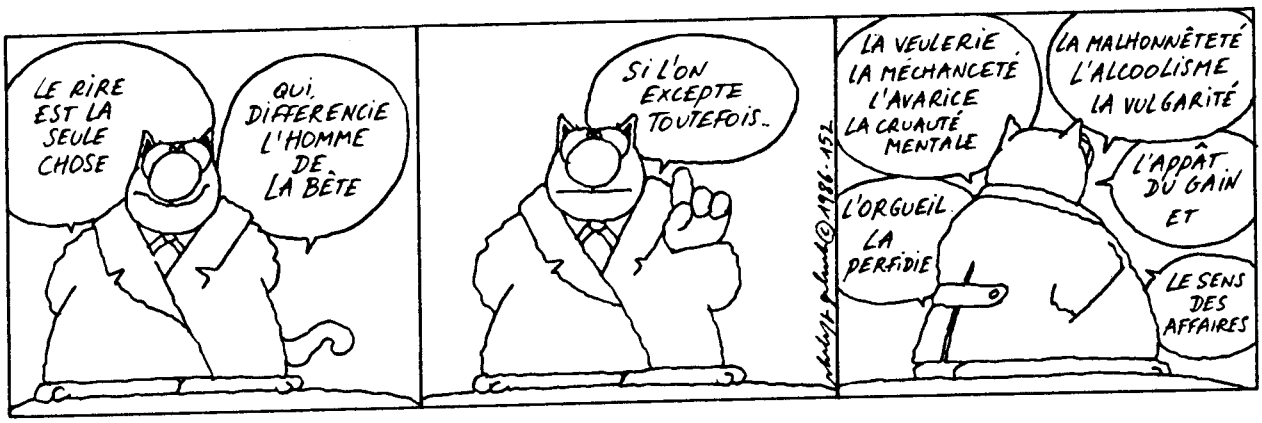
NOMBRES ALGEBRIQUES ET APPROXIMATIONS


LE RIRE EST LA SEULE CHOSE
QUI DIFFERENCIE L'HOMME DE LA BÊTE
SI L'ON EXCEPTE TOUTEFOIS..
LA VEULERIE LA MÉCHANCETÉ L'AVARICE LA CRUAUTÉ MENTALE
L'ORGUEIL LA PERFIDIE
LA MALHONNÊTETÉ L'ALCOOLISME LA VULGARITÉ
L'APPÂT DU GAIN ET
LE SENS DES AFFAIRES
Mark Parisi ©1986 152

NOMBRES ALGEBRIQUES ET APPROXIMATIONS

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.

Nous discutons l'efficacité des méthodes approximatives, et leur necessité lorsqu'on manipule de "vrais" nombres réels ou complexes, en particulier pour ce qui concerne la recherche des racines.

Ceci nous conduit à étudier la classe des fonctions définies sur un intervalle compact et approchables en temps polynomial par des polynômes à coefficients rationnels, au sens de la norme uniforme. Cette classe de fonctions est en fait la classe des fonctions Gevrey qui sont calculables en temps polynomial au sens de Ko-Friedman. Nous obtenons dans ce cadre des théorèmes agréables et de démonstration très simple, qui améliorent les résultats précédents de Ko-Fridman et de Müller sur les fonctions analytiques calculables en temps polynomial.

Mots clé

Nombres algébriques, codage, calcul formel, système D5, calculabilité en temps polynomial, fonctions calculables en temps polynomial, classe de Gevrey.

ALGEBRAIC NUMBERS AND APPROXIMATIONS

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.

We discuss the efficiency or approximative methods, and their necessity when we have to handle Cauchy real or complex numbers, in particular for the root searching problem.

This leads us to study the class of functions on a compact interval that are polynomial time approximable (in the uniform norm) by rational polynomials. This class of functions is in fact the class of Gevrey functions that are polynomial time computable (in the sense of Ko-Friedman). We obtain good and simple theorems concerning this class, improving previous results of Ko-Friedman and Müller on polynomial time computable analytic functions.

Introduction

Ce travail se situe dans la lignée directe de **[Lom1]** . Nous reprenons ici en partie la terminologie développée dans cet article, en l'explicitant autant que possible à chaque fois. Après l'algèbre linéaire en temps polynomial dans les corps les plus usuels (extensions de type fini de $\mathbb{Q}$ ou d'un corps fini), nous étudions maintenant dans quelle mesure les calculs dans la clôture algébrique de $\mathbb{Q}$ peuvent être présentés de manière à être en temps polynomial. Comme on peut s'y attendre, les résultats sont moins agréables et une explosion exponentielle de la taille des objets manipulés et du temps de calcul semble à peu près inévitable.

L'importance d'avoir une bonne description des nombres algébriques réels ou complexes dans les systèmes de calcul formel n'est plus à démontrer. Nous développons dans cette étude quelques considérations à ce sujet. Le point de vue qui nous guide est de montrer l'efficacité des méthodes approximatives dans la solution de ce problème et de problèmes connexes.

Dans le chapitre 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 $\mathbb{Z}[X]$ 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 $\mathbb{Z}[X]$ sont en temps polynomial, mais ces opérations enchaînées conduisent à une explosion de la taille des objets manipulés. A la fin du chapitre, nous donnons des conditions suffisantes pour remplacer $\mathbb{Q}$ par un autre sous-corps de $\mathbb{R}$ et obtenir néanmoins les mêmes majorations de temps de calculs.

Dans le chapitre B , 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 § a) 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 § b) , 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 chapitre 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 $\mathbb{R}_{alg}$.
Dans le § c) 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 *a priori* 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 § b). 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.

L'étude faite en B c) a montré l'efficacité assez bonne des méthodes approximatives pour calculer avec des nombres algébriques réels ou complexes.

Nous examinons dans le chapitre C deux théorèmes "en temps polynomial" qui relèvent par leur nature même de méthodes approximatives. Ces méthodes sont indispensables chaque fois qu'on a à résoudre un problème dont les variables sont dans $\mathbb{R}$, $\mathbb{C}$, ou un espace de fonctions.
Le théorème fondamental de l'algèbre est de ceux-là. Il peut être traité soit par une méthode approximative en tant que telle (algorithme de Schönage ou de Victor Pan), soit en utilisant une théorème effectif de perturbation des racines.
Quand on passe à la recherche des racines réelles d'un polynôme à coefficients réels, une méthode classique comme la méthode de Sturm devient impraticable dans un contexte constructif pour la simple raison qu'il n'y a pas de test d'égalité à 0 pour un nombre réel "en général". L'affirmation classique selon laquelle on peut situer les racines réelles d'un polynôme à coefficients réels devient *fausse* d'un point de vue constructif. Il y a néanmoins un substitut constructif à cette affirmation: la possibilité de dresser un tableau de signes "approché" pour un tel polynôme (cf § C b) pour plus de précision).

Ceci nous amène à faire une brève étude, au § C c) , de la classe des fonctions "approchables en temps polynomial par des polynômes, pour la norme uniforme, sur un intervalle compact". Cette classe est en fait celle des fonctions Gevrey $\mathcal{P}$-calculables. Tous les calculs élémentaires dans cette classe de fonction s'avèrent être en temps polynomial, pour des raisons tout à fait immédiates. Nous obtenons ainsi une amélioration des théorèmes de Ko-Friedman ([**KF1**] et [**KF2**]) et Müller ([**Mü2**]) concernant les fonctions analytiques et $\mathcal{P}$-calculables, et une simplification de leurs preuves.
Nous concluons par quelques perspectives de travail dans le cadre ainsi tracé : la géométrie algébrique réelle exacte dans la clôture réelle de $\mathbb{Q}$ pourrait, selon nous, être avantageusement remplacée par une géométrie algébrique réelle approximative dans tous les problèmes appliqués.

Quelques points de terminologie :

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

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

Nous parlons d'un $\mathcal{P}$-ensemble E ou d'un ensemble $\mathcal{P}$-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 $\mathcal{P}$-partie de A^* (c.-à-d. une partie $\mathcal{P}$-testable de A^*), et 2) le test d'égalité dans E (pour deux mots de A^* qui codent des éléments de E) est un $\mathcal{P}$-test.

Nous notons $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ les $\mathcal{P}$-ensembles correspondants présentés en binaire. Nous notons $\mathbb{N}_1$ pour le $\mathcal{P}$-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 $\mathbb{Z}$, ce sera donc la taille pour l'écriture en binaire.

Les polynômes de $\mathbb{Q}[X]$, $\mathbb{Q}[X,Y]$, $\mathbb{Q}[X_1,X_2,...,X_n]$ sont supposés donnés en présentation dense. Si $P \in \mathbb{Q}[X_1,X_2,...,X_n]$ 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 : $l_{creux} \leq l_{dense} \leq d_1...d_n.l_{creux}$. Les résultats de complexité qui font intervenir l_{dense} sont alors facilement traduisibles en résultats qui font intervenir l_{creux} .

A) LE CORPS DES NOMBRES REELS ALGEBRIQUES : PRESENTATION NAIVE

Introduction

Nous étudions dans ce chapitre 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 $\mathcal{P}$ les calculs élémentaires concernant les nombres algébriques. Mais les calculs "en cascade" ont un comportement exponentiel. Nous verrons dans le chapitre B qu'il est difficile d'espérer beaucoup mieux.
On notera qu'on se passe entièrement des algorithmes de décomposition en facteurs premiers dans $\mathbb{Q}[X]$. 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.

a) Présentation de $\mathbb{R}_{alg}$

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

Définition A.a1 :

- Soient $P \in \mathbb{Q}[X]$, a et $b \in \mathbb{Q}$ 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 $b \in \mathbb{Q}$ 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 $\mathbb{Q}$, 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 $\mathbb{Q}[X]$, avec pgcd(P,Q) = 1 , et [r', r] un intervalle rationnel.
On peut $\mathcal{P}$-calculer (à partir des polynômes P et Q et des rationnels r' , $r \in \mathbb{Q}$) un entier $n \in \mathbb{N}_1$ tel que :
si $r \le a \le b \le r'$ et $| b - a | \le 1/2^n$, alors P ou Q est évidemment-de-signe-constant sur [a , b]

preuve> Nous allons traiter le cas où $r' < 0 < r$, qui est le plus compliqué (si $r.r' \ge 0$ l'adaptation est immédiate). Nous notons p et q les degrés de P et Q .
Supposons tout d'abord $0 \le a < b$. Ecrivons $P = P_1 + P_2$ et $Q = Q_1 + Q_2$ en vue de tester "l'évidence du signe constant". Soit M un majorant de $|P_1'|, |P_2'|, |Q_1'|, |Q_2'|$ sur [0 , r] .
On a alors :

$$|P(a) - (P_1(a) + P_2(b))| = |P_2(a) - P_2(b)| \le M.(b - a) , \text{ et}$$
$$|P(a) - (P_1(b) + P_2(a))| = |P_1(a) - P_1(b)| \le M.(b - a) .$$

De sorte que :

$|P(a)| > M.(b - a) \Rightarrow$ P est évidemment-de-signe-constant sur [a , b] .

De même :

$|Q(a)| > M.(b - a) \Rightarrow$ Q est évidemment-de-signe-constant sur [a , b] .

Par ailleurs on sait $\mathcal{P}$-calculer U(X) et V(X) tels que :

$P(X).U(X) + Q(X).V(X) =$ **Res**(P,Q) (le résultant de P et Q) .

Les coefficients de U et V sont des cofacteurs de la matrice de Sylvester de P et Q , d'après l'inégalité de Hadamard sur les déterminants on a donc la majoration :

$$| \text{ coeff de U ou V } | \le || P ||_2^{q-1} \, || Q ||_2^{p-1} \, \mathbf{sup}(|| P ||_2, || Q ||_2) \quad (1)$$

Soit N un majorant de |U(x)| et |V(x)| sur [r', r] . On a alors les implications :
$|P(a)| < |\mathbf{Res}(P,Q)|/2N \Rightarrow |Q(a)|.|V(a)| > |\mathbf{Res}(P,Q)|/2 \Rightarrow |Q(a)| > |\mathbf{Res}(P,Q)|/2N.$
Donc : $|P(a)| \ge |\mathbf{Res}(P,Q)|/2N$ **ou** $|Q(a)| \ge |\mathbf{Res}(P,Q)|/2N$.
Donc : **si** $b - a < |\mathbf{Res}(P,Q)|/2NM$, **alors** P ou Q est évidemment-de-signe-constant sur [a , b] .

Dans le cas où $a < b \le 0$, on a une conclusion analogue avec une valeur M' à la place de M . On pose donc M" = **sup**(M,M') pour obtenir la même minoration dans les 2 cas.

Enfin, dans le cas où $a < 0 < b$, on a pareillement :

$$|P(0)| \ge |\mathbf{Res}(P,Q)|/2N \quad \mathbf{ou} \quad |Q(0)| \ge |\mathbf{Res}(P,Q)|/2N$$

$|P(0)| > M".(b - a) \Rightarrow$ P est évidemment-de-signe-constant sur [a , 0] et sur [0 , b] .

$|Q(0)| > M".(b - a) \Rightarrow$ Q est évidemment-de-signe-constant sur [a , 0] et sur [0 , b] .

Conclusion : dans tous les cas,
si $b - a < |\mathbf{Res}(P,Q)|/2NM"$, **alors** P ou Q est évidemment-de-signe-constant sur [a , b] .

---

[1] $|| P ||_2 := (\sum \mathbf{cf}_i(P)^2)^{1/2}$

La minoration a été $\mathcal{P}$-calculée dans $\mathbb{Q}$ à partir des polynômes P et Q et des rationnels r' , r . Il ne reste qu'à en déduire $n \in \mathbb{N}_1$ tel que :

$$1/2^n < |\mathbf{Res}(P,Q)| \,/2NM'' \,. \qquad \square$$

Appliquons ce lemme avec $Q = P'$: lorsque P ou P' est de signe constant sur [a , b] , P admet au plus une racine sur l'intervalle et on sait déterminer s'il en admet une ou non.

Notons que, pour $P = \sum_{0 \le i \le p} a_i.X^i$, l'intervalle $[\,-r\,,\,r\,]$ contient toutes les racines réelles de P dès que r est égal à

$$1 + \sup_{0 \le i < p} (|a_i|/|a_p|) \text{ ou encore à } \sup_{0 \le i < p} \left(\sqrt[p-i]{p|a_i|/|a_p|} \right).$$

Le lemme 1 justifie donc une méthode de calcul **PSPACE** pour situer les racines réelles d'un polynôme sans facteur carré de $\mathbb{Q}[X]$: découper l'intervalle [- r , r] en intervalles de longueur assez petite pour que le test du signe évidemment constant marche sur tous ces intervalles, soit pour P , soit pour P' .
De plus, dans le lemme 1 , la dépendance de n par rapport aux bornes de l'intervalle rationnel pourrait être supprimée (parce que P(x) est évidemment-de-signe-constant pour | x | assez grand), avec pour prix à payer une valeur de n trop grande si l'intervalle rationnel est petit .

Par ailleurs, ce lemme justifie la présentation suivante de l'ensemble $\mathbb{R}_{alg}$ des réels algébriques :

Présentation naïve de $\mathbb{R}_{alg}$

Définition A.a2 : Nous désignerons par $\mathbb{R}_{alg}$ l'ensemble des réels algébriques présenté de la manière décrite ci-dessous. (pour le moment on ne sait pas si c'est une $\mathcal{P}$-présentation).

Un nombre réel algébrique u est présenté par un triplet

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

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

On remarquera qu'un réel algébrique rationnel c/d peut être représenté par (d.X − c , a , b) , avec $a < c/d < b$, et que l'injection canonique $\mathbb{Q} \to \mathbb{R}_{alg}$ est une $\mathcal{P}$-opération. On verra plus précisément que $\mathbb{Q}$ s'identifie à une $\mathcal{P}$-partie de $\mathbb{R}_{alg}$. (corollaire de la prop A.a6)

On remarquera également qu'on n'exige pas que le polynôme P soit irréductible.

On sait que les réels algébriques forment un ensemble discret, mais on ne peut affirmer d'emblée que la séparation de 2 réels algébriques peut être testée en temps polynomial. On a néanmoins tout de suite :

Proposition A.a3 :

$\mathbb{R}_{alg}$ ainsi présenté est une $\mathcal{P}$-partie du $\mathcal{P}$-ensemble $\mathbb{Z}[X] \times \mathbb{Q} \times \mathbb{Q}$

preuve> La 4ème condition doit être prise pour une définition de u lorsque les 3 autres conditions sont vérifiées. Ces conditions sont vérifiées au moyen d'un calcul de résultant, et d'évaluations du polynôme P et de polynômes "extraits" de P' en vue de tester l'évidence du signe constant. Tous ces calculs sont en temps polynomial. ❑

Opérations élémentaires avec des rationnels

Proposition A.a4 : On peut construire :

- une $\mathcal{P}$-opération Pr : $\mathbb{R}_{alg} \times \mathbb{Q} \to \mathbb{R}_{alg}$ vérifiant Pr(u,r) = u.r
- une $\mathcal{P}$-opération Sm : $\mathbb{R}_{alg} \times \mathbb{Q} \to \mathbb{R}_{alg}$ vérifiant Sm(u,r) = u + r
- une $\mathcal{P}$-opération Comp : $\mathbb{R}_{alg} \times \mathbb{Q} \to (<, =, >)$ qui donne le résultat de la comparaison du réel algébrique u au rationnel r
- une $\mathcal{P}$-opération Min : $\mathbb{R}_{alg} \to \mathbb{Q}$ qui donne, pour un réel algébrique non nul, une minoration rationnelle de sa valeur absolue

preuve> Soit u le réel algébrique représenté par (P , a , b) , avec d = deg(P) , $P = \sum_i c_i.X^i$ et r le rationnel.
Pour la somme et le produit : on fait le changement de variable Y = X + r ou Y = X.r : cela n'affecte pas le changement de signe pour P ni l'évidence-du-signe constant pour P' .
Pour la comparaison : si r est extérieur à l'intervalle] a , b [, la comparaison est immédiate, sinon on calcule le signe de P(r) : si P(r) = 0 alors r = u , sinon on compare avec le signe de P(a) pour situer r , soit sur l'intervalle] a , u [soit sur l'intervalle] u , b [.
Pour la minoration de la valeur absolue (u étant supposé non nul) : on majore 1/u en considérant le polynôme aux inverses, ce qui donne : $|u| > |c_0| / (|c_0| + \sup_{i>0}(|c_i|))$. ❑

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

Définition A.a5 : Soit A un $\mathcal{P}$-ensemble et f une fonction de A vers $\mathbb{R}$. On dira que f est une $\mathcal{P}$-fonction, ou une $\mathcal{P}$-suite, ou encore que f est une fonction $\mathcal{P}$-calculable, si il existe une $\mathcal{P}$-opération F : $A \times \mathbb{N}_1 \to \mathbb{Q}$ 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 $\mathcal{P}$-nombre réel (ou réel de complexité $\mathcal{P}$). Des définitions analogues vaudraient d'ailleurs pour toute autre classe de complexité.

Proposition A.a6 :

Il existe une $\mathcal{P}$-opération F : $\mathbb{R}_{alg} \times \mathbb{N}_1 \to \mathbb{D}$ telle que $F(v,n) = r/2^n$ (avec $r \in \mathbb{Z}$) est une approximation de v avec la précision 2^{-n} .
C'est-à-dire: l'injection naturelle $\mathbb{R}_{alg} \to \mathbb{R}$ est une $\mathcal{P}$-fonction

On notera que cette opération F n'est pas une fonction puisque F(v,n) va dépendre de la présentation de v . Par ailleurs, il est clair qu'on aurait le même résultat en remplaçant 2^{-n}

---

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

(représenté par l'entrée n) par un élément $\varepsilon > 0$ arbitraire de $\mathbb{D}$ ou $\mathbb{Q}$. Cette proposition A.a6 est un cas particulier du lemme suivant :

Lemme 2 :

Soit DICHOT le $\mathcal{P}$-ensemble formé des triplets $(P , a , b) \in \mathbb{Q}[X] \times \mathbb{Q} \times \mathbb{Q}$ vérifiant $P(a).P(b) < 0$.

Il existe une $\mathcal{P}$-opération $G : DICHOT \times \mathbb{N}_1 \to \mathbb{D}$ telle que $G(P , a , b , n) = r/2^n$ (avec $r \in \mathbb{Z}$) est une approximation avec la précision 2^{-n} d'une racine u de P située sur l'intervalle [a , b] (la racine u ne dépendant pas de n).

preuve> L'opération G est obtenue par une dichotomie classique, avec pour points de départ a et b . Posons $k = \mathbf{sup}(0 , n + [\mathbf{log}_2(b - a)]^1)$. Après avoir divisé k fois l'intervalle [a , b] en 2 , on obtient un intervalle de longueur $< 2^{-n}$. Les bornes successives des intervalles sont de la forme $x_i = (m_i.a + (2^i - m_i).b)/2^i$; avec $2^i \geq m_i \geq 0$, $i \leq k$. Il y a k évaluations $P(x_i)$ nécessaires. Si l'intervalle obtenu est [a ' , b '] , on prend $r = \mathbf{Ent}(b'.2^n)$.
Le tout est un $\mathcal{P}$-calcul à partir de l'entrée (P , a , b , n) . ❑

Un corollaire de la proposition A.a6 est le suivant :

Corollaire : $\mathbb{Q}$ s'identifie à une $\mathcal{P}$-partie de $\mathbb{R}_{alg}$

preuve> Soit u = (P , a , b) et soit c la valeur absolue du coefficient dominant de P et d son degré. Il s'agit de tester en temps polynomial si u est rationnel : il suffit de calculer l'entier algébrique $u.c = (c^{d-1}.P(X/c) , a.c , b.c)$ avec une précision meilleure que 1/2 : si l'intervalle obtenu contient un entier k , on teste si $P(k/c) = 0$. ❑

Une autre conséquence immédiate est la :

Proposition A.a7 : (réduction de la taille d'un réel algébrique)

Il existe un polynôme Q et une $\mathcal{P}$-opération $Rd : \mathbb{R}_{alg} \to \mathbb{R}_{alg}$ telle que : si $u = (P , a , b)$, alors $Rd(u) = v = (P , a' , b')$ et :

- $u = v$ au sens de $\mathbb{R}_{alg}$
- $\mathbf{lg}(a') + \mathbf{lg}(b') < Q(\mathbf{lg}(P))^2$

preuve> Cela résulte clairement des lemmes 1 et 2 et de la $\mathcal{P}$-majoration des valeurs absolues des racines réelles de P . ❑

Recherche d'une racine par dichotomie sur un intervalle rationnel

Proposition A.a8 : Le lemme 2 peut être précisé de la manière suivante :

Il existe un polynôme Q et une $\mathcal{P}$-opération $Rac : \mathbb{Q}[X] \times \mathbb{Q} \times \mathbb{Q} \to \mathbb{R}_{alg}$ 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 $\mathbf{lg}(u) < Q(\mathbf{lg}(P))$.

---

[1] [x] est un entier majorant le réel x

[2] 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 $\mathbb{Z}$, ce sera la taille pour l'écriture en binaire.

preuve> On calcule $R = P/pgcd(P,P')$, qui admet les mêmes racines que P , puis une approximation suffisante d'une racine de P sur $[\,a\,,\,b\,]$ pour que R' soit de signe-évidemment-constant sur l'intervalle obtenu. ❑

Test d'égalité. Séparation dans le cas de non égalité

Théorème A.a9 : Il existe une $\mathcal{P}$-opération $V : \mathbb{R}_{alg} \times \mathbb{R}_{alg} \to \mathbb{D} \times \mathbb{D} \times (\,<\,,\,=\,,\,>\,)$ telle que :

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

Proposition A.a10 : Avec l'opération V définie ci-dessus pour tester l'égalité de 2 réels algébriques, la présentation $\mathbb{R}_{alg}$ est une $\mathcal{P}$-présentation de l'ensemble des réels algébriques.

preuve> La proposition A.a10 découle immédiatement de la précédente. Voyons celle-ci.
Soit $u = (\,P_1\,,\,a_1\,,\,b_1\,)$, $v = (\,P_2\,,\,a_2\,,\,b_2\,)$. On calcule $R = pgcd(P_1\,,\,P_2)$, $R_1 = P_1/R$, $R_2 = P_2/R$.
Un seul des 2 polynômes R et R_1 change de signe sur l'intervalle $[\,a_1\,,\,b_1\,]$; appelons le S pour un instant. En appliquant les lemmes 1 et 2 , on peut $\mathcal{P}$-calculer un intervalle $[\,a'_1\,,\,b'_1\,]$ contenu dans $[\,a_1\,,\,b_1\,]$ et tel que , d'une part S change de signe , d'autre part S' soit évidemment-de-signe-constant sur l'intervalle. On peut alors affirmer $u = (\,S\,,\,a'_1\,,\,b'_1\,)$.
On procède de même pour v .
Deux cas se présentent alors.
– *Le 1er cas* est celui où u et v sont tous deux racines de R . Si les intervalles $[\,a'_1\,,\,b'_1\,]$ et $[\,a'_2\,,\,b'_2\,]$ se coupent, on a $u = v$; sinon, il suffit de calculer u et v avec une précision meilleure que $|u - v|/4$ pour obtenir c et d : or ceci ne prendra pas trop de temps puisqu'on a :

$$\mathbf{log}(|\mathbf{Res}(R,R')|) = k'.\mathbf{log}(r) + \sum_{i \neq j} \mathbf{log}(|x_i - x_j|)\ ,$$

où les x_i sont les racines de R , r son coefficient dominant positif, $k' = 2.deg(R) - 1$. Soit M un majorant des $|\,x_i\,|$. On obtient donc :

$$2.\mathbf{log}(|u - v|) > \mathbf{log}(|\mathbf{Res}(R,R')|) - \sum_{i\neq j,\{x_i,x_j\}\neq\{u,v\}} \mathbf{log}(|x_i - x_j|) - k'.\mathbf{log}(r) >$$

$$\mathbf{log}(|\mathbf{Res}(R,R')|) - k.\mathbf{log}(2.M) - k'.\mathbf{log}(r)$$

où $k = deg(R).(deg(R) - 1) - 2$
On peut donc terminer en appliquant le lemme 2 .
– *Le 2ème cas* est celui où u et v sont racines de 2 polynômes qui n'ont pas de racine commune. Appelons les S et T . Il s'agit de nouveau de calculer u et v avec une précision meilleure que $|u - v|/4$ pour obtenir c et d : ceci ne prendra pas trop de temps puisqu'on a de même :

$\mathbf{log}(|\mathbf{Res}(S,T)|) = k_1.\mathbf{log}(r_2) + k_2.\mathbf{log}(r_1) + \mathbf{log}(|x_i - y_j|)$; x_i racines de S , y_j racines de T , $k_1 = deg(S)$, $k_2 = deg(T)$, r_1 coeff dominant positif de S , r_2 coeff dominant positif de T; et donc :

$\log(|u - v|) > \log(|\mathrm{Res}(S,T)|) - k_1.\log(r_2) - k_2.\log(r_1) - (k_1.k_2 - 1).\log(M + N)$; M majore les $|x_i|$, N majore les $|y_j|$. ❑

La preuve du théorème A.a9 fait intervenir des calculs de résultants et PGCD .
Mais en pratique, si on sait, par un argument quelconque, que $u \neq v$, il suffit, pour séparer u et v , de les calculer chacun avec une précision de plus en plus grande, jusqu'à ce qu'ils soient séparés. Ce calcul est une dichotomie ne faisant intervenir que des évaluations de polynômes, et le nombre d'étapes est raisonnable.

Dans le cas où on ne sait pas si $u = v$ ou non , on commence par calculer le résultant des 2 polynômes. Si le résultant est non nul on est ramené au cas précédent. S'il est nul, le pgcd R est donné au cours du calcul et il faut calculer R_1 , R_2 : ce surcroît de calculs est néanmoins compensé par le fait que désormais, u et v seront plus simples à manipuler puisque racines de polynômes de degrés moindres.

Nous pouvons cependant remarquer que la preuve du théorème A.a9 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.a11 :

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 ,
$n := p \log_2(|cd(Q)|) + q \log_2(|cd(P)|) + (p.q-1).\log_2(M+N) - \log_2(|Res(P,Q)|)$
Si $|u - v| < 1/2^n$, **alors** $u = v$

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

preuve> On utilise les majorations établies dans la preuve du théorème A.a9 . Pour le b) on remarque que le résultant de 2 polynômes à coefficients entiers est un entier, donc de logarithme ≥ 0 . Les majorations établies dans la preuve du théorème A.a9 couvrent alors également le cas où P et Q ne sont pas premiers entre eux (et en particulier le cas $P = Q$).❑

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 $d(P) \leq p$ et **sup**(| coeffs de P |) $\leq H$, $\mathbf{lg}(H) = h$, 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 $s \geq p^2/2 + ((3p+4)\,\mathbf{lg}(p+1))/2 + 2\,p\,h$.

Vue le théorème A.a11, 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 [**Mü1**]).

Proposition A.a12 :

Soient $u = (P, a, b) \in \mathbb{R}_{alg}$, $x_0 \in]a, b[$, $r_0 = \inf(|x_0 - a|, |x_0 - b|)$, 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 $\mathbb{D} \cap]a, b[$ vérifiant a) peut être calculé en temps polynomial (pour l'entrée u).

preuve> *Le a)* résulte des majorations classiques pour la convergence de la méthode de Newton. Cf par exemple, **[DM]** p 164 .

Le b) résulte essentiellement du fait que l'itération dans la méthode de Newton est quadratique. D'autre part, à chaque itération, le calcul n'est fait qu'approximativement: on arrête dès que le nombre significatif de décimales est obtenu. Détails dans **[Mü1]** .

Le c) : on peut calculer en temps polynomial :
– un majorant $m \geq 1$ de $|P'(x)|$ sur $[a, b]$ – un majorant M de $|P^{(2)}(x)|$ sur $[a, b]$ – un minorant > 0 s de $|P'(u)|$ – un minorant r de $|u - a|/2$ et $|u - b|/2$.

Si x_0 vérifie $|x_0 - u| < \inf(s/4mM, r/3m)$, alors on a $r_0 > 2r/3$, $P(x_0) < r_0/2$, $|P'(x_0)| > s/2$ et $|P(x_0)| < s/4M < |P'(x_0)|/2M$. ❑

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.a12 soit vérifiée. C'est grosso modo la solution que nous développons dans le B , 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".

b) $\mathbb{R}_{alg}$ comme $\mathcal{P}$-structure

Calcul d'un réel algébrique à partir de ses valeurs approchées

Nous établissons maintenant un théorème général utile pour montrer qu'une fonction à valeur dans $\mathbb{R}_{alg}$ est $\mathcal{P}$-calculable.

Théorème A.b1 : Soit A un $\mathcal{P}$-ensemble et f une fonction de A vers $\mathbb{R}_{alg}$.
Pour que f soit $\mathcal{P}$-calculable, il faut et suffit que les 2 conditions suivantes soient vérifiées :

- la fonction $f : A \to \mathbb{R}$ est une $\mathcal{P}$-fonction
- il existe une $\mathcal{P}$-opération $G : A \to \mathbb{Z}[X] - \{0\}$ telle que :
  si $G(z) = S$, alors $f(z)$ est racine de S.

preuve> Les conditions sont clairement necessaires.
Montrons qu'elles sont suffisantes : soit $z \in A$ et voyons comment calculer $f(z)$.
Tout d'abord on remplace $S = G(z)$ par $T = S/pgcd(S,S')$.
Par le lemme 1 , on détermine un entier n tel que, sur tout intervalle de longueur $\leq 2^{-n}$, T ou T' est évidemment-de-signe-constant sur l'intervalle.
Ensuite on calcule une approximation dyadique de $f(z)$ avec la précision 2^{-n-1} , ce qui permet de situer $f(z)$ sur un intervalle rationnel [a , b] de longueur $\leq 2^{-n}$, sur lequel T s'annule et T' est évidemment-de-signe-constant.
Le réel algébrique $f(z)$ est donc correctement représenté par (T , a , b).
Le tout est un $\mathcal{P}$-calcul à partir de l'entrée z ❑

Remarque : on peut éviter de calculer n (par utilisation du lemme 1) : on calculerait des intervalles successifs (pour i = 0,1,2,...) de longueur $< 2^{-i}$, sur lesquels se trouve $f(z)$, en testant à chaque fois l'évidence du signe constant pour le polynôme T' . On est sûr d'aboutir en un temps raisonnable.

Evaluation $\mathbb{Q}[X] \times \mathbb{R}_{alg} \to \mathbb{R}_{alg}$

Proposition A.b2 :
Il existe une $\mathcal{P}$-opération $Ev : \mathbb{Q}[X] \times \mathbb{R}_{alg} \to \mathbb{R}_{alg}$ telle que : $Ev(Q,u) = Q(u)$
(égalité au sens de $\mathbb{R}_{alg}$)

preuve> Soit $u = (P , a , b)$ et M_P la matrice standard admettant P comme polynôme minimum et caractéristique. Le réel algébrique Q(u) est racine du polynôme caractéristique S de la matrice $Q(M_P)$. Le calcul de S à partir de P et Q est un $\mathcal{P}$-calcul.
Ensuite, on majore $|Q'|$ sur l'intervalle [a , b] par un entier m , ce qui permet, via le théorème des accroissements finis et le lemme 2 , de calculer un rationnel approchant Q(u) avec une précision meilleure que 2^{-n} , comme $\mathcal{P}$-calcul à partir des entrées Q , a , b , n (n dans $\mathbb{N}_1$).
On conclut par le théorème A.b1 . ❑

Evaluation $\mathbb{Q}[X,Y] \times \mathbb{R}_{alg} \times \mathbb{R}_{alg} \to \mathbb{R}_{alg}$

Théorème A.b3 :

Il existe une $\mathcal{P}$-opération Ev2 : $\mathbb{Q}[X,Y] \times \mathbb{R}_{alg} \times \mathbb{R}_{alg} \to \mathbb{R}_{alg}$ telle que :

$Ev2(R,u,v) = R(u,v)$ (égalité au sens de $\mathbb{R}_{alg}$)

Théorème A.b4 : : $\mathbb{R}_{alg}$ est un $\mathcal{P}$-corps-ordonné

preuve> Démontrons d'abord le théorème A.b3:
Supposons $u = (P_1 , a_1 , b_1)$, $k_1 = \deg(P_1)$, $v = (P_2 , a_2 , b_2)$, $k_2 = \deg(P_2)$. On va calculer R(u,v) en utilisant le théorème A.b1 .
Tout d'abord, à partir d'une majoration de $|\partial R/\partial X|$ et $|\partial R/\partial Y|$ sur le rectangle $[a_1 , b_1] \times [a_2 , b_2]$ on obtient un module de Lipschitz pour R , ce qui permet de calculer un rationnel approchant R(u,v) avec une précision meilleure que 2^{-n} , comme $\mathcal{P}$-calcul à partir des entrées R , u , v , n (n dans $\mathbb{N}_1$) .
Il reste à $\mathcal{P}$-calculer un polynôme S de $\mathbb{Z}[X]$ annulant R(u,v) .
Pour cela nous considérons l'idéal $\mathcal{J}$ de $\mathbb{Q}[X,Y]$ engendré par $P_1(X)$ et $P_2(Y)$. Le corps $\mathbb{Q}(u,v)$ est un quotient de l'algèbre $\mathcal{A} = \mathbb{Q}[X,Y]/\mathcal{J}$ par l'homomorphisme qui envoie X et Y en u et v . Il nous suffit donc de déterminer un polynôme S de $\mathbb{Z}[X]$ tel que $S(R) = 0$ dans $\mathcal{A}$.
Or $\mathcal{A}$ possède comme base "canonique" les monômes $X^i.Y^j$ où $i < k_1$ et $j < k_2$.
Nous savons que nous pouvons $\mathcal{P}$-calculer dans $\mathbb{Q}[X,Y]$ les polynômes $1 , R , R^2 , R^3 ,\ldots ,$ R^h ($h = k_1.k_2 - 1$) à partir des entrées R , k_1 , k_2 , puisque $\mathbb{Q}[X,Y]$ est un anneau c-$\mathcal{P}$-c .
Comme par ailleurs les relations de dépendance linéaire sont $\mathcal{P}$-calculables dans $\mathbb{Q}$, nous aurons terminé la preuve du théorème après avoir démontré le lemme suivant :

Lemme : L'application de $\mathbb{Q}[X,Y] \times \mathbb{Z}[X] \times \mathbb{Z}[Y]$ vers $\mathbb{Q}[X,Y]$ qui, au triplet (T , P_1 , P_2) associe le polynôme " T(X,Y) réduit modulo $P_1(X)$ et $P_2(Y)$ " est une $\mathcal{P}$-fonction.

(cette application consiste à exprimer l'élément T sur la base "canonique" dans l'algèbre $\mathcal{A} = \mathbb{Q}[X,Y]/\mathcal{J}$ où $\mathcal{J}$ est l'idéal $(P_1(X) , P_2(Y))$) .

preuve du lemme : Comme l'addition est c-$\mathcal{P}$-c, il suffit de le montrer lorsque le polynôme Q est un monôme $X^n.Y^m$. On réduit séparément X^n modulo $P_1(X)$ et Y^m modulo $P_2(Y)$ puis on fait le produit, et on sait que ce sont des $\mathcal{P}$-opérations.
prouvons maintenant le théorème A.b4:
On sait déjà que la relation d'ordre est $\mathcal{P}$-décidable. Pour l'addition et la multiplication, on applique le Théorème précédent avec X + Y et X.Y . Il reste à voir le calcul de l'inverse d'un élément non nul. Ce qui se démontre sans problème avec le théorème A.b1 . ❑

Remarque : Ces théorèmes ne signifient pas vraiment qu'on peut calculer dans $\mathbb{R}_{alg}$, en effet l'addition et le produit ne sont pas complètement $\mathcal{P}$-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. Nous discutons ce problème plus en détail dans B a) . Notons enfin qu'il existe des extensions infinies de $\mathbb{Q}$ contenues dans $\mathbb{R}_{alg}$ et où cependant les additions et produits en chaîne n'explosent pas (restent polynomialement majorés en taille, et donc en temps de calcul), par exemple :

$$K := \bigcup_n \mathbb{Q}[\sqrt[r^n]{2}] \quad \text{où r est un entier fixé}$$

On peut en effet se convaincre qu'il s'agit ici de la même présentation (à $\mathcal{P}$-équivalence près) que celle donné dans l'exemple de **[Lom1]** p 32 .

Evaluation $\mathbb{Q}[X_1,X_2,...,X_n] \times \mathbb{R}_{alg}^{\ n} \to \mathbb{R}_{alg}$

Proposition A.b5 :

L'application $E : \mathbb{Q}[X_1,X_2,...,X_n] \times \mathbb{R}_{alg}^{\ n} \to \mathbb{R}$ définie par :

$E(R , (\xi_1,\xi_2,...,\xi_n)) = R(\xi_1,\xi_2,...,\xi_n)$ est une $\mathcal{P}$-fonction

preuve> Supposons $\xi_i = (P_i , a_i , b_i)$. Comme l'évaluation $\mathbb{R}_{alg} \to \mathbb{R}$ est une $\mathcal{P}$-fonction, il suffit de savoir $\mathcal{P}$-calculer un module de Lipschitz pour R sur le pavé $B := \prod_i [a_i , b_i]$, donc de $\mathcal{P}$-majorer les $|\partial R/\partial X_i|$ à partir de l'entrée (R,B) ❑

Remarque : on peut définir comme en dimension 1 un majorant-évident et un minorant-évident d'un polynôme sur un pavé. Mais si le pavé contient l'origine en son intérieur, il faudra le décomposer en 2^n sous-pavés. Il peut donc sembler préférable de choisir un majorant plus grossier (obtenu à partir des valeurs absolues des coefficients et des **sup**($|a_i|$, $|b_i|$)) .

Proposition A.b6 :

Il existe une $\mathcal{P}$-opération $Ev_n : \mathbb{Q}[X_1,X_2,...,X_n] \times \mathbb{R}_{alg}^{\ n} \to \mathbb{R}_{alg}$ telle que :

$Ev_n(R , (\xi_1,\xi_2,...,\xi_n)) = R(\xi_1,\xi_2,...,\xi_n)$ (égalité au sens de $\mathbb{R}_{alg}$)

preuve> on raisonne exactement comme en 2 variables (Th A.b3) ❑

NB: a priori, le degré d'un élément de $\mathbb{Q}[\xi_1,\xi_2,...,\xi_n]$ est inférieur ou égal à $d_1.d_2. ... .d_n$.

Remarque : 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 $R(\xi_1,\xi_2,...,\xi_n)$ peut être obtenu de manière plus rapide que par le calcul de $R(\xi_1,\xi_2,...,\xi_n)$ dans $\mathbb{R}_{alg}$. 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 $| R(\zeta_1,\zeta_2,...,\zeta_n) |$ où les ζ_i sont des racines arbitraires des P_i . Le produit des $R(\zeta_1,\zeta_2,...,\zeta_n)$ non nuls est un entier algébrique, donc un entier, ce qui donne l'implication :

$$R(\xi_1,\xi_2,...,\xi_n) \neq 0 \Rightarrow | R(\xi_1,\xi_2,...,\xi_n) | \geq 1/m_R^{(d_1.d_2...d_n-1)} .$$

Par suite, il suffit de calculer une approximation rationnelle convenable de $R(\xi_1,\xi_2,...,\xi_n)$ pour connaître son signe. Or d'après la proposition A.a12 , le calcul d'approximations rationnelles est très rapide.

c) Situation des racines réelles d'un polynome de $\mathbb{Q}[X]$

Nous examinons dans ce paragraphe deux démonstrations du théorème :

Théorème A.c1:

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

Recherche de racine par dichotomie sur un intervalle réel algébrique

Proposition A.c2 : Soit S la $\mathcal{P}$-partie de $\mathbb{Q}[X] \times \mathbb{R}_{alg} \times \mathbb{R}_{alg}$ formée par les (P, x, y) vérifiant : $x < y$, $P(x).P(y) < 0$.

Il existe une $\mathcal{P}$-opération $S \rightarrow \mathbb{R}_{alg}$ qui calcule à partir de P, x, y une racine de P sur l'intervalle $[x, y]$.

preuve> On peut $\mathcal{P}$-calculer des dyadiques a et b tels que $x < a < b < y$, $P(a).P(x') > 0$ pour $x' \in [x, a]$, $P(b).P(y') > 0$ pour $y' \in [b, y]$: en effet :
si M est un majorant de $|P'|$ sur un intervalle contenant $[x, y]$ et si $|P(x)| > m > 0$ il suffira que $|x' - x| < m/M$ pour que $P(x')$ ait même signe strict que $P(x)$, or m est $\mathcal{P}$-calculable d'après les propositions A.b2 et A.a4, et a s'en déduit par les propositions A.a4 et A.a6. On est donc ramené au cas où x et y sont rationnels (proposition A.a8). ❑

Méthode élémentaire (tableau de variation)

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 $x_1, \ldots, x_k$, (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 $P(x_i)$ (cf proposition A.b2), 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 (cf proposition A.c2).

Il est clair que 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 $\mathcal{P}$-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. La majoration pour $P \rightarrow [P', P^{(2)}, \ldots, P^{(d)}]$ ($d = \deg(P)$) est immédiate. La majoration pour la taille des racines s'en déduit par la proposition A.a7.

Si on utilise le théorème A.a11 et la proposition A.a12, on peut conduire tout l'agorithme en utilisant uniquement des calculs de valeurs approchées des réels algébriques considérés, qui sont de la forme $P^{(j)}(\zeta)$ où ζ est une racine réelle de $P^{(j+1)}$.

Notons que l'algorithme calcule en fait tous les zéros des polynômes $P, P', P^{(2)}, \ldots, P^{(d)}$. On peut en déduire sans se fatiguer beaucoup plus un tableau complet de signes et de variations pour la liste $[P, P', P^{(2)}, \ldots, P^{(d)}]$.