NOMBRES ALGÉBRIQUES PRÉSENTÉS COMME SOLUTIONS DE SYSTÈMES D'ÉQUATIONS EN CASCADE

Henri LOMBARDI
laboratoire de Mathématiques
UFR des Sciences et Techniques
25030 Besançon

Abstract

We give a very simple description of real algebraic numbers and discuss the polynomial time computability of arithmetic operations and searching roots (relatively to this description).

We discuss then the same problem for a much more sophisticated description of real or complex algebraic numbers. This description is based upon the D5 system. We give systematic uniformly polynomial majorations (for the computing time) relatively to the input size **and** the "a priori degree" of the described algebraic numbers.

Key-Words

Algebraic numbers, codage, formal calculus, D5 system, polynomial time computability.

Résumé

Nous donnons tout d'abord une description très simple des nombres algébriques réels et disutons la calculabilité en temps polynomial des opérations arithmétiques et de la recherche des zéros relativement à cette description.

Nous discutons ensuite le même problème pour une description beaucoup plus sophistiquée des nombres algébriques, réels ou complexes. Cette description est basée sur le système D5 . Nous donnons dans ce cadre des majorations de temps de calcul uniformément polynomiales par rapport à la taille des entrées **et au** "degré a priori" des nombres algébriques décrits.

Mots clé

Nombres algébriques, codage, calcul formel, système D5, calculabilité en temps polynomial.

Nombres algébriques présentés comme solutions de systèmes d'équations en cascade

Introduction

Nous étudions dans quelle mesure les calculs dans la clôture algébrique de Q peuvent être présentés de manière à être en temps polynomial. Comme on peut s'y attendre, une explosion exponentielle de la taille des objets manipulés et du temps de calcul semble à peu près inévitable.

Dans le paragraphe a), nous explicitons la présentation des nombres algébriques réels la plus naïve qu'on puisse imaginer : un nombre algébrique réel est donné par un polynôme P de $Z[X]$ qui l'annule et par un intervalle où ce polynôme change de signe tout en étant strictement monotone. Pour que cette dernière condition soit tout à fait simple à constater, nous demandons que la dérivée de P reste de signe constant de manière évidente, en donnant un sens précis à ceci. Autrement dit, aucun recours au théorème de Sturm, et aux calculs de polynômes sous-résultants qu'il implique, n'est utilisé dans cette description. La recherche des racines réelles d'un polynôme est également faite de la manière naïve (celle du lycée) : on cherche les racines de sa dérivée et on dresse un tableau de variation. Il s'avère que, tant qu'on ne se préoccupe que de complexité en temps polynomial, cette présentation des réels algébriques et les calculs qu'elle induit sont *aussi bons* que ceux relevant de méthodes nettement plus sophistiquées. Pour résumer: les lois de corps et la recherche des racines d'un polynôme de $Z[X]$ sont en temps polynomial, mais ces opérations enchaînées conduisent à une explosion de la taille des objets manipulés. A la fin du paragraphe, nous donnons des conditions suffisantes pour remplacer Q par un autre sous-corps de R et obtenir néanmoins les mêmes majorations de temps de calculs.

Dans les paragraphes suivants, nous étudions le problème de savoir si les défauts constatés dans la présentation naïve peuvent être tournés en utilisant une présentation plus sophistiquée. Chaque fois qu'un calcul conduit à manipuler des objets trop gros (par rapport à la taille des entrées), il est a priori possible de tourner la difficulté en *n'effectuant pas le calcul et en indiquant seulement qu'il devrait être fait* . C'est par exemple le secret de la présentation des entiers en base 10 par rapport aux entiers "batons". Cette méthode universelle souffre cependant de quelques inconvénients. Si on l'applique par exemple pour la représentation des nombres algébriques réels, on obtient certes une représentation toujours compacte des nombres manipulés, mais le test de comparaison est, très probablement, en temps exponentiel ou pire. Nous discutons cette question dans le § b) et démontrons qu'en tout état de cause, il faut a priori accepter de céder du terrain d'un coté ou de l'autre. Récemment, D. Duval et C. Dicrecenzo ont développé et implanté un sytème de représentation appelé D5, dans lequel les nombres algébriques sont donnés comme solutions d'équations algébriques emboitées. Dans le § c), nous étudions le comportement de représentations des nombres algébriques dans le cadre D5 et nous vérifions que les calculs qui peuvent être qualifiés d'élémentaires (y compris certains calculs de déterminants, donc l'algèbre linéaire) sont *presque* en temps polynomial. En fait, le temps est polynomial, non par rapport à la taille des entrées, mais par rapport à la taille qu'occuperaient a priori ces entrées si elles étaient traduites dans une présentation naïve comme celle développée au paragraphe a). Le gain peut apparaître assez mince. La souplesse de D5 ou de systèmes analogues, relativement à la présentation naïve (ou une représentation analogue) est néanmoins bien certaine. D'autre part, le

fait de raisonner dans D5 pour les calculs de majoration est actuellement la meilleure manière de comprendre clairement ce qui se passe avec les nombres algébriques et où se situent les difficultés. Par exemple, le fait que les calculs de déterminants ne peuvent pas, a priori, être traités par la méthode de Bareiss. Ou encore, les majorations que nous obtenons dans le cadre D5 , par leur caractère uniforme, sont meilleures que celles qui pouvaient résulter de la simple application des résultats obtenus dans R_{alg} .

Dans le § d) nous nous situons dans un cadre directement hérité de D5 , mais en abandonnant ce qui fait une bonne partie de la philosophie de D5 , c.-à-d. que nous levons *apriori* l'ambiguité sur la solution considérée d'un système d'équations algébriques emboitées en le caractérisant par une approximation convenable. Nous obtenons les résultats qui pouvaient être espérés a priori, du même genre que ceux obtenus au § c).

Notons enfin que les résultats obtenus s'appliquent, via les mêmes méthodes, dans différents cadres voisins: nombres algébriques réels, nombres algébriques complexes, nombres algébriques p-adiques, clôture algébrique d'un corps de fonctions $\mathbf{F}(X)$ où $\mathbf{F}$ est un corps fini.

a) La présentation naïve des réels algébriques

Introduction

Nous étudions dans ce paragraphe la présentation des nombres réels algébriques la plus naïve qui soit. Selon ce point de vue, un nombre algébrique est donné par un polynôme P à coefficients entiers qui l'annule et un intervalle sur lequel P change de signe et P' est évidemment de signe constant. Cela suffit à rendre de complexité $\mathbf{P}$ les calculs élémentaires concernant les nombres algébriques. Mais les calculs "en cascade" ont un comportement exponentiel. Nous verrons dans les paragraphes suivants qu'il est difficile d'espérer beaucoup mieux.

On notera qu'on se passe entièrement des algorithmes de décomposition en facteurs premiers dans Q[X] . Autrement dit, on ne sait jamais a priori si le polynôme donné qui annule un réel algébrique ξ est le polynôme minimum de ξ ou non.

Les détails des calculs pour le § a) peuvent être trouvés dans [**Lom3**].

Quelques points de terminologie :

Nous reprenons, surtout dans le a) , la terminologie de [Lom1].

Nous parlons d'une $\mathbf{P}$-fonction ou d'une $\mathbf{P}$-opération pour signifier "opération calculable en temps polynomial par rapport à la taille des entrées".

Nous parlons d'un $\mathbf{P}$-ensemble E ou d'un ensemble $\mathbf{P}$-présenté E pour parler d'un ensemble dénombrable codé (présenté) dans un langage A^* sur un alphabet fini A lorsque les conditions suivantes sont réalisées: 1) les mots qui codent les éléments de E forment une $\mathbf{P}$-partie de A^* (c.-à-d. une partie $\mathbf{P}$-testable de A^*), et 2) le test d'égalité dans E (pour deux mots de A^* qui codent des éléments de E) est un $\mathbf{P}$-test.

Nous notons N , Z , Q les **P**-ensembles correspondants présentés en binaire. Nous notons N_1 pour le **P**-ensemble des entiers naturels présenté en unaire.
De manière générale **lg**(x) désignera la longueur d'un mot représentant l'objet x (élément de X) dans la présentation choisie de l'ensemble X. Pour des éléments de Z, ce sera donc la taille pour l'écriture en binaire.
Les polynômes de $Q[X]$, $Q[X,Y]$, $Q[X_1,X_2,\ldots,X_n]$ sont supposés donnés en présentation dense. Si P $Q[X_1,X_2,\ldots,X_n]$ et si $d_{X_j} = d_j$, si l_{creux} et l_{dense} représentent la longueur de P dans une présentation creuse et une présentation dense (les coefficients étant toujours écrits en binaire), on a : $l_{creux} \leq l_{dense} \leq d_1 \ldots d_n . l_{creux}$. Les résultats de complexité qui font intervenir l_{dense} sont alors facilement traduisibles en résultats qui font intervenir l_{creux}.

Présentation de R_{alg}

Evidence du signe constant d'un polynôme sur un intervalle donné

Définition a.1 :

- Soient P $Q[X]$, a et b Q avec $a.b \geq 0$, $a < b$. On écrit $P = P_1 + P_2$, où P_1 est la somme des monômes strictement croissants sur l'intervalle $[a, b]$ et P_2 est la somme des monômes décroissants.
- on dira que le nombre $P_1(a) + P_2(b)$ est le *minorant-évident de P sur l'intervalle* $[a, b]$ et que $P_1(b) + P_2(a)$ est le *majorant-évident de P sur l'intervalle* $[a, b]$
- si maintenant a et b Q avec $a < 0 < b$, on appelera minorant-évident (resp. majorant-évident) de P sur $[a, b]$ le plus petit (resp. le plus grand) des minorants-évidents (resp. majorants-évidents) de P sur $[a, 0]$ et sur $[0, b]$
- pour $a < b$ dans Q, on dira que P est *évidemment-de-signe-constant sur l'intervalle* $[a, b]$ lorsque le majorant-évident et le minorant-évident de P sur $[a, b]$ ont même signe, non nul.

Il est clair qu'un majorant-évident est un majorant, et que si un polynôme P est évidemment-de-signe-constant sur un intervalle $[a, b]$, alors il est de signe constant sur cet intervalle.
De plus le majorant-évident d'un polynôme sur un intervalle plus petit est inférieur au majorant-évident sur l'intervalle initial. De même l'évidence du signe constant sur un intervalle implique l'évidence du signe constant sur tout intervalle plus petit.

Lemme 1 : Soient P et Q dans $Q[X]$, avec $pgcd(P,Q) = 1$, et $[r', r]$ un intervalle rationnel. A partir de ces données on peut **P**-calculer un entier n N_1 tel que :
si $r \leq a \leq b \leq r'$ et $|b - a| \leq 1/2^n$, alors P ou Q est évidemment-de-signe-constant sur $[a, b]$

Ce lemme justifie la présentation suivante de l'ensemble R_{alg} des réels algébriques :

Présentation naïve de R_{alg}

Définition a.2 : Nous désignerons par R_{alg} l'ensemble des réels algébriques présenté de la manière décrite ci-dessous.

Un nombre réel algébrique u est présenté par un triplet

(P , a , b) $Z[X] \times Q \times Q$ vérifiant les conditions suivantes :

- $a < b$
- P est un polynôme sans facteur carré (i.e.: vérifiant **Res**(P,P') $\neq 0$)
- $P(a).P(b) < 0$, et P' est évidemment-de-signe-constant sur $[a , b]$
- $P(u) = 0$ et u $[a , b]$

Calcul des valeurs approchées d'un réel algébrique à partir de sa présentation

Définition a.3 : Soit A un **P**-ensemble et f une fonction de A vers R . On dira que f est une **P**-fonction, ou une **P**-suite, ou encore que f est une fonction **P**-calculable, si il existe une **P**-opération $F : A \times N_1 \rightarrow Q$ telle que F(z,n) est une approximation de f(z) avec la précision 2^{-n} (1)

En particulier, lorsque A est réduit à un point, on obtient la notion de **P**-nombre réel (ou réel de complexité **P**). Des définitions analogues vaudraient d'ailleurs pour toute autre classe de complexité.

Proposition a.4 :

Il existe une **P**-opération $F : R_{alg} \times N_1 \rightarrow D$ telle que $F(v,n) = r/2^n$ (avec r Z) est une approximation de v avec la précision 2^{-n} .

C'est-à-dire: l'injection naturelle $R_{alg} \rightarrow R$ est une **P**-fonction.

Corollaire : Q s'identifie à une **P**-partie de R_{alg}

Recherche d'une racine par dichotomie sur un intervalle rationnel . Test d'égalité. Séparation .

Proposition a.5 : Il existe un polynôme Q et une **P**-opération

$Rac : Q[X] \times Q \times Q \rightarrow R_{alg}$ telle que :

Si $P(a).P(b) < 0$, alors $Rac(P , a , b) = u$ avec : u est une racine de P sur $] a , b [$, et **lg**(u) < Q(**lg**(P)) .

Théorème a.6 : Il existe une **P**-opération $V : R_{alg} \times R_{alg} \rightarrow D \times D \times (< , = , >)$ telle que :

- $V(u,v) = (c,d," = ")$ $u = v$
- $V(u,v) = (c,d," < ")$ $u < c < d < v$ et $(d - c) > (v - u)/2$
- $V(u,v) = (c,d," > ")$ $u > d > c > v$ et $(d - c) > (u - v)/2$

---

1 On peut exiger de plus que F(z,n) soit de la forme $r/2^n$ (r Z) de sorte que f(z) $[(r - 1)/2^n , (r+1)/2^n]$

Remarque : La preuve du théorème a.6 nous fournit explicitement, un écart en deça duquel deux réels algébriques sont nécessairement confondus. C'est ce que nous précisons dans la proposition suivante. Il en découle que les calculs de PGCD ne sont jamais indispensables pour la comparaison des réels algébriques.

Théorème a.7 :

a) Soient P et Q 2 polynômes à coefficients réels, premiers entre eux, u une racine de P et v une racine de Q. Posons p := d(P), q := d(Q), M := un majorant des modules des racines de P, N := un majorant des modules des racines de Q, soit n un entier ≥
$p \log_2(|cd(Q)|) + q \log_2(|cd(P)|) + (p.q-1).\log_2(M+N) - \log_2(|Res(P,Q)|)$
Si $|u - v| < 1/2^n$, **alors** u = v

b) Soient u = (P , a , b), v = (Q , c , d) 2 éléments de R_{alg}.
Mêmes notations qu'en a) pour p, q, N et M ;
n := p.**lg**(cd(Q)) + q.**lg**(cd(P)) + (p.q-1).**lg**(M+N)
Si $|u - v| < 1/2^n$, **alors** u = v
Si P et Q sont unitaires on peut prendre n = (p.q-1).**lg**(M+N)

Remarque : La majoration ci-dessus, obtenue par un calcul grossier, peut sans doute être améliorée. Selon cette majoration, pour connaître le polynôme minimum P d'un nombre algébrique α, sachant que d(P) ≤ p et **sup**(| coeffs de P |) ≤ H, **lg**(H) = h, il suffit de connaître α avec une précision de $1/2^n$ où $n = 2 p h + p^2 (1+h) + 1$.
Dans [**KLL**] les auteurs, en utilisant l'algorithme LLL (cf [**LLL**] ou [**Val**]), retrouvent les coefficients de P en temps polynomial dès que sont connus s bits du développement binaire de α, où $s \geq p^2/2 + ((3p+4)$ **lg**$(p+1))/2 + 2 p h$.

Vu le théorème a.7, on note l'importance particulière dans la pratique d'une méthode de calcul particulièrement rapide des approximations de nombres réels algébriques. C'est par exemple le cas de la méthode de Newton (cf [**Mü**]).

Proposition a.8 :

Soient u = (P , a , b) R_{alg}, x_0] a , b [, $r_0 = \inf(|x_0 - a|, |x_0 - b|)$, M un majorant de $|P^{(2)}(x)|$ sur [a , b]

a) Si $|P(x_0)| \leq$ **inf**$(|P'(x_0)|/2M, r_0/2)$, la méthode de Newton peut être appliquée pour le calcul d'approximations de u en démarrant avec x_0

b) Si cette condition est réalisée et si on utilise les techniques de multiplication rapide, le calcul d'une approximation avec la précision 2^{-n} est alors en temps O(n log(n) loglog(n)) (l'unique entrée est n en unaire)

c) Un point x_0 de D ∩] a , b [vérifiant a) peut être calculé en temps polynomial (pour l'entrée u).

Remarque :
Ceci montre que tout réel algébrique est "individuellement" un réel de complexité en temps O(n log(n) loglog(n)), mais c'est une appréciation très individualiste dans la mesure où P, a, b ne sont pas considérées comme des entrées. Si on fait précéder la méthode de Newton d'une méthode par

dichotomie cela relativise le résultat obtenu. Notons cependant que si $P^{(2)}$ est de signe constant sur $[a, b]$ la méthode de Newton fonctionne sans phase préparatoire, en démarrant de l'extrémité de l'intervalle où P et $P^{(2)}$ sont de même signe.

Une solution "définitive" (au problème de calculer très rapidement les approximations rationnelles des nombres réels algébriques qu'on manipule) consisterait à donner toujours un réel algébrique sous la forme (P, a, b, x_0) sur un intervalle tel que la condition a) de la proposition a.8 soit vérifiée. C'est grosso modo la solution que nous développons dans le d), dans le cadre des systèmes d'équations emboitées.
Il serait intéressant d'étudier la complexité du calcul si on utilise le processus itératif dit "méthode regula falsi" (ou méthode de la sécante), qui a également une bonne vitesse de convergence. Cf par exemple [**Ost**] p 55 pour une comparaison des mérites respectifs des méthodes de Newton et "regula falsi".

R_{alg} comme **P**-structure

Le théorème général suivant est utile pour montrer qu'une fonction à valeur dans R_{alg} est **P**-calculable.

Théorème a.9 : Soit A un **P**-ensemble et f une fonction de A vers R_{alg}. Pour que f soit **P**-calculable, il faut et suffit que les 2 conditions suivantes soient vérifiées :
- la fonction $f : A \to R$ est une **P**-fonction
- il existe une **P**-opération $G : A \to Z[X] - \{0\}$ telle que :
  si $G(z) = S$, alors $f(z)$ est racine de S.

Théorème a.10 :
Il existe une **P**-opération $Ev_n : Q[X_1,X_2,...,X_n] \times R_{alg}^{\,n} \to R_{alg}$ telle que :
$Ev_n(R, (\xi_1,\xi_2,...,\xi_n)) = R(\xi_1,\xi_2,...,\xi_n)$ (égalité au sens de R_{alg})

Théorème a.11 : : R_{alg} est un **P**-corps-ordonné

Remarque :
1) Ces résultats ne signifient pas vraiment qu'on peut calculer dans R_{alg}, en effet l'addition et le produit ne sont pas complètement **P**-calculables : par exemple la somme de n nombres quadratiques est en général de degré 2^n, et donc les calculs en série explosent du fait de la taille des objets utilisés. Dans le théorème a.10 l'entier n est fixé, mais la dépendance par rapport à n est exponentielle.
2) Lorsque les polynômes P_i (où $\xi_i = (P_i, a_i, b_i)$) et R sont des polynômes unitaires, le calcul du signe de $R(\xi_1,\xi_2,\ldots,\xi_n)$ peut être obtenu de manière plus rapide que par le calcul de $R(\xi_1,\xi_2,\ldots,\xi_n)$ dans R_{alg}. En effet, soit m_i un majorant des modules des racines de P_i ($i = 1,...,n$). Il est alors facile de calculer un majorant m_R pour les $|R(\zeta_1,\zeta_2,\ldots,\zeta_n)|$ où les ζ_i sont des racines arbitraires des P_i. Le produit des $R(\zeta_1,\zeta_2,\ldots,\zeta_n)$ non nuls est un entier algébrique, donc un entier, ce qui donne l'implication :
$R(\xi_1,\xi_2,\ldots,\xi_n) \neq 0 \qquad |R(\xi_1,\xi_2,\ldots,\xi_n)| \geq 1/m_R^{(d_1.d_2...d_n-1)}$.

Par suite, il suffit de calculer une approximation rationnelle convenable de $R(\xi_1,\xi_2,\ldots,\xi_n)$ pour connaître son signe. Or d'après la proposition a.8 , le calcul d'approximations rationnelles est très rapide.

Situation des racines réelles d'un polynome de $Q[X]$

Théorème a.12:

Il existe une **P**-opération $Q[X] \rightarrow$ **Lst**(R_{alg}) qui calcule la liste ordonnée des racines réelles d'un polynôme à coefficients rationnels

On procède "par recurrence" sur le degré du polynôme P .
Soit r rationnel positif tel que l'intervalle $]-r, r[$ contienne toutes les racines réelles de P . Si on connaît la liste ordonnée des racines x_1 , ... , x_k , (éventuellement vide), du polynôme dérivé P' sur l'intervalle $[-r, r]$, on pose $x_0 = -r$, $x_{k+1} = r$, on connaît le signe de P' sur chacun des intervalles $]x_i, x_{i+1}[$, donc le tableau de variation de P sur l'intervalle $[-r, r]$. On calcule ensuite les réels algébriques $P(x_i)$, ou au moins leurs signes. On garde les x_i qui sont racines de P ; et il faut enfin calculer les racines sur les intervalles $]x_i, x_{i+1}[$ où P change de signe strict, ce qui se fait par dichotomie en démarrant de rationnels sufiisamment proches des extrémités de l'intervalle
Le calcul (décrit ci-dessus) de la liste des racines de P sur l'intervalle $[-r, r]$ à partir de celle des racines de P' , est un **P**-calcul. Il suffit donc de vérifier que l'on peut polynomialement majorer la taille des polynômes dérivés successifs et de leurs tableaux de racines à partir de la taille du polynôme de départ P .

Deux mots sur C_{alg}

Nous désignerons par C_{alg} l'ensemble des nombres complexes algébriques présenté sous la forme $R_{alg}[\sqrt{-1}]$, cad $R_{alg}^{\,2}$. On obtient alors les résultats suivants:

Théorème a.13 :

Il existe une **P**-opération $Ev_n : Q[\sqrt{-1}][Z_1,Z_2,\ldots,Z_n] \times C_{alg}^{\,n} \rightarrow C_{alg}$ avec :
$Ev_n(R , (\xi_1,\xi_2,\ldots,\xi_n)) = R(\xi_1,\xi_2,\ldots,\xi_n)$ (égalité au sens de C_{alg})

Théorème a.14:

Il existe une **P**-opération $Q[X] \rightarrow$ **Lst**(C_{alg}) qui calcule une liste des racines complexes d'un polynôme à coefficients rationnels, avec leurs multiplicités.

Question ouverte : un problème interessant consiste à trouver une borne inférieure de complexité pour les automorphismes non triviaux (c.-à-d. distincts de Id et de la conjugaison) de C_{alg} . On peut conjecturer que tout automorphisme non trivial est de complexité en temps au moins exponentiel.
Notons qu'il en existe en temps primitif récursif : considérer par exemple l'automorphisme de $Q[\sqrt{2}]$ qui échange $\sqrt{2}$ et $-\sqrt{2}$ et le prolonger de proche en proche à C_{alg} tout entier en rajoutant une à une les racines des polynômes de $Z[X]$ (à la $i^{ème}$ étape on obtient un

isomorphisme explicite d'un sous corps $Q[\zeta_i]$ de C_{alg} vers un sous corps $Q[\xi_i]$ où ζ_i et ξ_i sont conjugués).

Proposition a.15 :

Il existe une **P**-opération $Z[X] \rightarrow$ **Lst**$(Q^2 \times Q^+)$ qui , à partir d'un polynôme P sans facteur carré , calcule une liste d'éléments (x_i , y_i , r_i) vérifiant :

- chaque disque de centre (x_i , y_i) et de rayon r_i contient exactement une racine de P
- le processus itératif de Newton démarrant avec (x_i , y_i) converge vers la racine en question

Remarque : La présentation de C_{alg} via la partie réelle et la partie imaginaire n'est pas en fait une présentation très naturelle . Par exemple la proposition a.15 peut être réalisée par un algorithme, beaucoup plus performant que celui proposé ici, qui ne calcule pas en tant que telles les parties réelles et imaginaires des racines de P (cf par exemple [**Sch**] ou [**Pan**]). En conséquence, les racines de P sont représentées de manière nettement plus agréable sous la forme $(P, [x_i , y_i , r_i])$. Nous généralisons ce genre de présentation dans le § d) .

Une généralisation

Soit **Q'** un corps ordonné dénombrable dans une présentation telle que :

(i) la relation d'ordre est **P**-décidable

(ii) les lois de corps sont décrites par des **P**-opérations[1]

(iii) les déterminants sont **P**-calculables[2]

(iv) il existe une **P**-opération qui, à partir d'un x **Q'** , calcule un entier m(x) N majorant x dans **Q'** [3] .

On démontre alors facilement que:

(v) l'homomorphisme injectif Q → **Q'** est une **P**-fonction

(vi) l'homomorphisme injectif croissant **Q'** → R est une **P**-fonction

On peut alors chercher à avoir une représentation raisonnable de l'ensemble $\mathbf{R'}_{alg}$ des réels algébriques sur **Q'** . On relit le § a) en essayant de remplacer partout Q et Z par **Q'** . On présente un élément de $\mathbf{R'}_{alg}$ par un triplet (P , a , b) où P est un polynôme unitaire de **Q'**[X] , a,b **Q'** . On s'aperçoit que presque toutes les démonstrations restent valables (sauf quelques unes que nous signalons ensuite).

En particulier, on obtient :

---

1 (i) et (ii) signifient que, dans la présentation considérée, **Q'** est un **P**-corps-ordonné.

2 on dit encore que **Q'** est **det-cPc**

3 on dira alors que **Q'** est **P**-archimédien

Théorème a.16 : Sous les hypothèses (i), (ii), (iii), (iv) ci-dessus :

a) On peut construire une **P**-opération pour l'homorphisme d'évaluation de $\mathbf{Q}'[X_1,X_2,...,X_n] \times \mathbf{R}'^{\,n}_{alg}$ vers $\mathbf{R}'_{alg}$:

$$Ev_n(R , (\xi_1,\xi_2,...,\xi_n)) = R(\xi_1,\xi_2,...,\xi_n)$$

b) On peut construire une **P**-opération $\mathbf{Q}'[X] \to \mathbf{Lst}(\mathbf{R}'_{alg})$ qui calcule la liste ordonnée des racines réelles d'un polynôme à coefficients dans **Q'** .

On notera que dans le a) la dépendance polynomiale est pour n fixé. Ce qui relativise le résultat obtenu.

Les démonstrations qui ne sont plus valables sont les suivantes :

− les majorations explicites qui tiennent comptent de faits particuliers à Z : le fait qu'un résultant non nul entier est en valeur absolue ≥ 1 (théorème a.7),

− le fait que les produits dans Z sont en O(n log(n) loglog(n)) (prop a.8) ,

− et le fait qu'un élément de Z est exactement connu à partir d'une approximation à 1/4 près, dans la preuve du corollaire de la proposition a.4 .

Signalons un "non-résultat" analogue dans le cas récursif : si **Q'** est un corps récursivement présenté, il n'y a pas automatiquement un test récursif pour la question " u **Q'** ? " lorsque u $\mathbf{R}'_{alg}$: on peut par exemple considérer une extension algébrique de Q obtenue en rajoutant les $\sqrt{p_n}$ où la suite p_n est une suite récursivement énumérable mais non récursive de nombre premiers. Le test $\sqrt{m}$ **Q'** ?, pour m N n'est donc pas récursif.

Un exemple: Si α est un réel transcendant, le corps Q(α) est un **P**-corps **det-cPc**. Ce corps est **P**-archimédien si et seulement si le nombre α est **P**-transcendant au sens suivant :

il existe une **P**-opération Min : $Z[X] - \{0\} \to D$ telle que $0 < Min(P) \le | P(\alpha) |$

En outre, la relation d'ordre dans Q(α) est alors **P**-décidable, et on peut appliquer le théorème a.16 .

Notons enfin que le fait pour α d'être **P**-transcendant peut encore s'exprimer au moyen de la majoration polynomiale suivante:

il existe c , k , h N tels que pour tout polynôme non nul P de Z[X] on ait : $| P(\alpha) | \ge 1/2^{c\, d^h\, ls(P)^k}$

où d est le degré de P et ls(P) = **lg**(**sup**(| coeffs de P |))

b) Discussion à propos de différentes présentations des nombres réels algébriques

Un exemple : systèmes d'affectations polynomiales en cascade

Supposons que nous présentions un entier relatif sous forme du résultat d'un système d'affectations polynomiales en cascade. De ce point de vue, une liste

$$[\, x_1, P_1, P_2, \dots, P_k] \qquad \text{avec}$$

$$P_1 \quad Z[X_1]\,, \; P_2 \quad Z[X_1,X_2]\,, \; \dots, \; P_k \quad Z[X_1,X_2, \dots, X_k]\,,$$

(où les P_i sont écrits en présentation creuse ordinaire) sert à représenter l'élément $x = x_{k+1}$ de Z défini par les affectations en cascade:

$$x_2 := P_1(x_1)$$
$$x_3 := P_2(x_1,x_2)$$
$$\dots\dots\dots\dots\dots$$
$$x_{k+1} := P_k(x_1,x_2 \dots, x_k)$$

Nous noterons Z_{pol} la présentation ainsi obtenue de l'ensemble des entiers relatifs. Plus généralement si A désigne un anneau donné dans une présentation concrètement spécifiée, nous désignerons par **Sap**(A) la nouvelle présentation obtenue de manière analogue à Z_{pol}, par système d'affectations polynomiales en cascade.

La présentation Z_{pol} est par bien des égards supérieure à la présentation standard en binaire Z. En particulier, on peut effectuer *en temps linéaire* (c.-à-d. dans la classe **LINTIME**) les affectations polynomiales en cascade dans Z_{pol}. Il suffit en effet de "juxtaposer" les différentes affectations après avoir changé quelques noms de variables. Et à vrai dire, on a fait exactement ce qu'il fallait pour rendre les affectations polynomiales en cascade calculables en temps linéaire dans la présentation qu'on a construit[1].

On peut exprimer le résultat précédent comme suit : l'évaluation $\mathbf{Sap}(Z_{pol}) \rightarrow Z_{pol}$ est en temps linéaire. Par contre, si on considère l'élément de Z_{pol} défini par $[2, X_1^2, X_2^2, \dots, X_k^2]$, il est égal à 2^{2^k} et cela implique que l'évaluation $Z_{pol} \rightarrow Z$ est en espace exponentiel (au moins). Cela montre que la présentation Z_{pol} est nettement préférable à la présentation Z en ce qui concerne les affectations polynomiales en cascade.

Mais il y a un prix à payer ....

La raison poour laquelle on préfère en général travailler avec Z est qu'on ne sait pas bien faire dans Z_{pol} un certain nombre d'opérations et de tests considérés comme indispensables :

---

[1] De la même manière que les présentations en magma sont exactement ce qu'il faut pour rendre la partie "lois de composition" d'une structure algébrique calculable en temps linéaire. (cf [**Lom1**] § B.e)

Questions ouvertes :

(1) Peut-on tester en temps polynomial l'égalité 2 éléments de Z_{pol} ?

(2) Peut-on calculer en temps polynomial le signe d'un élément de Z_{pol} ?

(3) L'opération de division euclidienne est-elle une **P**-opération dans Z_{pol} ?

La réponse à la troisième question semble presque sûrement négative : lorsqu'on divise 2 nombres dont l'ordre de grandeur est $2^{2^{n+1}}$ et 2^{2^n} le reste de la division est a priori du même ordre de grandeur, les 2 premiers nombres peuvent être choisis de manière à être présentés par une liste de taille environ c.n (où c est constant) dans Z_{pol}, mais, pour un polynôme Q fixé, les listes de taille $\leq Q(c.n)$ ne représentent pas plus de $N^{Q(c.n)}$ nombres distincts[1], et il n'y a donc "aucune chance" pour que le reste de la division puisse être écrit *en espace polynomial* dans Z_{pol}.

Un système d'affectations polynomiales en cascade peut être vu sous forme d'un programme à exécuter, dans lequel seul un jeu fini d'instructions est autorisé, sans aucune boucle. C'est ce que l'on appelle encore un *straight-line program* dans la littérature : les présentations par straight-line program ont surtout été étudiées pour des anneaux de polynômes à coefficients dans Z ou dans Q, en général les seules instructions autorisées sont les instructions d'affectation : $Z \leftarrow c$ (c un élément de l'anneau donné dans une présentation "ordinaire"), $Z \leftarrow X$, $Z \leftarrow X + Y$, $Z \leftarrow X \times Y$, $Z \leftarrow X$ divisé par Y (le programme avorte si $Y = 0$ ou si X n'est pas divisible par Y). Un exemple typique d'un tel straight-line program est le programme permettant de calculer un déterminant par la méthode de Bareiss, sans recherche de pivot non nul. Si on exclut les divisions, on obtient une présentation **P**-équivalente à la présentation par systèmes d'affectations polynomiales. Les résultats obtenus dans l'étude de la présentation par straight-line programs sont essentiellement probabilistes : par exemple on peut tester rapidement avec une très faible probabilité d'erreur si 2 entiers de Z_{pol} sont égaux en les calculant modulo quelques nombre premiers. On pourra par exemple consulter l'article de Kaltofen: [**Kal**] .

Si on augmente le nombre d'instructions autorisées, on assouplit la présentation des objets considérés, au détriment de la facilité à exécuter certains tests ou opérations. Si on autorise les boucles **Répéter** i **fois** (où i est la valeur prise par une variable du programme) on obtiendra une présentation Z_{prim} pour les entiers (nous mettons prim en indice pour indiquer que l'algorithme qui calcule l'entier est de type primitif récursif).

Divertissement mathématique: Le test d'égalité dans Z_{prim} est-il primitif récursif ?

La structure algebrique de R_{alg}

Notons $\mathbf{R}_{alg}$ (avec un **R** gras) l'ensemble des nombres réels algébriques *abstrait* (c.-à-d. abstraction faite de tout présentation particulière de cet ensemble).

En tant qu'ensemble, c'est un ensemble *dénombrable* c.-à-d. *énumérable (1)* et *discret (2)* (nous reprenons la terminologie utilisée dans [**Lom1**]) .

Du point de vue de sa structure algébrique, nous retenons tout d'abord que c'est un *corps*

---

[1] N est le nombre de symboles dans l'alphabet utilisé

réel clos archimédien , ce qui signifie :

(3) une strucure de corps

(4) une relation d'ordre total compatible avec la structure de corps

(5) la majoration de tout élément par un entier

(6) l'existence d'un zéro pour un polynôme P sur un intervalle où il change de signe.

En outre, nous avons :

(7) une injection naturelle $\mathbf{R}_{alg} \rightarrow R$

(8) pour tout élément x de $\mathbf{R}_{alg}$ *l'existence d'un polynôme non nul de* $Z[X]$ *qui annule x .*

Cela suffit pour une description abstraite de $\mathbf{R}_{alg}$, c.-à-d. à isomorphisme unique près. D'un point de vue constructif, la traduction des éléments de structure numérotés de (1) à (8) ci-dessus doit être entièrement faite en termes d'opérations, tests, fonctions, au sens constructif de ces termes. Dressons un tableau pour expliciter ceci :

élément de la structure	opération correspondante
(1) ensemble énumérable	construction d'objets concrets représentant les nombres réels algébriques abstraits : tout processus analogue à la construction des entiers naturels. On notera désormais R_a le préensemble ainsi construit.
(2) discret	on donne un test d'égalité dans R_a : c'est désormais un ensemble énumérable discret
(3) structure de corps	on donne les constantes 0 et 1 ainsi que les fonctions correspondant aux 4 opérations de la structure de corps (la fonction $x \rightarrow 1/x$ est définie pour $x \neq 0$)
(4) relation d'ordre	on donne un test pour $x < y$? en termes constructifs, on dit que la relation d'ordre est discrète
(5) archimédien	on donne une opération $Maj : R_a \rightarrow N$ telle que $x \leq Maj(x).1$ pour tout x
(6) réel clos	on donne une opération $Rac : R_a[X] \times R_a \times R_a \rightarrow R_a$ telle que : Si $a < b$ et $P(a).P(b) < 0$, alors $Rac(P , a , b) = u$ avec : u est une racine de P sur $] a , b [$ (a priori Rac n'est pas une fonction)
(7) injection canonique $R_a \rightarrow R$	on donne une opération $F : R_a \times N_1 \rightarrow D$ telle que $F(x,n) = r/2^n$ (avec r Z) est une approximation de x avec la précision 2^{-n} .
(8) tous les éléments sont algébriques sur Q	on donne une opération $Pol : R_a \rightarrow Z[X] - \{0\}$ telle que : $Pol(x)(x) = 0$ pour tout x (a priori Pol n'est pas une fonction)

Considérons maintenant la présentation naïve R_{alg} définie en a). C'est une **P**-présentation de la structure dans la mesure où les éléments de structure (2) (3) (4) (5) (7) (8) sont réalisables comme des **P**-opérations. Mais il y a manifestement deux points faibles. D'une part, lorsqu'on fait des opérations arithmétiques en chaîne, par exemple lorsqu'on évalue un polynôme avec un nombre d'indéterminées non fixé a priori, il y a une croissance exponentielle inévitable de la taille des réels calculés, à cause de l'explosion de leur degré. Autrement dit, R_{alg} n'est pas une présentation complètement-**P**-calculable de la structure de corps. D'autre part, pour ce qui concerne la recherche des racines d'un polynôme à coefficients dans R_{alg} on a le même problème d'explosion exponentielle du degré donc de la taille.

Présentations **P**-équivalentes à la présentation naïve

En fait, on ne peut avoir les opérations (2) → (8) simultanément en temps polynomial.

Proposition b.1 :

Soit R_a un corps ordonné, donné dans une présentation telle que :

(3') les lois de corps sont **P**-calculables

(4') le signe d'un élément est **P**-calculable

(6') il existe une **P**-opération $Rac : Z[X] \times Q \times Q \to R_a$ telle que :

$(a < b , P(a).P(b) < 0)$ $Rac(P, a, b) = u$ est une racine de P sur $]a, b[$

(8') Il existe une opération $Pol : R_a \to Z[X] - \{0\}$ avec: $Pol(x)(x) = 0$ pour tout x.

Alors R_a et R_{alg} sont deux présentations **P**-isomorphes de $\mathbf{R}_{alg}$

Ceci ne signifie pas pour autant que certaines présentations **P**-isomorphes à R_{alg} ne soient pas préférables à d'autres.

Par exemple, nous pouvons accepter de représenter un nombre algébrique sous forme $R(\xi_1,\xi_2,\ldots,\xi_n) / d$, où n est a priori majoré par un n_0 fixe, où les ξ_i sont des éléments de R_{alg} définis comme racines de polynômes unitaires, où R est à coefficients dans Z, et où d est un entier. D'après la proposition a.10 on obtient une présentation **P**-isomorphe à R_{alg}, mais les calculs y sont plus souples (voir notamment la remarque qui suit la proposition a.10).

Nous étudions dans le § c) une présentation très souple, par systèmes d'équations emboitées, non **P**-isomorphe à R_{alg}, mais pour laquelle les majorations de taille et de temps de calcul sont essentiellement les mêmes que dans R_{alg}.

L'espoir de tout réaliser en temps polynomial étant exclu, la tentative raisonnable serait de laisser tomber (8) (la **P**-calculabilité d'un polynôme annulant x) en ne conservant qu'une caratérisation indirecte de l'algébricité de x.

Même dans ce cas, il semble cependant improbable qu'une autre présentation du corps des réels algébriques puisse rendre à la fois le test de comparaison **P**-décidable et l'addition et le produit c-**P**-c. Une réponse définitivement négative serait obtenue si on démontrait un résultat analogue à celui énoncé ci-dessous:

Question ouverte :

? l'opération qui, à partir d'une liste d'entiers $[x_1, \ldots, x_n]$, (les x_i dans Z écrits en binaire) calcule le signe de la somme $\sum x_i^{1/3}$ *n'est pas* calculable en temps polynomial.

c) Systèmes d'équations en cascade, avant la levée de l'ambiguïté

Position du problème, notations

Signalons pour commencer qu'il est nettement plus agréable, plutôt que travailler dans R_{alg}, de travailler avec les *entiers algébriques réels* en considérant la partie $R_{e,alg}$ formée des triplets (P, a, b) où P est un polynôme unitaire et où a et b sont de la forme $(c-1)/2^n$ et $(c+1)/2^n$ avec $c \in Z$. Par ailleurs tout calcul dans R_{alg} se ramène facilement à un calcul dans $R_{e,alg}$. On peut enfin noter $C_{e,alg}$ la présentation des entiers algébriques complexes via leurs parties réelles et imaginaires (présentées dans $R_{e,alg}$).

Nous étudions dans ce paragraphe une présentation des entiers algébriques réels ou complexes, que nous notons $C_{sae,N}$ et qui est directement inspirée du système D5 ([**DD**]). Ce dernier utilise des systèmes d'équations emboîtées: de tels systèmes d'équations peuvent avoir plusieurs solutions et il y a donc ambiguïté quant au nombre algébrique décrit. Le problème le plus immédiat qui se pose avec D5 est celui de la levée des ambiguïtés "en cours de calcul". Cette levée des ambiguïtés, avec en sortie tous les cas possibles, peut manifestement prendre un temps exponentiel, si par exemple on demande d'additionner $2n$ nombres racines de l'équation $X^2 = 2$, et qu'on pose le problème de savoir si la somme obtenue est nulle. Par ailleurs, le maintien des ambiguïtés *aussi longtemps que possible* peut très bien être vu aussi comme le principal avantage de D5. L'ambition de D5 est d'être utilisable pour tous calculs usuels sur les nombres algébriques, à la demande, un peu comme on utilise des entiers de longueur arbitraire dans n'importe quel système de calcul formel.

Nous étudions ici ce qui se passe lorsqu'on lève a priori l'ambiguïté en donnant une approximation rationnelle (dans $Q[\sqrt{-1}]$) convenable de la solution. En ce qui concerne les entiers algébriques réels, ils sont simplement obtenus lorsqu'on impose à l'approximation rationnelle d'être réelle. Il va de soi que le système pourrait être adapté pour des calculs avec des entiers algébriques p-adiques.

Le résultat auquel on arrive est celui-ci :

> *tout* calcul *raisonnable* dans $C_{sae,N}$ peut être mené en temps uniformément polynomial par rapport à, d'une part la taille de l'entrée, d'autre part les "degrés a priori" (voir définition un peu plus loin) des entiers algébriques entrés.

Et ces calculs raisonnables comprennent le calcul de valeurs approchées, le test de comparaison, la recherche des racines d'une équation et la résolution de certains systèmes d'équations linéaires (ceux dont les coefficients restent dans un sous-corps convenablement contrôlé).

On pourra objecter que, finalement, on n'obtient rien de fondamentalement meilleur qu'avec $R_{e,alg}$. La réponse est que D5 possède beaucoup plus de souplesse, ce qui permet dans bien des cas d'avoir un calcul en temps polynomial par rapport à la seule taille des entrées, qui peut être

beaucoup plus petite que la taille des entrées analogues dans $R_{e,alg}$. D'autre part, la meilleure méthode pour démontrer les majorations correspondantes dans R_{alg} est sans doute via la présentation D5 .

Systèmes d'équations algébriques emboîtées

Un *système d'équations algébriques emboîtées* (ou encore "en cascade") est donné par une liste de polynômes $\mathbf{P} := [P_1,P_2,\ldots,P_k]$ avec

$$P_1 \quad Z[X_1] \text{ , } P_2 \quad Z[X_1,X_2] \text{ , } \ldots \text{ , } P_k \quad Z[X_1,X_2,\ldots,X_k]$$

chaque P_j étant unitaire de degré d_j en tant que polynôme en X_j

Le système est dit *normalisé* si les conditions suivantes sur les degrés sont réalisées

$$d_j \geq 2 \text{ pour tout } j \quad \text{et} \quad d_{X_h}(P_j) < d_h \text{ pour tout } h < j$$

Dans un système normalisé, on évite les affectations polynomiales en cascade pour se concentrer sur l'aspect "solution d'équations algébriques".

Une *solution réelle (resp. complexe) du système défini par la liste* $\mathbf{P}$ est un k-uple $\xi = [\xi_1,\xi_2,\ldots,\xi_k]$ de nombres réels (resp. complexes) vérifiant

$$P_1(\xi_1) = 0 \text{ , } P_2(\xi_1,\xi_2) = 0 \text{ , } \ldots \text{ , } P_1(\xi_1,\xi_2,\ldots,\xi_k) = 0 \text{ .}$$

On est alors amené naturellement à travailler dans l'anneau $Z[\xi_1,\xi_2,\ldots,\xi_k]$. Nous noterons $\mathbf{A}_\xi$ cet anneau.

Le problème de la levée de l'ambiguïté

Un système normalisé d'équations algébriques emboîtées étant donné, se pose le problème de la levée de l'ambiguïté, c.-à-d. comment coder une solution particulière du système.
Dans le cas des solutions réelles, on peut envisager pour cela plusieurs méthodes:

- codage de la racine ξ_i de $P_i(\xi_1,\ldots,\xi_{i-1},X_i)$ via les signes que prennent les dérivées successives de P_i (par rapport à la variable X_i), en utilisant le lemme de Thom (cf [**CoR**])
- codage de la racine ξ_i de $P_i(\xi_1,\ldots,\xi_{i-1},X_i)$ par son numéro d'ordre (le nombre de racines réelles est connu par le théorème de Sturm)
- on situe la racine sur un intervalle rationnel où le polynôme admet une seule racine réelle (de nouveau utilisation du théorème de Sturm)
- méthode naïve: on situe la racine sur un intervalle rationnel où le polynôme change de signe et où la dérivée reste de signe constant de manière évidente
- méthode analytique (ou "purement numérique"): on donne une approximation rationnelle[1] $(x_1,x_2,\ldots,x_k)$ de $(\xi_1,\xi_2,\ldots,\xi_k)$ avec l'assurance que le processus de Newton, appliqué pour la valeur initiale $(x_1,x_2,\ldots,x_k)$ convergera vers $(\xi_1,\xi_2,\ldots,\xi_k)$.

A priori, dans le cas réel, il semble que la meilleure solution doive être recherchée à l'une des 2 extrémités, selon que l'on se situe dans un cadre de géométrie algébrique réelle ou de géométrie analytique réelle.

---

[1] Comme déjà signalé, dans le cas complexe, nous parlons d'approximation rationnelle pour une approximation dans $Q[\sqrt{-1}\,]^k$

Nous étudierons ici les résultats de complexité quand on adopte le dernier point de vue, et nous nous situerons d'emblée dans le cas complexe. Signalons quelques avantages qui sautent immédiatement au regard:

− comme la solution $(\xi_1,\xi_2,\ldots,\xi_k)$ est traitée globalement, on n'aura pas de récurrence sur k à assumer, et la taille des calculs sera plus aisée à maîtriser

− tous les calculs " dans C " sont a priori très aisés (grande efficacité de la méthode de Newton)

− la méthode est facilement généralisable au cas réel ou p-adique; et dans ce dernier cas, Hensel (c.-à-d. Newton p-adique) est encore plus facile à contrôler.

Signalons également deux désavantages (liés entre eux d'ailleurs)

− seules les racines *simples* d'un système d'équations donné (c.-à-d.: chaque ξ_i est racine simple du polynôme correspondant) sont *immédiatement* codables, c.-à-d. sans changer de système d'équations (en fait, voir l'extension du codage donnée dans la définition d.8) .

− certaines racines d'un système "peu encombrant" peuvent avoir un code "relativement encombrant" (en particulier les racines "presque doubles") .

Il semble clair que les désavantages sont exactement symétriques des avantages. Sans doute à l'autre extrémité, avec la méthode à la Thom, la situation serait elle renversée.

Nous noterons $C_{sae,\,N}$ l'ensemble des entiers algébriques complexes dans la présentation via des systèmes d'équations algébriques emboîtées, la levée de l'ambiguïté étant faite à la Newton (nous précisons plus loin exactement cette présentation et en particulier comment on assure la convergence). Nous dirons que *le couple* $(\mathbf{P},[x_1,\ldots,,x_k])$ *constitue une présentation de la liste* $\xi = [\xi_1,\xi_2,\ldots,\xi_k]$ dans $C_{sae,\,N}$. Enfin, si le polynôme R de $Z[X_1,X_2,\ldots,X_k]$ a son degré en chaque X_i inférieur à d_i nous dirons que *le triplet* $(\mathbf{P},[x_1,\ldots,,x_k],R)$ *constitue une présentation de l'entier algébrique* $R(\xi_1,\xi_2,\ldots,\xi_k)$ dans $C_{sae,\,N}$.

L'entier $\mathbf{d} := d_1\, d_2 \ldots d_k$ est par définition le *degré a priori* des entiers algébriques ξ_k et $R(\xi_1,\xi_2,\ldots,\xi_k)$ dans cette présentation. Dans un contexte où plusieurs systèmes d'équations emboîtées interviennent, on notera $dg(\mathbf{P})$ pour $d_1\, d_2 \ldots d_k$.

Enfin, nous noterons $R_{sae,\,N}$ l'ensemble des entiers algébriques réels, donnés dans la présentation analogue à $C_{sae,\,N}$ (l'approximation rationnelle étant dans Q^k).

L'anneau $\mathbf{A_P}$

Un système *normalisé* d'équations algébriques emboîtées étant donné par la liste $\mathbf{P}$, l'anneau $\mathbf{A_P}$ est par définition le quotient $Z[X_1,X_2,\ldots,X_k] / <\mathbf{P}>$, où $<\mathbf{P}>$ est l'idéal engendré par $P_1(X_1)$, $P_2(X_1,X_2)$, ... , $P_k(X_1,X_2,\ldots,X_k)$. C'est un Z-module libre de dimension $\mathbf{d}$ dont une base canonique est donnée par les monômes unitaires de $Z[X_1,X_2,\ldots,X_k]$ de degré $< d_j$ en chaque variable X_j . Cet anneau (variable au cours des calculs puisqu'on doit pouvoir introduire de nouveaux nombres algébriques à volonté) est le cadre de travail naturel dans D5 . C'est à la fois parce que cet anneau est "variable" et parce que les calculs raisonnables sont (relativement) bien maîtrisés dans cet anneau que la présentation $C_{sae,\,N}$ est (relativement) efficace.

Un élément α *de l'anneau* $\mathbf{A_P}$ *est toujours considéré comme présenté via ses coordonnées sur la base canonique, a priori en présentation creuse*. Si $\mathbf{lg}(\alpha)$ est sa taille en présentation creuse, sa

taille en présentation dense est majorée par $\mathbf{d}\,\mathbf{lg}(\alpha)$. Il est cependant "exceptionnel" que la taille en présentation creuse reste significativement plus petite que la taille en présentation dense après que quelques calculs (des produits, notamment) aient été effectués dans $\mathbf{A_P}$.
Nous notons $\mathbf{lg}(\mathbf{P})$ la taille de la liste $\mathbf{P}$, les entiers étant écrits en binaire et la présentation des polynômes pouvant être creuse. La taille de la liste en présentation dense est alors majorée par $k\,\mathbf{d}\,\mathbf{lg}(\mathbf{P})$.

Si $\xi = [\xi_1,\xi_2,\ldots,\xi_k]$ est une solution réelle (ou complexe, ou p-adique) du système défini par la liste $\mathbf{P}$, l'anneau $\mathbf{A}_\xi = Z[\xi_1,\xi_2,\ldots,\xi_k]$ est évidemment un quotient de $\mathbf{A_P}$. Alors que dans $\mathbf{A_P}$ nous avons une écriture unique pour chaque élément, il n'en est pas de même pour $\mathbf{A}_\xi$, et cela pose quelques problèmes pour majorer la taille des calculs dans $\mathbf{A}_\xi$.

Un des buts essentiels de ce § est de montrer le résultat suivant :

la recherche des solutions (comme éléments de $C_{e,alg}{}^k$ *ou comme éléments de* $C_{sae,N}{}^k$*) d'un système normalisé d'équations algébriques emboîtées* $\mathbf{P}$ *peut être réalisée en temps uniformément polynomial par rapport à* $\mathbf{d}$ *et* $\mathbf{lg}(\mathbf{P})$.

En tant que résultat général, on ne peut évidemment espérer mieux, vu que le degré a priori de l'entier algébrique dans la présentation $C_{sae,N}$ est bien souvent son vrai degré, et vu le nombre de solutions possibles a priori. Si la taille d'*une* solution dans $C_{e,alg}{}^k$ est en règle générale contrôlée polynomialement par $\mathbf{lg}(\mathbf{P})$ et $\mathbf{d}$, il semble relativement fréquent que la taille dans $C_{sae,N}{}^k$ soit, elle, contrôlée seulement par $\mathbf{lg}(\mathbf{P})$, ce qui montrerait la supériorité des présentations à la D5.

Majorations polynomiales uniformes pour les calculs dans $\mathbf{A_P}$

Les techniques de majoration que nous utilisons ici sont celles données dans [**Lom1**] à propos des $\mathbf{P_0}$'-anneaux. Nous sommes cependant obligés de redémontrer certains résultats dans la mesure où nous souhaitons des majorations uniformes (avec $\mathbf{P}$ variable, donc $\mathbf{A_P}$ variable). Nous rappelons que nous travaillons avec un système $\mathbf{P}$ normalisé.

Notations pour différentes grandeurs reliées à la taille d'une matrice

Lorsque M est une matrice, ou un polynôme, ou une liste de matrices etc... à coefficients dans Z, donné dans une présentation précisée (creuse ou dense) nous noterons :

$|M|_1 := \mathbf{lg}(\Sigma|\text{ coeffs de } M|)$ $\qquad$ $|M|_2 := \mathbf{lg}\left(\sqrt{\Sigma|\text{ coeffs de } M|^2}\right)$

$|M|_\infty := \mathbf{lg}(\sup|\text{ coeffs de } M|)$

dim(M) := le nombre de coefficients dans la présentation dense "naturelle"

Par exemple, pour la liste de polynômes $\mathbf{P}$ considérée ici :
$\dim(\mathbf{P}) = d_1 + d_1\,d_2 + \ldots + d_1\,d_2 \ldots d_k$
On a : $|M|_\infty \le |M|_2 \le |M|_1 \le \mathbf{lg}(\dim(M)) + |M|_\infty$ et la taille en présentation dense est majorée par $\dim(M)\,|M|_\infty$.

Le résultat vraiment utile est le suivant : si M et N sont 2 polynômes, ou 2 matrices (de dimensions convenables), alors $|MN|_1 \le |M|_1 + |N|_1$.

Majoration pour l'addition et le produit dans $\mathbf{A_P}$

Nous noterons α , β , γ ... des éléments de $\mathbf{A_P}$. Nous noterons $\lambda_1,\lambda_2,\ldots,\lambda_k$ les variables $X_1,X_2,\ldots,X_k$ vues comme éléments de $\mathbf{A_P}$.

L'addition dans $\mathbf{A_P}$ est simplement l'addition coefficient par coefficient, ce qui donne la majoration :

$$|\alpha + \beta|_1 \le \mathbf{sup}(|\alpha|_1, |\beta|_1) + 1 \qquad (1)$$

et donc également :

$$\left|\sum_{i=1}^{n} \alpha_i\right|_1 \le \mathbf{sup}_{i=1,\ldots,n}(|\alpha_i|_1) + \mathbf{lg}(n) \qquad (2)$$

Le produit dans $\mathbf{A_P}$ est à peine plus compliqué. Notons P_α et P_β les polynômes (de degrés $\le d_i - 1$ en X_i $(i=1,\ldots,k)$) qui correspondent à α et β . Le produit $\alpha.\beta$ dans $\mathbf{A_P}$ s'obtient en réduisant modulo l'idéal $<\mathbf{P}>$ (engendré par la liste $\mathbf{P}$) le polynôme $P_\alpha.P_\beta$. On a déjà $|P_\alpha.P_\beta|_1 \le |P_\alpha|_1 + |P_\beta|_1 = |\alpha|_1 + |\beta|_1$. Le polynôme $P_\alpha.P_\beta$ est de degré $\le 2d_i - 2$ en X_i $(i=1,\ldots,k)$.

Notons $\mathbf{P_d}$ le Z-module libre des polynômes de degré $\le 2d_i - 2$ en X_i $(i=1,\ldots,k)$, c'est un module de dimension :

$$\mathbf{d'} = \prod_{i=1}^{k} (2d_i - 1) \le \mathbf{d}^2 \qquad (3)$$

La réduction modulo $<\mathbf{P}>$ pour un polynôme Q de $\mathbf{P_d}$ revient à réécrire Q sur la base $\mathbf{B_P}$ définie ci-après, et à garder les coordonnées utiles. La base $\mathbf{B_P}$ est formée des monômes de degré $\le d_i - 1$ en X_i $(i=1,\ldots,k)$, puis de produits $P_i.M_{i,h}$ où les $M_{i,h}$ sont tous les monômes de degrés majorés selon le tableau suivant, où on a noté $r_i = 2d_i - 2$:

i	degré en X_1	degré en X_2	degré en X_3	degré en X_4	.....	degré en X_k
1	$\le r_1 - d_1$	$\le r_2$	$\le r_3$	$\le r_4$	.....	$\le r_k$
2	$< d_1$	$\le r_2 - d_2$	$\le r_3$	$\le r_4$	.....	$\le r_k$
3	$< d_1$	$< d_2$	$\le r_3 - d_3$	$\le r_4$	.....	$\le r_k$
.	...	...	...	...	.....	...
.	...	...	...	...	.....	...
k	$< d_1$	$< d_2$	$< d_3$	$< d_4$	.....	$\le r_k - d_k$

Si $M = c\,X_1^{s_1} X_2^{s_2} \ldots X_k^{s_k}$ est un monôme, nous dirons que le k-uple $\mathbf{s} := [s_0,s_1,\ldots,s_k]$ est l'exposant du monôme, et nous noterons $c\,\mathbf{X^s}$ ce monôme. Nous ordonnons les exposants selon l'ordre lexicographique suivant :

$[s_0,s_1,\ldots,s_k]$ précède $[t_0,t_1,\ldots,t_k]$ ssi $\quad i \;\; s_i < t_i \,,\; s_{i+1} = t_{i+1} \,,\; \ldots \,,\; s_k = t_k$

Alors le monôme dominant de P_i est $X_i^{d_i}$ et le monôme dominant de $P_i \mathbf{X}^{\mathbf{s}}$ est $X_i^{d_i} \mathbf{X}^{\mathbf{s}}$. Par ailleurs, pour tout exposant $\mathbf{s}$ pour un monôme $\mathbf{X}^{\mathbf{s}}$ de $\mathbf{P_d}$, ou bien $\mathbf{X}^{\mathbf{s}}$ est dans la base canonique de $\mathbf{A_P}$, ou bien il existe un i unique tel que : $d_1 < s_1$, ..., $d_{i-1} < s_{i-1}$, $d_i \geq s_i$; de sorte que $\mathbf{X}^{\mathbf{s}}$ est le monôme dominant d'un unique polynôme de la base $\mathbf{B_P}$. En d'autres termes, la base $\mathbf{B_P}$ est triangulaire par rapport à la base canonique de $\mathbf{P_d}$, formée des monômes $\mathbf{X}^{\mathbf{s}}$ rangés selon l'ordre lexicographique défini ci-dessus. Réduire le polynôme $P_\alpha.P_\beta$ modulo $< \mathbf{P} >$, revient à multiplier la matrice $\Gamma_{\mathbf{P}}$, inverse de la matrice de la base $\mathbf{B_P}$, par le vecteur colonne correspondant au polynôme $P_\alpha.P_\beta$. Cette matrice inverse a pour coefficients des cofacteurs de la matrice de la base $\mathbf{B_P}$. D'après l'inégalité de Hadamard pour majorer les déterminants, on a donc :

$$| \Gamma_{\mathbf{P}} |_\infty \leq (\mathbf{d'} - \mathbf{d})\, \mathbf{sup}(\, | P_i |_2 \,) \leq (\mathbf{d'} - \mathbf{d})\, | \mathbf{P} |_2 \leq (\mathbf{d'} - \mathbf{d})\, | \mathbf{P} |_1$$

d'où : $$| \Gamma_{\mathbf{P}} |_1 \leq 2\, \mathbf{lg}(\mathbf{d'}) + (\mathbf{d'} - \mathbf{d})\, \mathbf{sup}(\, | P_i |_2 \,)$$

nous noterons $$\boxed{m_{\mathbf{P}} = 2\, \mathbf{lg}(\mathbf{d'}) + (\mathbf{d'} - \mathbf{d})\, \mathbf{sup}(\, | P_i |_2 \,)} \qquad (4)$$

d'où enfin $$\boxed{| \alpha \times \beta |_1 \leq m_{\mathbf{P}} + | \alpha |_1 + | \beta |_1} \qquad (5)$$

et $$\boxed{\left| \prod_{i=1}^{n} \alpha_i \right|_1 \leq \sum_{i=1}^{n} | \alpha_i |_1 + (n-1)\, m_{\mathbf{P}}} \qquad (6)$$

NB: Le calcul du produit $\alpha \times \beta$ dans $\mathbf{A_P}$ est donc en temps uniformément polynomial par rapport à $\mathbf{d}$ et la taille des entrées, c.-à-d. encore par rapport à $| \alpha |_1$, $| \beta |_1$, $\mathbf{d}$ et $\mathbf{lg}(\mathbf{P})$. Par exemple en résolvant le système triangulaire par substitutions successives.

Remarques :

1) Si on pose $| \alpha |_{\mathbf{P}} := m_{\mathbf{P}} + | \alpha |_1$, alors on a les 2 majorations :
$| \alpha + \beta |_{\mathbf{P}} \leq \mathbf{sup}(| \alpha |_{\mathbf{P}}, | \beta |_{\mathbf{P}}) + 1$ et $| \alpha \times \beta |_{\mathbf{P}} \leq | \alpha |_{\mathbf{P}} + | \beta |_{\mathbf{P}}$

Pour $\mathbf{P}$ fixé, les calculs de majorations dans $\mathbf{A_P}$ sont donc entièrement analogues à ceux dans Z.

2) Si on a "beaucoup" de calculs à faire dans $\mathbf{A_P}$ avec $\mathbf{P}$ fixé, on peut construire une fois pour toutes la table de multiplication de $\mathbf{A_P}$, c.-à-d. évaluer une fois pour toutes les expressions $\lambda_1^{n_1} \ldots \lambda_h^{n_h}$ où $n_1 \leq 2\, d_1 - 1$, $n_2 \leq 2\, d_2 - 1$, ..., $n_{h-1} \leq 2\, d_{h-1} - 1$, $d_h < n_h \leq 2\, d_h - 1$ $(1 \leq h \leq k)$.

On déduit des majorations précédentes les 2 propositions qui suivent :

Théorème c.1 :

a) Soit $[\alpha_i]_{i=1,\ldots,m}$ une liste d'éléments de $\mathbf{A_P}$ et $\mathrm{Expr}(Y_1,\ldots,Y_m)$ une expression algébrique écrite explicitement avec des $+$, $\times$, des entiers écrits en binaire, et les variables Y_i, alors l'évaluation de $\mathrm{Expr}(\alpha_1,\ldots,\alpha_m)$ dans $\mathbf{A_P}$ est en temps uniformément polynomial par rapport à $\mathbf{d}$ et la taille des entrées, c.-à-d. encore par rapport à $\Sigma | \alpha_i |_1$, $\mathbf{lg}(\mathrm{Expr})$, $\mathbf{d}$ et $\mathbf{lg}(\mathbf{P})$

b) En particulier si $R \in Z[Y_1,...,Y_m]$, $d_i = d_{X_i}(R)$, $d_R = d_1 + ... + d_m$, n_R = nombre de coefficients non nuls de R, on a :

$$\boxed{|R(\alpha_1,...,\alpha_k)|_1 \leq (m_{\mathbf{P}} + \mathbf{sup}(|\alpha_j|_1))\, d_R + |R(Y_1,...,Y_m)|_\infty + \mathbf{lg}(n_R)} \quad (7)$$

preuve> *a)* Le nombre d'opérations élémentaires de $\mathbf{A_P}$ est majoré par $\mathbf{lg}$(Expr). Le résultat final et chaque résultat intermédiaire sont convenablement majorés en appliquant (1) et (5), chaque opération élémentaire de $\mathbf{A_P}$ est donc en temps convenablement majoré.

b) Si $c X_1^{r_1} \dots X_m^{r_m}$ est un monôme de R, la majoration (6) donne :

$$\begin{aligned} |c\,\alpha_1^{r_1} \dots \alpha_m^{r_m}|_1 &\leq |c|_\infty + (r_1+\dots+r_m-1)\, m_{\mathbf{P}} + r_1|\alpha_1|_1 + \dots + r_m|\alpha_m|_1 \\ &\leq |R|_\infty + (d_R - 1)\, m_{\mathbf{P}} + d_R\, \mathbf{sup}(|\alpha_j|_1) \end{aligned}$$

et on conclut par l'inégalité (2)

<findepreuve

Remarque: La méthode qui consisterait à évaluer l'expression dans $Z[X_1,X_2,\dots,X_k]$ et à la réduire ensuite modulo <**P**> ne permet pas d'obtenir une majoration en temps uniformément polynomial, à cause du trop grand nombre de monômes qui apparaissent dans l'expression avant sa réduction modulo <**P**>. Ceci complique nettement la tâche pour certains calculs à venir (les calculs de déterminants notamment) parce que l'anneau $\mathbf{A_P}$, contrairement à $Z[X_1,X_2,\dots,X_k]$, n'est pas intègre.

Proposition c.2 :

Soit $R \in Z[X_1,X_2,...,X_k]$ de degré r_i en X_i, et soit

$$r = \sup_{j \in \{1,2,...k\}} (\mathbf{Ent}(r_j/(d_j - 1))) \qquad \mathbf{r} = \prod_{j=1}^{k} r_j$$

a) On note $\lambda_1, \lambda_2, \dots, \lambda_k$ les variables $X_1, X_2, ..., X_k$ vues comme éléments de $\mathbf{A_P}$. Alors, l'évaluation de $R(\lambda_1,...,\lambda_k)$ dans $\mathbf{A_P}$ est en temps uniformément polynomial par rapport à $\mathbf{d}$, $\mathbf{r}$ et la taille des entrées, c.-à-d. encore par rapport à $|R|_1$, $\mathbf{r}$, $\mathbf{d}$ et $\mathbf{lg}(\mathbf{P})$

b) On a la majoration

$$\boxed{|R(\lambda_1,...,\lambda_k)|_1 \leq r\,(1 + m_{\mathbf{P}}) + |R(X_1,X_2,...,X_k)|_\infty + \mathbf{lg}(r_1...r_k)} \quad (8)$$

preuve> Montrons la majoration (8).

On considère un monôme $c.X_1^{s1}.X_2^{s2}.\dots.X_k^{sk}$ de R, on l'écrit sous forme d'un produit de facteurs qui sont des monômes d'exposants inférieurs ou égal à $(d_1-1,\dots,d_k-1)$, le premier de ces facteurs a sa $|\ |_1$ majorée par $|c|_1 \leq |R|_\infty$ les autres par 1. Le nombre des facteurs est $r + 1$. On conclut par (6) que :

$$|c.X_1^{s1}.X_2^{s2}.\dots.X_k^{sk}|_1 \leq r\, m_{\mathbf{P}} + r + |R(X_1,X_2,\dots,X_k)|_\infty$$

Enfin, il y a au plus $r_1 \dots r_k$ monômes à ajouter.

La majoration du temps de calcul est claire. Elle peut être sensiblement améliorée si le polynôme R est creux, puisqu'il y a peu d'addition de monômes qui interviennent.

<findepreuve

Majoration de la taille dans C_{alg}^{k} des solutions d'un système normalisé d'équations algébriques emboîtées

Proposition c.3 :

Le calcul du polynôme minimum dans $Z[X]$ d'un élément α de $\mathbf{A_P}$ est en temps uniformément polynomial par rapport à $|\alpha|_1$, **d** et **lg(P)** .

preuve> On calcule la liste $[\alpha^i]_{i=0,...,\mathbf{d}-1}$ dans $\mathbf{A_P}$ (proposition précédente), il reste à établir la première relation de dépendance Q-linéaire entre ces vecteurs, par exemple en triangulant à la Bareiss dans Z la matrice $\mathbf{d} \times \mathbf{d}$ dont les colonnes sont les α^i écrits sur la base canonique de $\mathbf{A_P}$ convenablement ordonnée.
<findepreuve

Remarque : Un élément α de $\mathbf{A_P}$ est inversible (dans $\mathbf{A_P}$ Q) si et seulement si il est non diviseur de 0 , si et seulement si son polynôme minimum T vérifie $T(0) \neq 0$. *Il y a donc un test d'inversibilité dans* $\mathbf{A_P}$ Q *en temps uniformément polynomial par rapport à* $|\alpha|_1$, **d** *et* **lg(P)** .
De plus, lorsque α est inversible, $T(0)\,\alpha^{-1}$ s'exprime comme polynôme en α de degré $< d(T)$ (avec les coefficients de T en ordre inverse) et peut donc lui aussi être calculé en temps uniformément polynomial.
Une autre méthode consiste à regarder l'équation en β (β $\mathbf{A_P}$ Q) : $\alpha\,\beta = 1$, comme un système de **d** équations à **d** inconnues dans Q (les coefficients de β sur la base canonique de $\mathbf{A_P}$). Ce système d'équations est facile à écrire une fois qu'on a construit la table de multiplication de $\mathbf{A_P}$.

Proposition c.4 :

La taille de toute solution dans R_{alg}^{k} ou C_{alg}^{k} d'un système normalisé d'équations algébriques emboîtées défini par la liste **P** est uniformément majorable par un polynôme en **d** et **lg(P)** .

preuve> Soit ξ_1 , ..., ξ_k une solution du système. On applique la proposition précédente à ξ_1 , ..., ξ_k vus comme éléments de $\mathbf{A_P}$. Il est ensuite aisé de majorer polynomialement la taille d'un élément dans R_{alg} ou dans C_{alg} d'un élément à partir ce celle d'un polynôme qu'il annule
<findepreuve

Remarque :
On peut obtenir immédiatement le résultat suivant (qui sera amélioré par la suite)
Le calcul de toutes les solutions dans R_{alg}^{k} d'un système normalisé d'équations algébriques emboîtées défini par la liste **P** peut être effectué en temps uniformément polynomial à partir de $\mathbf{d}^k$ et **lg(P)** .
preuve > notons λ_i la valeur de X_i dans $\mathbf{A_P}$. Pour $i = 1,...,k$, on peut calculer en temps uniformément polynomial les polynômes minimaux T_i des λ_i dans $\mathbf{A_P}$, puis, en appliquant le théorème a.12, toutes les racines de ces polynômes T_i . Il s'agit de tester ensuite chaque k-uple ξ_1 , ..., ξ_k pour savoir s'il est une solution du système emboîté **P** .
Pour cela considérons le système $\mathbf{T} := [T_1(X_1), T_2(X_2), ..., T_k(X_k)]$, pour lequel

$dg(\mathbf{T}) = d_1^{k}.d_2^{k-1}\ldots d_k$. Le polynôme $P_j(X_1,X_2,\ldots,X_j)$ définit un élément π_j de $\mathbf{A_T}$ dont on peut calculer le polynôme minimum S_j . Le réel algébrique $P_j(\xi_1,\xi_2,\ldots,\xi_j)$ est une racine de S_j , et on sait rapidement en calculer une bonne approximation rationnelle.
Or une racine non nulle de S_j est minorée par $\dfrac{|\,c_h\,|}{|\,c_h\,| + \mathbf{sup}(|\,c_i\,|)}$ où c_h est le coefficient non nul de degré minimum de S_j .

<findepreuve

La même preuve donne le résultat suivant au niveau de R_{alg} :
Soient $\xi_1, \xi_2, \ldots, \xi_n$ *des éléments de* R_{alg} *racines de polynômes* $Q_1, \ldots, Q_n$ *de* $Z[X]$ *et de degrés* $d_1, \ldots, d_n$. *Alors les racines réelles du polynôme* $X^n + \xi_1 X^{n-1} + \ldots + \xi_n$ *peuvent être calculées comme éléments de* R_{alg} *en temps uniformément polynomial par rapport à* $d_1\ldots d_n$ *et à* $\Sigma\,|\,Q_i\,|_1$

Produit d'une liste de matrices à coefficients dans $\mathbf{A_P}$

Proposition c.5 :

a) Soient Δ et Δ' deux matrices de dimensions $n \times p$ et $p \times q$. On a la majoration

$$|\,\Delta \times \Delta'\,|_1 \leq m_{\mathbf{P}} + |\,\Delta\,|_1 + |\,\Delta'\,|_1 + \mathbf{lg}(n) + \mathbf{lg}(p) + \mathbf{lg}(q) \qquad (9)$$

b) Soit $\Gamma = [\Gamma_i]_{i=1,\ldots,m}$ une liste de matrices à coefficients dans $\mathbf{A_P}$, de dimensions adéquates pour qu'on puisse calculer le produit $\prod \Gamma_i$.
Alors le calcul dans $\mathbf{A_P}$ du produit $\prod \Gamma_i$ peut être effectué en temps uniformément polynomial par rapport à $\mathbf{d}$, $\dim(\Gamma)$ et la taille des entrées, c.-à-d. encore par rapport à $|\,\Gamma\,|_1$, $\dim(\Gamma)$, $\mathbf{d}$ et $\mathbf{lg(P)}$.

preuve> *Le produit de 2 matrices tout d'abord* (Δ et Δ' de dimensions $n \times p$ et $p \times q$) : le nombre d'opérations élémentaires dans $\mathbf{A_P}$ est polynomialement majoré à partir n , p , q . De plus les inégalités (2) et (6) montrent que la taille des résultats intermédiaires est convenablement contrôlée et donnent pour chaque coefficient $\gamma_{i,j}$ du produit $\Delta \times \Delta'$ le majoration : $|\,\gamma_{i,j}\,|_1 \leq m_{\mathbf{P}} + |\,\Delta\,|_1 + |\,\Delta'\,|_1 + \mathbf{lg}(p)$ d'où on déduit immédiatement (9)
Pour le produit de m matrices : l'inégalité (9) montre que la taille des matrices intermédiaires est bien contrôlée.

<findepreuve

Calculs de déterminants dans $\mathbf{A_P}$

Théorème c.6 :

Soit Γ une matrice carrée à coefficients dans $\mathbf{A_P}$, de dimension $m \times m$.
Alors le calcul dans $\mathbf{A_P}$ du déterminant de Γ est en temps uniformément polynomial par rapport à $\mathbf{d}$, m et la taille des entrées, c.-à-d. encore par rapport à $|\,\Gamma\,|_1$, m , $\mathbf{d}$ et $\mathbf{lg(P)}$.

preuve> On pourrait songer à utiliser la méthode de Bareiss, mais il y a un risque qu'à une certaine étape tous les coefficients "candidats pivots" soient diviseurs de 0 sans que le déterminant

soit nul. Par contre, la méthode de Leverrier, vue la proposition c.5 , fonctionne correctement en temps uniformément majoré. Même démonstration que pour le Théorème B.b1 dans [**Lom1**]. La méthode de Fadeev peut également être utilisée[1].

<findepreuve

On notera qu'il est également possible d'utiliser la méthode de Samuelson (cf. [**Sam**] et [**Ber**]) pour calculer les déterminants puisque tous les résultats intermédiaires sont convenablement majorés en taille. L'avantage est que cette méthode peut se généraliser en caractéristique p , en particulier si on veut travailler dans la clôture algébrique d'un corps fini **F** ou dans la clôture algébrique du corps des fractions rationnelles correspondant **F**(X).

---

[1] La méthode de Fadeev est une version améliorée de la méthode de Leverrier. Comme l'anneau $\mathbf{A}_{\mathbf{P}}$ est traité à travers une représentation sans ambiguïté, la condition de **P**-réductibilité exigée dans [**Lom1**] pour une majoration correcte de la taille des objets manipulés pendant l'exécution de l'algorithme de Fadeev est automatiquement vérifiée.

d) Systèmes d'équations en cascade, après une levée de l'ambiguïté à la Newton

Le cadre de travail

Si $(\mathbf{P},[x_1,\ldots,x_k])$ est une présentation dans $C_{sae,N}$ de la liste $[\xi_1,\xi_2,\ldots,\xi_k]$ nous cherchons à travailler dans l'anneau $\mathbf{A}_\xi$ quotient de $\mathbf{A}_\mathbf{P}$. Si $\alpha \quad \mathbf{A}_\mathbf{P}$ nous noterons α_ξ l'élément correspondant de $\mathbf{A}_\xi$ et nous dirons que *le triplet* $(\mathbf{P},[x_1,\ldots,x_k],\alpha)$ *est une présentation de l'entier algébrique* α_ξ *dans* $C_{sae,N}$.
Nous disons que $\mathbf{d} = d_1\ldots d_k$ est *le degré a priori* de l'entier algébrique α_ξ.
Nous notons $\mathbf{lg}(\alpha_\xi)$ la taille de $(\mathbf{P},[x_1,\ldots,x_k],\alpha)$ ($\mathbf{P}$ et α peuvent être donnés en présentation creuse).

Les remarques qui suivent les propositions c.3 et c.4 montrent (à très peu près) qu'on pourrait systématiquement "désemboîter" les systèmes d'équations algébriques emboîtées et garder des bornes de complexité "en temps uniformément polynomial par rapport à $\mathbf{d}$ et $\mathbf{lg}(\alpha_\xi)$". Le but est cependant justement de désemboîter le moins possible en espérant que la complexité effective soit plus faible (ce qui serait à peu près exclu si on désemboîtait systématiquement), c'est en tout cas là la philosophie de D5.

Précisions concernant les conditions de convergence du processus de Newton

Une étude particulièrement détaillée des conditions de convergence du processus de Newton est donnée dans [**Ost**] notamment chap. 38 → 42.
Nous nous en tiendrons à des conditions plus classiques quoique moins fines données dans [**DM**] chap. XIII § 3, 4, 5, 6.
On considère un système réel de n équations (algébriques ou transcendantes) à n inconnues $f_i(z_1,\ldots,z_n) = 0 \quad (i = 1,\ldots, n)$, où les f_i sont 2 fois continûment dérivables. Nous notons encore $\mathbf{f}$ l'application de U (ouvert de R^n) vers R^n définie par les f_i.
Le processus de Newton démarre en un n-uple $\mathbf{x} = (x_1,\ldots,x_n)$ tel que la matrice jacobienne de $\mathbf{f}$ soit inversible en $\mathbf{x}$. On suppose que l'ouvert U contient la boule fermée $\bar{B}_\rho(\mathbf{x})$ de centre $\mathbf{x}$ et de rayon ρ. On note Γ_0 la matrice inverse de la matrice jacobienne de $\mathbf{f}$ en $\mathbf{x}$.
On choisit pour norme dans R^n, $\| \mathbf{z} \| := \mathbf{sup}(|z_i|)$. On utilise pour les matrices la norme correspondante, plus précisément :
Si a_{ij} sont les coefficients de Γ_0, on note $\| \Gamma_0 \| := \mathbf{sup}_i\left(\sum_j |a_{ij}| \right)$.

On suppose que les majorations suivantes sont vérifiées :

$$\| \Gamma_0 \| \leq A_o$$

$$\| \Gamma_0 \, \mathbf{f}(\mathbf{x}) \| \leq B_o \leq \rho/2$$

$$\sum_{k=1,\ldots,n} \left| \frac{\partial^2 f_i(\mathbf{z})}{\partial z_j \, \partial z_k} \right| \leq C \quad \text{pour } z \in \bar{B}_\rho(\mathbf{x}),\ i,j \in \{1,\ldots n\}$$

$$2\, n\, A_0\, B_0\, C = \mu_0 < 1$$

Alors on est assuré que le processus itératif converge vers un point ξ de la boule $\bar{B}_\rho(\mathbf{x})$ qui est l'unique solution de $\mathbf{f}(\mathbf{x}) = 0$ dans cette boule. En fait, si $\mathbf{x}^{(p)}$ est le p-ème itéré, on a $\| \xi - \mathbf{x}^{(p)} \| \leq (1/2^{p-1}\ \mu_0^{\,2^p-1}\ B_o$. En outre si $2B_o/\mu_0 \leq \rho$, alors tout point $\mathbf{x}'$ de la boule de centre $\mathbf{x}$ et de rayon $(1 - \mu_0)\, B_o / 2\, \mu_0$ peut être choisi comme début du processus itératif.

Pour le cas qui nous intéresse, les f_i sont les polynômes de la liste $\mathbf{P}$. La matrice jacobienne de $\mathbf{f}$ est triangulaire, et son déterminant, calculé au point $\mathbf{x}$ est égal à :

$$\frac{\partial P_1(x_1)}{\partial X_1} \quad \frac{\partial P_2(x_1,x_2)}{\partial X_2} \quad \ldots \quad \frac{\partial P_k(x_1,\ldots,x_k)}{\partial X_k}$$

Dans les majorations désirées, la plus difficile à contrôler est a priori celle de $\| \Gamma_0 \|$ or les coefficients de Γ_0 sont égaux à des cofacteurs de la matrice jacobienne divisés par le déterminant. Une *minoration* contrôlée des dérivées partielles ci-dessus est donc la clef du problème.

Dans le cas d'un système complexe de n équations à n inconnues dans C on obtient des résultats tout à fait semblables: le système peut d'ailleurs être traité en le considérant comme un système de 2n équations réelles à 2n inconnues réelles.

Majorations polynomiales pour les calculs dans $C_{sae,\,N}$

Conséquences des majorations dans $\mathbf{A_P}$

Tous les calculs dans $\mathbf{A_P}$ peuvent être considérés comme des calculs dans $\mathbf{A}_\xi$ et les majorations obtenues dans $\mathbf{A_P}$ sont ipso facto des majorations pour les calculs dans $\mathbf{A}_\xi$. Bien que nous n'ayons pas encore les moyens de montrer la calculabilité en temps convenable des solutions d'un système normalisé d'équations algébriques emboîtées, nous avons la possibilité de majorer convenablement la taille des solutions, comme conséquence de la proposition c.4 :

Proposition d.1 :

Il existe une majoration polynomiale uniforme en fonction de **d** et **lg**(**P**) pour la taille de $[x_1,x_2,\ldots,x_k]$ où $(\mathbf{P},[x_1,\ldots,x_k])$ est une présentation dans $C_{sae,\,N}$ de $[\xi_1,\xi_2,\ldots,\xi_k]$ solution complexe *simple* du système normalisé d'équations algébriques emboîtées défini par la liste $\mathbf{P}$.

preuve> Dans toute cette preuve, nous dirons "convenable" pour "polynomiale uniforme en fonction de **d** et **lg**(**P**)". Nous donnons la preuve pour le cas d'une solution réelle. L'adaptation au cas complexe ne présente pas de difficulté.

D'après la proposition c.4 la taille de $[\xi_1,\xi_2,\ldots,\xi_k]$ vus comme éléments de R_{alg} est

correctement contrôlée. Si ξ_i est représenté par (T_i,a_i,b_i) dans R_{alg}, on peut se situer a priori sur le pavé produit des $[\,a_i\,,\,b_i\,]$. On calcule une majoration convenable des dérivées partielles secondes sur ce pavé. Cela fournit en particulier une majoration du taux de variation des dérivées partielles premières intervenant dans le déterminant de la jacobienne. Par ailleurs posons $\alpha_j := \partial P_j(\xi_1,\ldots,\xi_j) / \partial X_j$. La taille de α_j dans $\mathbf{A_P}$ est simplement celle du polynôme $\partial P_j(X_1,\ldots,X_j) / \partial X_j$. On a donc une majoration convenable des coefficients du polynôme minimum de α_j dans $\mathbf{A_P}$, ce qui fournit une minoration convenable de $|\alpha_j|$ (qui est par hypothèse non nul). En couplant ce renseignement avec la majoration du taux de variation de la dérivée partielle, on aura alors une minoration convenable du déterminant de la jacobienne sur un nouveau pavé "pas trop minuscule" autour de ξ et donc une majoration convenable de $||\,\Gamma_0\,||$ sur ce pavé, d'où on déduit une majoration convenable de l'écart entre $\mathbf{x}$ et $[\xi_1,\xi_2,\ldots,\xi_k]$ pour que le processus de Newton converge, ce qui majore convenablement la taille de $\mathbf{x}$.
<findepreuve

Théorème d.2 :

Soit $(\mathbf{P},[x_1,...,x_k],\alpha)$ une présentation de l'entier algébrique α_ξ dans $C_{sae,\,N}$.

a) Le calcul d'une approximation de α_ξ avec la précision $1/2^n$ est en temps uniformément polynomial par rapport à $\mathbf{d}$ et la taille des entrées, c.-à-d. encore par rapport à n, $|\alpha|_1$, $\mathbf{d}$ et $\mathbf{lg(P)}$[1].

b) Le calcul de α_ξ dans C_{alg} est en temps uniformément polynomial par rapport à $|\alpha|_1$, $\mathbf{d}$ et $\mathbf{lg(P)}$.

preuve> *pour le a)* on utilise la méthode de Newton pour calculer ξ avec une approximation arbitraire, en ne conservant à chaque étape que la partie significative du développement en base 2 du rationnel obtenu, ce qui permet de contrôler la taille des calculs intermédiaires[2].

pour le b) cela résulte du a) et du fait qu'on sait calculer en temps convenable un polynôme non nul de $Z[X]$ annulant α_ξ : on termine en appliquant la proposition a.9 ou son analogue dans le cas complexe.
<findepreuve

---

1 En langage plus imagé, on pourrait dire que l'évaluation $\mathbf{A}_\xi \to C$ est en temps uniformément polynomial par rapport à $\mathbf{d}$ et la taille des entrées (cf la définition A.a5 dans un contexte voisin.

2 Ceci mériterait un développement détaillé à soi tout seul.

Test d'égalité à zéro d'un élément de $\mathbf{A}_\xi$ (calcul du signe dans le cas réel), et calcul de son inverse

Proposition d.3 :

Soit $(\mathbf{P},[x_1,...,x_k],\alpha)$ une présentation de l'entier algébrique α_ξ dans $C_{sae,N}$. Alors le test d'égalité à 0 pour α_ξ, le calcul du signe de α_ξ dans le cas réel et, lorsque $\alpha_\xi \neq 0$, le calcul de l'inverse de α_ξ (dans $\mathbf{A}_\xi$ Q) sont en temps uniformément polynomial par rapport à $\mathbf{d}$ et la taille des entrées, c.-à-d. encore par rapport à $|\alpha|_1$, $\mathbf{d}$ et $\mathbf{lg(P)}$.

preuve> *pour le signe ou le test d'égalité à 0* on majore les coefficients du polynôme minimum de α. Si $\alpha_\xi \neq 0$, on a donc une majoration des coefficients d'un polynôme de $Z[X]$ annulant $1/\alpha_\xi$, ce qui nous donne la précision avec laquelle il faut calculer α_ξ pour être assuré de son signe. En pratique, on a intérêt à mener en parallèle le calcul de plus en plus approché de α_ξ d'une part, et celui de la précision souhaitée d'autre part, le premier calcul pouvant aboutir à un résultat effectif bien avant la limite de précision imposé.

Une autre méthode pour déterminer un degré de précision suffisant (et cependant pas trop grand) pour connaître le signe de α_ξ est la suivante :

- on majore les modules des conjugués des ξ_i (ce qui peut être fait une fois pour toutes)
- on en déduit une majoration m des modules des conjugués de α_ξ
- comme α_ξ est un entier algébrique de degré $\leq \mathbf{d}$ on a :

$$\alpha_\xi \neq 0 \qquad |\alpha_\xi| > 1 / m^{\mathbf{d}-1}$$

pour l'inverse il semble difficile de se passer en général du calcul du polynôme minimum P_α de α (sauf si on sait par un argument quelconque que α est inversible dans $\mathbf{A_P}$ Q). A partir de P_α on obtient (en le divisant par une puissance de X) un polynôme Q $Z[X]$ tel que $Q(0) \neq 0$ et $Q(\alpha_\xi) = 0$, ce qui permet alors de calculer l'inverse de α_ξ sous forme β_ξ / n, où β $\mathbf{A_P}$.

<findepreuve

Calculs de déterminants dans $\mathbf{A}_\xi$

Pour le calcul du déterminant d'une matrice à coefficients dans $\mathbf{A}_\xi$ on peut donc hésiter entre, d'une part, la méthode de Leverrier (ou celle de Fadeev, ou celle de Samuelson) dans $\mathbf{A_P}$ et, d'autre part, la méthode de Bareiss dans $\mathbf{A}_\xi$.

Cependant, il faut noter que la méthode de Bareiss est a priori peu sûre : lorsque l'homomorphisme d'évaluation $\mathbf{A_P} \rightarrow \mathbf{A}_\xi$ n'est pas injectif (ce qui doit être considéré comme le cas général), un même élément de $\mathbf{A}_\xi$ peut être représenté par des éléments de $\mathbf{A_P}$ de taille arbitrairement grande. Quand la méthode de Bareiss exige une division exacte dans $\mathbf{A}_\xi$ avec un dénominateur non inversible dans $\mathbf{A_P}$ Q, il faudrait donc préciser quel algorithme de division exacte dans $\mathbf{A}_\xi$ on utilise, et démontrer qu'aucune explosion de la taille des objets manipulés n'en résulte.

En outre, le calcul du déterminant directement dans $\mathbf{A_P}$ présente l'avantage de pouvoir être spécialisé pour toute solution du système d'équations emboîtées considéré.

Calculs dans la clôture intégrale de $\mathbf{A}_\xi$

Il serait donc intéressant de donner une bonne majoration explicite des dénominateurs possibles pour un élément de $\mathbf{A}_\mathbf{P}$ Q dont l'image dans $\mathbf{A}_\xi$ Q est dans la clôture intégrale de $\mathbf{A}_\xi$. Notons $\mathbf{B}_\xi$ cette clôture intégrale.

Ceci donnerait une version améliorée de $C_{sae,N}$ où on représenterait tous les éléments de $\mathbf{B}_\xi$ plutôt que les seuls éléments de $\mathbf{A}_\xi$, tout en gardant le même genre de majorations pour les temps calculs :

En effet, si $n_\mathbf{P}$ peut servir de dénominateur commun à tous les éléments de $\mathbf{A}_\mathbf{P}$ Q dont l'image est dans $\mathbf{B}_\xi$, alors si $\alpha/n_\mathbf{P} = \beta/n$ irréductible, avec $\alpha_\xi/n_\mathbf{P}$ $\mathbf{B}_\xi$, on peut noter

$|\alpha_\xi/n_\mathbf{P}|_{\mathbf{B}_\xi} = |\beta_\xi/n|_{\mathbf{B}_\xi} = |\alpha|_1$ et on obtient :

$|\beta_\xi/n|_{\mathbf{B}_\xi} \le |\beta|_1 + |n_\mathbf{P}|_1$

$|\beta_\xi/n + \gamma_\xi/m|_{\mathbf{B}_\xi} \le \mathbf{sup}(|\beta_\xi/n|_{\mathbf{B}_\xi}, |\gamma_\xi/m|_{\mathbf{B}_\xi}) + 1$

$|\beta_\xi/n \,.\, \gamma_\xi/m|_{\mathbf{B}_\xi} \le |\beta_\xi/n|_{\mathbf{B}_\xi} + |\gamma_\xi/m|_{\mathbf{B}_\xi} + m_\mathbf{P}$ (cf § c pour $m_\mathbf{P}$)

Recherche des solutions simples d'un système d'équations algébriques emboîtées

Nous traitons tout d'abord le cas des racines simples, qui est naturel dans notre cadre de travail.

Proposition d.4 :

Soit $(\mathbf{P},[x_1,...,x_k])$ une présentation dans $C_{sae,N}$ de la solution simple $[\xi_1,\xi_2,...,\xi_k]$ du système d'équations algébriques emboîtées **P** .

Soit Q un polynôme unitaire de $\mathbf{A}_\xi[X]$.

On désire calculer les racines simples de Q sous la forme suivante:

si λ est une de ces racines, alors $[\xi_1, \xi_2, ..., \xi_k, \lambda]$ est représenté dans $C_{sae,N}$ par $(\mathbf{R},[y_1,...,y_k,y_{k+1}])$ où **R** est la liste **P** prolongée par Q

Ce calcul peut être réalisé en temps uniformément polynomial par rapport à **d** et la taille des entrées, c.-à-d. plus précisément par rapport à $|Q|_1$, deg(Q), **d** et **lg(P)** .

preuve> On utilise l'algorithme de Schönage (cf [**Sch**]) ou celui de Victor Pan (cf [**Pan**]) pour calculer des approximations arbitraires des racines de Q. Cet algorithme ne nécessite que la connaissance des valeurs approchées des coefficients de Q. Ces évaluations sont en temps convenablement contrôlé grâce au théorème d.2 a). Par ailleurs, dans la mesure où on ne s'intéresse qu'aux racines simples, la précision requise est convenablement contrôlée grâce à la proposition d.1. Plus précisément, soit T le polynôme minimum de λ_{k+1} $\mathbf{A}_\mathbf{R}$. Le polynôme T est calculable en temps convenable. On en déduit une minoration convenable, soit ε, pour l'écart entre 2 racines distinctes de T, et donc aussi entre 2 racines distinctes de $Q(\xi_1,\xi_2,\ldots,\xi_k,X)$. Si l'algorithme de Victor Pan situe 2 ou plusieurs racines de ce polynôme à une distance inférieure à ε on est assuré qu'il s'agit d'une racine multiple.

<findepreuve

Remarques :

1) En cas de racine multiple, cette racine multiple peut alors être explicitée sous la forme suivante: c'est l'unique racine du polynôme située dans un certain disque de centre $a + \sqrt{-1}\, b$ et de rayon r, où a, b, r sont des rationnels calculables en temps convenable.

2) Dans le cas réel, on peut utiliser plusieurs autres méthodes pour déterminer les racines simples de **P** :

a) la méthode des tableaux de signes approchés (cf § C.b dans [**Lom3**]) pour trouver des intervalles contenant chacun exactement une racine de Q en utilisant uniquement des évaluations approchées de Q et de ses dérivées, et assez petits pour que Newton fonctionne à partir d'un bord de l'intervalle.

b) une méthode à la Sturm améliorée genre Sturm-Habicht (cf [**GLRR**] ou [**Lom2**]) : la taille des polynômes sous-résultants est bien contrôlée puisque les coefficients de ces polynômes sont des déterminants. Noter l'intérêt qu'il y a à calculer ces coefficients dans $\mathbf{A_P}$, puisque le même calcul servira pour toutes les solutions réelles de **P** : ce n'est qu'au moment de l'évaluation des signes que le calcul se particularise.

c) ou la méthode élémentaire (vrais tableaux de signes). Là encore, on aura des calculs de résultants lors des tests de signes, mais on n'a plus l'avantage signalé en b) d'un "précalcul" commun à toutes les solutions réelles de **P** .

Les solutions b) et c) sont semble-t-il beaucoup plus coûteuses que la solution a), dans la mesure où ces 2 méthodes utilisent systématiquement des calculs de déterminants et des évaluations exactes de signes, alors que la méthode a) se contente de calculs d'évaluations approchées du polynôme et de ses dérivées.

Théorème d.5 :

Soit **P** un système normalisé d'équations algébriques emboîtées.

On désire calculer les solutions simples du système sous la forme présentée dans $C_{sae,\,N}$:

plus précisément toute solution $\xi_1, \xi_2, ..., \xi_k$ doit être explicitée sous forme $(\mathbf{P},[x_1,...,x_k])$.

Ce calcul est en temps uniformément polynomial par rapport à **d** et **lg(P)** .

preuve> On applique la proposition d.4 de manière itérative. Pour avoir une majoration du temps convenable, il suffit de montrer que la taille de tous les objets utilisés comme "entrées" lors des différentes applications de d.4 est convenablement majorée. Il suffit pour cela de s'assurer que la taille de toutes les approximations rationnelles $[y_1,\ldots,y_j]$ $(j \le k)$ obtenues au cours du calcul est correctement maîtrisée, ce qui est donné par d.1 .

<findepreuve

En combinant le résultat précédent et le théorème d.2 b) on obtient :

Corollaire d.6**:**

Soit **P** un système normalisé d'équations algébriques emboîtées. Les solutions simples du système peuvent être calculées comme éléments de C_{alg}^{k} en temps uniformément polynomial par rapport à **d** et **lg(P)** .

La recherche des solutions non simples

Nous discutons maintenant la question des racines multiples.
Une racine multiple de $P_{i+1}(\xi_1,\xi_2,\ldots,\xi_i,X)$ peut être vue comme une racine simple de l'une des dérivées de P_{i+1} par rapport à X. Nous établissons donc tout d'abord la proposition analogue à la proposition d.4 .

Proposition d.7 :

Soit $(\mathbf{P},[x_1,...,x_k])$ une présentation dans $C_{sae,N}$ de la solution simple $[\xi_1,\xi_2,...,\xi_k]$ du système d'équations algébriques emboîtées **P** .
Soit Q un polynôme unitaire de $\mathbf{A}_{\xi}[X]$.
On désire calculer les racines multiples de Q sous la forme suivante:

si λ est une de ces racines, alors on détermine son ordre de multiplicité i+1 et $[\xi_1, \xi_2, ..., \xi_k, \lambda]$ est représenté dans $C_{sae,N}$ par $(\mathbf{R},[y_1,...,y_k,y_{k+1}])$ où **R** est la liste **P** prolongée par $Q^{(i)}$

Ce calcul peut être réalisé en temps uniformément polynomial par rapport à **d** et la taille des entrées, c.-à-d. plus précisément par rapport à $|Q|_1$, deg(Q) , **d** et **lg(P)** .

preuve> on raisonne comme à la proposition d.4, la conclusion est qu'on connaît la multiplicité de chacune des racines de Q , ce qui nous ramène au cas d'un racine simple de $Q^{(i)}$.
<findepreuve

Ceci justifie que nous étendions la présentation $C_{sae,N}$, par exemple la manière suivante :

Définition d.8 :

Nous dirons qu'une liste $[\xi_1,\xi_2,...,\xi_k]$ est une solution d'ordre $\mathbf{s} = [s_1,s_2,\ldots,s_k]$ du sytème emboîté **P** si chaque ξ_i est racine d'ordre s_i de l'équation correspondante. Nous noterons $\mathbf{P^{(s)}}$ l'application de C^k vers C^k définie par les $P^{(s_i)}$ (dérivée par rapport à X_i).
Nous dirons que $(\mathbf{P}, [(x_1, s_1),...,(x_k,s_k)])$ *est une présentation de la solution* $[\xi_1,\xi_2,...,\xi_k]$ *de* **P** *dans* $C_{sae,N}$ *(étendue)* si la méthode de Newton appliquée à $\mathbf{P^{(s)}}$ et initialisée à $[x_1,...,x_k]$ converge vers $[\xi_1,\xi_2,...,\xi_k]$.
En outre si α est un élément de $\mathbf{A_P}$ nous dirons que $(\mathbf{P}, [(x_1, s_1),...,(x_k,s_k)], \alpha)$ *est une présentation de l'entier algébrique* α_ξ *dans* $C_{sae,N}$ *(étendue)* .

Avec cette extension de la présentation $C_{sae,N}$, il n'est pas difficile de vérifier que tous les résultats du § d jusqu'à la proposition d.7 restent valables. D'où finalement, avec les mêmes arguments que pour la preuve du théorème d.5 :

Théorème d.9 :

Soit **P** un système normalisé d'équations algébriques emboîtées.

On désire calculer toutes les solutions (simples ou multiples) du système dans la présentation $C_{sae,N}$ étendue (définition d.8) :

plus précisément toute solution $\xi_1, \xi_2, ..., \xi_k$ doit être explicitée sous forme $(\mathbf{P}, [(x_1, s_1),...,(x_k,s_k)])$.

Ce calcul est en temps uniformément polynomial par rapport à **d** et **lg(P)** .

Corollaire d.10 :

Soit **P** un système normalisé d'équations algébriques emboîtées. Les solutions du système peuvent être calculées comme éléments de C_{alg}^{k} en temps uniformément polynomial par rapport à **d** et **lg(P)** .

Bibliographie, références

[**Bar**] Bareiss E. H. : Sylvester's Identity and Multistep Integer-Preserving Gaussian Elimination . Math. Comp. 22 565-578 (1968) .

[**Ber**] Berkovitz S. J. : On computing the determinant in small parallel time using a small number of processors . Information Processing Letters 18 n°3 147-150 (1984) .

[**CL**] Collins G. E., Loos R. : Real Zeros of Polynomials p 83-94 dans Computer Algebra, Symbolic and Algebraic Computation édité par Buchberger, Collins, Loos . Springer Verlag 1982 .

[**CoR**] Coste M., Roy M.-F. : Thom's lemma, the coding of real algebraic numbers and the computation of the topology of semi-algebraic sets. J. Symbolic Computation 5 , 121-129 (1988) .

[**DD**] Dominique Duval, Claire Dicrescenzo : Le système D5 de calcul formel avec des nombres algébriques. in Thèse (de D. Duval) présentée à l'Université Scientifique, Technologique et Médicale de Grenoble. (1987) .

[**DM**] Demidovitch, Maron : Eléments de calcul numérique. Editions MIR (1973) .

[**GLRR**] Gonzalez L., Lombardi H., Recio T., Roy M.F.: Spécialisation de la suite de Sturm et sous-résultants. 1988 . A paraître au RAIRO Informatique théorique. Version détaillée dans ce même numéro de CALSYF.

[**Kal**] Erich Kaltofen : GCD divisors of polynomials given by straight-line programs. JACM, v 35 n°1, Jan 1988, 231-264 .

[**KLL**] Kannan R., Lenstra A. K., Lovasz L. : Polynomial Factorisation and Nonrandomness of Bits of Algebraic and Some Transcendental Numbers. Mathematics of Computation, vol 50, n°181, Jan 1988, 235-250 .

[**LLL**] Lenstra A. K., Lenstra H. W. Jr. , Lovasz L. : Factoring polynomials with rational coefficients . Math Ann. v 261, 1982, 513-534 .

[**Lom1**] Lombardi Henri. : Calculabilité dans les structures algébriques dénombrables. 1ère partie de la thèse.soutenue en juin 89 à Nice.

[**Lom2**] Lombardi Henri : Sous-résultants, suite de Sturm, spécialisation. 2ème partie de la thèse.soutenue en juin 89 à Nice.

[**Lom3**] Lombardi Henri : Nombres algébriques et approximations. 3ème partie de la thèse.soutenue en juin 89 à Nice.

[**MRR**] R. Mines, F. Richman, W. Ruitenburg : A Course in Constructive Algebra (Springer-Verlag; Universitext; 1988) .

[**Mü**] N. Th. Müller : Subpolynomial complexity classes of real functions and real numbers Proc 13th ICALP LNCS 226 (1986) 284-293 .

[**Ost**] A. M. Ostrowski **:** Solution of Equations in Euclidean and Banach Spaces: 3ème édition de: Solution of equations and systems of equations (Academic Press; 1973) .

[**Pan**] Pan Victor : Algebraic complexity of computing polynomial zeros. Comput. Math. Applic. vol 14, n°4, 1987, 285-304 .

[**Sam**] Samuelson P. A. : A method for determining explicitly the coefficients of the characteristic equation . Ann. Math. Stat. 13 (1942) 424-429.

[**Sch**] Schönage A. : The Fundamental Theorem of Algebra in Terms of Computational Complexity . Preliminary Report. Math. Inst. der Univ. Tübingen 1982 .

[**Val**] Brigitte Vallée. Un problème central en Géométrie algorithmique des Nombres: La réduction des réseaux (autour de l'algorithme LLL). Publication de l'Université de Caen, UFR des Sciendes. Juin 87 .