa 93]. Nous les reprenons ici par commodité pour le lecteur.

1.1. Notations de base

Soit k un corps commutatif (à la rigueur un anneau intègre, voir [Gi-He 91]), infini, et effectif, c'est-à-dire que les opérations arithmétiques de base : addition, soustraction, multiplication, division, et test d'égalité sont réalisées par des algorithmes. Quand la caractéristique de k est positive, il convient de supposer que l'anneau de base est fermé sous l'extraction des racines $p^{\text{ièmes}}$, et c'est pour cette raison que nous demandons que k soit parfait. Mais comme nous voulons que toutes les opérations arithmétiques de base soient effectives, nous supposerons encore que l'extraction des racines $p^{\text{ièmes}}$ est réalisée par un algorithme.

Soient $x_1, \ldots, x_n$ des indéterminées sur k. Le degré total d'un polynôme f de $k[x_1, \ldots, x_n]$ sera noté $\deg f$ et, pour un indice r compris entre 1 et n, son degré partiel par rapport aux variables $x_1, \ldots, x_r$ $(1 \leq r < n)$ par $\deg_{x_1,\ldots,x_r} f$.

Soient $f_1, f_2, \ldots, f_s$ des polynômes non constants de $k[x_1, \ldots, x_n]$. L'idéal engendré par ces polynômes dans $k[x_1, \ldots, x_n]$ sera noté $(f_1, \ldots, f_s)$. 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 $k[x_1, \ldots, x_n]$ à $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$, où r est un entier compris entre 1 et n.

Soit $\bar{k}$ une clôture algébrique de k. Afin de traiter des systèmes d'équations où interviennent des polynômes en n variables à coefficients dans k, nous allons considérer comme espace ambiant l'espace affine $\mathbf{A}(\bar{k})^n$ de dimension n, muni de la topologie de Zariski, et noté plus simplement $\mathbf{A}^n$. La variété algébrique, au sens classique, affine définie par $(f_1, \ldots, f_s)$ dans $\mathbf{A}^n$ sera notée $\{f_1 = 0, \ldots, f_s = 0\}$ ou plus simplement V.

Nous aurons à considérer des quantités géométriques intrinsèques liées à V, 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 des intersections à effectuer (voir [He 83]).

1.2. Structures de données, modèles d'algorithmiques et de complexités

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 $k[x_1, \ldots, x_n]$ introduit dans 1.1. Soit d un entier majorant n et le plus grand des degrés totaux des f_i. Chaque polynôme peut être codé par le vecteur de ses coefficients correspondant à tous les monômes de degré au plus d : c'est ce que nous appellerons son *écriture dans la représentation dense*. La longueur de l'écriture des polynômes $f_1, \ldots, f_s$ dans cette représentation dense sera la *taille* de l'ensemble $f_1, \ldots, f_s$.
Il existe un cas particulier important de corps de base : celui des rationnels $\mathbf{Q}$. 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. Si les polynômes $f_1, \ldots, f_s$ sont à coefficients entiers, cela signifie que 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 majoré 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 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 $O(sd^n t)$ 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.

1.2.2. Description du modèle d'algorithmique

Tous nos algorithmes s'appuient sur les opérations suivantes, dites arithmétiques, dans le corps 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 $p^{ièmes}$ dans le cas d'une caractéristique positive p. 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.

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 [vzGa 86]. A chaque sommet interne correspond un processeur qui effectue une opération élémentaire du corps 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 le corps de base est celui des rationnels, 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 de la longueur binaire 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. Néanmoins, comme l'inclusion de la complexité binaire dans l'étude de complexité complique considérablement l'exposition de nos idées, sans ajouter rien de d'essentiellement nouveau nous omettrons ici cet aspect. (Nous pensons y revenir ultérieurement dans un contexte plus large). Nous nous limiterons donc dans ce travail aux algorithmes représentés par des réseaux arithmétiques sur k, donc à l'aspect de la *complexité algébrique*.

Pour une discussion plus approfondie de ce modèle de complexité, citons [vzGa 86] et [Fi-Ga-Mo 90].

1.2.3. Une autre représentation des polynômes (par calcul d'évaluation)

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"*). La *complexité séquentielle* ou *longueur* d'un tel calcul d'évaluation sera le nombre d'opérations arithmétiques qu'il contient. Un calcul d'évaluation peut servir à coder un polynôme à plusieurs variables, calculant sa valeur en un point de $\mathbf{A}^n$. Dans ce contexte rappelons brièvement les notions suivantes. Un *calcul d'évaluation* dans $k(x_1, \ldots, x_n)$ est une suite $\beta = (q_1, \ldots, q_w)$ de fonctions rationnelles de $k(x_1, \ldots, x_n)$ (les *résultats intermédiaires*) telle que pour tout indice i compris entre 1 et w une des conditions suivantes soit satisfaite :

(a) q_i est un élément de k ou l'une des variables $x_1, \ldots, x_n$
(b) il existe des indices i_1 et i_2 compris entre 1 et $i-1$ tels que la fonction rationnelle q_i s'écrive $q_i = q_{i_1} * q_{i_2}$, où * est l'une des opérations arithmétiques d'addition, soustraction, multiplication ou division.

Au calcul d'évaluation β correspond de manière naturelle un graphe acyclique orienté (*directed acyclic graph = DAG*) dont les nœuds sont constitués des indices $1, \ldots, w$. Les arêtes sont donnés de la manière suivante : chaque application de l'instruction (b) ci-dessus crée deux arêtes $i_1 \to i$ et $i_2 \to i$, et toutes les arêtes sont construites de cette manière. Les nœuds internes du DAG associé à β sont ceux qui reçoivent au moins une arête. Le DAG représente β comme circuit : la longueur du calcul d'évaluation est la taille du circuit (le nombre de ses nœuds internes) et sa profondeur est la longueur maximale des chemins orientés contenus dans le DAG. Nous disons que β ne contient aucune *division par zéro* si dans aucune des instructions (b) où * est la division la fonction rationnelle q_{i_2} n'est nulle. Soit g une fonction rationnelle de $k(x_1, \ldots, x_n)$; nous disons que β *calcule* ou *représente* g si β ne contient aucune division par zéro et si g est contenu dans les résultats intermédiaires de β. Nous appelons β un calcul d'évaluation ou circuit arithmétique dans $k[x_1, \ldots, x_n]$ si tous ses résultats intermédiaires sont des polynômes de $k[x_1, \ldots, x_n]$. Nous dirons que β ne contient aucune division (ou est sans divisions) si dans aucune des instructions (b) l'opération * n'est la division.

Nous n'allons considérer en général que des calculs dans $k(x_1, \ldots, x_n)$ sans divisions : ce sont des circuits qui peuvent être considérés comme réseaux arithmétiques sans tests d'égalité ni branchements. Nous renvoyons à [Stra 72], [vzGa 86], [Sto 89] et [He 89] pour plus de précisions sur les calculs d'évaluation.

1.2.4. Définition de bonnes bornes de complexité

L'entrée de tous de nos algorithmes incluera des polynômes $f_1, \ldots, f_s$ de $k[x_1, \ldots, x_n]$ de degré majoré par $d \geq n$, donnés par leur écriture dans la représentation dense qui est de taille $O(sd^n)$ (voir 1.2.1). En général, le nombre s de ces polynômes sera majoré par n, ce qui réduira la taille de leur donnée à $O(nd^n)$. De plus, l'entrée d'un algorithme pourra contenir un polynôme g représenté par un calcul d'évaluation dans $k[x_1, \ldots, x_n]$ (ou dans $k(x_1, \ldots, x_n)$) de longueur L et profondeur l (voir par exemple 4.1 et 5.1). Exceptionnellement, l'entrée d'un algorithme pourra inclure un second polynôme f, donné par un calcul d'évaluation ou son écriture dans la représentation dense (voir 4.2 et 4.2.5).

Ainsi, nos algorithmes seront en général des familles de réseaux arithmétiques paramétrées par les quantités d, s, n ou d, s, n, L, l (rappelons que pratiquement toujours s sera majoré par n). Dans ce cadre, nous dirons qu'un algorithme est de complexité séquentielle *polynomiale en la taille de l'entrée* si le réseau correspondant de paramètres d, s, n (respectivement d, s, n, L, l) admet une complexité séquentielle $s^{O(1)}d^{O(n)}$ (respectivement $(Ls)^{O(1)}d^{O(n)}$). Cette terminologie est justifiée quand on considère la taille $O(sd^n)$ (respectivement $L + O(sd^n)$) de notre entrée $f_1, \ldots, f_s$ (respectivement $f_1, \ldots, f_s, g$) pour la structure de données choisie (la représentation dense pour $f_1, \ldots, f_s$ et la représentation par calcul d'évaluation pour g), puisqu'un polynôme en $O(sd^n)$ (respectivement en $L+O(sd^n)$) est bien un $s^{O(1)}\, d^{O(n)}$ (respectivement un $(Ls)^{O(1)}\, d^{O(n)}$).

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

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

1.3. Des notions un peu plus sophistiquées

Dans l'étude algorithmique des idéaux polynomiaux et 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 $s^{O(1)}\, d^{\,O(n)}$. Nos algorithmes ne font pas exception (voir par exemple le théorème et la proposition 5.2). De toute façon, c'est sans doute inévitable, dès lors par exemple qu'un dévissage par projection est utilisé, comme dans la démonstration du théorème 5.1 dont dépendent les résultats de 5.2.

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. Mais cela doit s'effectuer de manière plus subtile qu'un passage brutal de la représentation dense à la représentation par calcul d'évaluation.

1.3.1. Extension du corps de base et représentation mixte des polynômes

L'idée principale de nos algorithmes consiste à introduire des paramètres auxiliaires. Le rôle de ces paramètres est en général joué par certaines des indéterminés $x_1, \ldots, x_n$, par exemple comme dans 4.2 par les r premières, où r est la dimension de la variété algébrique définie par $f_1, \ldots, f_s$. Nous remplacerons alors provisoirement le corps de base k par l'anneau $A := k[x_1, \ldots, x_r]$ ou le corps $K := k(x_1, \ldots, x_r)$. Les résultats intermédiaires de nos algorithmes représentent des polynômes considérés comme dépendant de variables principales (les variables $x_{r+1}, \ldots, x_n$ dans notre cas) à coefficients eux-mêmes des polynômes ou des fonctions rationnelles en les paramètres ($x_1, \ldots, x_r$ dans notre cas). Par rapport aux variables principales les polynômes sont codés par leur écriture dans la représentation dense, mais les polynômes ou fonctions rationnelles coefficients sont eux-mêmes représentés par des calculs d'évaluation.

Nos algorithmes exécutent alors des opérations arithmétiques (en général sans divisions) et des comparaisons dans la k-algèbre des coefficients, des polynômes de $A = k[x_1, \ldots, x_r]$ si nous prenons l'exemple de 4.2. Le point essentiel pour la complexité de cette nouvelle arithmétique va résider dans ces comparaisons, et plus exactement les tests de nullité et non-nullité. Ces tests doivent être exécutés lors de spécialisations des paramètres 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 le corps de base k (voir aussi [He-Sie 81], [Ka 88], [He-Gi 91], [He-Gi-Sa 91] pour l'utilisation de cette représentation des polynômes en calcul formel).

Dans le cas d'une caractéristique positive p, nous aurons aussi à envisager l'extraction de racines $p^{\text{ièmes}}$ dans la k-algèbre des polynômes en les paramètres. Pour une discussion détaillée de cette question nous renvoyons le lecteur à [Gi-He 91], paragraphe 2.1.

Voyons maintenant comment traiter la question cruciale des comparaisons. Nous nous appuyerons de manière essentielle sur un résultat de Heintz-Schnorr [He-Schn 82] dont nous rappellerons l'énoncé précis dans le paragraphe 2.1, qui aboutit à :

Test de nullité polynomiale : *Soient n, L, l trois entiers strictement positifs. Il existe un réseau arithmétique sur k de taille $O(L(L+n)^2)$ et de profondeur $O(l)$ qui vérifie la nullité d'un polynôme de $k[x_1, \ldots, x_n]$ donné par un calcul d'évaluation dans $k[x_1, \ldots, x_n]$ sans divisions, de longueur et de profondeur respectivement majorées par L et l.*

1.3.2. Les modèles de complexité non uniforme et probabilistes

La construction des réseaux arithmétiques décrivant nos algorithmes, à commencer par le test ci-dessus, dépend du choix judicieux de certaines opérations constantes, c'est-à-dire de certains éléments de k (provenant d'ensembles dits *questeurs*, voir 2.1) qui paramètrent l'algorithme.

Traitons d'abord le cas du test 1.3.1. La sélection de ces ensembles de constantes peut bien sûr se faire à chaque fois algorithmiquement, mais à un coût relativement élevé. Cependant, ces ensembles ne dépendent que des quantités n, L, l, mais pas du tout du polynôme d'entrée lui-même. Il serait dommage de ne pas tirer parti de ce fait en considérant donc que, pour un triplet n, L, l fixé, nous en avons déterminé un une bonne 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. En ce sens, nous dirons que cet algorithme de test est *non uniforme*.

Maintenant plus généralement, nous donnerons pour chacun de nos algorithmes définis en 1.2.4 une description non uniforme en démontrant pour chaque triplet d, s, n (ou d, s, n, L, l ou $d, n, L, l, \deg g$) l'existence d'un réseau arithmétique qui résoud une certaine tâche en temps séquentiel $s^{O(1)}\, d^{O(n)}$ (ou $(Ls)^{O(1)}\, d^{O(n)}$ ou $(L \deg g)^{O(1)}\, d^{O(n)}$). Le temps parallèle utilisé sera d'ordre $(n \log sd)^{O(1)}$ ou $(ln \log sd)^{O(1)}$ ou $(l \log(\deg g) n \log d)^{O(1)}$. Cette démonstration sera toujours constructive, mais dans ce modèle non uniforme le coût lui-même de cette construction n'est pas compté.

Enfin, venons-en aux modèles *probabilistes*, en l'illustrant d'abord sur l'algorithme de test 1.3.1. Le choix des ensembles questeurs peut se faire de manière aléatoire, selon [He-Schn 82], Theorem 4.4. Ceci implique que le réseau arithmétique introduit précédemment pour tester la nullité polynomiale, puis tous les autres, peuvent être construits par un algorithme probabiliste, *mais malheureusement avec une certaine probabilité d'erreur* (néanmoins uniformément majorée par un rationnel strictement inférieur à $\frac{1}{2}$, voir le corollaire 2.1). Ceci dit, nous observerons que cet algorithme probabiliste est d'un type plus agréable que le banal *Monte Carlo*, puisque c'est seulement la réponse positive qui est entachée d'erreur. Nous qualifierons dans la suite d'*aléatoire* (*"randomized"*) un algorithme probabiliste vérifiant une telle condition.
Tout ceci se transmet aux algorithmes envisagés dans 1.2.4, dont la version probabiliste sera généralement aléatoire. Les temps séquentiels et parallèles de déroulement de nos algorithmes deviennent alors des variables aléatoires dont l'espérance mathématique est du même ordre que les complexités non uniformes. Enfin la borne supérieure de complexité uniforme et déterministe, obtenue en examinant de manière exhaustive tous les ensembles candidats au statut de questeurs, atteint $s^{O(1)}\, d^{O(n^2)}$.

Evidemment, nous voudrions obtenir des résultats plus forts avec des algorithmes probabilistes de type *Las Vegas*. Expliquons cette notion toujours sur l'exemple du test 1.3.1. Un algorithme de décision probabiliste de type Las Vegas dépend de certains paramètres qui sont choisis de manière aléatoire. Dans notre cas, ce choix correspond à la sélection d'un ensemble questeur. Les réponses possibles sont au nombre de trois : acceptation ou rejet de l'entrée, et échec. La probabilité d'échec doit être strictement inférieure à $\frac{1}{2}$; par contre, si le test accepte ou rejette une entrée, il ne commet pas d'erreur, et l'entrée se trouve dans ou en dehors de l'ensemble à décider, selon le cas. Ainsi, pour nous résumer, un test probabiliste de type Las Vegas possède une probabilité d'erreur nulle, tandis que sa probabilité d'échec est strictement majorée par $\frac{1}{2}$. Le temps nécessaire au test pour arriver à une réponse définitive d'acceptation ou rejet devient une variable aléatoire avec une certaine espérance mathématique. Par contre, un algorithme aléatoire accepte ou rejette une entrée. En cas de réponse positive, la probabilité d'erreur est strictement majorée par $\frac{1}{2}$, tandis qu'un rejet est toujours correct (probabilité d'erreur réduite à zéro). Les notions d'algorithmes probabilistes aléatoires et de type Las Vegas peuvent être transportés sans problèmes aux algorithmes probabilistes dont la sortie consiste en des polynômes ou fonctions rationnelles, et dont le déroulement dépend de certaines décisions. La même terminologie sera alors employée.

Dans le travail présenté ici, le lemme 3.4 et la proposition 4.2 sont cruciaux. De la technique utilisée dans leur démonstration, basée sur les résultats de complexité de [Gi-He 91]), nous voyons immédiatement que la version probabiliste des algorithmes sous-jacents est de type aléatoire. Ceci se vérifie aussi dans la preuve des théorèmes 5.1 et 5.2 où nous utilisons de manière répétée les algorithmes [Gi-He 91], 3.5 et 3.7.2 (voir 2.3) calculant la dimension d'une variété algébrique et mettant les variables en position de Noether. Nous n'avions donné dans le travail cité qu'une version non uniforme, néanmoins les preuves s'adaptent parfaitement au modèle probabiliste des algorithmes aléatoires. Il serait souhaitable de trouver pour tous ces algorithmes de base une version Las Vegas (ce qui entraînerait d'ailleurs immédiatement la version probabiliste Las Vegas de l'ensemble des résultats présentés ici). Toute la question est là ...

Rappelons enfin que tout résultat de complexité pour les modèles probabilistes aléatoire ou Las Vegas entraîne le résultat correspondant pour le modèle non uniforme (voir [Ba-Dí-Ga 88], Corollary 6.4 et Corollary 6.6, au chapitre 6 duquel nous renvoyons plus généralement pour plus de détails sur les notions d'algorithmes probabilistes).

1.4. Enoncé des résultats principaux

Ce travail apporte une contribution aux conjectures affirmant que l'appartenance d'un polynôme à un idéal de $k[x_1, \dots, x_n]$ définissant une intersection complète et la trivialité d'un idéal de $k[x_1, \dots, x_n]$ (c'est-à-dire l'appartenance de 1) peuvent être décidées en temps séquentiel *uniforme* polynomial en la taille de l'entrée. Avec les précisions sur les structures de données employées pour les entrées/sorties explicitées dans 1.2.4, ces conjectures sont démontrées sous une forme généralisée, *mais pour les modèles non uniforme et probabiliste* dans 4.1, 5.1 et 5.2. La généralisation consiste en ce que nous ne nous limitons pas à un simple test d'appartenance d'un polynôme mais que nous donnons aussi, en cas de réponse positive, une *représentation* de ce polynôme comme combinaison $k[x_1, \dots, x_n]$-linéaire des générateurs de l'idéal. Cette représentation est (quasi)-optimale dans le sens que sa taille est polynomiale (ou non loin de l'être) en la taille de l'entrée mesurée par les paramètres introduit dans 1.2.4. Néanmoins ce résultat reste insatisfaisant du point de vue pratique et intuitif parce que la taille de la sortie contient un terme exponentiel en le nombre de variables du problème. Au vu des évidences obtenues dans [He-Mo 92], nous soupçonnons malheureusement que ce caractère exponentiel est foncièrement intrinsèque à tous les problèmes géométriques et algébriques de l'élimination algorithmique.

Formulons maintenant les deux résultats de complexité capitaux de ce travail :

Théorème 1 : *Soient $f_1, \dots, f_s$ des polynômes de $k[x_1, \dots, x_n]$ de degré majoré par $d \geq n$, représentés par leur écriture dense, et possédant la propriété suivante : pour tout indice i compris entre $n-s$ et $n-1$, les polynômes $f_1, \dots, f_{n-i}$ définissent une variété V_i intersection complète réduite de dimension i. Soit g un polynôme de $k[x_1, \dots, x_n]$ représenté par un calcul d'évaluation β dans $k[x_1, \dots, x_n]$ qui ne contient aucune division. Soient L la longueur et l la profondeur du calcul β.*

Alors il existe un réseau arithmétique sur le corps de base k de taille $L' := L^6(\deg g)^2 d^{O(n)}$ et de profondeur $l' := O(l^2 \log(\deg g) n^7 \log^4 d)$ qui décide si le polynôme g appartient à l'idéal $(f_1, \dots, f_s)$.
Si c'est le cas, le réseau construit un calcul d'évaluation β' dans $k[x_1, \dots, x_n]$ de longueur $(L \deg g)^2 d^{O(n)}$ et de profondeur $O(l^2 \log(\deg g) n^7 \log^4 d)$, ne contenant aucune division et qui représente des polynômes $p_1, \dots, p_s$ vérifiant les propriétés suivantes :
– $g = p_1 f_1 + \dots + p_s f_s$

– le degré des $p_1, \ldots, p_s$ est d'ordre $(\deg g)\, d^{O(n)}$.
Enfin il existe un algorithme de type aléatoire qui construit le réseau ci-dessus en temps séquentiel et parallèle du même ordre que L' et l'.

Théorème 2 : *Soient $f_1, \ldots, f_s$ des polynômes de $k[x_1, \ldots, x_n]$ de degré majoré par $d \geq n$ et représentés par leur écriture dense. Alors il existe un réseau arithmétique sur le corps de base k de taille $L := s^{O(1)}\, d^{O(n)}$ et de profondeur $l := O(n^2 \log^2 sd)$ qui décide si l'idéal $(f_1, \ldots, f_s)$ est trivial. Si c'est le cas, le réseau produit un calcul d'évaluation dans $k[x_1, \ldots, x_n]$ de longueur $s^{O(1)}\, d^{O(n)}$ et de profondeur $O(n^2 \log^2 sd)$, ne contenant aucune division, et qui représente des polynômes $p_1, \ldots, p_s$ de degré d'ordre $d^{O(n)}$ vérifiant $1 = p_1 f_1 + \cdots + p_s f_s$. Enfin ce réseau peut être construit par un algorithme probabiliste de type aléatoire en temps séquentiel du même ordre que L et parallèle un peu supérieur en $O(n^{12} \log^9 sd)$.*

Le Théorème 1 traite le problème de la division par un idéal de $k[x_1, \ldots, x_n]$, si ce dernier définit une intersection complète réduite, du point de vue du degré et de la complexité; tandis que le Théorème 2 considère le problème de l'obtention en général de l'identité de Bézout.

Les deux résultats affirment l'existence des polynômes quotients $p_1, \ldots, p_s$ de degré et complexité séquentielle essentiellement un $d^{O(n)}$. Rappelons d'abord que les meilleures bornes de degré et de complexité connues avant 1987 étaient de caractère doublement exponentiel en n. Ces bornes étaient déduites d'un résultat contenu dans [Her 26] pour le problème plus général de l'appartenance d'un polynôme donné à un idéal arbitraire.

Dans le cas général les bornes de [Her 26] sont optimales (voir [Ma-Me 82]), mais certainement pas dans les circonstances particulières que nous considérons ici. En effet, des bornes de degré et de complexité séquentielle simplement exponentielles en n sont une conséquence des Nullstellensätze affines effectifs [Bro 87], [Ca-Ga-He 88], [Ca-Ga-He 89], [Ko 88] et [Ca-Gu-Gu 91], [Di-Fi-Gi-Se 91], [Be-Yg 90], [Am 89] (voir aussi [Phi 88], [Fi-Ga 90], [Sa-So 92] et [Du 93] pour des preuves élémentaires). Les meilleures bornes de degré dans les Nullstellensätze mentionnés sont de type d^n et les bornes de complexité séquentielle qui en découlent sont de type $d^{O(n^2)}$. Les algorithmes sont uniformes. Les bornes de degré sont optimales à cause du théorème de Bézout et les bornes de complexité le sont aussi si l'on représente les polynômes de la sortie par leur écriture.

Ceci nous a conduit à chercher à améliorer ces bornes de complexité en changeant la structure de données utilisée pour représenter les polynômes de sortie. Ce problème a été abordé dans les papiers [Gi-He 91] et [Gi-He-Sa 93] qui s'appuient sur une représentation des polynômes par calcul d'évaluation.

Nous démontrons dans [Gi-He 91] que la trivialité de l'idéal engendré par $f_1, \ldots, f_s$ peut être décidée en temps séquentiel non-uniforme (ou aléatoire) $s^{O(1)} d^{O(n)}$, ce qui constitue une amélioration significative par rapport à [Di-Fi-Gi-Se 91] où ce coût (pour le modèle uniforme) est un $s^{O(1)} d^{O(n^2)}$.

Dans [Gi-He-Sa 93] nous prouvons que si l'idéal engendré par $f_1, \ldots, f_s$ est trivial, il existe des polynômes $p_1, \ldots, p_s$ de degré $d^{O(n^2)}$ représentés par un calcul d'évaluation β dans $k(x_1, \ldots, x_n)$ (contenant des divisions) tels que l'égalité $1 = p_1 f_1 + \ldots + p_s f_s$ soit satisfaite et tels que la taille de β soit un $s^{O(1)} d^{O(n)}$. Comme le degré des $p_1, \ldots, p_s$ est d'ordre $d^{O(n^2)}$, il n'est pas possible d'éliminer les divisions dans β sans augmenter la taille du nouveau calcul d'évaluation jusqu'à $s^{O(1)}d^{O(n^2)}$, ce qui n'est pas mieux que le résultat de [Di-Fi-Gi-Se 91]. C'est ce défaut du résultat principal de [Gi-He-Sa 93] qui est corrigé dans le Théorème 2.

En ce qui concerne le Théorème 1, signalons que la complexité séquentielle uniforme obtenue dans [Di-Fi-Gi-Se 91] est d'ordre $(\max\{d, \deg g\})^{O(n^2)}$. Le Théorème 1 représente donc une amélioration significative de ce résultat.

Finalement annonçons que des versions analogues des Théorèmes 1 et 2 pour le modèle de la complexité booléenne ont été obtenues récemment par T. Krick et L. M. Pardo [Kri-Par 93]. Ce dernier progrès n'est pas seulement significatif du point de vue informatique (puisque le modèle booléen est plus réaliste que le modèle purement algébrique que nous utilisons ici), mais encore plus pour ses conséquences en théorie arithmétique de l'élimination et en géométrie diophantienne. Ainsi sont redémontrés de manière tout-à-fait élémentaire les résultats arithmétiques principaux de [Be-Yg 90] et [Be-Yg 91]. T. Krick et L. M. Pardo obtiennent aussi un nouveau résultat sur les hauteurs des polynômes qui interviennent dans la division par un idéal intersection complète de $\mathbf{Q}[x_1, \ldots, x_n]$. Ces bornes ont aussi été trouvées par une méthode différente par M. Elkadi [El 93].

2. Rappels

Soient $x_1, \ldots, x_n$ et $t_1, \ldots, t_n$ deux jeux d'indéterminées sur k.

2.1. Test probabiliste de nullité de polynômes donnés par calcul d'évaluation

Les algorithmes que nous allons décrire dans ce travail utilisent de manière essentielle un test probabiliste de non-nullité de polynômes donnés par un calcul d'évaluation.

Soient δ, L et l trois entiers strictement positifs. Nous définissons l'ensemble $W(\delta, n, L)$ constitué des polynômes de $k[t_1, \ldots, t_n]$, de degré au plus δ, qui peuvent être évalués par un circuit arithmétique dans $k(t_1, \ldots, t_n)$ de taille au plus L. Posons $m := 6(L+n)(L+n+1)$, et considérons des ensembles éventuellement ordonnés $\gamma := \{\gamma_1, \ldots, \gamma_m\}$ de m points de k^n. Suivant une jolie terminologie due à [Hen-Mer 87], 7.2 nous appellerons un tel ensemble *questeur* pour $W(\delta, n, L)$ s'il satisfait à la propriété suivante : tout polynôme de $W(\delta, n, L)$ qui s'annule sur les points de γ est en réalité identiquement nul. Comme dans [Gi-He 91], 2.2 nous l'utiliserons pour exprimer en français (châtié, mais non recherché, comme il se doit) la locution anglaise *correct test sequence* originellement introduite dans l'article [He-Schn 82], Theorem 4.4. (échappant ainsi au fumet plutôt *basique* d'une traduction littérale ... mais pourquoi l'humanité a-t-elle été privée de la merveilleuse terminologie "einwandfreie Prüfungsfolge!? [voir *Effective Methods in Algebraic Geometry*, Proc. Intern. Conf. MEGA 90, Castiglioncello 1990, T. Mora and C. Traverso eds. *Progress in Mathematics* **94**, Birkhäuser (1991) p. viii]).

Proposition ([He-Schn 82], Theorem 4.4) **:** *Avec les notations ci-dessus, fixons-nous un sous-ensemble Γ de k de cardinal $\#\Gamma = 2L(\delta+1)^2$. Appelons $\tau(\delta, n, L, \Gamma)$ le sous-ensemble de k^{nm} formé des ensembles questeurs pour $W(\delta, n, L)$ dont les points n'ont que des coordonnées dans Γ (autrement dit τ est un sous-ensemble de Γ^{nm}). Alors l'inégalité suivante est vraie :*

$$(\#\Gamma)^{nm}(1 - (\#\Gamma)^{-\frac{m}{6}}) \leq \#\tau(\delta, n, L, \Gamma)$$

Nous renvoyons à l'article cité pour la démonstration de cette proposition, que nous utiliserons sous la forme de l'énoncé suivant (comparer à [Gi-He 91], 2.2 et [Gi-He-Sa 93], 1.2.3) :

Corollaire : *Il existe un réseau arithmétique sur k de taille $O(Lm) = O(L(L+n)^2)$ et de profondeur $O(l)$ qui vérifie la nullité d'un polynôme de $k[t_1, \ldots, t_n]$, donné par un calcul d'évaluation sans divisions dans $k[t_1, \ldots, t_n]$ de longueur et profondeur respectivement majorées par L et l. Le réseau ci-dessus peut être construit par un algorithme probabiliste en temps séquentiel $O(L(L+n)^2)$ et parallèle $O(l)$ avec une probabilité d'échec au plus $(2L(2^l+1)^2)^{-(L+n)(L+n+1)}$, majorée uniformément par $\varepsilon := \frac{1}{262144}$.*

Démonstration : Soit $\delta := 2^l$. Observons que tout polynôme qui peut être représenté par un calcul d'évaluation dans $k[t_1, \ldots, t_n]$ de profondeur au plus l a un degré majoré par δ. Choisissons un sous-ensemble Γ de k de cardinal $\#\Gamma = 2L(\delta+1)^2$ (sans problème, puisque k est infini). Comme tous les entiers introduits sont strictement positifs, ce cardinal est trivialement minoré 8, et m par 36. La proportion d'ensembles ordonnés non questeurs dans Γ^{nm}, au plus $(\#\Gamma)^{-\frac{m}{6}}$ par la proposition précédente, est donc majorée par $\varepsilon = \frac{1}{262144}$. Ceci prouve d'une part qu'il existe des ensembles questeurs pour $W(\delta, n, L)$ dans Γ^{nm}, et d'autre part qu'un choix aléatoire d'un γ dans l'ensemble Γ^{nm} n'a qu'une probabilité au plus ε de ne pas conduire à un tel ensemble questeur.

Soit donc $\gamma = (\gamma_1, \ldots, \gamma_m)$ un ensemble questeur pour $W(\delta, n, L)$; considérons maintenant un polynôme g de $k[t_1, \ldots, t_n]$, donné par un circuit arithmétique β dans $k[t_1, \ldots, t_n]$ sans divisions. Supposons que la longueur de β soit majorée par L et que de plus sa profondeur soit majorée par l (donc g est un élément de $W(\delta, n, L)$). Pour tester la nullité de g, il suffit de calculer la suite des valeurs $(g(\gamma_1), \ldots, g(\gamma_m))$, ce qui peut se faire par un réseau arithmétique sur k de taille $O(mL)$ et de profondeur $O(l)$ (puisque β ne contient par hypothèse aucune division). Notons que le construction de ce réseau ne dépend que des paramètres δ, n, L, l et surtout pas du polynôme g ou de son calcul β. En d'autres termes, au prix d'une préparation préalable qui consiste en la recherche d'un ensemble questeur, nous pouvons vérifier en temps séquentiel $O(L(L+n)^2)$ et parallèle $O(l)$ si notre polynôme g est identiquement nul, cfqd.

Enfin, à cause de la probabilité d'erreur non nulle ε sur le choix d'un ensemble questeur, l'algorithme probabiliste correspondant n'est malheureusement pas du type Las Vegas. Nous obtenons ainsi un algorithme aléatoire qui vérifie en temps cubique en L et n, et linéaire en l la nullité d'un polynôme donné par un calcul d'évaluation sans divisions dans $k[t_1, \ldots, t_n]$ de longueur L et profondeur l. L'algorithme peut se tromper quand il affirme la nullité d'un polynôme d'entrée, avec une probabilité d'erreur bornée par ε. Mais une réponse négative (non-nullité du polynôme d'entrée) n'est jamais entachée d'erreur : elle est toujours correcte. Néanmoins nous n'appliquerons la proposition et son corollaire que dans des circonstances où l'évaluation des polynômes apparaissant comme résultats intermédiaires est possible dans le temps prescrit, ce qui rendra les algorithmes probabilistes dérivés de type aléatoire (voir [Gi-He 91], 2.2 et [Gi-He-Sa 93], 1.2.3 pour une discussion plus détaillée).

2.2. Elimination des divisions (Vermeidung von Divisionen)

Proposition : *Soient L, l, n et δ des entiers strictement positifs. Supposons $\delta \le 2^l$. Il existe un réseau arithmétique de taille $O(L^3 n^2 \delta^2)$ et de profondeur $O(l \log \delta)$ qui opère sur les calculs d'évaluation dans $k(t_1, \ldots, t_n)$ comme suit :*

Soit β un calcul d'évaluation dans $k(t_1, \ldots, t_n)$, de longueur et profondeur respectivement majorées par L et l, représentant un polynôme g de $k[t_1, \ldots, t_n]$ de degré au plus δ. Alors le réseau arithmétique transforme le circuit β en un circuit β^* dans $k[t_1, \ldots, t_n]$ sans divisions. La longueur de β^* est d'ordre $O(L\delta^2)$, sa profondeur d'ordre $O(l \log \delta)$, et sa construction peut être effectuée par un algorithme probabiliste de type Las Vegas en temps séquentiel $O(L^3 n^2 \delta^2)$ et parallèle $O(l \log \delta)$.

Démonstration : Remarquons d'abord qu'une version non uniforme et séquentielle de cette proposition se trouve dans [Stra 73], Satz 2 et sa preuve. Nous nous contenterons ici d'indiquer comment modifier cette preuve pour inclure les aspects de complexité parallèle et probabiliste.

Considérons donc un calcul d'évaluation β dans $k(t_1, \ldots, t_n)$ représentant un polynôme g. Ce calcul est de la forme $\beta = (q_1, \ldots, q_w)$, où $q_1, \ldots, q_w$ sont des fonctions rationnelles de $k(t_1, \ldots, t_n)$ constituant les résultats intermédiaires de β. Sans restriction de généralité, nous pouvons supposer que le nombre w des résultats intermédiaires est majoré par $L+n+1$ et que q_w est égal à g. Ce calcul ne contient aucune division par zéro, ce qui veut dire que s'il exécute une division par un résultat intermédiaire q_i, la fonction rationnelle q_i n'est pas nulle. Pour tout indice i compris entre 1 et w, nous allons maintenant réécrire chaque q_i comme un couple numérateur/dénominateur (q_i', q_i'') de polynômes dans $k[t_1, \ldots, t_n]$, de degré au plus 2^l et avec q_i'' non nul. De plus, les polynômes $q_1', q_1'', \ldots, q_w', q_w''$ forment les résultats intermédiaires d'un calcul d'évaluation β_1, de longueur et profondeur respectivement majorés par $4L$ et $2l$, produit à partir de β par un algorithme (uniforme) en temps séquentiel $O(L)$ et parallèle $O(l)$, comme suit :

Le premier q_1 est soit une constante de k soit l'une des variables $t_1, \ldots, t_n$: nous posons $q_1' := q_1$ et $q_1'' := 1$. Soit maintenant i un indice compris entre 2 et w. Supposons que les fonctions rationnelles $q_1, \ldots, q_{i-1}$ soient déjà réécrites en couples $(q_1', q_1''), \ldots, (q_{i-1}', q_{i-1}'')$. Si q_i est une constante de k ou l'une des variables $t_1, \ldots, t_n$, nous posons comme auparavant $q_i' := q_i$ et $q_i'' := 1$. Sinon, la fonction rationnelle q_i est de la forme $q_i = q_{i_1} * q_{i_2}$, où i_1 et i_2 sont des indices compris entre 1 et $i-1$ et $*$ est une opération arithmétique. Si $*$ est l'addition ou la soustraction, nous posons $q_i' := q_{i_1}' q_{i_2}'' * q_{i_2}' q_{i_1}''$ et $q_i'' := q_{i_1}'' q_{i_2}''$. Si $*$ est la multiplication, nous posons $q_i' := q_{i_1}' q_{i_2}'$ et $q_i'' := q_{i_1}'' q_{i_2}''$. Enfin si $*$ est la division, nous posons $q_i' := q_{i_1}' q_{i_2}''$ et $q_i'' := q_{i_1}'' q_{i_2}'$. Nous vérifions immédiatement que les polynômes $q_1', q_1'', \ldots, q_w', q_w''$ ont les propriétés requises et qu'ils peuvent être évalués par un circuit β_1 dans $k[t_1, \ldots, t_n]$, sans divisions, de longueur et de profondeur respectivement $4L$ et $2l$. Aucun polynôme dénominateur q_i'' $(1 \le i \le w)$ ne peut être nul, puisque par définition le calcul β ne contient pas de division par zéro. Observons que les égalités $g = q_w$ et $q_w = \frac{q_w'}{q_w''}$ entraînent qu'au prix d'une seule division terminale, nous pouvons prolonger le circuit β_1 pour obtenir comme résultat final le polynôme g.

Pour nous résumer, nous pouvons supposer sans restriction de généralité que le calcul d'évaluation $\beta = (q_1, \ldots, q_w)$ satisfait aux conditions suivantes :
– sa longueur et sa profondeur sont respectivement majorées par $4L+1$ et $2l+1$,
– le sous-calcul $(q_1, \ldots, q_{w-1})$ s'exécute dans $k[t_1, \ldots, t_n]$ et ne contient aucune division,
– q_{w-1} est non nul, et g est égal à $q_w = \frac{q_{w-2}}{q_{w-1}}$,
– le degré des polynômes $q_1, \ldots, q_w$ et en particulier δ sont majorés par 2^l.

Choisissons maintenant un sous-ensemble Γ de k de cardinal $8L(1+2^l)^2$ (ce qui est possible en raison de l'hypothèse de non-finitude de k). Vu les caractéristiques du polynôme q_{w-1} rappelées ci-dessus, nous pouvons en appliquant la proposition et le corollaire 2.1 trouver dans

Γ^n un point γ n'annulant q_{w-1}, par un algorithme probabiliste du type Las Vegas en temps séquentiel $O(L(L+n)^2)$ et parallèle $O(l)$. Sans restriction de généralité, nous pouvons supposer que ce point γ est l'origine $(0,\ldots,0)$, et que la valeur de q_{w-1} en ce point est 1. Pour simplifier les notations nous écrirons $q_{w-1} := 1 - r$, où r est maintenant un polynôme qui s'annule à l'origine. Calculons ensuite à partir de q_{w-1} les puissances successives de r, les polynômes $r_0 := r^0 = 1, \ldots, r_\mu := r^\mu, \ldots, r_\delta := r^\delta$. Cette tâche peut être exécutée par un circuit dans $k[t_1,\ldots,t_n]$, sans divisions, de taille et de profondeur respectivement majorées par $\delta + 1$ et $2\log\delta + 1$. Finalement, les polynômes $q_{w-2}, r_0, \ldots, r_\delta$ peuvent être représentés par un calcul d'évaluation β_2 dans $k[t_1,\ldots,t_n]$, sans divisions, de taille et de profondeur respectivement majorées par $4L+\delta+2$ et $2(l+\log\delta)+1$. Ce calcul β_2 peut être construit à partir de β par un algorithme probabiliste du type Las Vegas en temps séquentiel $O(L(L+n)^2+\delta)$ et parallèle $O(l+\log\delta)$.

Interprétons maintenant les polynômes $q_1,\ldots,q_{w-1},q_w,r_0,\ldots,r_\delta$ comme des éléments de la k-algèbre de séries formelles $k[[t_1,\ldots,t_n]]$: q_{w-1} devient une unité, et son inverse est la série $1+\sum_{\mu>0} r^\mu$. Etant donné une série quelconque q de $k[[t_1,\ldots,t_n]]$ et un entier strictement positif ν, nous noterons $q^{(\nu)}$ sa partie homogène de degré ν, qui est un polynôme de $k[t_1,\ldots,t_n]$. De la preuve de [Stra 73], Satz 2 nous déduisons immédiatement que nous pouvons transformer en temps séquentiel $O(L\delta^2)$ et parallèle $O(l\log\delta)$ le circuit β_2 en un calcul β_3 dans $k[t_1,\ldots,t_n]$, sans divisions, qui pour tout indice ν conpris entre 0 et δ évalue les polynômes homogènes $q_w^{(\nu)}, r_0^{(\nu)}, \ldots, r_\delta^{(\nu)}$. La longueur et la profondeur de β_3 sont d'ordre $O(L\delta^2)$ et $O(l\log\delta)$. Maintenant de l'égalité dans $k[[t_1,\ldots,t_n]]$

$$g = q_{w-2}(1-r)^{-1} = q_{w-2}(1+\sum_{\mu>0} r^\mu)$$

nous déduisons pour tout ν compris entre 0 et δ l'égalité dans $k[t_1,\ldots,t_n]$

$$g^{(\nu)} = q_{w-2}^{(\nu)} + \sum_{0\le\mu\le\delta} \quad \sum_{0\le\nu_1, 0\le\nu_2, \nu_1+\nu_2=\nu} q_{w-2}^{(\nu_1)}\ r_\mu^{(\nu_2)}.$$

Comme le degré de g est au plus δ, nous obtenons ce polynôme comme somme de ses parties homogènes de degré au plus δ, et donc nous le représentons par un calcul d'évaluation β^* dans $k[t_1,\ldots,t_n]$, sans divisions, de longueur et de profondeur d'ordre $O(L\delta^2)$ et $O(l\log\delta)$. Il s'obtient à partir de β par un algorithme probabiliste du type Las Vegas en temps séquentiel $O(L(L+n)^2 + L\delta^2) = O(L^3n^2\delta^2)$ et parallèle $O(l\log\delta)$, cqfd.

2.3. Normalisation de Noether effective

Dans ce paragraphe, conformément aux notations de base introduites en 1.1 et 1.2.1, soient $f_1, f_2, \ldots, f_s$ des polynômes non constants de $k[x_1,\ldots,x_n]$, de degré majoré par $d \ge n$. Ils seront supposés donnés par leur écriture dans la représentation dense, qui est donc de taille $O(sd^n)$. Soit $V = \{f_1 = 0, \ldots, f_s = 0\}$ la sous-variété algébrique de $\mathbf{A}^n$ qu'ils définissent, de dimension $\dim V = r$. Comme ils sont non nuls, cette dimension est comprise entre -1 et $n-1$.

Rappelons d'après [Gi-He 91], 3.5.1 la terminologie suivante. Supposant que la dimension r soit positive ou nulle. Nous dirons que les variables $x_1,\ldots,x_r$ sont *libres* par rapport à la variété V si l'intersection dans $k[x_1,\ldots,x_n]$ de $k[x_1,\ldots,x_r]$ et de $(f_1,f_2,\ldots,f_s)$ se réduit à (0). Les variables $x_1,\ldots,x_n$ seront dites *en position de Noether* par rapport à V si les r premières sont libres par rapport à V et si 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. Avec ces conventions nous avons le résultat suivant :

2.3.1. Proposition :

(voir [Gi-He 91], Théorèmes 3.5 et 3.7.2 ; [Gi-He-Sa 93], Proposition A)
Il existe un réseau arithmétique sur k de taille $s^{O(1)}\, d^{O(n)}$ et de profondeur $O(n^2 \log^2 sd)$ qui exécute les tâches suivantes :
– il détermine la dimension $r = \dim V$ de la variété définie par $f_1, \ldots, f_s$.
– il calcule 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, elles soient en position de Noether par rapport à V.
En fait, les coefficients de cette matrice non singulière peuvent être choisis dans un sous-ensemble de k qui ne dépend que des paramètres d, s, n, qu'on peut se fixer a priori et arbitrairement sous réserve que son cardinal soit assez grand (d'ordre $s^{O(1)}\, d^{O(n)}$).
Le réseau ci-dessus peut être construit par un algorithme probabiliste de type aléatoire en temps séquentiel $s^{O(1)}\, d^{O(n)}$ et parallèle $O(n^2 \log^2 sd)$.

L'existence du réseau en question est démontré dans [Gi-He 91], Théorèmes 3.5 et 3.7.2. Le fait qu'il puisse être construit par un algorithme probabiliste aléatoire dans le temps prescrit découle immédiatement des propositions citées en appliquant l'outil technique [He-Schn 82], Theorem 4.4 dans sa version probabiliste (voir 2.1).

2.3.2. Définitions

Supposons pour le moment que V soit non vide (c'est-à-dire $r \geq 0$) et que les variables $x_1, \ldots, x_n$ soient en position de Noether par rapport à V, les r premières étant libres. Fixons alors pour ce paragraphe et ses deux successeurs les notations suivantes : appelons respectivement A l'algèbre $k[x_1, \ldots, x_r]$ et K son corps de fractions $k(x_1, \ldots, x_r)$. Rappelons que nous noterons $(f_1, \ldots, f_s)$ l'idéal engendré par $f_1, \ldots, f_s$ indifféremment dans $A[x_{r+1}, \ldots, x_n] = k[x_1, \ldots, x_n]$ ou $K[x_{r+1}, \ldots, x_n]$. Les algèbres quotients correspondantes seront notées B et B' :

$$\begin{aligned} B &:= A[x_{r+1}, \ldots, x_n]/(f_1, \ldots, f_s) = k[x_1, \ldots, x_n]/(f_1, \ldots, f_s) \\ B' &:= K[x_{r+1}, \ldots, x_n]/(f_1, \ldots, f_s) = k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]/(f_1, \ldots, f_s) \end{aligned}$$

Le morphisme canonique $A \to B$ est injectif et constitue une extension entière d'anneaux. L'algèbre B devient donc un A-module de type fini. Parallèlement, B' devient une K-algèbre de dimension finie. Notons D sa dimension, qui est strictement positive vu notre hypothèse sur V.

Si les polynômes $f_1, \ldots, f_s$ forment une suite régulière de $k[x_1, \ldots, x_n]$, B est un A-module libre, donc plat (voir une démonstration de ce fait bien connu par exemple dans [Gi-He-Sa 93] Lemma 3.3.1 et Corollary 3.3.2). Son rang est D. Et si de plus l'idéal engendré par $f_1, \ldots, f_s$ dans $k[x_1, \ldots, x_n]$ est radical, les k-algèbres B et B' sont réduites et on déduit des différentes versions de l'inégalité de Bézout les majorations $D \leq \deg V \leq d^n$ (voir par exemple [He 83], Theorem 1 et [Ca-Ga-He 89], Proposition 5 ou [Fu 84], Example 8.4.6).

Enfin nous noterons $\overline{} : k[x_1, \ldots, x_n] \longrightarrow B$ et $\overline{} : K[x_{r+1}, \ldots, x_n] \longrightarrow B'$ les morphismes de projection canoniques.

2.3.3. Diverses notions de complexité

Soit maintenant h un polynôme de $k[x_1, \ldots, x_n] = A[x_{r+1}, \ldots, x_n]$. Dans les sections 3.2, 3.4 et 4.2, nous allons utiliser le fait que h peut être codé par son écriture dans la représentation dense d'une part comme polynôme en les variables $x_1, \ldots, x_n$ (vecteur de ses coefficients éléments de k) et d'autre part comme polynôme en les variables $x_{r+1}, \ldots, x_n$ (vecteur de ses coefficients éléments de A ou de K). Dans la section 4.2 nous considérerons aussi le codage de h par un calcul d'évaluation β (avec ou sans divisions) dans $K[x_{r+1}, \ldots, x_n]$, en lui associant quatre mesures différentes de complexité, suivant que le corps de base est k ou K, et le déroulement séquentiel ou parallèle.

Si k est le corps de base, nous appellons suivant 1.2.3 *taille* ou *longueur*, *complexité séquentielle* ou *temps de déroulement séquentiel* de β le nombre de nœuds du circuit correspondant aux opérations arithmétiques d'addition, soustraction, multiplication et division dans $K[x_{r+1}, \ldots, x_n]$. Observons que les nœuds correspondant au choix d'une des variables $x_1, \ldots, x_n$ (nœuds d'entrées) ou d'une constante de k sont ignorés dans cette mesure de complexité. Parallèlement nous définissons la *profondeur*, *complexité parallèle* ou *temps de déroulement parallèle* du circuit le nombre maximal de nœuds correspondant à des opérations arithmétiques contenus dans un sous-chemin de β.

En prenant maintenant K comme corps de base, nous obtenons les notions correspondantes *non scalaires*. La longueur non scalaire (par rapport à K) est le nombre de nœuds qui ne correspondent pas à l'introduction de variables ou d'éléments de K comme opérations constantes, ou des opérations K-linéaires (addition, soustraction, multiplication par un élément de K et division par un élément de K). Les autres opérations effectuées par le circuit, qui dans toutes nos applications seront uniquement des multiplications dans $K[x_{r+1}, \ldots, x_n]$ par des éléments non contenus dans K, seront considérées comme non scalaires. La profondeur non scalaire du circuit (par rapport à K) est le nombre maximal de nœuds correspondant à des opérations non scalaires contenus dans un sous-chemin. Observons qu'en particulier les nœuds correspondant à des opérations effectuées dans K ne contribuent ni à la longueur ni à la profondeur non scalaires. Pour plus de précisions sur cette notion de complexité non scalaire nous renvoyons le lecteur à [Gi-He-Sa 93], section 3.4. La complexité séquentielle de la fonction h est le minimum les longueurs de tous les circuits qui représentent (c'est-à-dire évaluent) h. La complexité parallèle de h, ainsi que ses complexités séquentielle et parallèle non scalaires se définissent de manière analogue.

Dans les sections 3.4 et 4.2 nous allons considérer des $D \times D$-matrices à coefficients dans A ou K. Notons $A^{D\times D}$ la A-algèbre des $D \times D$-matrices à coefficients dans A et $K^{D\times D}$ la K-algèbre des $D \times D$-matrices à coefficients dans K. Soit M une matrice de $A^{D\times D}$ ou plus généralement de $K^{D\times D}$; son déterminant sera noté $\det M$. Nous dirons qu'un calcul d'évaluation dans K ou A représente M s'il évalue tous ses coefficients. De même, la complexité séquentielle ou parallèle de M sera celle de tous ses coefficients. Si M est à coefficients dans A le degré maximal de ses coefficients sera appelé son degré et noté $\deg M$ (voir aussi [Gi-He-Sa 93], section 3.4).

2.3.4. Définition de la complexité convenable

Donnons-nous une famille de polynômes de $k[x_1, \ldots, x_n]$ paramétrée par d et n (entiers strictement positifs). Nous dirons que le degré de cette famille est *convenable* s'il est d'ordre $d^{O(n)}$. S'il s'agit d'une famille de matrices à coefficients dans $k[x_1, \ldots, x_n]$, son degré sera convenable s'il vérifie la même propriété. Nous dirons que la complexité d'une famille de polynômes est convenable s'ils sont représentables par des calculs d'évaluation sans divisions de longueur $d^{O(n)}$ et de profondeur $O(n^2 \log^2 d)$. Dans le modèle de complexité probabiliste nous demanderons pour être convenable que les circuits qui représentent les polynômes de la famille soient engendrés par un algorithme probabiliste de type aléatoire en temps séquentiel $d^{O(n)}$ et parallèle $O(n^2 \log^2 d)$.

2.4. Algèbre linéaire effective dans l'anneau des coordonnées

Nous conservons les notations et hypothèses introduites dans la section précédente. En particulier nous supposons la variété non vide, ce qui implique que sa dimension r est positive ou nulle. Nous supposerons aussi que les variables $x_1, \ldots, x_n$ sont en position de Noether, les r premières étant libres.

Nous allons considérer le problème de trouver une base de la K-algèbre B' et de décrire l'opérateur de multiplication de manière effective. Ceci revient essentiellement au calcul d'une base standard (ou de Gröbner) de l'idéal de dimension zéro engendré par $f_1, \ldots, f_s$ dans l'algèbre $K[x_{r+1}, \ldots, x_n]$. Si l'algèbre B' est réduite, cette tâche peut être effectuée par un algorithme probabiliste de type aléatoire en temps séquentiel $s^{O(1)}d^{O(n)}$ et parallèle $O(n^2 \log^2 sd)$ (voir [Gi-He 91], 3.4.6, 3.4.7 et Lemme 3.6.1 ; [Gi-He-Sa 93] Proposition A et Lemma 3.4.2) :

2.4.1. Proposition principale

(voir [Gi-He-Sa 93], Lemma 3.4.2)
Supposons que l'idéal engendré par les polynômes $f_1, \ldots, f_s$ dans $k[x_1, \ldots, x_n]$ soit radical. Il existe un algorithme probabiliste aléatoire qui calcule à partir des coefficients de l'entrée $f_1, \ldots, f_s$ en temps séquentiel $s^{O(1)}d^{O(n)}$ et parallèle $O(n^2 \log^2 sd)$ les quantités suivantes :
– un polynôme non nul τ de $A = k[x_1, \ldots, x_r]$
– des polynômes $e_1 = 1, \ldots, e_D$ de $k[x_1, \ldots, x_n]$
– des $D \times D$ matrices $M_{r+1}, \ldots, M_n$ à coefficients dans A
tels que les images canoniques $\overline{e}_1, \ldots, \overline{e}_D$ dans B' forment une K-base $\overline{e}$ du K-espace vectoriel B' et $\frac{1}{\tau}M_{r+1}, \ldots, \frac{1}{\tau}M_n$ soient les matrices dans cette base des applications linéaires qu'induisent dans B' les multiplications par $\overline{x}_{r+1}, \ldots, \overline{x}_n$.
Du point de vue de la complexité nous avons les propriétés suivantes :
– la dimension $D = \dim_K B$ est majorée par $d^{n-r} \leq d^n$
– les coefficients des matrices $M_{r+1}, \ldots, M_n$, les polynômes $e_1 = 1, \ldots, e_D$ et τ sont des polynômes de degré $d^{O(n)}$ représentés par des calculs d'évaluation sans divisions dans A (ou $k[x_1, \ldots, x_n]$) de longueur $s^{O(1)}d^{O(n)}$ et de profondeur $O(n^2 \log^2 sd)$.

Cette proposition représente une légère généralisation de [Gi-He-Sa 93], Lemma 3.4.2 et sa preuve que nous omettons ici est identique à celle de *loc. cit.*

2.4.2. Raffinement

Dans la proposition précédente, l'hypothèse que l'idéal $f_1, \ldots, f_s$ soit radical (ou la K-algèbre B' soit réduite) est essentielle pour sa démonstration, basée sur une application de [Gi-He 91], Lemme 3.6.1. Au prix de la perte du caractère bien parallélisable de l'algorithme (à savoir la borne $O(n^2 \log^2 sd)$ pour la complexité parallèle qui peut croître exponentiellement tout en maintenant les mêmes bornes pour la complexité séquentielle et les degrés des polynômes), nous obtenons en abandonnant cette hypothèse une version analogue de la proposition 2.4.1. Pour obtenir ce résultat, il nous suffit de remplacer dans la preuve de la proposition 2.4.1 toutes les applications de [Gi-He 91], lemme 3.6.1 par le théorème 3.6.2 *loc. cit.*

2.5. Passage d'un calcul d'évaluation à la matrice associée

Nous conservons les notations de 2.3 et 2.4, nous supposant fixé un jeu d'objets construits par la proposition 2.4. En particulier nous nous donnons des polynômes $e_1 = 1, \ldots, e_D$ de $k[x_1, \ldots, x_n]$ tels que les images canoniques $\overline{e}_1, \ldots, \overline{e}_D$ forment une K-base $\overline{e}$ de B'. A un polynôme h de $K[x_{r+1}, \ldots, x_n]$ nous associons la matrice M_h dans la base $\overline{e}$ de l'application linéaire qu'induit dans B' la multiplication par h. La matrice M_h appartient à $K^{D\times D}$, et n'est pas autre chose que $h(M_{x_{r+1}}, \ldots, M_{x_n}) = h(\frac{1}{\tau}M_{r+1}, \ldots, \frac{1}{\tau}M_n)$ (voir [Gi-He-Sa 93], section 3.4). Nous pouvons alors formuler le résultat suivant :

2.5.1. Proposition principale

(voir [Gi-He-Sa 93], Lemma 3.4.4)
Supposons que l'idéal engendré par $f_1, \ldots, f_s$ soit radical. Soit g un polynôme de $K[x_{r+1}, \ldots, x_n]$ représenté par un calcul d'évaluation β dans $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$ de longueur L, de longueur non scalaire Λ, de profondeur l et de profondeur non scalaire λ, les complexités non scalaires étant prises par rapport à $K = k(x_1, \ldots, x_r)$. Supposons aussi que β ne contienne que des divisions par des éléments de K. Alors la $D \times D$-matrice M_g peut être représentée par un calcul d'évaluation β' dans $k(x_1, \ldots, x_r)$ de longueur $L + c\Lambda^2 D^3 + s^c d^{cn}$ et profondeur $l + c(\lambda \log D + n^2 \log^2 sd)$, où c est une constante positive qui ne dépend pas de K.
De plus β' peut être construit à partir de β et des coefficients de $f_1, \ldots, f_s$ en temps séquentiel $L + c\Lambda^2 D^3 + s^c d^{cn}$ et parallèle $l + c(\lambda \log D + n^2 \log^2 sd)$ par un algorithme probabiliste de type aléatoire. Le circuit β' peut être étendu à un calcul d'évaluation dans $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$, de même longueur et profondeur, qui contient β et donc représente le polynôme g. Le nouveau calcul ne contient que des divisions par des éléments de $k(x_1, \ldots, x_r)$ et a pour longueur et profondeur non scalaires Λ et λ.

Cette proposition représente une légère généralisation de [Gi-He-Sa 93], Lemma 3.4.4 et sa preuve que nous omettons ici est identique à celle de *loc. cit.*.

2.5.2. Raffinement

Dans la proposition précédente, l'hypothèse que l'idéal $f_1, \ldots, f_s$ soit radical (ou la K-algèbre B' soit réduite) est essentielle pour sa démonstration. Au prix de la renonciation à la borne $l + O(\lambda \log D + n^2 \log^2 sd)$ pour la complexité parallèle (qui peut croître exponentiellement en n tout en maintenant la même borne pour la complexité séquentielle), nous obtenons en abandonnant cette hypothèse une version analogue de la proposition 2.4. Les arguments sont les mêmes que dans la remarque 2.4.2.

3. Théorie élémentaire de la trace pour les intersections complètes

Dans toute cette partie, nous supposerons que les polynômes $f_1, \ldots, f_s$ forment une suite régulière de $k[x_1, \ldots, x_n]$. Uniquement pour des considérations de complexité, nous ajouterons l'hypothèse que l'idéal qu'ils engendrent est égal à son radical. La dimension de l'intersection complète V ainsi définie dans $\mathbf{A}^n$ sera notée $r := n - s$. Nous supposerons de plus effectué un changement de coordonnées linéaire mettant les variables en position de Noether par rapport à la variété (voir 2.3), et les variables renommées de telle façon que les r premières soient libres par rapport à la variété.

Rappelons encore de 2.3 que nous notons A l'algèbre $k[x_1,\ldots,x_r]$, K son corps de fractions $k(x_1,\ldots,x_r)$, respectivement B et B' les algèbres quotients $B := k[x_1,\ldots,x_n]/(f_1,\ldots,f_s)$ et $B' := k(x_1,\ldots,x_r)[x_{r+1},\ldots,x_n]/(f_1,\ldots,f_s)$. La théorie de la trace s'applique donc à la A-algèbre ci-dessus qui est intersection complète (donc de Gorenstein), finie et plate, de même qu'à la K-algèbre B' qui possède les mêmes propriétés. Nous allons rappeler les éléments dont nous aurons besoin ci-dessous, en nous inspirant de l'exposition de [Ku 86] Appendices E et F. La base théorique de nos résultats est un théorème de dualité dû à [Wie 69] et [Sche-Stor 75] (comparer avec [Ku 86], Corollary E.21). Notons aussi que dans un contexte différent mais toujours avec une préoccupation effective cette dualité apparaît explicitement dans [Jou 92] (formes de Morley) et implicitement dans [Be-Yg 91].

3.1. Rappels

Le A-module $B^* := \mathrm{Hom}_A(B, A)$ devient un B-module comme suit : si b et β sont respectivement des éléments de B et B^*, le produit $b.\beta : B \to A$ est l'application A-linéaire définie par $(b.\beta)(x) = \beta(bx)$. En tant que B-modules, B et son dual B^* sont isomorphes (voir [Ku 86] Example F.19 et Corollary F.10), et une *trace* est un générateur σ du B-module monogène B^* (un tel générateur existe puisque l'anneau B est de Gorenstein). Tout ceci reste valable pour B' *mutatis mutandis*. Remarquons que par localisation toute trace σ de B peut être étendue à une trace σ' de B', qui néanmoins envoie encore B dans A.

Considérons maintenant le produit tensoriel $B \otimes_A B$ que nous pouvons considérer à la fois comme A-algèbre et B-bimodule. Le morphisme de A-algèbres $\mu : B \otimes_A B \to B$ défini par $\mu(a \otimes b) := ab$ est aussi un morphime de bimodules. Son noyau $\mathcal{K}$ est l'idéal engendré par les éléments de la forme $b \otimes 1 - 1 \otimes b$, où b parcourt B (voir par exemple [Iv 73] démonstration de la Proposition 1.3).

L'annulateur $\mathrm{Ann}_{B\otimes_A B}(\mathcal{K})$ hérite maintenant de deux structures de B-module. Mais vu la forme des générateurs mentionnés de $\mathcal{K}$, les produits à gauche et à droite d'un élément de $\mathrm{Ann}_{B\otimes_A B}(\mathcal{K})$ par un même élément de B sont égaux :

$$\sum_m ba_m \otimes c_m = \sum_m a_m \otimes bc_m \tag{1}$$

et donc les deux structures coïncident. Cet annulateur est donc en fait canoniquement un B-module. Comme B admet une trace, cet annulateur lui est isomorphe, donc est monogène (voir [Ku 86] Corollary F.10).

Même faute, même punition pour $\mathrm{Ann}_{B'\otimes_K B'}(\mathcal{K}')$, en introduisant de manière analogue le morphisme μ' et son noyau $\mathcal{K}'$.

Rappelons maintenant comment calculer un générateur de $\mathrm{Ann}_{B\otimes_A B}(\mathcal{K})$ ou de $\mathrm{Ann}_{B'\otimes_K B'}(\mathcal{K}')$ à partir de $f_1,\ldots,f_s$.

3.2. Un déterminant pseudo-jacobien

Nous allons d'abord expliciter les produits tensoriels. Introduisons s nouvelles indéterminées $y_{r+1},\ldots,y_n$. Etant donné un polynôme h de $k[x_1,\ldots,x_n] = A[x_{r+1},\ldots,x_n]$ (ou une fraction rationnelle de $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n] = K[x_{r+1}, \ldots, x_n]$), associons-lui le polynôme $h^{(y)}$ de $A[y_{r+1}, \ldots, y_n]$ (ou la fraction rationnelle de $K[y_{r+1}, \ldots, y_n]$) défini par :

$$h^{(y)} := h(x_1, \ldots, x_r, y_{r+1}, \ldots, y_n).$$

Notons alors $I^{(y)}$ (resp. $I^{(y)\prime}$) les idéaux engendrés par $(f_1^{(y)}, \ldots, f_s^{(y)})$ dans $A[y_{r+1}, \ldots, y_n]$ (resp. $K[y_{r+1}, \ldots, y_n]$). Le produit tensoriel $B \otimes_A B$ s'identifie à $A[x_{r+1}, \ldots, x_n, y_{r+1}, \ldots, y_n]/I + I^{(y)}$, et $B' \otimes_K B'$ à $K[x_{r+1}, \ldots, x_n, y_{r+1}, \ldots, y_n]/I' + I^{(y)\prime}$.

L'image canonique dans B (resp. B') d'un polynôme h de $A[x_{r+1}, \ldots, x_n]$ (resp. d'une fraction rationnelle de $K[x_{r+1}, \ldots, x_n]$) sera notée $\overline{h}$. De même, étant donné un polynôme g de $A[x_{r+1}, \ldots, x_n, y_{r+1}, \ldots, y_n]$ qui admet donc une décomposition de la forme $\sum_{1 \leq m \leq N} a_m c_m$ ($a_m \in A[x_{r+1}, \ldots, x_n]$, $c_m \in A[y_{r+1}, \ldots, y_n]$), nous noterons encore $\overline{g}$ l'image $\sum_{1 \leq m \leq N} \overline{a}_m \otimes \overline{c}_m$ dans $B \otimes_A B$. Même notation pour l'image d'une fraction de $K[x_{r+1}, \ldots, x_n, y_{r+1}, \ldots, y_n]$ dans $B' \otimes_K B'$.

Soit $(l_{ij})_{1 \leq i,j \leq s}$ une $s \times s$-matrice de polynômes de $A[x_{r+1}, \ldots, x_n, y_{r+1}, \ldots, y_n]$ vérifiant les s relations linéaires suivantes :

$$f_i^{(y)} - f_i = \sum_{j=1}^{s} l_{ij}(y_{r+j} - x_{r+j}) \tag{2}$$

pour tout indice i entre 1 et s. L'existence d'une telle matrice est assurée par le théorème de Taylor sans reste. Les l_{ij} peuvent être choisis comme des polynômes de $k[x_1, \ldots, x_n, y_{r+1}, \ldots, y_n]$, de degré encore majoré par d, et dont nous pouvons calculer une écriture dans la représentation dense en temps séquentiel $d^{O(n)}$ et parallèle $O(n \log d)$ à partir des coefficients de $f_1, \ldots, f_s$.

Soit Δ le déterminant de cette matrice. C'est un polynôme de $A[x_{r+1}, \ldots, x_n, y_{r+1}, \ldots, y_n]$ et comme tel, il admet comme nous l'avons vu ci-dessus une représentation (non unique!) :

$$\Delta = \sum_{1 \leq m \leq N} a_m c_m \ , \ a_m \in A[x_{r+1}, \ldots, x_n] \ , \ c_m \in A[y_{r+1}, \ldots, y_n], \tag{3}$$

où a_m est un élément de $A[x_{r+1}, \ldots, x_n] = k[x_1, \ldots, x_r, x_{r+1}, \ldots, x_n]$ et c_m un élément de $A[y_{r+1}, \ldots, y_n] = k[x_1, \ldots, x_r, y_{r+1}, \ldots, y_n]$. Ce déterminant est de degré est au plus nd, et l'algorithme de Berkowitz [Ber 84] le donne par un calcul d'évaluation sans divisions dans $k[x_1, \ldots, x_n, y_{r+1}, \ldots, y_n]$ avec lequel nous pouvons reconstruire son écriture dans la représentation dense en temps séquentiel $d^{O(n)}$ et parallèle $O(n^2 \log d)$. Nous pouvons trouver par un algorithme uniforme l'écriture de $2N = d^{O(n)}$ polynômes a_m et c_m vérifiant (3), de degré également majoré par nd, avec les mêmes ordres de complexités.

Associons maintenant à Δ son image $\overline{\Delta} = \sum_{1 \leq m \leq N} \overline{a}_m \otimes \overline{c}_m$ par l'application canonique dans $B \otimes_A B$. Cette décomposition n'est pas uniquement déterminée par les générateurs donnés de l'idéal I, mais néanmoins l'élément $\overline{\Delta}$ de $B \otimes_A B$ est indépendant de la représentation (2) (voir [Ku 86] Lemma E.19 et Example F.19), et $\mu(\overline{\Delta})$ est égal à l'image dans B du déterminant de la matrice jacobienne $(\frac{\partial f_i}{\partial x_{r+j}})_{1 \leq i,j \leq s}$. De plus, $\overline{\Delta}$ engendre le B-module $\mathrm{Ann}_{B \otimes_A B}(\mathcal{K})$ et le B'-module $\mathrm{Ann}_{B' \otimes_K B'}(\mathcal{K}')$ (voir [Ku 86] Corollary E.21 et Example F.19). Enfin, observons que vu la forme particulière des générateurs du noyau $\mathcal{K}$ nous avons d'après (1) :

$$b\overline{\Delta} = \sum_{1 \leq m \leq N} b\overline{a}_m \otimes \overline{c}_m = \sum_{1 \leq m \leq N} \overline{a}_m \otimes b\overline{c}_m = \overline{\Delta}b \tag{4}$$

pour tout élément b de B.

3.3. Construction théorique d'une trace

Il existe des isomorphismes canoniques de B-bimodules :

$$B \otimes_A B \cong B \otimes_A B^* \cong \mathrm{Hom}_A(B^*, B).$$

Le premier est une conséquence de l'existence d'une trace de la A-algèbre B), tandis que pour la seconde nous utilisons de plus que B est un A-module libre de type fini. Soit $\Phi : B \otimes_A B \to \mathrm{Hom}_A(B^*, B)$ l'isomorphisme composé, qui est défini explicitement par :

$$\Phi\,(\sum_p u_p \otimes v_p)(\beta) := \sum_p u_p\,\beta(v_p) \tag{5}$$

Cet isomorphisme de B-bimodules induit un isomorphisme de B-modules, encore noté Φ :

$$\Phi : \mathrm{Ann}_{B\otimes_A B}(\mathcal{K}) \longrightarrow \mathrm{Hom}_B(B^*, B)$$

(voir [Ku 86] Proposition F.9). Donc $\Phi(\overline{\Delta})$ est un générateur du B-module $\mathrm{Hom}_B(B^*, B)$ (qui est isomorphe à B). Observons qu'un élément σ de B^* est une trace de la A-algèbre B si et seulement si $\Phi(\overline{\Delta})(\sigma)$ est une unité de B. Il existe donc une trace de σ de la A-algèbre B uniquement déterminée par la relation :

$$\Phi(\overline{\Delta})(\sigma) = \sum_{1\leq m\leq N} \overline{a}_m\,\sigma(\overline{c}_m) = 1. \tag{6}$$

La trace σ déterminée par la relation (6) s'appelle la trace associée à $\overline{\Delta}$ (voir [Ku 86] Corollary F.10). Soit σ' la trace étendue de la K-algèbre B' obtenue par localisation de σ. Elle vérifie encore une relation du type :

$$\sum_{1\leq m\leq N} \overline{a}_m\,\sigma'(\overline{c}_m) = 1.$$

3.4. Explicitation d'une matrice de la trace et sa complexité

Nous allons maintenant appliquer les outils théoriques rappelés dans les paragraphes 3.1, 3.2 et 3.3 à notre contexte. Ce qui nous intéresse ici est l'emploi de cette dualité en toute dimension. Dans le cas particulier d'une intersection complète de dimension zéro, l'utilité de ces techniques pour l'algorithmique a été découverte indépendemment par d'autres auteurs (voir par exemple [Car 93] et les références citées dans [Moe 93]).

Posons donc D égal à la dimension de B' sur K. Nous allons maintenant calculer explicitement la matrice de la trace σ' dans une base de B', et évaluer la complexité de cet algorithme.

3.4.1. Lemme

Au prix d'une préparation préalable ou par un algorithme probabiliste de type aléatoire, nous pouvons calculer à partir des coefficients de $f_1, \ldots, f_s$ en temps séquentiel $d^{O(n)}$ et parallèle $O(n^2 \log^2 d)$ les objets suivants :

– *un polynôme non nul τ de $A = k[x_1, \ldots, x_r]$,*
– *des polynômes $e_1 = 1, \ldots, e_D$ de $k[x_1, \ldots, x_n]$,*
– *des $D \times D$-matrices $M_{r+1}, \ldots, M_n$ à coefficients dans A,*

tels que les images canoniques $\overline{e}_1, \ldots, \overline{e}_D$ *dans* B' *forment une* K*-base* $\overline{e}$ *du* K*-espace vectoriel* B' *et* $\frac{1}{\tau}M_{r+1}, \ldots, \frac{1}{\tau}M_n$ *soient les matrices dans cette base des applications* K*-linéaires qu'induisent dans* B' *les multiplications par* $\overline{x}_{r+1}, \ldots, \overline{x}_n$*,*
– des polynômes a_m *de* $A[x_{r+1}, \ldots, x_n]$ *et* c_m *de* $A[y_{r+1}, \ldots, y_n]$ $(1 \leq m \leq N)$ *tels que l'élément* $\Delta := \sum_{1 \leq m \leq N} a_m c_m$ *induise dans* $B \otimes_A B$ *un générateur* $\overline{\Delta} = \sum_{1 \leq m \leq N} \overline{a}_m \otimes \overline{c}_m$ *du* B*-module* $\mathrm{Ann}_{B \otimes_A B}(\mathcal{K})$*,*
– des polynômes $\theta_1, \ldots, \theta_D$ *de* A *tels que la matrice dans la base* $\overline{e}$ *de la trace de* B' *associée à* $\overline{\Delta}$ *soit la matrice* $(\theta_1, \ldots, \theta_D)$*.*

Du point de vue de la complexité, nous avons les propriétés suivantes :

– la dimension D *est majorée par* d^n*,*
– les a_m *et les* c_m *sont des polynômes de degré au plus* nd *en nombre* $N = d^{O(n)}$*, donnés par leur écriture dans la représentation dense de* $k[x_1, \ldots, x_r, x_{r+1}, \ldots, x_n]$ *et* $k[x_1, \ldots, x_r, y_{r+1}, \ldots, y_n]$*,*
– les coefficients des matrices M_i*, les* τ *et* θ_i *sont des polynômes de degré* $d^{O(n)}$ *représentés par un calcul d'évaluation dans* $k[x_1, \ldots, x_r]$ *de longueur* $d^{O(n)}$ *et de profondeur* $O(n^2 \log^2 d)$*.*

Avant de commencer la preuve du lemme, ajoutons la remarque suivante à son énoncé : les calculs d'évaluation qui représentent les coefficients des matrices $M_{r+1}, \ldots, M_n$ et le polynôme τ ne contiennent aucune division. Néanmoins, pour la représentation de chaque polynôme θ_i $(1 \leq i \leq D)$ dans le temps prescrit, nous avons besoin d'une division (et d'une seule) qui s'exécute à la fin du calcul dans $k[x_1, \ldots, x_n]$. En principe nous pouvons éliminer cette division en appliquant la proposition 2.2. De cette manière nous laissons inchangé l'ordre asymptotique de la complexité séquentielle de notre algorithme, qui reste un $d^{O(n)}$, tandis que la complexité parallèle saute à $O(n^3 \log^3 d)$.

3.4.2. Démonstration

Nous ne donnerons ici qu'une preuve complète pour le modèle non uniforme. En observant que tous les algorithmes utilisés possèdent une version aléatoire, il est facile de vérifier la version probabiliste.
Comme par hypothèse les variables sont en position de Noether par rapport à la variété V définie par $f_1, \ldots, f_s$ et que l'idéal $I = (f_1, \ldots, f_s)$ est égal à son radical, nous déduisons des différentes versions de l'inégalité de Bézout que nous avons $D \leq \deg V \leq d^s \leq d^n$ (voir par exemple [He 83], Theorem 1, [Ca-Ga-He 89], Proposition 5 ou [Fu 84], Example 8.4.6).

A partir des coefficients de $f_1, \ldots, f_s$, nous pouvons d'après 2.4 et 3.2 calculer au prix d'une préparation préalable dans le temps prescrit des polynômes $e_1, \ldots, e_D$, τ, a_m et c_m $(1 \leq m \leq N)$ et des matrices $M_{r+1}, \ldots, M_n$ possédant les propriétés requises. En particulier $M_{r+1}, \ldots, M_n$ et τ sont de degré et de complexité convenables (voir 2.3.4 ; dans la suite de la démonstration nous supposerons ces objets fixés).

3.4.3. Les matrices induites par les multiplications

Comme dans 2.5, à chaque fraction rationnelle h de $K[x_{r+1}, \ldots, x_n] = k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$ associons l'endomorphisme linéaire $\overline{h}$ de B' qu'induit la multiplication par h. La matrice correspondante dans la K-base fixée $\overline{e}_1, \ldots, \overline{e}_D$ de B' s'appellera M_h. En particulier, les matrices

M_{x_i} ne sont autres que les $\frac{1}{\tau}M_i$ $(r+1 \leq i \leq n)$, et la matrice M_h de $K^{D\times D}$ s'écrit :

$$M_h = h(x_1, \ldots, x_r, M_{x_{r+1}}, \ldots, M_{x_n}).$$

Considérons maintenant la matrice $Q_m := \tau^{nd} M_{a_m}$, pour un indice m compris entre 1 et N. Posons pour simplifier $\rho := \tau^{nd}$; c'est un polynôme non nul de $k[x_{r+1}, \ldots, x_n]$ de complexité convenable. Vu que le polynôme a_m est de degré au plus nd, la matrice Q_m est à coefficients dans A et est en fait un polynôme de degré au plus nd en les matrices $M_{r+1}, \ldots, M_n$, avec des coefficients dans A. Mais comme l'écriture de a_m est de taille $d^{O(n)}$, que D est majoré par d^n et que $M_{r+1}, \ldots, M_n$ sont des matrices de $A^{D\times D}$ de complexité et de degré convenables, il en est de même pour la matrice Q_m. De plus, la construction à partir de $f_1, \ldots, f_s$ de ces N calculs d'évaluation représentant les Q_m requiert, après une préparation préalable, un temps séquentiel $d^{O(n)}$ et parallèle $O(n^2 \log^2 d)$.

Soit q_{jm} $(1 \leq j \leq D,\ 1 \leq m \leq N)$ le coefficient de Q_m sur la ligne j et la première colonne ; la matrice formée par les q_{jm} sera appelée Q. Nous construisons des polynômes e_j^* en nombre D comme suit :

$$e_j^* := \sum_{1\leq m\leq N} q_{jm} c_m^{(x)},$$

où $c_m^{(x)}$ est le polynôme de $A[x_{r+1}, \ldots, x_n]$ obtenu en substituant dans c_m les variables $x_{r+1}, \ldots,$ x_n aux variables $y_{r+1}, \ldots, y_n$. Comme polynômes de $A[x_{r+1}, \ldots, x_n]$, les e_j^* sont de degré majoré par nd (par rapport aux variables $x_{r+1}, \ldots, x_n$) et leur écriture est de taille $d^{O(n)}$. Leurs coefficients sont des polynômes de $k[x_1, \ldots, x_r]$ de complexité et de degré convenables. Par conséquent les coefficients de la $D\times D$-matrice $\rho M_{e_j^*} = \rho e_j^*(x_1, \ldots, x_r, \frac{1}{\tau}M_{r+1}, \ldots, \frac{1}{\tau}M_n)$ sont des polynômes de $k[x_1, \ldots, x_r]$ de complexité et de degré convenables. Pour nous résumer, tous ces résultats s'obtiennent donc à partir de $f_1, \ldots, f_s$, après une préparation préalable, en temps séquentiel $d^{O(n)}$ et parallèle $O(n^2 \log^2 d)$.

En ajoutant aux considérations précédentes la remarque que le premier élément $\overline{e}_1$ de la base $\overline{e}$ de B' est l'unité 1, nous obtenons l'écriture :

$$\rho\overline{a}_m = q_{1m}\overline{e}_1 + \cdots + q_{Dm}\overline{e}_D$$

ou autrement dit, les égalités matricielles :

$$\begin{array}{rcl} (\rho\overline{a}_1, \ldots, \rho\overline{a}_N) & = & (\overline{e}_1, \ldots, \overline{e}_D)\, Q \\ \begin{pmatrix} \overline{e}_1^* \\ \vdots \\ \overline{e}_D^* \end{pmatrix} & = & Q \begin{pmatrix} \overline{c}_1 \\ \vdots \\ \overline{c}_N \end{pmatrix}. \end{array}$$

Ceci implique les égalités :

$$\begin{array}{rcl} \rho\overline{\Delta} & = & \displaystyle\sum_{1\leq m\leq N} \rho\overline{a}_m \otimes \overline{c}_m = \sum_{1\leq j\leq D\,,\,1\leq m\leq N} q_{jm}\overline{e}_j \otimes \overline{c}_m \\ & = & \displaystyle\sum_{1\leq j\leq D\,,\,1\leq m\leq N} \overline{e}_j \otimes q_{jm}\overline{c}_m = \sum_{1\leq j\leq D} \overline{e}_j \otimes \overline{e}_j^*. \end{array}$$

D'où l'expression de $\overline{\Delta}$ dans $B' \otimes_A B'$:

$$\overline{\Delta} = \sum_{1 \le j \le D} \overline{e}_j \otimes \frac{1}{\rho} \overline{e}_j^*. \tag{7}$$

Soit σ la trace de la A-algèbre B associée au générateur $\overline{\Delta}$ du B-module $\mathrm{Ann}_{B \otimes B}(\mathcal{K})$. De manière analogue, soit σ' la trace de la K-algèbre B' associée à $\overline{\Delta}$, qui est obtenue par localisation de σ. Comme $\overline{e}_1, \ldots, \overline{e}_D$ est une base de B', nous déduisons immédiatement de [Ku 86] Proposition F.11 les relations d'orthogonalité :

$$\sigma(\overline{e}_i \overline{e}_j^*) = \sigma'(\overline{e}_i \overline{e}_j^*) = \rho \delta_{ij} \tag{8}$$

où δ_{ij} est le symbole de Kronecker. La même proposition assure que $(\overline{e}_1^*, \ldots, \overline{e}_D^*)$ est une K-base de B'. Soit $E = (\varepsilon_{ij})_{1 \le i,j \le D}$ la $D \times D$-matrice à coefficients dans A formée par les premières colonnes des matrices $\rho M_{e_1^*}, \ldots, \rho M_{e_D^*}$, ε son déterminant et $(\eta_1, \ldots, \eta_D)$ la première ligne de la matrice adjointe. Les ε_{ij}, ε et η_j sont des polynômes de $k[x_1, \ldots, x_r]$ de complexité et de degré convenables. De plus, tous ces polynômes s'obtiennent à partir de $f_1, \ldots, f_s$, après une préparation préalable, en temps séquentiel $d^{O(n)}$ et parallèle $O(n^2 \log^2 d)$. Finalement nous avons :

$$\begin{pmatrix} \rho \overline{e}_1^* \\ \vdots \\ \rho \overline{e}_D^* \end{pmatrix} = E \begin{pmatrix} \overline{e}_1 \\ \vdots \\ \overline{e}_D \end{pmatrix}.$$

ce qui prouve que ε n'est pas nul, et comme $\overline{e}_1$ vaut 1, ce déterminant s'écrit $\varepsilon = \eta_1 \rho \overline{e}_1^* + \cdots + \eta_D \rho \overline{e}_D^*$. Les relations d'orthogonalité (8) impliquent alors pour tout i :

$$\varepsilon \sigma(\overline{e}_i) = \rho \sum_{1 \le j \le D} \eta_j \sigma(\overline{e}_i \overline{e}_j^*) = \rho^2 \, \eta_i.$$

Comme σ est une trace de la A-algèbre B et comme $\rho^2 \, \eta_i$ est un polynôme de A de degré $d^{O(n)}$, nous en déduisons que $\theta_i := \sigma(\overline{e}_i) = \frac{1}{\varepsilon} \rho^2 \, \eta_i$ aussi, et qu'il s'évalue par un calcul bien parallélisable dans A de longueur $d^{O(n)}$ avec une seule division finale par un élément de A qui est de degré $d^{O(n)}$ et qui est compris dans les résultats précédents du circuit. D'après la proposition 2.2 nous pouvons éliminer cette division en laissant inchangé l'ordre $d^{O(n)}$ de la complexité séquentielle de l'algorithme, tandis que la parallèle grimpe à $O(n^3 \log^3 d)$.

4. Deux propositions techniques

4.1. Test d'annulation d'un polynôme sur une variété équidimensionnelle

Soient $f_1, \ldots, f_s$ des polynômes de $k[x_1, \ldots, x_n]$ de degré majoré par d, représentés par leur écriture dense, et définissant une variété V équidimensionnelle et réduite de dimension r. Par ailleurs, soit g un polynôme de $k[x_1, \ldots, x_n]$ représenté par un calcul d'évaluation sans divisions de longueur L et de profondeur l.

Alors au prix d'une préparation préalable ou par un algorithme probabiliste de type aléatoire, nous pouvons tester par un algorithme sans divisions en temps séquentiel $L^4 s^{O(1)} d^{O(n)}$ et parallèle $O(l n \log d + n^2 \log^2 sd)$ si g appartient à l'idéal $(f_1, \ldots, f_s)$. Dans le cas où $f_1, \ldots, f_s$ forment une suite régulière, nous pouvons tester avec la même complexité si l'image $\overline{g}$ de g dans

$B = k[x_1, \ldots, x_n]/(f_1, \ldots, f_s)$ *est un diviseur de zéro.*

Démonstration : Nous ne donnerons ici qu'une preuve complète pour le modèle non uniforme. En observant que tous les algorithmes utilisés possèdent une version aléatoire, il est facile de vérifier la version probabiliste.
Notons d'abord que la mise en position de Noether s'est effectuée par un algorithme bien parallélisable, et largement dans le temps prescrit (voir 2.3).

L'idéal J engendré par $f_1, \ldots, f_s$ dans l'algèbre $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$ définit alors une variété réduite de dimension 0 sur une clôture algébrique de $k(x_1, \ldots, x_r)$. Nous pouvons donc lui appliquer la proposition 2.4 pour obtenir une base du $k(x_1, \ldots, x_r)$-espace vectoriel $B' := k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]/J$, et ce toujours par un algorithme bien parallélisable en temps $s^{O(1)}d^{O(n)}$, donc dans le temps prescrit.

La même proposition nous fournit un polynôme non nul τ de $A := k[x_1, \ldots, x_n]$ et des matrices $M_{r+1}, \ldots, M_n$ à coefficients dans A. Le polynôme τ et les matrices $M_{r+1}, \ldots, M_n$ sont de degré $d^{O(n)}$ et représentés par un calcul d'évaluation sans divisions dans A de longueur et profondeur $s^{O(1)}d^{O(n)}$ et $O(n^2 \log^2 sd)$. Ils satisfont aux conditions $\frac{1}{\tau}M_{r+1} = M_{x_{r+1}}, \ldots, \frac{1}{\tau}M_n = M_{x_n}$.

Par ailleurs, la proposition 2.5 nous construit à partir de l'entrée g la $D \times D$-matrice M_g à coefficients dans K. Les coefficients de la matrice sont représentés par un calcul d'évaluation dans $k(x_1, \ldots, x_r)$ qui s'obtient en temps séquentiel $L^2 d^{O(n)} + s^{O(1)}d^{O(n)}$ et parallèle $O(ln \log d + n^2 \log^2 d)$. La longueur et la profondeur de ce calcul d'évaluation sont du même ordre. Soit $\gamma := 2^l$; observons que nous avons $2^L \geq \gamma \geq \deg g$. De l'égalité $M_g = g(x_1, \ldots, x_r, M_{x_{r+1}}, \ldots, M_{x_n})$ nous déduisons que la matrice $M := \tau^\gamma M_g$ appartient à $A^{D \times D}$ et que son degré est d'ordre $\gamma d^{O(n)}$. Comme g et $M_{r+1} = \tau M_{x_{r+1}}, \ldots, M_n = \tau M_{x_n}$ s'évaluent sans divisions, le même résultat est vrai pour les coefficients de M (voir la démonstration de Lemma 3.4.4 dans [Gi-He-Sa 93]). Par conséquent M est représenté par un calcul d'évaluation sans divisions dans $k[x_1, \ldots, x_n]$ de longueur $L^2 d^{O(n)} + s^{O(1)}d^{O(n)}$ et de profondeur $O(ln \log d + n^2 \log^2 sd)$.

Remarquons ensuite que, vu l'hypothèse d'équidimensionnalité sur V, le fait que g s'annule sur V est équivalent à la nullité de la matrice M_g, elle-même équivalente à la nullité de M. D'après la proposition et le corollaire 2.1, il existe un ensemble questeur de $L^4 s^{O(1)}d^{O(n)}$ points sur lesquels l'annulation des calculs d'évaluation représentant les coefficients de M implique en fait leur nullité. La vérification de la nullité de M se fait donc bien par un algorithme sans divisions en temps séquentiel $L^4 s^{O(1)}d^{O(n)}$ et parallèle $O(ln \log d + n^2 \log^2 sd)$. Observons que cette dernière complexité n'est pas affectée par le cardinal de l'ensemble questeur.

Supposons maintenant que $f_1, \ldots, f_s$ forment une suite régulière de $k[x_1, \ldots, x_n]$. Le fait que l'image $\overline{g}$ de g dans B soit un diviseur de zéro est équivalent à la singularité de la matrice M_g, elle-même équivalente à la nullité du déterminant de M. En appliquant l'algorithme de Berkowitz [Be 84] à la matrice M, nous pouvons représenter ce déterminant par un calcul d'évaluation sans divisions. Comme précédemment, il existe un ensemble questeur de taille similaire, et la vérification de la nullité de ce déterminant se fait avec les mêmes complexités, y compris la remarque sur la complexité parallèle.

4.2. Division exacte de fonctions sur une variété intersection complète réduite

Nous noterons respectivement A, B et K les k-algèbres $k[x_1,\ldots,x_r]$, $k[x_1,\ldots,x_n]/(f_1,\ldots,f_s)$ et $k(x_1,\ldots,x_r)$. Nous supposerons une fois de plus que la variété définie par $f_1,\ldots,f_s$ est de dimension r et que les variables $x_1,\ldots,x_n$ sont en position de Noether par rapport à la variété, les variables libres étant les r premières (voir 2.3).

Proposition : *Soient $f_1,\ldots,f_s$ des polynômes de $k[x_1,\ldots,x_n]$ de degré majoré par d, représentés par leur écriture dense, et définissant une variété V intersection complète réduite de dimension $r := n-s$. Supposons de plus que d vaut au moins n.*
Soient f et g deux polynômes de $k[x_1,\ldots,x_n]$, représentés par des calculs d'évaluations β_* et β dans $k(x_1,\ldots,x_r)[x_{r+1},\ldots,x_n]$, qui ne contiennent que des divisions par des éléments de $k(x_1,\ldots,x_r)$. Soient L_* la longueur, Λ_* la longueur non scalaire (par rapport à $k(x_1,\ldots,x_r)$), l_* la profondeur et λ_* la profondeur non scalaire (par rapport à $k(x_1,\ldots,x_r)$) du calcul β_*. De manière analogue nous nous donnons les caractéristiques L, Λ, l et λ du calcul β.
Soient δ et v les degrés partiels de g respectivement en les variables $x_1,\ldots,x_r$ et $x_{r+1},\ldots,x_n$.
Supposons de plus que l'image $\overline{f}$ de f dans B ne soit pas un diviseur de zéro et que $\overline{f}$ divise $\overline{g}$.

Alors il existe un réseau arithmétique sur le corps de base k, de taille $L' := L + L_* + O((\Lambda^2 + \Lambda_*^2)d^{3n}) + d^{O(n)}$ et de profondeur $l' := l + l_* + O(n(\lambda+\lambda_*)\log d + n^2\log^2 d)$, qui exécute la tâche ci-dessous :
le réseau construit un calcul d'évaluation β' dans $k(x_1,\ldots,x_r)[x_{r+1},\ldots,x_n]$, de taille $L' = L + L_* + O((\Lambda^2+\Lambda_*^2)d^{3n}) + d^{O(n)}$ et de profondeur $l' = l + l_* + O(n(\lambda+\lambda_*)\log d + n^2\log^2 d)$, n'effectuant que des divisions par des éléments de $k(x_1,\ldots,x_r)$, et représentant un polynôme p de $k[x_1,\ldots,x_n]$ qui possède les propriétés suivantes :
– $\overline{g} = \overline{p}\,\overline{f}$ dans B,
– le degré partiel de p en les variables $x_1,\ldots,x_r$ est égal à $\delta + (1 + v + \deg f)d^{O(n)}$,
– le degré partiel de p en les variables $x_{r+1},\ldots,x_n$ est majoré par nd.
La longueur et la profondeur non scalaires de β' par rapport à $k(x_1,\ldots,x_r)$ sont respectivement d'ordre $\Lambda + \Lambda_* + d^{O(n)}$ et $\lambda + \lambda_* + O(n\log d)$, et β' contient comme sous-calcul β.

Enfin il existe un algorithme probabiliste de type aléatoire qui construit le réseau ci-dessus en temps séquentiel et parallèle du même ordre que L' et l'.

Démonstration : Elle va résulter des points suivants, que nous présenterons uniquement dans leur version non uniforme (la version probabiliste se démontrant de manière absolument analogue) :

4.2.1. Rappel

Nous nous plaçons sous les hypothèses de 3.4 dont nous suivrons les notations. En particulier fixons nous $e_1 = 1,\ldots,e_D$ dans $k[x_1,\ldots,x_n]$, τ non nul dans A, $a_1,\ldots,a_N$ de $A[x_{r+1},\ldots,x_n]$ et $c_1,\ldots,c_N$ dans $A[y_{r+1},\ldots,y_n]$. Considérons d'abord les matrices M_{c_m} $(1 \le m \le N)$. De manière absolument analogue à 3.4.3, nous en déduisons que les coefficients de la matrice $\tau^{nd}M_{c_m}$ sont des polynômes de A de degré et de complexité et de degré convenables, et que comme N est un $d^{O(n)}$, c'est l'ensemble de ces N matrices qui est de complexité et de degré convenables. Ceci entraîne que les N matrices M_{c_m} $(1 \le m \le N)$ peuvent être représentées par un calcul d'évaluation dans K qui est bien parallélisable et de longueur $d^{O(n)}$.
Rappelons que $\overline{f}$ divise $\overline{g}$ dans B.

4.2.2. Complexité en termes de degrés

Soient δ_* et v_* les degrés partiels de f respectivement en les variables $x_1, \dots, x_r$ et $x_{r+1}, \dots, x_n$. La somme $\delta_* + v_*$ est donc encadrée par $\deg f$ et $2 \deg f$. Considérons les matrices M_f et M_g de $K^{D\times D}$. En les multipliant par la puissance *ad hoc* de τ (à savoir respectivement v_* et v), il est clair qu'elles deviennent à coefficients dans $A = k[x_1, \dots, x_r]$ de degré respectivement $\delta_* + v_* d^{O(n)}$ et $\delta + v d^{O(n)}$. L'hypothèse que $\overline{f}$ est non diviseur de zéro dans B implique que la matrice M_f est régulière. Le déterminant de $\tau^{v_*} M_f$ est un polynôme de A de degré $D(\delta_* + v_* d^{O(n)}) = (\delta_* + v_*) d^{O(n)} = \deg f d^{O(n)}$, et les coefficients de la matrice $\det(\tau^{v_*} M_f) M_f^{-1}$ possèdent la même propriété. Enfin soit ϱ le polynôme $\tau^{v+nd} \det(\tau^{v_*} M_f)$; c'est un élément non nul de A de degré $(v + \deg f + 1) d^{O(n)}$. Pour tout indice m compris entre 1 et N, les coefficients de la $D \times D$-matrice $\varrho\, M_g M_f^{-1} M_{c_m}$ sont des polynômes de A de degré $\delta + (v + \deg f + 1) d^{O(n)}$.

Soit (η_{jm}) la $D \times N$-matrice à coefficients dans K formée par les premières colonnes des matrices $M_g M_f^{-1} M_{c_m}$ $(1 \leq m \leq N)$. Les $\varrho\, \eta_{jm}$ sont des polynômes de A de degré $\delta + (v + \deg f + 1) d^{O(n)}$.

Rappelons que par hypothèse il existe un polynôme q de $k[x_1, \dots, x_n]$ vérifiant l'identité dans B :

$$\overline{g} = \overline{q}\, \overline{f} \tag{9}$$

qui se traduit aisément pour tout m compris entre 1 et N en :

$$M_{q c_m} = M_g M_f^{-1} M_{c_m}$$

et comme le premier élément $\overline{e}_1$ de la base de B' vaut l'unité, en :

$$\varrho\, \overline{q}\, \overline{c}_m = (\varrho\, \eta_{1m})\, \overline{e}_1 + \cdots + (\varrho\, \eta_{Dm})\, \overline{e}_D \tag{10}$$

Finalement, comme les $\theta_j = \sigma(\overline{e}_j)$ sont d'après le lemme 3.4 des polynômes de A de degré $d^{O(n)}$, nous en déduisons de l'identité précédente que $u_m := \varrho\, \sigma(\overline{q}\, \overline{c}_m)$ est un polynôme de A de degré $\delta + (v + \deg f + 1) d^{O(n)}$. Mais comme $\overline{q}\, \overline{c}_m$ est un élément de B, son image par la trace σ appartient à A et son degré est aussi $\delta + (v + \deg f + 1) d^{O(n)}$.

4.2.3. Complexité en termes de calculs d'évaluation

Etudions maintenant comment représenter les $\sigma(\overline{q}\, \overline{c}_m)$ par des calculs d'évaluation dans K (donc avec divisions).

La proposition 2.5 implique qu'au prix d'une préparation préalable, nous pouvons construire à partir des données $f_1, \dots, f_s, g$ en temps séquentiel $L + O(\Lambda^2 d^{3n}) + d^{O(n)}$ et parallèle $l + O(n\lambda \log d + n^2 \log^2 d)$ un calcul d'évaluation dans K avec les deux mêmes complexités qui représente les coefficients de la matrice M_g. Le même résultat est valable *mutatis mutandis* à partir des donnés $f_1, \dots, f_s, f$ pour aboutir à une représentation de la matrice non singulière M_f et de son inverse par un calcul d'évaluation de longueur $L_* + O(\Lambda_*^2 d^{3n}) + d^{O(n)}$ et de profondeur $l_* + O(n\lambda_* \log d + n^2 \log^2 d)$. Finalement d'après la même proposition 2.5 nous pouvons étendre les algorithmes qui représentent les matrices M_g et M_f à un calcul d'évaluation dans $K[x_{r+1}, \dots, x_n]$ de longueur L', de longueur non scalaire $\Lambda + \Lambda_*$, de profondeur l' et de profondeur non scalaire $\lambda + \lambda_*$, et qui contient comme sous-calcul β.

En joignant ce qui précède à 4.2.1, nous obtenons un calcul d'évaluation dans K de longueur L' et de profondeur l' qui représente les matrices $M_{qc_m} = M_g M_f^{-1} M_{c_m}$ et a fortiori la matrice (η_{jm}).

D'un autre côté d'après 3.4 les polynômes $\theta_1 = \sigma(\overline{e}_1), \ldots, \theta_D = \sigma(\overline{e}_D)$ sont de degré $d^{O(n)}$ et ils sont représentés par un calcul d'évaluation dans A (avec divisions) de complexité séquentielle $d^{O(n)}$ et parallèle $O(n^2 \log^2 d)$. De l'identité (10) nous déduisons maintenant pour tout m (compris entre 1 et N) l'égalité $\overline{q}\,\overline{c}_m = \eta_{1m}\,\overline{e}_1 + \cdots + \eta_{Dm}\,\overline{e}_D$ et donc que les N polynômes $\sigma(\overline{qc}_1), \ldots, \sigma(\overline{qc}_N)$ sont représentés par un calcul d'évaluation dans K de longueur L' et de profondeur l', obtenu à partir des entrées $f_1, \ldots, f_s, f, g$ par un réseau arithmétique sur k de même complexité.

4.2.4. La dernière ligne droite

Considérons maintenant le polynôme p de $k[x_1, \ldots, x_n]$ défini par :

$$p := \sum_{1 \leq m \leq N} a_m\, \sigma(\overline{qc}_m). \tag{11}$$

Nous déduisons alors immédiatement des bornes obtenues en 3.4 et 4.2.2 que ce polynôme satisfait aux conditions sur ses degrés partiels demandées dans le lemme. De plus, de la décomposition (11) nous voyons qu'il est représenté par un calcul d'évaluation β' dans $K[x_{r+1}, \ldots, x_n]$ de longueur L' et de profondeur l'. Il ne contient que des divisions par des éléments de K et peut être construit à partir des entrées $f_1, \ldots, f_s, f, g$ par un réseau arithmétique sur k de même complexité. D'après 4.2.3, le calcul β' contient comme sous-calcul β. De plus, nous déduisons immédiatement de la décomposition (11) que la longueur et la profondeur non scalaires (par rapport à $k(x_1, \ldots, x_r)$) de β' sont respectivement d'ordre $\Lambda + \Lambda_* + d^{O(n)}$ et $\lambda + \lambda_* + O(n \log d)$. Des identités (4) et (6) découle la suite d'identités :

$$\begin{aligned} \overline{q} &= \overline{q}\Phi(\overline{\Delta})(\sigma) = \sum_{1\leq m\leq N} \overline{q}\,\overline{a}_m \sigma(\overline{c}_m) = \Phi(\sum_{1\leq m\leq N} \overline{q}\,\overline{a}_m \otimes \overline{c}_m)(\sigma) \\ &= \Phi(\sum_{1\leq m\leq N} \overline{a}_m \otimes \overline{q}\,\overline{c}_m)(\sigma) = \sum_{1\leq m\leq N} \overline{a}_m \sigma(\overline{q}\,\overline{c}_m) = \overline{p}. \end{aligned}$$

et finalement de (9) la relation de divisibilité recherchée :

$$\overline{g} = \overline{p}\,\overline{f}.$$

4.2.5. Corollaire

Soient $f_1, \ldots, f_s, g$, β, A, B, K et les complexités $L, \Lambda, l, \lambda, \delta, v$ comme dans la proposition précédente. Soit f un polynôme de degré au plus d donné par son écriture dense, et supposons que l'image $\overline{f}$ de f dans B ne soit pas diviseur de zéro. Alors il existe un réseau arithmétique sur k de taille $L + O(\Lambda^2 d^{3n}) + d^{O(n)}$ et de profondeur $l + O(n\lambda \log d + n^2 \log^2 d)$ possédant les propriétés suivantes :

– le réseau construit un calcul d'évaluation β_1 dans $k(x_1, \ldots, x_r)[x_{r+1}, \ldots, x_n]$ qui représente un polynôme g^* de $k[x_1, \ldots, x_n]$ ayant même image que g dans B, de degré partiel en les variables $x_{r+1}, \ldots, x_n$ et $x_1, \ldots, x_r$ respectivement majoré par nd et $\delta + (v+1)d^{O(n)}$. Le calcul β_1 n'exécute que des divisions par des éléments de $k(x_1, \ldots, x_r)$; il est de longueur $L + O(\Lambda^2 d^{3n}) + d^{O(n)}$ et de profondeur $l + O(n\lambda \log d + n^2 \log^2 d)$. Sa longueur et sa profondeur non scalaires (par rapport à K) sont respectivement d'ordre $\Lambda + d^{O(n)}$ et $\lambda + O(n \log d)$. De plus, il contient comme

sous-calcul le circuit β qui représente g.

– au cas où $\overline{f}$ divise $\overline{g}$ dans B, le réseau produit un calcul d'évaluation β_2 dans $K[x_{r+1}, \ldots, x_n]$, de mêmes caractéristiques que β_1, qui représente un polynôme p de $k[x_1, \ldots, x_n]$ tel que les images de g et de pf coïncident dans B. Le degré partiel en les variables $x_{r+1}, \ldots, x_n$ et $x_1, \ldots, x_r$ est respectivement majoré par nd et $\delta + (v+1)d^{O(n)}$. Enfin il existe un algorithme probabiliste de type aléatoire qui construit le réseau ci-dessus en temps séquentiel $L + O(\Lambda^2 d^{3n}) + d^{O(n)}$ et parallèle $l + O(n\lambda \log d + n^2 \log^2 d)$.

La preuve de ce corollaire découle immédiatement de la proposition précédente en prenant pour la première partie de l'énoncé f égal à 1 et en notant pour la seconde que les complexités d'évaluation séquentielle et parallèle d'un polynôme de degré d à n variables (c'est-à-dire f) donné par son écriture valent $d^{O(n)}$ et $O(n \log d)$.

4.2.6. Remarque

La proposition 4.2 et le corollaire 4.2.5 restent vraies en ce qui concerne la complexité *séquentielle* et le degré si l'on supprime l'hypothèse que l'idéal $f_1, \ldots, f_s$ est égal à son radical. Par contre, nous ne connaissons pas dans ce cas plus général de bornes satisfaisantes en fonction de la taille de l'entrée pour la complexité parallèle.

Ceci est dû au fait que nos arguments utilisent de manière essentielle les propositions 2.4 et 2.5. Celles-ci sont basées sur le calcul d'une base standard du *radical* d'un idéal donné par générateurs en écriture dense, par un algorithme non uniforme (respectivement probabiliste) qui est bien parallélisable et polynomial en la taille de l'entrée (voir [Gi-He 91] lemme 3.6.1). Si l'on veut supprimer l'hypothèse d'idéal radical, il faut remplacer cet algorithme par un algorithme généraliste qui calcule une base standard de l'idéal lui-même. Un tel algorithme est donné dans [Gi-He 91] théorème 3.6.2. Malheureusement, il n'est pas bien parallélisable (voir les remarques 2.4.2 et 2.5.2). Le reste de la démonstration du lemme 3.4, de la proposition 4.2 et du corollaire 4.2.5 s'adaptent ensuite sans problème à ce remplacement.

Voyons maintenant un énoncé d'algèbre commutative conséquence de la proposition et de la remarque. Ce corollaire est dans l'esprit des théorèmes des zéros effectifs d'algèbre commutative [Bro 87], [Ca-Ga-He 88], [Ca-Ga-He 89], [Ko 88] (voir aussi [Phi 88], [Fi-Ga 90], [Be-Yg 90], [Shi 89], [Am 89], [Bro 89], [Ca-Gu-Gu 91]), mais il n'est conséquence d'aucun d'entre eux. A la différence des travaux [Ko 88], [Phi 88], [Fi-Ga 90], [Am 89], [Bro 89], [Ca-Gu-Gu 91] qui aboutissent à des théorèmes des zéros avec bornes sur les degrés du type d^n ($d \geq 3$ et $n \geq 2$), sa preuve est totalement élémentaire, si tenté que des arguments d'algèbre homologique relèvent de techniques plus sophistiquées ...

4.2.7. Corollaire

Soit k un corps commutatif arbitraire et soient $f_1, \ldots, f_s, f, g$ des polynômes de $k[x_1, \ldots, x_n]$ tels que $f_1, \ldots, f_s, f$ forment une suite régulière de $k[x_1, \ldots, x_n]$. Posons $r := n - s$ et $d := \max\{\deg f_1, \ldots, \deg f_s\}$. Supposons que les variables $x_1, \ldots, x_n$ (resp. les r premières) soient en position de Noether (resp. libres) par rapport à la variété algébrique définie par $f_1, \ldots, f_s$. Appelons enfin respectivement δ et v le degré partiel de g par rapport aux r premières et $n - r$ dernières variables.

Alors si g appartient à l'idéal $(f_1, \ldots, f_s, f)$, il existe un polynôme p de $k[x_1, \ldots, x_n]$ tel que g soit congru à pf modulo l'idéal $(f_1, \ldots, f_s)$, les degrés partiels de p par rapport à $x_{r+1}, \ldots, x_n$ et $x_1, \ldots, x_r$ étant majorés respectivement par nd et $\delta + (1 + v + \deg f)d^{O(n)}$.

Ajoutons ici que sous une hypothèse additionnelle, un raffinement de nos méthodes permet de préciser la borne sur le degré de p. Si le jacobien de $f_1, \ldots, f_s$ par rapport aux variables $x_{r+1}, \ldots, x_n$ n'est pas un diviseur de zéro modulo l'idéal $(f_1, \ldots, f_s)$, le degré partiel de p par rapport à $x_1, \ldots, x_r$ peut être borné par $\deg V(1 + \max\{\deg f + s(d-1), \deg g\} + s(d-1)$ (voir [Sa-So 92]).

Remarquons enfin que dans toutes les bornes de degré apparaissant dans le lemme 3.4, la proposition 4.2 et ses corollaires 4.2.5 et 4.2.7, le paramètre n (dimension ambiante) peut être remplacé par s (codimension de la variété algébrique définie par $f_1, \ldots, f_s$). Ceci reste vrai également pour les bornes de complexité avec la modification suivante : si les polynômes $f_1, \ldots, f_s$ sont donnés par un calcul d'évaluation sans divisions de longueur L_1 et de profondeur l_1, il y a lieu de remplacer dans toutes les bornes de complexité mentionnées le terme $d^{O(n)}$ par $L_1^{O(1)} d^{O(s)}$ et le terme $n \log d$ par $l_1 + s \log d$. Cet argument permet d'interpréter la proposition 4.2 comme une généralisation du résultat principal de [Ka 88] qui traite du problème du calcul du pgcd de deux polynômes à n variables donnés par un calcul d'évaluation. Nous renonçons à donner ici une preuve de ce raffinement, parce qu'elle impliquerait une révision complète de nos résultats antérieurement rédigés [Gi-He 91] et [Gi-He-Sa 93], sans apporter une innovation essentielle des techniques. L'intérêt porté actuellement aux résultats généraux de complexité en calcul formel ne justifierait peut-être pas un tel effort.

5. Deux théorèmes des zéros effectifs en termes de calculs d'évaluation

5.1. Un théorème des zéros effectif pour l'annulation d'un polynôme sur une intersection complète réduite

Théorème : *Soient $f_1, \ldots, f_s$ des polynômes de $k[x_1, \ldots, x_n]$ de degré majoré par $d \geq n$, représentés par leur écriture dense, et possédant la propriété suivante : pour tout indice i compris entre $n-s$ et $n-1$, les polynômes $f_1, \ldots, f_{n-i}$ définissent une variété V_i intersection complète réduite de dimension i. Soit g un polynôme de $k[x_1, \ldots, x_n]$ représenté par un calcul d'évaluation β dans $k[x_1, \ldots, x_n]$ qui ne contient aucune division. Soient L la longueur et l la profondeur du calcul β.*

Alors il existe un réseau arithmétique sur le corps de base k de taille $L' := L^6(\deg g)^2 d^{O(n)}$ et de profondeur $l' := O(l^2 \log(\deg g) n^7 \log^4 d)$ qui décide si le polynôme g appartient à l'idéal $(f_1, \ldots, f_s)$.
Si c'est le cas, le réseau construit un calcul d'évaluation β' dans $k[x_1, \ldots, x_n]$ de longueur $(L \deg g)^2 d^{O(n)}$ et de profondeur $O(l^2 \log(\deg g) n^7 \log^4 d)$, ne contenant aucune division et qui représente des polynômes $p_1, \ldots, p_s$ vérifiant les propriétés suivantes :
– $g = p_1 f_1 + \cdots + p_s f_s$
– le degré des $p_1, \ldots, p_s$ est d'ordre $(\deg g)\, d^{O(n)}$.
Enfin il existe un algorithme probabiliste de type aléatoire qui construit le réseau ci-dessus en temps séquentiel et parallèle du même ordre que L' et l'.

Démonstration : L'idéal $(f_1, \ldots, f_s)$ est par définition radical et définit une variété algébrique intersection complète, donc équidimensionnelle. D'après 4.1 nous pouvons donc décider en temps

séquentiel $L^4 d^{O(n)}$ et parallèle $O(nl \log d + n^2 \log^2 d)$ par un algorithme probabiliste de type aléatoire si le polynôme g appartient à $(f_1, \ldots, f_s)$. Supposons dorénavant que ce soit le cas.
En appliquant la proposition 2.3 simultanément aux variétés $V_{n-s}, \ldots, V_{n-2}$ nous pouvons aussi supposer que pour tout indice i compris entre $n-s$ et $n-2$ les variables $x_1, \ldots, x_n$ (resp. $x_1, \ldots, x_i$) soient en position de Noether (resp. libres) par rapport à V_i.
Posons $v := \max\{\deg g, (n+1)d\}$. Par récurrence sur i compris entre $n-s$ et $n-2$ nous construisons des calculs d'évaluation β_i dans $k(x_1, \ldots, x_{i+1})[x_{i+2}, \ldots, x_n]$ ne contenant que des divisions par des éléments de $k(x_1, \ldots, x_{i+1})$ qui représentent des polynômes $p_s, \ldots, p_{n-i}$ de $k[x_1, \ldots, x_n]$ vérifiant les affirmations I et II suivantes.

Notons L_i la longueur du calcul β_i, l_i sa profondeur, Λ_i et λ_i sa longueur et profondeur non scalaire (par rapport à $k(x_1, \ldots, x_{i+1})$). Soit δ_i le maximum des degrés partiels des polynômes $p_s, \ldots, p_{n-i}$ en les variables $x_1, \ldots, x_{i+1}$. Nous allons choisir une constante universelle $c > 0$ qui soit notamment indépendante des paramètres d, n, L, l et suffisamment grande pour que les affirmations suivantes soient satisfaites.

Affirmation I :
Soit p_s le polynôme représenté par le circuit β_{n-s}. Alors le polynôme g est congru à $p_s f_s$ modulo l'idéal $f_1, \ldots, f_{s-1}$. Le degré partiel de p_s en les variables $x_{n-s+2}, \ldots, x_n$ est majoré par nd. Les quantités $L_{n-s}, \Lambda_{n-s}, l_{n-s}, \lambda_{n-s}, \delta_{n-s}$ vérifient les inégalités suivantes :

$$\begin{array}{lrcl}
(I_1) & L_{n-s} & \leq & L^2\, d^{cn} \\
(I_2) & \Lambda_{n-s} & \leq & L + d^{cn} \\
(I_3) & l_{n-s} & \leq & c(nl \log d + n^2 \log^2 d) \\
(I_4) & \lambda_{n-s} & \leq & l + cn \log d \\
(I_5) & \delta_{n-s} & \leq & v\, d^{cn}.
\end{array}$$

Le calcul β_{n-s}, qui contient β comme sous-calcul, peut être construit par un algorithme probabiliste de type aléatoire en temps séquentiel $L^2\, d^{cn}$ et parallèle $c(nl \log d + n^2 \log^2 d)$.

Affirmation II :
Soit i un indice compris entre $n-s+1$ et $n-2$, et soient $p_s, \ldots, p_{n-i}$ les polynômes représentés par le circuit β_i. Alors le polynôme g est congru à $p_s f_s + \cdots + p_{n-i} f_{n-i}$ modulo l'idéal $f_1, \ldots, f_{n-i-1}$. Le degré partiel de $p_s, \ldots, p_{n-i}$ en les variables $x_{i+2}, \ldots, x_n$ est majoré par nd. Les quantités $L_i, \Lambda_i, l_i, \lambda_i, \delta_i$ vérifient les inégalités suivantes :

$$\begin{array}{lrcl}
(II_1) & L_i & \leq & L_{i-1} + c\Lambda_{i-1}^2\, d^{3n} + d^{cn} \\
(II_2) & \Lambda_i & \leq & \Lambda_{i-1} + d^{cn} \\
(II_3) & l_i & \leq & l_{i-1} + c(n\lambda_{i-1}^2 \log d + n^2 \log^2 d) \\
(II_4) & \lambda_i & \leq & \lambda_{i-1} + cn \log d \\
(II_5) & \delta_i & \leq & \delta_{i-1} + v\, d^{cn}.
\end{array}$$

Le calcul β_i, qui contient β comme sous-calcul, peut être construit à partir de β_{i-1} par un algorithme probabiliste de type aléatoire en temps séquentiel $L_{i-1} + c\Lambda_{i-1}^2\, d^{3n} + d^{cn}$ et parallèle $l_{i-1} + c(n\lambda_{i-1}^2 \log d + n^2 \log^2 d)$.

Pour tout indice i compris entre $n-s+1$ et $n-2$, appelons B_i la k-algèbre quotient $k[x_1, \ldots, x_n]/(f_1, \ldots, f_{n-i-1})$ et notons $\bar{\ } : k[x_1, \ldots, x_n] \longrightarrow B_i$ le morphisme de projection canonique.

Montrons d'abord qu'il existe un circuit β_{n-s} vérifiant l'affirmation I. Le polynôme g, dont le degré partiel en les variables $x_{n-s+2}, \ldots, x_n$ est majoré par v, appartient par hypothèse à l'idéal $(f_1, \ldots, f_s)$. Par conséquent l'image $\overline{f_s}$ de f_s divise l'image $\overline{g}$ de g dans $B_{n-s+1} = k[x_1, \ldots, x_n]/(f_1, \ldots, f_{s-1})$, et n'est pas diviseur de zéro puisque les polynômes $f_1, \ldots, f_s$ forment une suite régulière de $k[x_1, \ldots, x_n]$. Comme par hypothèse les polynômes $f_1, \ldots, f_{s-1}$ définissent une variété intersection complète réduite V_{n-s+1}, et que les variables $x_1, \ldots, x_n$ (resp. $x_1, \ldots, x_{n-s+1}$) soient en position de Noether (resp. libres) par rapport à V_{n-s+1}, l'application du corollaire 4.2.5 aboutit à un polynôme p_s de $k[x_1, \ldots, x_n]$, représenté par un calcul d'évaluation β_{n-s} dans $k(x_1, \ldots, x_{n-s+1})[x_{n-s+2}, \ldots, x_n]$ satisfaisant les conditions de l'affirmation I. Observons finalement que la construction esquissée du circuit β_{n-2} peut être effectuée par un algorithme probabiliste de type aléatoire dans le temps prescrit.

Soit maintenant i un indice compris entre $n - s + 1$ et $n - 2$, et supposons donné un calcul d'évaluation β_{i-1} dans $k(x_1, \ldots, x_i)[x_{i+1}, \ldots, x_n]$ ne contenant que des divisions par des éléments de $k(x_1, \ldots, x_i)$ qui représente des polynômes $p_s, \ldots, p_{n-i+1}$ de $k[x_1, \ldots, x_n]$, et vérifiant les conditions suivantes :

– le polynôme $r := g - (p_s f_s + \cdots + p_{n-i+1} f_{n-i+1})$ appartient à l'idéal $(f_1, \ldots, f_{n-i})$

– le degré partiel de $p_s, \ldots, p_{n-i+1}$ en les variables $x_{i+1}, \ldots, x_n$ est majoré par nd.

– β_{i-1} contient le circuit β comme sous-calcul et n'effectue que des divisions par des éléments de $k(x_1, \ldots, x_i)$.

Notons L_{i-1} et l_{i-1} la longueur et profondeur de β_{i-1}, Λ_{i-1} et λ_{i-1} sa longueur et profondeur non scalaires par rapport à $k(x_1, \ldots, x_i)$. Soit δ_{i-1} le maximum des degrés partiels des polynômes $p_s, \ldots, p_{n-i+1}$ en les variables $x_1, \ldots, x_i$. Par hypothèse le polynôme r appartient à l'idéal $f_1, \ldots, f_{n-i}$, peut être calculé à partir de β_{i-1} avec $2n$ multiplications et additions et son degré partiel en les variables $x_{i+1}, \ldots, x_n$ est majoré par v. Observons que le degré partiel de r en les variables $x_1, \ldots, x_i$ est majoré par le maximum de v et $d + \delta_{i-1}$, tandis que le degré total de $p_s, \ldots, p_{n-i+1}$ l'est par $\delta_{i-1} + nd$. Pour pouvoir appliquer le corollaire 4.2.5, il faut comme dans la preuve de l'affirmation I vérifier que l'image $\overline{f}_{n-i}$ de f_{n-i} n'est pas diviseur de zéro dans $B_i = k[x_1, \ldots, x_n]/(f_1, \ldots, f_{n-i-1})$, que $\overline{f}_{n-i}$ divise l'image $\overline{r}$ et observer que $f_1, \ldots, f_{n-i-1}$ définissent bien une intersection complète réduite V_{i+1}, par rapport à laquelle les variables sont en position de Noether (les $i + 1$ premières étant libres). Nous obtenons alors un polynôme p_{n-i} de $k[x_1, \ldots, x_n]$ représenté par un calcul β_i dans $k(x_1, \ldots, x_{i+1})[x_{i+2}, \ldots, x_n]$ tel que les conclusions de l'affirmation II soient établies :

– l'égalité $\overline{r} = \overline{p}_{n-i}\overline{f}_{n-i}$ a lieu dans B_i, ce qui implique bien que le polynôme g est congru à $p_s f_s + \cdots + p_{n-i} f_{n-i}$ modulo l'idéal $f_1, \ldots, f_{n-i-1}$.

– le degré partiel de p_{n-i} en les variables $x_{i+2}, \ldots, x_n$ est majoré par nd. Comme par hypothèse de récurrence le degré partiel de $p_s, \ldots, p_{n-i+1}$ en les mêmes variables est aussi majoré par nd, nous concluons.

– le degré partiel de p_{n-i} en les variables $x_1, \ldots, x_{i+1}$ est d'ordre $\delta_{i-1} + vd^{O(n)}$. Comme par hypothèse de récurrence le degré total de $p_s, \ldots, p_{n-i+1}$ est majoré par $\delta_{i-1} + nd$, nous en concluons qu'il existe une constante $c > 0$ telle que le degré partiel de $p_s, \ldots, p_{n-i}$ en les variables $x_1, \ldots, x_{i+1}$ est au plus $\delta_{i-1} + vd^{cn}$, ce qui constitue bien l'affirmation $(II)_5$.

– le calcul β_i, qui représente p_{n-i}, n'effectue que des divisions par des éléments de $k(x_1, \ldots, x_{i+1})$ et contient le circuit β_{i-1} comme sous-calcul. Par conséquent, il contient aussi β et il représente de plus les polynômes $p_s, \ldots, p_{n-i+1}$. Enfin, il existe bien une constante $c > 0$ telle que les quatre complexités de β_i vérifient $(II)_1, \ldots, (II)_4$ et telle qu'il existe un algorithme probabiliste de type aléatoire qui construise β_i à partir de β_{i-1} dans les temps annoncés.

Ceci achève la démonstration de l'affirmation (II).

Considérons maintenant un indice i compris entre $n-s$ et $n-2$. Les inégalités (I_5) et (II_5) impliquent

$$\delta_i \leq ivd^{cn} \leq nvd^{cn}. \tag{12}$$

La quantité δ_i borne le degré partiel du polynôme p_{n-i} en les variables $x_1, \ldots, x_{i+1}$. Par ailleurs, son degré partiel en les variables $x_{i+2}, \ldots, x_n$ est majoré par nd d'après I et II. Donc l'inégalité (12) implique

$$\deg p_{n-i} \leq \delta_i + nd \leq n(vd^{cn} + c). \tag{13}$$

Comme la quantité v est égale au maximum du degré de g et de $(n+1)d$, et que d est minoré par n, nous déduisons de (13) la borne

$$\deg p_{n-i} = (\deg g)\, d^{O(n)}. \tag{14}$$

Quant aux inégalités (I_2), (II_2), (I_4) et (II_4), elles entraînent

$$\Lambda_i \leq L + id^{cn} \leq L + nd^{cn} \tag{15}$$

et

$$\lambda_i \leq l + cin \log d \leq l + cn^2 \log d. \tag{16}$$

Puis à l'aide de (15) et (16) nous déduisons de (II_1) et (II_3) pour tout indice i compris entre $n-s+1$ et $n-2$ les inégalités :

$$L_i \leq L_{i-1} + c(L + nd^{cn})^2 d^{3n} + d^{cn} \tag{17}$$

et

$$l_i \leq l_{i-1} + c((l + cn^2 \log d)^2 n \log d + n^2 \log^2 d). \tag{18}$$

Pour tout indice i compris entre $n-s$ et $n-2$, nous établissons alors comme conséquences de (I_1) et (17) les estimations

$$L_i \leq L^2 d^{cn} + ci(L + nd^{cn})^2 d^{3n} + id^{cn} \leq L^2 d^{cn} + cn(L + nd^{cn})^2 d^{3n} + nd^{cn},$$

d'où la borne

$$L_i = L^2 d^{O(n)}. \tag{19}$$

Enfin de manière analogue, nous obtenons comme conséquences de (I_3) et (18) les estimations

$$\begin{aligned} l_i &\leq c(nl \log d + n^2 \log^2 d) + ci((l + cn^2 \log d)^2 n \log d + n^2 \log^2 d) \\ &\leq c(nl \log d + (l + cn^2 \log d)^2 n^2 \log d + n^2 \log^2 d + n^3 \log^2 d) \end{aligned}$$

ce qui entraîne la borne

$$l_i = O(l^2 n^4 \log^2 d + n^6 \log^3 d). \tag{20}$$

Les affirmations (I), (II) et les bornes (19), (20) conduisent aussi à l'existence d'un algorithme probabiliste de type aléatoire qui, pour tout indice i compris entre $n-s$ et $n-2$, construit le circuit β_i en temps séquentiel $L^2 d^{O(n)}$ et parallèle $O(l^2 n^4 \log^2 d + n^6 \log^3 d)$.

Considérons maintenant le circuit β_{n-2}. Ce calcul d'évaluation s'exécute dans la k-algèbre $k(x_1, \ldots, x_{n-1})[x_n]$ et représente des polynômes $p_2, \ldots, p_s$ de $k[x_1, \ldots, x_n]$ tels que $r' := g - (p_2 f_2 + \cdots + p_s f_s)$ appartienne à l'idéal (f_1). D'après (14), le degré de $p_2, \ldots, p_s$ est d'ordre $(\deg g) d^{O(n)}$, et d'après (19) et (20) la longueur et la profondeur de β_{n-2} sont d'ordre $L^2 d^{O(n)}$ et $O(l^2 n^4 \log^2 d + n^6 \log^3 d)$. De plus d'après les affirmations (I) et (II) le circuit β_{n-2} contient β comme sous-calcul et n'effectue que des divisions par des éléments de $k(x_1, \ldots, x_{n-1})$. Comme le polynôme $r' = g - (p_2 f_2 + \cdots + p_s f_s)$ appartient à l'idéal (f_1), il est divisible par f_1 dans la k-algèbre $k[x_1, \ldots, x_n]$; posons donc $p_1 := r'/f_1$. Nous vérifions immédiatement que p_1 est un polynôme de $k[x_1, \ldots, x_n]$ de degré $(\deg g) d^{O(n)}$, satisfaisant à l'égalité

$$g = p_1 f_1 + \cdots + p_s f_s. \tag{21}$$

Nous pouvons calculer p_1 à partir du circuit β_{n-2} avec moins de $2n$ multiplications et additions, plus une division (il faut tenir compte du fait que β_{n-2} contient le circuit β, et donc calcule aussi g).
En résumé, les polynômes $p_2, \ldots, p_s$ satisfont à l'égalité (21), sont de degré $(\deg g) d^{O(n)}$ et sont représentés par un calcul d'évaluation β^* dans $k(x_1, \ldots, x_n)$ de longueur $L^2 d^{O(n)}$ et de profondeur $O(l^2 n^4 \log^2 d + n^6 \log^3 d)$. Il peut être construit par un algorithme probabiliste de type aléatoire avec des complexités séquentielle et parallèle respectivement du même ordre.
Appliquons maintenant la proposition 2.2 au circuit β^*. Nous obtenons un calcul d'évaluation β' dans $k[x_1, \ldots, x_n]$ qui représente les polynômes $p_1, \ldots, p_s$ et qui ne contient aucune division. Sa longueur et profondeur sont d'ordre $(L \deg g)^2 d^{O(n)}$ et $O(l^2 \log(\deg g) n^7 \log^4 d)$. Enfin, il peut être construit par un algorithme probabiliste de type aléatoire en temps séquentiel $L^6 (\deg g)^2 d^{O(n)}$ et parallèle $O(l^2 \log(\deg g) n^7 \log^4 d)$.

Ceci achève la démonstration du théorème.

5.1.1. Remarque et Corollaire

En remplaçant dans la preuve du théorème précédent toutes les applications de 4.2.5 par 4.2.7 nous obtenons le résultat suivant :

Corollaire : *Soit k un corps commutatif arbitraire et soient $f_1, \ldots, f_s, g$ des polynômes de $k[x_1, \ldots, x_n]$ tels que $f_1, \ldots, f_s$ forment une suite régulière de $k[x_1, \ldots, x_n]$. Notons d le maximum des degrés des $f_1, \ldots, f_s$ et supposons que g appartienne à l'idéal $(f_1, \ldots, f_s)$.*
Alors il existe une représentation de l'écriture de g dans la base des f_i de degré $(\deg g) d^{O(n)}$, c'est-à-dire des polynômes $p_1, \ldots, p_s$ de $k[x_1, \ldots, x_n]$ de degré $(\deg g) d^{O(n)}$ tels que $g = p_1 f_1 + \cdots + p_s f_s$.

L'intérêt de ce corollaire réside dans sa preuve "élémentaire" (voir la remarque 4.2.6), à comparer avec l'énoncé plus précis obtenu à l'aide de méthodes homologiques ([Di-Fi-Gi-Se 91], Theorem 5.1, [Ca-Gu-Gu 91] Corollary 3.3, [Be-Yg 90] et [Am 89]) :

Aux hypothèses précédentes ajoutons $n > 1$ et $d \geq 3$. Alors il existe des polynômes $p_1, \ldots, p_s$ de $k[x_1, \ldots, x_n]$ satisfaisant à l'écriture $g = p_1 f_1 + \cdots + p_s f_s$, tels que le degré des $p_i f_i$ soit majoré *par* $\deg g + d^s$.

5.2. Un théorème des zéros effectif pour la trivialité d'un idéal polynomial

Théorème : *Soient $f_1, \ldots, f_s$ des polynômes de $k[x_1, \ldots, x_n]$ de degré majoré par $d \geq n$ et représentés par leur écriture dense. Alors il existe un réseau arithmétique sur le corps de base k de taille $L := s^{O(1)} d^{O(n)}$ et de profondeur $l := O(n^{12} \log^9 sd)$ qui décide si l'idéal $(f_1, \ldots, f_s)$ est trivial. Si c'est le cas, le réseau produit un calcul d'évaluation dans $k[x_1, \ldots, x_n]$ de longueur $s^{O(1)} d^{O(n)}$ et de profondeur $O(n^{12} \log^9 sd)$, ne contenant aucune division, et qui représente des polynômes $p_1, \ldots, p_s$ de degré d'ordre $d^{O(n)}$ vérifiant $1 = p_1 f_1 + \cdots + p_s f_s$. Enfin ce réseau peut être construit par un algorithme probabiliste de type aléatoire en temps séquentiel et parallèle du même ordre que L et l.*

Démonstration : La proposition 2.3 nous permet de décider par un algorithme probabiliste de type aléatoire en temps séquentiel et parallèle respectivement $s^{O(1)} d^{O(n)}$ et $O(n^2 \log^2 sd)$ si la variété définie par les f_i est vide, c'est-à-dire que l'idéal $(f_1, \ldots, f_s)$ est trivial. Supposons dorénavant que ce soit le cas. En appliquant [Gi-He-Sa 93], Lemma 3.2.1, nous pouvons même supposer sans perte de généralité que les polynômes $f_1, \ldots, f_s$ sont en nombre $s = n + 1$ tout en engendrant toujours l'idéal trivial. De plus, les variétés intermédiaires définies par $f_1, \ldots, f_{n-i}$ $(0 \leq i \leq n-1)$ peuvent elles aussi être supposées intersections complètes, c'est-à-dire de dimension i, et réduites.

Considérons l'idéal $I := (f_1, \ldots, f_n)$, la variété V qu'il définit et la k-algèbre $B := k[x_1, \ldots, x_n]/I$. Notons comme d'habitude $\overline{} : k[x_1, \ldots, x_n] \longrightarrow B$ le morphisme de projection canonique. Par hypothèse, V est une variété intersection complète et réduite de dimension 0 et $\overline{f}_{n+1}$ n'est pas diviseur de zéro dans B ; comme tel, il divise $\overline{1}$. Puisque la dimension de V est 0, aucune des variables n'est libre et donc elles sont automatiquement en position de Noether par rapport à V. En appliquant à cette situation particulière le corollaire 4.2.5, nous en déduisons l'existence d'un calcul d'évaluation β_1 dans $k[x_1, \ldots, x_n]$, sans divisions, de longueur $L_1 := d^{O(n)}$ et de profondeur $l_1 := O(n^2 \log^2 d)$, qui représente un polynôme p_{n+1} de $k[x_1, \ldots, x_n]$ de degré $d^{O(n)}$ vérifiant $1 = \overline{p}_{n+1} \overline{f}_{n+1}$. Le polynôme $g := 1 - p_{n+1} f_{n+1}$ est de degré $d^{O(n)}$ et appartient à l'idéal $I = (f_1, \ldots, f_n)$. Enfin le circuit β_1 peut être construit par un algorithme probabiliste de type aléatoire en temps séquentiel L_1 et parallèle l_1 ; sans restriction de généralité nous pouvons supposer qu'il représente aussi le polynôme g.

Puis observons que les polynômes $f_1, \ldots, f_n, g$ satisfont aux hypothèses du théorème 5.1. Il existe donc un calcul d'évaluation β_2 dans $k[x_1, \ldots, x_n]$, sans divisions, de longueur $L_2 := (L_1 \deg g)^2 d^{O(n)} = d^{O(n)}$ et profondeur $l_2 := O(l_1^2 (\log(\deg g) n^7 \log^4 d) = O(n^{12} \log^9 d)$ qui représente des polynômes $p_1, \ldots, p_n$ de $k[x_1, \ldots, x_n]$ de degré $(\deg g) d^{O(n)}$ vérifiant $g = p_1 f_1 + \cdots + p_n f_n$. Nous obtenons donc la représentation $1 = p_1 f_1 + \cdots + p_{n+1} f_{n+1}$, et comme $\deg g$ est d'ordre $d^{O(n)}$, il en est de même des degrés des p_i. De plus, le circuit β_2 peut être construit par un algorithme probabiliste de type probabiliste de type aléatoire en temps séquentiel $L_1^6 (\deg g)^2 d^{O(n)} = d^{O(n)}$ et parallèle $O(l_1^2 \log(\deg g) n^7 \log^4 d) = O(n^{12} \log^9 d)$.

En joignant le circuit β_2 au circuit β_1, nous fabriquons un calcul d'évaluation sans divisions β dans $k[x_1, \ldots, x_n]$, qui représente les polynômes $p_1, \ldots, p_{n+1}$. Comme L_1 et L_2, sa longueur $L_1 + L_2$ est d'ordre $d^{O(n)}$. Sa profondeur $l_1 + l_2$ est d'ordre $O(n^{12} \log^9 d)$. Enfin, le circuit β peut être construit par un algorithme aléatoire en temps séquentiel $d^{O(n)}$ et parallèle $O(n^{12} \log^9 d)$.

Ceci achève la démonstration du théorème.

Donnons aussi une version non uniforme du théorème précédent avec une borne de complexité bien parallélisable.

Proposition : *Soient $f_1, \ldots, f_s$ des polynômes de $k[x_1, \ldots x_n]$ de degré majoré par $d \geq n$ et représentés par leur écriture dense.*
Alors si l'idéal engendré par $f_1, \ldots f_s$ dans $k[x_1, \ldots x_n]$ est trivial, il existe un calcul d'évaluation sans divisions dans $k[x_1, \ldots x_n]$ de longueur $s^{O(1)} d^{O(n)}$ et de profondeur $O(n^2 \log^2 sd)$ qui représente des polynômes $p_1, \ldots, p_s$ de degré d'ordre $d^{O(n)}$ vérifiant $1 = p_1 f_1 + \ldots + p_s f_s$.

Démonstration : Du théorème précédent nous déduisons qu'il existe un calcul d'évaluation β' sans divisions dans $k[x_1, \ldots, x_n]$ de longueur $s^{O(1)} d^{O(n)}$ qui représente des polynômes $p_1, \ldots p_s$ de degré $d^{O(n)}$ vérifiant $1 = p_1 f_1 + \ldots + p_s f_s$. En parallélisant le circuit β' d'après [Va-Sky-Be-Ra 83] ou [Mi-Ram-Ka 88] nous obtenons un calcul d'évaluation β sans divisions dans $k[x_1, \ldots, x_n]$ de longueur et profondeur $s^{O(1)} d^{O(n)}$ et $O(n^2 \log^2 sd)$ qui représente les polynômes $p_1, \ldots p_s$.

5.2.1. Remarque

Dans [Gi-He-Sa 93], Theorem et Proposition 3.5.1 est démontré le résultat suivant :

Soient $f_1, \ldots, f_s$ des polynômes de $k[x_1, \ldots, x_n]$, de degré majoré par $d \geq n$, tel que l'idéal $(f_1, \ldots, f_s)$ soit trivial. Supposons que $f_1, \ldots, f_s$ soient donnés par leur écriture dense. Alors il existe un algorithme probabiliste de type aléatoire qui en temps séquentiel $s^{O(1)} d^{O(n)}$ et parallèle $O(n^4 \log^2 sd)$ construit un calcul d'évaluation dans $k(x_1, \ldots, x_n)$, qui contient des divisions, de longueur $s^{O(1)} d^{O(n)}$ et de profondeur $O(n^4 \log^2 sd)$, et qui représente des polynômes $p_1, \ldots, p_s$ de degré d'ordre $d^{O(n^2)}$ vérifiant $1 = p_1 f_1 + \cdots + p_s f_s$.

La démonstration de cet énoncé utilise les Nullstellensätze effectifs [Di-Fi-Gi-Se 91], Theorem 5.1 ou [Ca-Gu-Gu 91], Theorem 1.3 et Corollary 3.3 qui sont basés sur des techniques d'algèbre homologique (voir la remarque 4.2.6). Le théorème et la proposition 5.2 possèdent une démonstration tout à fait élémentaire et améliorent le résultat cité dans plusieurs directions :

(i) les polynômes $p_1, \ldots, p_s$, qui font partie du circuit β du théorème et de la proposition 5.2 , ont des degrés d'ordre $d^{O(n)}$ (au lieu de $d^{O(n^2)}$)

(ii) le circuit d'évaluation β du théorème et de la proposition 5.2 ne contient plus de divisions (c'est une conséquence de (i) et de la proposition 2.2)

(iii) le circuit β de la proposition 5.2 est bien parallélisable (pour les mêmes raisons que (ii)).

Comme dans la remarque 5.1.1, nous obtenons la conséquence suivante :

5.2.2. Corollaire

Soit k un corps commutatif arbitraire, et soient $f_1, \ldots, f_s$ des polynômes de $k[x_1, \ldots, x_n]$ tels que l'idéal $(f_1, \ldots, f_s)$ soit trivial. Notons d le maximum des degrés des f_i. Alors il existe des polynômes $p_1, \ldots, p_s$ de degré d'ordre $d^{O(n)}$ vérifiant $1 = p_1 f_1 + \cdots + p_s f_s$.

A l'aide de méthodes homologiques, et en supposant de plus $n \geq 1$ et $d \geq 3$ on obtient dans l'énoncé précédent la borne plus précise :

$$\max\{\deg p_1 f_1, \ldots, \deg p_s f_s\} \leq d^n$$

(voir [Ko 88], [Phi 88], [Fi-Ga 90]).

Néanmoins un raffinement de nos méthodes élémentaires permet d'obtenir la borne $4nd^n$ si la caractéristique de k est zéro ou $d = 2$ et $4n(d+1)^n$ sinon (voir [Sa-So 92]). Cette borne est très similaire à celle obtenue dans [Bro 87] avec des méthodes plus sophistiquées. Une autre méthode élémentaire pour obtenir ce genre de résultats est contenue dans [Du 93].

5.2.3. Une application

De la proposition 5.2 on peut déduire une nouvelle forme algorithmique du théorème de Quillen-Suslin qui améliore le résultat [Fi-Ga 90], Théorème 15. Introduisons d'abord les notions et notations suivantes.

Soit $R := k[x_1, \ldots, x_n]$. Pour des polynômes $f_1, \ldots, f_s$ de R nous notons $[f_1, \ldots, f_s]$ le vecteur de R^s dont ils représentent les coefficients. Nous disons que le vecteur $[f_1, \ldots, f_s]$ est unimodulaire si l'idéal engendré par $f_1, \ldots, f_s$ dans R est trivial. De façon analogue une $s \times s$-matrice M à coefficients dans R est appelée unimodulaire si son déterminant est un élément non nul de k. Avec ces notations nous avons le résultat suivant :

Théorème : *Soient $f_1, \ldots, f_s$ des polynômes de $k[x_1, \ldots, x_n]$ de degré majoré par $d \geq n$. Supposons que $f_1, \ldots, f_s$ soient donnés par leur écriture dense et supposons que le vecteur $f := [f_1, \ldots, f_s]$ de R^s soit unimodulaire. Alors il existe une $s \times s$-matrice unimodulaire M à coefficients dans R avec les propriétés suivantes :*

(i) $f.M = [1, 0, \ldots, 0]$

(ii) $\deg M = d^{O(n)}$

(iii) les coefficients de M sont représentés par un calcul d'évaluation dans $k[x_1, \ldots, x_n]$ de longueur $s^{O(1)} d^{O(n)}$ et de profondeur $O(n^2 \log^2 sd)$ ne contenant aucune division.

La démonstration de ce théorème est textuellement la même que celle du Théorème 15 de [Fi-Ga 90]. La modification consiste à remplacer la remarque 18 du travail cité par la proposition 5.2.

REFERENCES

[Am 89]
F. Amoroso, *Tests d'appartenance d'après un théorème de Kollár*, C.R. Acad. Sci. Paris, Série I Math **309** (1989), 691-694.

[Ba-Dí-Ga 88]
J. L. Balcázar, J. Díaz, J. Gabarró, *Structural Complexity I*, EATCS Monographs on Theoretical Computer Science **11**, Springer Verlag (1988).

[Be-Yg 90]
C.A. Berenstein, A. Yger, *Bounds for the degrees in the division problem*, Michigan Math. J. **37** (1990), 25-43.

[Be-Yg 91]
C.A. Berenstein, A. Yger, *Une formule de Jacobi et ses conséquences*, Ann. scient. Ec. Norm. Sup. 4$^{\text{ième}}$ série, **24** (1991), 363-377.

[Ber 84]
S. J. Berkowitz, *On computing the determinant in small parallel time using a small number of processors*, Information Processing Letters **18** (1984), 147-150.

[Bro 87]
W. D. Brownawell, *Bounds for the degree in the Nullstellensatz*, Ann. Math. (Second Series) **126** (1987), 577-591.

[Bro 89]
W. D. Brownawell, *A prime power product version of the Nullstellensatz*, Manuscript Penn State University (1989).

[Ca-Ga-He 88]
L. Caniglia, A. Galligo, J. Heintz, *Borne simple exponentielle pour les degrés dans le théorème des zéros sur un corps de caractéristique quelconque*, C.R. Acad. Sci. Paris, Série I Math **307** (1988), 255-258.

[Ca-Ga-He 89]
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, Roma 1988, T. Mora, ed., Springer LN Comput. Sci. **357** (1989), 131-151.

[Ca-Gu-Gu 91]
L. Caniglia, J. A. Guccione, J. J. Guccione, *Local membership problems for polynomial ideals*, Proc. Intern. Conf. Effective Methods in Algebraic Geometry MEGA 90, Castiglioncello 1990, T. Mora et C. Traverso, eds., Progress in Mathematics **94**, Birkhäuser Verlag (1991), 31–45.

[Car 93]
J. P. Cardinal, *Dualité et algorithmes itératifs pour la résolution de systèmes polynomiaux*, Thèse, Université de Rennes I (1993).

[Di-Fi-Gi-Se 91]
A. Dickenstein, Noaï Fitchas, M. Giusti, C. Sessa, *The membership problem for unmixed polynomial ideals is solvable in single exponential time*, Discrete Appl. Math. **33** (1991) 73–94, Special issue 7th Intern. Conf. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes AAECC–7, Toulouse 1989.

[Du 93]
T. W. Dubé, *A combinatorial proof of the effective Nullstellensatz*, J. Symbolic Computation **15** (1993), 277-296.

[El 93]
M. Elkadi, *Bornes pour le degré et les hauteurs dans le problème de la division*, (1993), à paraître dans Michigan Math. J.

[Fi-Ga 90]
Noaï Fitchas, A. Galligo, *Nullstellensatz effectif et Conjecture de Serre (Théorème de Quillen-Suslin) pour le Calcul Formel*, Math. Nachrichten **149** (1990), 231-253.

[Fi-Ga-Mo 90]
Noaï Fitchas, A. Galligo, J. Morgenstern, *Algorithmes rapides en séquentiel et en parallèle pour l'élimination des quantificateurs en géométrie élémentaire*, Séminaire sur les structures algébriques ordonnées 1984-87, vol. I, F. Delon, M. Dickmann et D. Gondard, eds., Publ. Math. Univ. Paris VII **32** (1990), 103-145.

[Fu 84]
W. Fulton, *Intersection Theory*, Ergebnisse der Mathematik, 3. Folge. Band 2, Springer Verlag (1984).

[vzGa 86],
J. von zur Gathen, *Parallel arithmetic computations : a survey*, Proc. 13th Symp. MFCS 1986, Springer LN Comput. Sci. **233** (1986), 93-112.

[Gi-He 91]
M. Giusti, J. Heintz, *La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial*, Manuscrit Centre de Mathématiques, École Polytechnique, Palaiseau, France (1991), à paraître dans Proc. Intern. Meeting on Commutative Algebra, Cortona 1991.

[Gi-He-Sa 93]
M. Giusti, J. Heintz, J. Sabia, *On the efficiency of effective Nullstellensätze*, Comput. Complexity **3** (1993), 56-95.

[He 83]
J. Heintz, *Definability and fast quantifier elimination over algebraically closed fields*, Theoret. Comput. Sci. **24** (1983), 239-277 ; traduction russe dans Kyberneticeskij Sbornik, Novaja Serija **22**, Mir Moskva (1985), 113-158.

[He 89]
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.

[He-Mo 92]
J. Heintz, J. Morgenstern, *On the intrinsic complexity of elimination theory*, Manuscrit Université de Nice (1992).

[He-Schn 82]
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 Ann. ACM Symposium on Computing (1980), 262-268.

[He-Sie 81]
J. Heintz, M. Sieveking, *Absolute primality of polynomials is decidable in random polynomial time in the number of variables*, Proc. 8th Int. Coll. Automata, Languages and Programming ICALP 81, Akko 1981, S. Even et O. Karir, eds., Springer LN Comput. Sci. **115** (1981), 16-28.

[Hen-Mer 87]
J. P. Henry, M. Merle, *Conditions de régularité et éclatements*, Annales de l'Institut Fourier Grenoble **37** (3) (1987), 159-190.

[Her 26]
G. Herrmann *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Ann. **95** (1926) 736-788.

[Iv 73]
B. Iversen, *Generic local structure in Commutative Algebra*, Springer LN Math. **310** (1973).

[Jou 92]
J.-P. Jouanolou, *Formes d'inertie et résultant : un formulaire*, Publications IRMA, Université de Strasbourg (1992).

[Ka 88]
E. Kaltofen, *Greatest common divisors of polynomials given by straight-line programs*, J. ACM **35** (1) (1988), 231-264.

[Ko 88]
J. Kollár, *Sharp effective Nullstellensatz*, J. AMS **1** (1988) 963–975.

[Kri-Par 93]
T. Krick, L. M. Pardo, *Une approche informatique pour l'approximation diophantienne*, (1993), à paraître dans C. R. Acad. Sci. Paris.

[Ku 86]
E. Kunz, *Kähler Differentials*, Advanced Lectures in Mathematics, Vieweg Verlag 1986.

[Ma-Me 82]
E. Mayr, A. Meyer, *The complexity of the word problem for commutative semigroups and polynomial ideals*, Adv. in Math. **46** (1982) 305-329.

[Mi-Ram-Ka 88]
G. L. Miller, V. Ramachandran, E. Kaltofen, *Efficient parallel evaluation of straight-line code and arithmetic circuits*, SIAM J. Comput. **17** (4) (1988), 687-695.

[Moe 93]
M. Möller, *Systems of algebraic equations solved by means of endomorphism*, Proc. 10th. Intern. Conf. on Applied Algebra, Algebraic Algorithms and Error Correcting Codes (AAECC-10), G. Cohen, T. Mora, O. Moreno, eds. Springer LN Comp. Sci. (1993), 41-56.

[Phi 88]
P. Philippon, *Théorème des zéros effectif d'après J. Kollár*, dans Problèmes diophantiens, Publ. Math. Univ. Paris **88** (1988-89).

[Sa-So 92]
J. Sabia, P. Solernó, *Bounds for traces in complete intersections and degrees in the Nullstellensatz*, Manuscrit Universidad de Buenos Aires (1992).

[Sche-Sto 75]
G. Scheja, U. Storch, Über Spurfunktionen bei vollständigen Durchschnitten, J. reine angew. Math. **278/279** (1975), 174-190.

[Sto 89]
H. J. Stoss, *On the representation of rational functions of bounded complexity*, Theoret. Comput. Sci. **64** (1989), 1-13.

[Stra 72]
V. Strassen, *Berechnung und Programm I*, Acta Inform. **1** (1972), 320-334.

[Stra 73]
V. Strassen, *Vermeidung von Divisionen*, Crelle J. Reine Angew. Math. **264** (1973), 184-202.

[Va-Sky-Be-Ra 83]
L.G. Valiant, S. Skyum, S. Berkowitz, C. Rackoff, *Fast parallel computation of polynomials using few processors*, SIAM J. Comput. **12** (1983) 641–644.

[Wie 69]
H. Wiebe, Über homologische Invarianten lokaler Ringe, Math. Ann. 179 (1969), 257-274.