=

UN ALGORITHME ET DES BORNES POUR LE NULLSTELLENSATZ REEL EFFECTIF EN UNE VARIABLE

WAROU Harouna

Introduction

Dans cet article, nous reprenons l'algorithme de construction d'un positivstellensatz effectif donné dans [LOM2], pour le cas particulier d'une famille de polynômes en une variable à coefficients dans un corps réel clos.
Nous donnons une étude détaillée des formules de Taylor mixtes et généralisées, qui sont des outils essentiels pour le nullstellensatz réel effectif. En particulier, nous donnons une preuve directe et plus générale pour les formules Taylor mixtes, nous démontrons que les coefficients intervenant dans les formules de Taylor mixtes et formules de Taylor généralisées sont des entiers, et nous établissons des majorations les concernant.
Nous montrons par ailleurs qu'un bon controle de la procédure de "recollement" conduit à une majoration sur les degrés dans l'identité algébrique finale par $8md^2$, où d majore le degrés des polynômes de depart et m majore le nombre des zéros réels de ces polynômes et de leurs dérivées successives.

1. Quelques notions de base

1.1 Système incompatible et implications fortes

Nous précisons d'abord les notations et terminologies utilisées. Dans toute la suite nous appelerons *condition de signe strict* l'un des symboles suivants $<, >$. Une *condition de signe généralisée* est l'un des éléménts de $\{<, \leq, =, \geq, >, \neq\}$. Quand on remplace la condition de signe strict $<$ (resp $>$) par la condition de signe $\leq$ (resp. $\geq$) on dit que la condition de signe a été *relachée*. Nous dirons aussi que le symbole $>$ (resp. $\geq, =, \leq, <$) est la condition de signe *opposée* à la condition de signe $\leq$ (resp. à $<, \neq, >, \geq$) ou vice-versa.

On considère un corps ordonné $\mathbf{K}$ de clôture réelle $\mathbf{R}$ et $\mathbf{K}[\mathbf{X}]$ l'anneau des polynômes $\mathbf{K}[X_1, \ldots, X_n]$.

Soit F une partie finie non vide de $\mathbf{K}[\mathbf{X}]$.

On note par F^2 l'ensemble des carrés des éléments non nuls de F.

Le *monoïde multiplicatif engendré* par F est l'ensemble des produits d'éléments de $F \cup \{1\}$, on le note $\mathcal{M}(F)$.

L'ensemble des sommes d'éléments du type $k.P.Q^2$ où k est positif dans $\mathbf{K}$,P dans $\mathcal{M}(F)$, Q dans $\mathbf{K}[\mathbf{X}]$, est un cône, appelé *cône positif engendré* par F. Ce cône est noté $\mathcal{C}_p(F)$.

Enfin on note $\mathcal{I}(F)$ l'idéal engendré par F.

Définition 1 : *Soient quatre parties finies de* $\mathbf{K}[\mathbf{X}]$: $F_>$, $F_\geq$, $F_=$, $F_\neq$,*contenant des polynômes auxquels on souhaite imposer des conditions* $>, \geq, =, \neq$. *On dira que le système* $F=[F_>, F_\geq, F_=, F_\neq]$ *est fortement incompatible dans* $\mathbf{K}$ *si on a une identité algébrique dans* $\mathbf{K}[\mathbf{X}]$ *du type suivant* :

$$S + P + Z = 0 \tag{1}$$

avec $S \in \mathcal{M}(F_>^2 \cup F_\neq^2)$, $P \in \mathcal{C}_p(F_> \cup F_\geq)$, $Z \in \mathcal{I}(F_=)$

L'incompatibilité forte d'un système F est noté : $\downarrow F \downarrow$
Si une identité du type (1) a lieu pour un système de conditions de signes généralisées F portant sur des polynômes à coefficients dans un corps ordonné $\mathbf{K}$ de clôture réelle $\mathbf{R}$, alors le système F n'a jamais de solutions, dans *n'importe quelle* extension ordonnée de $\mathbf{K}$.

L'impossibilité d'un système de conditions de signes généralisées peut être formulée sous-forme d'implications diverses. Par exemple le système $[P = 0, Q = 0]$ est fortement incompatible dans $\mathbf{R}$ (c'est-à-dire que l'ensemble algébrique $\{x \in \mathbf{R}^n / P(x) = 0 \text{ et } Q(x) = 0\} = \emptyset$) équivaut à l'implication "$P = 0 \Longrightarrow Q \neq 0$", cette dernière implication signifiant que :

$$\forall x \in \mathbf{R}^n, P(x) = 0 \Longrightarrow Q(x) \neq 0$$

Soient un système de conditions de signes généralisées portant sur les éléments de $\mathbf{K}[\mathbf{X}]$ et $'$ le système de conditions de signes généralisées suivant $[Q_1 \tau_1 0, \ldots, Q_m \tau_0]$, nous utiliserons la notation $^*(\Longrightarrow Q\tau 0)^*$ pour signifier $\downarrow [, Q\tau' 0] \downarrow$ où τ' est la condition de signe opposée à τ et nous écrirons $^*(\Longrightarrow ')^*$ pour exprimer $^*(\Longrightarrow Q_1 \tau_1 0)^*$ et ... et $^*(\Longrightarrow Q_m \tau_m 0)^*$. Dans toute la suite nous parlerons sans distinction d'incompatibilité forte, d'implication forte ou d'évidence forte, en nous ramenant toujours explicitement à une incompatibilité forte.

1.2 Le théorème des zeros réels et ses variantes

Un théorème général (ci-dessous) est à la base de toutes les variantes du théorème des zéros dans le cas réel.

Théorème 2 : [BCR] *Soit* $\mathbf{K}$ *un corps ordonné et* $\mathbf{R}$ *une extension réelle close de* $\mathbf{K}$. *Soit* $F = [F_>, F_\geq, F_=, F_\neq]$ *un système de conditions de signes généralisées portant sur des polynômes de* $\mathbf{K}[X]$ *et* S *l'ensemble semi-algébrique de* $\mathbf{R}^n$ *défini par :*

$S = \{\mathbf{x} \in \mathbf{R}^n / \forall\ f \in F_>, f(\mathbf{x}) > 0$ *et* $\forall\ g \in F_\geq, g(\mathbf{x}) \geq 0$, *et* $\forall\ h \in F_=, h(\mathbf{x}) = 0$ *et* $\forall\ q \in F_\neq, q(\mathbf{x}) \neq 0\}$

Les trois conditions suivantes sont équivalentes :

F *est fortement incompatible dans* $\mathbf{K}$

S *est vide dans* $\mathbf{R}$

S *est vide dans toute extension ordonnée de* $\mathbf{K}$

Nous introduisons maintemant des résultats qui nous seront utiles par la suite, concernant les manipulations des incompatibilitées fortes et des implications fortes.

Définition 3 : *on appelle degré d'une compatibilité forte, le degré maximum des polynômes qui "composent" l'identité algébrique correspondante.*
Par exemple, si nous avons une incompatibilité forte : $\downarrow [A > 0, B > 0, C \geq 0, D \geq 0, E = 0, G = 0] \downarrow$ explicitée sous forme d'identité algébrique :

$$A^2.B^6 + C.\sum_{i=1}^{h} p_i.P_i^2 + A.B.D.\sum_{j=1}^{k} q_i.Q_j^2 + E.U + G.V = 0$$

le degré de l'incompatibilité est :

$$\sup\{d(A^2.B^6), d(C.P_i^2)(i = 1, \ldots, h), d(A.B.D.Q_j^2)(j = 1, \ldots, k), d(E.U), d(G.V)\}$$

Dans la proposition suivante, nous donnons quelques précisions concernant les degrés des incompatibilités fortes construites dans la procédure de recollement donnée dans [LOM1].

Proposition 4 : *Soit* H *un système de conditions de signes généralisées portant sur des polynômes de* $\mathbf{K}[\mathbf{X}]$ *et* $Q \in \mathbf{K}[\mathbf{X}]$. *Alors :*

(i) *A partir de* $\downarrow [[, Q \leq 0] \downarrow$ et $\downarrow [, Q \geq 0]$ *on peut construire* $\downarrow\ \downarrow$

(ii) *A partir de* $[, Q < 0] \downarrow$ *avec un degré* δ *et de* $\downarrow [, Q > 0] \downarrow$ *avec un degré* δ', *on peut construire* $\downarrow [, Q \neq 0] \downarrow$ *avec un degré majoré par* $\delta + \delta'$

(iii) *A partir de* $\downarrow [, Q \neq 0] \downarrow$ et $\downarrow [, Q = 0] \downarrow$ *on peut construire* $\downarrow \quad \downarrow$. *De plus si* $\downarrow [, Q \neq 0] \downarrow$ *a un degré* δ *avec* $Q^r S$ *dans la partie monoïde, et* $\downarrow [, Q = 0] \downarrow$ *a un degré* δ' *et si deg* $Q = q$. *On a l'incompatibilité forte* $\downarrow \quad \downarrow$ *avec un degré majoré par* $\delta + 2r\delta' - 2rq$

Preuve : On peut supposer que H est constituée de quatres parties finies $F_>, F_\geq, F_=, F_\neq$ de $\mathbf{K}[\mathbf{X}]$.

(i) Les deux incompatibilités fortes $\downarrow [, Q \leq 0] \downarrow$ et $\downarrow [, Q \geq 0] \downarrow$ correspondent aux identités algébriques suivantes :

$$S_1 - Q.P_1 + R_1 + Z_1 = 0 \tag{1}$$

$$S_2 + Q.P_2 + R_2 + Z_2 = 0 \tag{2}$$

avec $S_1, S_2 \in \mathcal{M}(F_>^2 \cup F_\neq^2)$; $P_1, P_2 \in \mathcal{C}_p(F_> \cup F_\geq)$; $Z_1, Z_2 \in I(F_=)$

Après avoir isolé au second membre $Q.P_1$ et $Q.P_2$ multiplions membre à membre (1) et (2), il vient :

$$S_1.S_2 + [S_1.R_2 + S_2.R_1 + R_1.R_2 + Q^2.P_1.P_2] + (S_1 + R_1).Z_2 - Q.P_2.Z_1 = 0$$

ce qui est exactement l'incompatibilité forte cherchée.

(ii) Même construction qu'en (i)

(iii) L'hypothèse $\downarrow [, Q \neq 0] \downarrow$ correspond à l'identité : $Q^{2r}S_1 + P_1 + Z_1 = 0$ (1) avec $S_1 \in M(F_>^2 \cup F_{\neq 0}^2), P_1 \in \mathcal{C}_p(F_> \cup F_\geq), Z_1 \in \mathcal{I}(F_=)$. Pour la deuxième hypothèse on a : $S_2 + P_2 + Z_2Q + Z_3 = 0$ (2) avec $S_2 \in M(F_>^2 \cup F_{\neq 0}^2), P_2 \in \mathcal{C}_p(F_> \cup F_\geq), Z_1, Z_2 \in \mathcal{I}(F_=)$. Dans (1) on a deg $S_1 \leq \delta - 2rq$ et dans (2) deg $Z_2 \leq \delta' - q$. On réecrit (2) sous forme de : $S_2 + P_2 + Z_3 = -Z_2Q$ et on élève les deux membres de cette égalité à la puissance $2r$, ce qui donne l'égalité : $S_3 + P_3 + Z_4 = Q^{2r}Z_5$ (3) où deg $Z_5 \leq 2r(\delta' - q)$. Ensuite on multiplie (1) par Z_5 et (3) par S_1, on obtient alors l'incompatibilité cherchée : $\underbrace{S_1S_3 + PS_1 + Z_4S_1}_{\deg \leq 2r\delta' + (\delta - 2rq)} - \underbrace{P_1Z_5 - Z_1Z_5}_{\deg \leq \delta + 2r(\delta' - q)} = 0$

o

2. Formules de Taylor mixtes et généralisées

Les formules de Taylor (mixtes et généralisées) sont des outils algébriques essentiels pour la construction des identités pour le nullstellensätz réel effectif. Nous commencerons par une extension du théorème des formules de Taylor mixtes aux fonctions différentiables ce qui nous permettra de démontrer par une méthode directe le théorème algébrique donné dans [LOM1]. Nous étudions ensuite les identités algébriques appelées formules de Taylor généralisées ([LOM2]). Ces formules généralisent les formules de Taylor mixtes au moins dans le cas polynomial. Leur utilisation permet de rendre fortement évident le signe d'un polynôme sur un intervalle ouvert du tableau complet des signes.

2.1 Formules de Taylor mixtes

Notations :

On appelle signe un élément de $\{-, 0, +\}$ et signe strict un élément de $\{-, +\}$.

Soit $e = [\epsilon_1, \epsilon_2, \ldots, \epsilon_n]$ $(n > 1)$ une liste de signes stricts avec $\epsilon_1 = 1$. Nous notons par

$e_k = [\epsilon_1, \ldots, \epsilon_k]$ la liste des k premiers termes de e

ξ_{n-1} la quantité $\xi_{n-1} = \dfrac{1}{2}(1 + \epsilon_{n-1}\epsilon_n)$

P_{e_n} le polynôme à coefficients rationnels défini par la recurrence :

$$P_{e_1}(t) := 1$$

$$P_{e_n}(t) := (-1)^{\xi_{n-1}}(n-1)\int_{\xi_{n-1}}^{t} P_{e_{n-1}}(x)dx$$

Les polynomes P_{e_n} sont formés de manière analogue aux polynômes dans le reste intégral pour les fomules de Taylor classiques. Il n'est donc pas surprenant de trouver des points communs entre les deux théories.

$c_{k,e}$ le rationnel défini par : $c_{k,e} = k\int_0^1 \mathrm{P}_{e_k}(t)dt$, $c_{k,e}$ ne dépend en fait que de e_k

Soit u et v deux réels avec $u < v$ nous noterons par Δ la différence $\Delta = u - x$ pour un $u \leq x \leq v$ et $y_k = \begin{cases} x & si\ \ \epsilon_k\epsilon_{k+1} < 0 \\ u & si\ \ \epsilon_k\epsilon_{k+1} > 0 \end{cases}$ Par ailleurs on note par D_k l'opérateur differentiel $\dfrac{d^k}{k!dx^k}$

Théorème 5 : *Pour chaque fonction* $f : [u,v] \longrightarrow \mathbb{R}$ *de classe* C^{n+1}, $n \geq 0$, *il y a* 2^n *formules de Taylor mixtes et toutes les combinaisons de signes possibles apparaissent. Plus précisement soit* $e = [\epsilon_1, \epsilon_2, \ldots, \epsilon_{n+1}]$ *un* $(n+1)$ *- uplet de signes strits avec* $\epsilon_1 = 1$. *Alors*

$$f(x) = f(u) + \sum_{k=1}^{n} \epsilon_k c_{k,e} \Delta^k D_k(f)(y_k) + \epsilon_{n+1}\frac{\Delta^{n+1}}{n!}\int_0^1 \mathrm{P}_{e_{n+1}}(t) f^{(n+1)}(u + t\Delta)dt \qquad (1)$$

Preuve : Nous montrons (1) par recurrence sur n. La formule (1) est immédiate pour $n = 0$, en effet pour f de classe C^1 on a :

$$f(x) - f(u) = \Delta\int_0^1 f'(u + t\Delta)dt$$

Supposons la formule établie pour f de classe C^n, $n \geq 1$ sur $[u,v]$. Pour une fonction de classe $C^{(n+1)}$, nous distinguons les deux cas suivants.

<u>1ercas</u> : $\epsilon_n\epsilon_{n+1} = -1$

dans ce cas $y_n = x$. En intégrant par parties

$$\mathrm{R} = \epsilon_n\frac{\Delta^n}{(n-1)!}\int_0^1 \mathrm{P}_{e_n}(t) f^{(n)}(u + t\Delta)dt$$

égal par hypothèse de recurrence à

$$f(x) - f(u) - \sum_{k=1}^{n-1} \epsilon_k c_{k,e}\frac{\Delta^k}{k!} f^{(k)}(y_k)$$

on obtient :

$$\mathrm{R} = \epsilon_n\frac{\Delta^n}{(n-1)!}[\mathrm{Q}(t) f^{(n)}(u + t\Delta)]_0^1 - \epsilon_n\frac{\Delta^{n+1}}{(n-1)!}\int_0^1 \mathrm{Q}(t) f^{(n+1)}(\mathrm{u} + t\Delta)dt$$

où $\mathrm{Q}(t) = \displaystyle\int_0^t \mathrm{P}_{e_n}(x)dx = \frac{1}{n}\mathrm{P}_{e_{n+1}}(t)$. Par suite on a :

$$\mathrm{R} = \epsilon_n c_{n,e}\frac{\Delta^n}{n!} f^{(n)}(y_n) + \epsilon_{n+1}\frac{\Delta^{n+1}}{n!}\int_0^1 \mathrm{P}_{e_{n+1}}(t) f^{(n+1)}(u + t\Delta)dt$$

avec $c_{n,e_{n+1}} = n\displaystyle\int_0^1 \mathrm{P}_{e_n}(t)dt = \mathrm{P}_{e_{n+1}}(1)$.

<u>2^{ieme}cas</u> : $\epsilon_n\epsilon_{n+1} = 1$

maintenant $y_n = u$ comme dans le cas précédent en intègre par parties R et on a

$$\mathrm{R} = \epsilon_n\frac{\Delta^n}{(n-1)!}[\mathrm{Q}(t) f^{(n)}(u + t\Delta)]_0^1 - \epsilon_n\frac{\Delta^{n+1}}{(n-1)!}\int_0^1 \mathrm{Q}(t) f^{(n+1)}(u + t\Delta)dt$$

mais cette fois-çi on choisit $Q(t) = \int_1^t P_{e_n}(x)dx = -\frac{1}{n}P_{e_{n+1}}(t)$

ce qui donne précisement

$$R = \epsilon_n c_{n,e}\frac{\Delta^n}{n!}f^{(n)}(y_n) + \epsilon_{n+1}\frac{\Delta^{n+1}}{n!}\int_0^1 P_{e_{n+1}}(t)f^{(n+1)}(u+t\Delta)dt$$

avec $c_{n,e} = n\int_0^1 P_{e_n}(t)dt = P_{e_{n+1}}(0)$. o

Proposition 6 : *Soit $n \geq 1$. Alors P_{e_n} est un polynôme de degré $n-1$, à coefficients dans $\mathbb{Z}$ et qui est strictement positif sur l'intervalle $]0,1[$.*

Preuve : Nous montrons que P_{e_n} est un polynôme à coefficients entiers, le reste des propriétés concernant $P_{[\epsilon_1,\epsilon_2,\ldots,\epsilon_n]}$ découlent immédiatement de la définition.
C'est clair pour $n = 2$ en effet $P_{e_2}(t) = (-1)^{\xi_1}(t - \xi_1)$. On suppose donc que P_{e_n} $n \geq 2$, est à coefficients entiers. Ecrivons

$$P_{e_{n+1}}(t) = \sum_{i=0}^{n} a_i t^i$$

on a

$$P^{(k)}_{e_{n+1}}(t) = \sum_{i=k}^{n} i(i-1)\ldots(i-k+1)a_i t^{i-k}$$

En utilisant la définition, il est facile de constater que

$$P^{(k)}_{e_{n+1}}(t) = k!\binom{n}{k}(-1)^{\left(\sum_{j=n-k+1}^{n}\xi_j\right)}P_{e_{n-k+1}}$$

et par identification il s'ensuit que pour $k = 1,\ldots,n$

$$a_k = \binom{n}{k}(-1)^{\left(\sum_{j=n-k+1}^{n}\xi_j\right)}P_{e_{n-k+1}}(0)$$

On en déduit que $a_k \in \mathbb{Z}$, $k = 1,\ldots,n$ et $P_{e_{n+1}} \in \mathbb{Z}[t]$ en observant que $a_0 = 0$ ou $a_0 = -(a_1 + a_2 + \ldots + a_n)$ suivant que $\epsilon_n\epsilon_{n+1} = -1$ ou 1. o

Soit $\mathbf{R}$ un corps réel clos, $P \in \mathbf{R}[X]$ de degré d et $\sigma_0,\ldots,\sigma_d$ une liste de signes stricts. Le lemme de Thom affirme entre autres que l'ensemble $\{x \in \mathbf{R}/P(x)\ \sigma_0\ 0,\ldots,P^{(d)}(x)\ \sigma_d\ 0\}$ est soit vide soit un un intervalle ouvert. Nous verrons grâce aux formules de Taylor mixtes (corollaire qui suit) et encore mieux aux formules de Taylor généralisées que ce fait géometrique peut se traduire explicitement en identités algébriques.

Corollaire 7 : (Formules de Taylor mixtes pour les polynômes)
Soit $\mathbf{A}$ un anneau commutatif. Alors pour chaque polynôme de degré $n \geq 1$, à coefficients dans $\mathbf{A}$ il y a 2^{n-1} formules de Taylor mixtes et toutes les combinaisons de signes possibles apparaissent. On considère deux variables U et V et on pose $\Delta = U - V$. Soit $e = [\epsilon_1,\epsilon_2,\ldots,\epsilon_n]$ une combinaison de signes stricts avec $\epsilon_1 = 1$, alors la formule de Taylor mixte pour un polynôme P de degré $n \geq 1$, correspondante à la combinaison e est une identité algébrique du type suivant, où les $c_{k,e}$ sont des entiers strictement positifs :

$$P(U) - P(V) = \sum_{k=1}^{n-1}\epsilon_k c_{k,e}\Delta^k D_k(P)(Y_k) + \epsilon_n c_{n,e}\Delta^n D_n(P) \qquad (1)$$

$$avec\ Y_k = \begin{cases} U & si\ \epsilon_k\epsilon_{k+1} > 0 \\ V & si\ \epsilon_k\epsilon_{k+1} < 0 \end{cases}$$

Preuve : Comme il s'agit d'identités algébriques en les variables U, V et les coefficients du polynôme P il suffit donc de le démontrer pour l'anneau $\mathbb{Z}$. Or cela se déduit du théorème 4 o

Remarque : En pratique nous utiliserons la formule ci-dessous, manifestement préferable à celle donnée dans les notations qui précèdent le théorème 4, pour calculer les coefficients $c_{k,e}$. Elle est obtenue, en prenant le cas particulier où $P = X^n$ dans le corollaire précédent.

$$\epsilon_k c_{k,e} = 1 - \sum_{i=1}^{k-1} \epsilon_i \delta_i c_{i,e} \binom{k}{i} \tag{2}$$

avec $\delta_i = 1 - \xi_i,\ i = 1, \ldots, k-1,\ k = 1, \ldots, n.$

Proposition 8 : *Soit n un entier ≥ 1 alors pour toute combinaison de signes stricts $e = [\epsilon_1, \epsilon_2, \ldots, \epsilon_n]$* avec $\epsilon_1 = 1$, *les coefficients $c_{i,e}$ $(i = 1, \ldots, n)$* vérifient :

$$c_{i+1,e} \leq (i+1)c_{i,e} \quad et \quad c_{i,e} \leq 2(n!)\alpha(n)\left(\frac{2}{\pi}\right)^{n+1}$$

avec $\alpha(n) = \begin{cases} 1 & \text{si n est pair} \\ \frac{2^{n+1}-1}{2^{n+1}-2} & \text{si n est impair} \end{cases}$

Preuve voir [WAR] o

Proposition 9 : *Soit $e = [\epsilon_1, \epsilon_2, \ldots, \epsilon_n]$ une combinaison de signes stricts avec $\epsilon_1 = 1$, alors le calcul de la liste des coefficients $c_{i,e}$, $i = 1, \ldots, n$ est de l'ordre $O(n^4\,[\log(n)]^2)$*

Preuve : De l'égalité (2) de la page 5 on déduit que le nombre d'opérations arithmétiques pour calculer $c_{n,e}$ est en $O(n^2)$. La taille des entiers et coefficients $c_{i,e}$ $(i \leq n-1)$ précédemment calculés est bornée par $n.\log(n)$ d'après l'inégalité de la proposition précédente. Il faut donc compter un coût de l'ordre $O(n^4\,[\log(n)]^2)$ pour calculer $c_{i,e_n}, i = 1, \ldots, n$ o

Remarques :
1) La taille d'une formule de Taylor mixte pour un polynôme P de degré n est en $O(n^2 \log(n))$.
2) Un algorithme de multiplication rapide des entiers donnerait, pour le calcul de $c_{i,e}$, $i = 1, \ldots, n$, une borne en $O(n^3[\log n]^3)$

2.2 Formules de Taylor généralisées

Nous commençons par un exemple pour préciser la position du problème. Considérons un polynôme général de degré 4 :

$$P(X) = c_0X^4 + c_1X^3 + c_2X^2 + c_3X + c_4$$

Considérons le système de conditions de signes généralisées portant sur le polynôme P et ses dérivées successives par rapport à la variable X :

$$(X) : \quad \left[P(X) > 0,\ P'(X) > 0,\ P^{(2)}(X) < 0,\ P^{(3)}(X) < 0,\ P^{(4)}(X) > 0\right]$$

Considérons également le système de conditions de signes généralisées obtenues en relachant toutes les inégalités, sauf la dernière :

$$'(X) : \quad \left[P(X) \geq 0,\ P'(X) \geq 0,\ P^{(2)}(X) \leq 0,\ P^{(3)}(X) \leq 0,\ P^{(4)}(X) > 0\right]$$

Le lemme de Thom affirme (entre autres) : $[']U),']V),\ U < Z < V] \Rightarrow (Z)$
Voyons comment on peut traduire ce fait géometrique par des identités algébriques.
On écrit les formules de Taylor mixtes suivantes pour $P^{(i)}$ $i = 3, \ldots, 0$:

a. $P^{(3)}(Z) = P^{(3)}(V) + P^{(4)}(Z - V)$

b. $P^{(2)}(Z) = P^{(2)}(U) + P^{(3)}(Z).(Z - U) - 1/2P^{(4)}.(Z - U)^2$

c. $P'(Z) = P'(V) + P^{(2)}(Z).(Z - V) - 1/2P^{(3)}(V).(Z - V)^2 - 1/3P^{(4)}.(Z - V)^3$

d. $P(Z) = P(U) + P'(Z).(Z - U) - 1/2P^{(2)}(U).(Z - U)^2 - 1/3P^{(3)}(Z).(Z - U)^3 + 5/24P^{(4)}.(Z - U)^4$

Posons $\Delta_1 = Z - U$ et $\Delta_2 = V - Z$
Dans **b.** on remplace $P^{(3)}(Z)$ par son expression en **a.** on obtient :

b'. $P^{(2)}(Z) = P^{(2)}(U) + P^{(3)}(V).\Delta_1 - P^{(4)}.\left[\frac{1}{2}\Delta_1^2 + \Delta_1\Delta_2\right]$

On obtient également par substitutions :

c'. $P'(Z) = P'(V) - P^{(2)}(U).\Delta_2 - P^{(3)}(V)\left[\Delta_1\Delta_2 + \frac{1}{2}\Delta_2^2\right] + P^{(4)}\left[\frac{1}{2}\Delta_1^2\Delta_2 + \Delta_1\Delta_2^2 + \frac{1}{3}\Delta_2^3\right]$

d'. $P(Z) = P(U) + P'(V)\Delta_1 - P^{(2)}(U)\left[\frac{1}{2}\Delta_1^2 + \Delta_1\Delta_2\right] - P^{(3)}(V)\left[\frac{1}{3}\Delta_1^3 + \Delta_1^2\Delta_2 + \frac{1}{2}\Delta_1\Delta_2^2\right] + P^{(4)}\left[\frac{5}{24}\Delta_1^4 + \frac{5}{6}\Delta^3\Delta_2 + \Delta_1^2\Delta_2^2 + \frac{1}{3}\Delta_1\Delta_2^3\right]$

Les égalités **a.**, **b'.**, **c'.**, **d'.** donnent l'implication ci-dessus sous forme d'implication forte. La première égalité est une formule de Taylor habituelle portant sur le polynôme $P^{(3)}$. Les trois autres sont des formules de Taylor généralisées portant sur les polynômes $P^{(2)}$, P' et P.

De façon générale nous avons le théorème ci-dessous concernant les formules de Taylor généralisées.
Si $e = [\epsilon_0, \ldots, \epsilon_{n+1}]$ est un $(n+1)$-uplet de signes stricts, nous désignons par $e^{(k)} = [\epsilon_k, \ldots, \epsilon_{n+1}]$, $k = 1, \ldots, n$.
Nous notons $\Delta_{\epsilon_0,\epsilon_1} = \begin{cases} \Delta_1 & \text{si } \epsilon_0\epsilon_1 > 0 \\ \Delta_2 & \text{si } \epsilon_0\epsilon_1 < 0 \end{cases}$

Théorème 10 : *Pour chaque degré n il y a 2^n, formules de Taylor généralisées. Plus précisement soit* **A** *un anneau commutatif et* $P \in \mathbf{A}[X]$ *un polynône de degré* $n \geq 1$ en X. *On considère deux variables* U *et* V *et on pose* $\Delta_1 = X - U$, $\Delta_2 = V - X$. *Soit* $e = [\epsilon_0, \epsilon_1, \ldots, \epsilon_n]$ *un* $(n+1)$*-uplet de signes stricts, alors la formule de Taylor généralisée pour* P *associée à la combinaiason e est une identité algébrique du type suivant :*

$$P(X) = P(Y_0) + \sum_{k=1}^{n-1} \epsilon_0\epsilon_k D_k(P)(Y_k)H_{k,e}(\Delta_1, \Delta_2) + \epsilon_0\epsilon_n D_n(P)H_{n,e}(\Delta_1, \Delta_2)$$

où $Y_k = \begin{cases} U & si\ \epsilon_k\epsilon_{k+1} > 0 \\ V & si\ \epsilon_k\epsilon_{k+1} < 0 \end{cases}$

et $H_{k,e}$ *est un polyôme homogène de degré k, à coefficients entiers positifs ou nuls, non identiquement nul. Le polynôme* $H_{n,e}(\Delta_1, \Delta_2)$ *est donné par la relation de recurrence :*

$$H_{n,e}(\Delta_1, \Delta_2) = \sum_{k=1}^{n-1} \frac{1 - \epsilon_0\epsilon_1\epsilon_k\epsilon_{k+1}}{2}\binom{n}{k} c_{k,e'}\Delta^k_{\epsilon_0,\epsilon_1} H_{n-k,e^{(k)}}(\Delta_1, \Delta_2) + c_{n,e'}\Delta^n_{\epsilon_0,\epsilon_1} \quad (\star)$$

où $e' = \left[(\epsilon_0\epsilon_1)^k\epsilon_0\epsilon_k\right]_{k=1\ldots n}$.

Preuve : Raisonnons par recurrence sur le degré n de P. Si $n = 1$ le théorème est évident.
Soit P un polynôme de degré $n > 1$. Nous distinguons deux cas :

1^{er}cas : $\epsilon_0\epsilon_1 = -1$: Ecrivons la formule de Taylor mixte pour P correspondant à la combinaison de signes $s = [\sigma_k]$ avec $\sigma_k = (-1)^k\epsilon_0\epsilon_k, k = 1, \ldots, n$:

$$\begin{aligned} \mathrm{P}(\mathrm{X}) &= \mathrm{P}(\mathrm{V}) + \sum_{k=1}^{n-1} \sigma_k c_{k,s}(\mathrm{X}-\mathrm{V})^k D_k(\mathrm{P})(\mathrm{Z}_k) + \sigma_n c_{n,s}(\mathrm{X}-\mathrm{V})^n D_n(\mathrm{P}) \\ &= \mathrm{P}(\mathrm{V}) + \epsilon_0 \sum_{k=1}^{n-1} \epsilon_k c_{k,s}\Delta_2^k D_k(\mathrm{P})(\mathrm{Z}_k) + \epsilon_0\epsilon_n c_{n,s}\Delta_2^n D_n(\mathrm{P}) \end{aligned}$$

avec $\mathrm{Z}_k = \begin{cases} \mathrm{V} & \text{si } \epsilon_k\epsilon_{k+1} = -1 \\ \mathrm{X} & \text{sinon} \end{cases}$
Alors ou bien $\mathrm{Z}_k = \mathrm{V}, k = 1, \ldots, n-1$ auquel cas le théorème est démontré, ou bien il exite deux ensembles disjoints I et J (avec J non vide,$I \cup J = \{1, \ldots, n\}$,) tels que :

$$\mathrm{P}(\mathrm{X}) = \mathrm{P}(\mathrm{V}) + \epsilon_0 \sum_{k\in I} \epsilon_k c_{k,s}\Delta_2^k D_k(\mathrm{P})(\mathrm{V}) + \epsilon_0 \sum_{k\in J} \epsilon_k c_{k,s}\Delta_2^k D_k(\mathrm{P})(\mathrm{X}) + \epsilon_0\epsilon_n c_{n,s}\Delta_2^n D_n(\mathrm{P})$$

Posons

$$\mathrm{Q}(\mathrm{X}) = \epsilon_0 \sum_{k\in J} \epsilon_k c_{k,s}\Delta_2^k D_k(\mathrm{P})(\mathrm{X})$$

d'après l'hypothèse de recurrence on a

$$\begin{aligned} D_k(\mathrm{P})(\mathrm{X}) &= D_k(\mathrm{P})(Y_k) + \epsilon_k \sum_{j=1}^{n-k} \epsilon_{k+j} D_j[D_k(\mathrm{P})](\mathrm{Y}_{k+j})\mathrm{H}_{j,e^{(k)}}(\Delta_1, \Delta_2) \\ &= D_k(\mathrm{P})(Y_k) + \epsilon_k \sum_{m=k+1}^{n} \epsilon_m \binom{m}{m-k} D_m(\mathrm{P})(\mathrm{Y}_m)\mathrm{H}_{m-k,e^{(k)}}(\Delta_1, \Delta_2) \end{aligned}$$

avec $\mathrm{H}_{m-k,e^{(k)}}$ homogène, de degré $m-k$ et à coefficients entiers positifs ou nuls. Si j_0 est le plus petit indice dans J, il vient alors

$$\begin{aligned} \mathrm{Q}(\mathrm{X}) &= \epsilon_0 \sum_{k\in J} \sum_{j=k}^{n} \epsilon_j D_j(\mathrm{P})(\mathrm{Y}_j)\mathrm{G}_{j,e^{(k)}}(\Delta_1, \Delta_2) \\ &= \epsilon_0 \sum_{l=j_0}^{n} \epsilon_l D_l(\mathrm{P})(\mathrm{Y}_l)\mathrm{G}_{l,e}(\Delta_1, \Delta_2) \end{aligned}$$

avec $\mathrm{G}_{j,e^{(k)}} = \binom{j}{j-k} c_{k,s}\Delta_2^k \mathrm{H}_{j-k,e^{(k)}}$ $j \geq k$ et $\mathrm{G}_{l,e} = \sum_{k\in J} \mathrm{G}_{l,e^{(k)}}$ **(h)**. On déduit donc

$$\mathrm{P}(\mathrm{X}) = \mathrm{P}(\mathrm{V}) + \epsilon_0 \sum_{k\in I} \epsilon_k D_k(\mathrm{P})(\mathrm{V}) c_k \Delta_2^k + \epsilon_0 \sum_{l=j_0}^{n} \epsilon_l D_l(\mathrm{P})(\mathrm{Y}_l)\mathrm{G}_{l,e}(\Delta_1, \Delta_2)$$

On observe maintemant que si un $l \in I$ alors $\epsilon_l\epsilon_{l+1} = -1$ et d'après l'hypothèse de recurrence $\mathrm{Y}_l = V$. Ce qui achève la démonstration dans ce cas.
Pour le cas $\epsilon_0\epsilon_1 = 1$ écrire la formule de Taylor mixte pour P correspondante au n-uplet $(\sigma_k = \epsilon_0\epsilon_k)_k = 1, \ldots, n$ et refaire le même raisonnement qu'au cas précédent o

Proposition 11 : *Pour toute combinaison de signes stricts* $e = [\epsilon_0, \ldots, \epsilon_{n+1}]$, *la somme des coefficients du polynôme homogène* $\mathrm{H}_{k,e}$, $k = 1, \ldots, n$, *est majorée par* :

$$\frac{n!}{2}\left(\left[1+\sqrt{2}\left(\frac{2}{\pi}\right)^{\frac{3}{2}}\right]^n + \left[1-\sqrt{2}\left(\frac{2}{\pi}\right)^{\frac{3}{2}}\right]^n\right) \leq \frac{n!}{2}\Big((1,75)^n + 1\Big)$$

Preuve : Cela resulte facilement de la proposition 7 et lemme 10. o

Corollaire 12 : *Soit* $\mathrm{P} \in \mathbf{K}[\mathbf{C}, \mathrm{X}]$ *de degré* d *en* X, $\sigma_0, \sigma_1, \ldots, \sigma_d$ *une liste de signes stricts. On note* H[C,X] ou H(X) *le système* :

$$\Big[\mathrm{P}(\mathbf{C}, \mathrm{X})\ \sigma_0\ 0, \mathrm{P}'(\mathbf{C}, \mathrm{X})\ \sigma_1\ 0, \ldots, \mathrm{P}^{(d)}(\mathbf{C}, \mathrm{X})\ \sigma_d\ 0\Big]$$

(*les dérivées sont par rapport à* X). *Soit* H'(X) *le système obtenu à partir de* H(X) *en relachant toutes les conditions de signes sauf relative* à $\mathrm{P}^{(d)}$.

Alors $\quad {}^*([{}'(\mathrm{U}), {}'(\mathrm{V}), \mathrm{U} < \mathrm{X} < \mathrm{V}] \Longrightarrow (\mathrm{X}))^*$

Preuve : L'implication forte se démontre en utilisant pour la $i^{ième}$ dérivée $\mathrm{P}^{(i)}$ i de $d-1$ à 0, la formule de Taylor généralisée associée à la combinaison de signes stricts $[\sigma_i, \sigma_{i+1}, \ldots, \sigma_d]$. Puisque $\mathrm{H}_d \neq 0$, le fait de supposer $\mathrm{P}^{(d)}(\mathbf{C}, \mathrm{X})$ avec un signe strict permet d'avoir un terme qui assure le signe strict de $\mathrm{P}^{(i)}(\mathbf{C}, \mathrm{X})$ lorsque utilise la formule de Taylor généralisée indiquée pour $\mathrm{P}^{(i)}$ o

2.3 quelques exemples de formules de Taylor généralisées

Si deg(P)=2 on a les quatre formules de Taylor généralisées suivantes

$$\mathrm{P}(\mathrm{X}) = \mathrm{P}(\mathrm{U}) + \mathrm{P}'(\mathrm{U}).\Delta_1 + \mathrm{P}^{(2)}.\left[\frac{1}{2}\Delta_1^2\right]$$

$$\mathrm{P}(\mathrm{X}) = \mathrm{P}(\mathrm{U}) + \mathrm{P}'(\mathrm{V}).\Delta_1 - \mathrm{P}^{(2)}(\mathrm{V}).\left[\frac{1}{2}\Delta_1^2 + \Delta_1\Delta_2\right]$$

$$\mathrm{P}(\mathrm{X}) = \mathrm{P}(\mathrm{V}) - \mathrm{P}'(\mathrm{V}).\Delta_2 + \mathrm{P}^{(2)}.\left[\frac{1}{2}\Delta_2^2\right]$$

$$\mathrm{P}(\mathrm{X}) = \mathrm{P}(\mathrm{V}) - \mathrm{P}'(\mathrm{U}).\Delta_2 - \mathrm{P}^{(2)}.\left[\Delta_1\Delta_2 + \frac{1}{2}\Delta_2^2\right]$$

Notez que les deux dernières formules résultent des deux premières par l'échange de U et V (ce qui implique le remplacement de Δ_1 par $-\Delta_2$ et de Δ_2 par $-\Delta_1$)

Si deg(P) = 3 chaque formule de Taylor généralisée précédente se scinde en deux et on a huit formules de Taylor généralisées, les quatre suivantes et leurs symétriques obtenues par échange de U et V :

$$\mathrm{P}(\mathrm{X}) = \mathrm{P}(\mathrm{U}) + \mathrm{P}'(\mathrm{U}).\Delta_1 + \mathrm{P}^{(2)}(\mathrm{U}).\left[\frac{1}{2}\Delta_1^2\right] + \mathrm{P}^{(3)}.\left[\frac{1}{6}\Delta_1^3\right]$$

$$\mathrm{P}(\mathrm{X}) = \mathrm{P}(\mathrm{U}) + \mathrm{P}'(\mathrm{U}).\Delta_1 + \mathrm{P}^{(2)}(\mathrm{V}).\left[\frac{1}{2}\Delta_1^2\right] - \mathrm{P}^{(3)}.\left[\frac{1}{3}\Delta_1^3 + \frac{1}{2}\Delta_1^2\Delta_2\right]$$

$$\mathrm{P}(\mathrm{X}) = \mathrm{P}(\mathrm{U}) + \mathrm{P}'(\mathrm{V}).\Delta_1 - \mathrm{P}^{(2)}(\mathrm{V}).\left[\frac{1}{2}\Delta_1^2 + \Delta_1\Delta_2\right] + \mathrm{P}^{(3)}.\left[\frac{1}{6}\Delta_1^3 + \frac{1}{2}\Delta_1^2\Delta_2 + \frac{1}{2}\Delta_1\Delta_2^2\right]$$

$$\mathrm{P}(\mathrm{X}) = \mathrm{P}(\mathrm{U}) + \mathrm{P}'(\mathrm{V}).\Delta_1 - \mathrm{P}^{(2)}(\mathrm{U}).\left[\frac{1}{2}\Delta_1^2 + \Delta_1\Delta_2\right] - \mathrm{P}^{(3)}.\left[\frac{1}{3}\Delta_1^3 + \Delta_1^2\Delta_2 + \frac{1}{2}\Delta_1\Delta_2^2\right]$$

3. Algorithme de construction de l'identité donnant le positivstellensatz

Soit $\mathbf{A}$ un anneau intègre, de corps de fractions $\mathbf{K}$. On suppose que $\mathbf{K}$ est muni d'un ordre $\leq$ et on note $\mathbf{R}$ la cloture réelle de $\mathbf{K}$. Soit $Q_1, \ldots, Q_k$ une suite de polynômes dans $\mathbf{A}[\mathrm{X}]$, le tableau complet de signes des Q_i :

$\mathcal{T} = \mathcal{T}_k[Q_1, \ldots, Q_k]$ sera la donnée du nombre N des zéros réels dans $\mathbf{R}$: $\zeta_1 < \zeta_2 < \ldots < \zeta_N$ des différents polynômes Q_i et d'un tableau à k lignes et $2N+1$ colonnes donnant le signe de chaque Q_i en chaque zéro ζ_i et sur chaque intervalle $]-\infty, \zeta_1[,]\zeta_i, \zeta_{i+1}[,]\zeta_N, +\infty[$.
Notez que le tableau ne donne pas la valeur des zéros autrement que par leurs codages à la Thom.

Proposition 13 : *Soit* (P_j) *une famille de polynômes dans* $\mathbf{A}[X]$ *stable par dérivation. Soit* (ζ_j) *la famille des zéros réels des* βP_j *dans* $\mathbf{R}$. *Alors on peut établir le tableau complet* $\mathcal{T}$ *de signes* $(-, 0, +)$ *pour la famille* (P_j), *à partir de la seule connaissance des signes de* $P_j(\zeta_i)$

Preuve : C'est une conséquence facile du lemme de Thom o

Soit $L = [P_1, \ldots, P_s]$ une liste de polynômes de $\mathbf{A}[X]$ et $s = (\sigma_i)_{i=1,\ldots,s}$ un s-uplet de conditions de signes généralisées et $H = [P_1\sigma_1 0, \ldots, P_s\sigma_s 0]$ le système de conditions de signes généralisées associé à L et s. On considère P la famille engendrée par L et l'opération dérivation, $\zeta_1 < \zeta_2 < \ldots < \zeta_m$ les zéros réels des polynômes de P et $\mathcal{T}$ le tableau complet de signes correspondant.

Lemme 14 : *On suppose que l'on a*
a) *des incompatibilités* $\downarrow [, X < \zeta_1] \downarrow, \downarrow [, \zeta_1 < X < \zeta_2] \downarrow, \downarrow [, \zeta_2 < X < \zeta_3] \downarrow, \ldots, \downarrow [, X < \zeta_m] \downarrow$ *avec un degré majoré par* δ.
b) *des incompatibilités* $\downarrow [, X = \zeta_i] \downarrow$ $i = 1, \ldots, m$ *avec un degré majoré par* δ'.
Alors on peut construire $\downarrow \downarrow$ *avec un degré majoré par* $2m\delta\delta'$

Preuve : En appliquant m fois la proposition 4(ii) on construit $\downarrow [, X_1 \neq \zeta_1, X_2 \neq \zeta_2, \ldots, X_k \neq \zeta_m] \downarrow$ avec un degré majoré par $(m+1)\delta$, selon le schéma suivant :

$$\underbrace{\underbrace{E_1 \quad E_2}_{E_{1,2}} \; E_3 \cdots\cdots E_{k+1}}_{E_{1,2,3}}$$
$$\vdots$$
$$\underbrace{\qquad\qquad\qquad}_{E_{1,\ldots,k+1}}$$

L'incompatibilité $E_{1,2} = \downarrow [, Q_1 \neq 0, Q_2 < 0] \downarrow$ résulte de la proposition 4(ii) appliqué à E_1 et E_2. L'incompatibilité $E_{1,2,3} = \downarrow [, Q_1 \neq 0, Q_2 \neq 0, \; Q_3 < 0] \downarrow$ est obtenue à partir de $E_{1,2}$ et de E_3 comme précédemment. Ce procéssus itéré jusqu'à E_{k+1} nous donne l'incompatibilité $E_{1,\ldots,k+1} := \downarrow [, Q_1 \neq 0, Q_2 \neq 0, \ldots, Q_k \neq 0]$
Nous appliquons ensuite m fois la proposition 4(iii) avec $q = 1$. En remarquant que l'exposant de $X - \zeta_i$ est majoré par 2δ à chaque pas, on déduit que le degré augmente au plus de $2\delta(\delta' - 1)$.
En fin de compte on obtient la majoration $(m+1)\delta + 2m\delta(\delta' - 1)$ o

Théorème 15 :(positivstellensatz effectif réel en une variable et borne sur les degrés)
Ou bien H(x) *est impossible dans* $\mathbf{R}$ *et alors* $\downarrow \downarrow$ *dans* $\mathbf{K}$ *et donc* H(x) *est impossible dans toute extension ordonnée de* $\mathbf{K}$. *De plus si d majore les degrés des* $P_i, i = 1, \ldots, s$ *alors le degré de* $\downarrow \downarrow$ *est majoré par* $8md^2$
Ou bien H(x) *est possible dans* $\mathbf{R}$

Preuve Soient $\zeta_1 < \zeta_2 < \ldots < \zeta_k$ la liste ordonnée des points finis de $\mathcal{T}$. Posons $\zeta_0 = -\infty$ et $\zeta_{k+1} = +\infty$.

L'existence d'un x dans $\mathbf{R}$ vérifiant $H(x)$ est directement lisible sur le tableau complet de signes de la famille et se teste uniquement par des calculs dans $\mathbf{K}$. Pour cela on compare sur chaque intervalle ouvert et en chaque point fini de $\mathcal{T}$, la condition de signe imposée à un polynôme dans L et son signe donné dans $\mathcal{T}$. Si aucune contradiction n'est relevée pour les polynômes dans L sur au moins un intervalle ou un point alors H est possible dans $\mathbf{R}$.

Si au contraire sur chaque intervalle ouvert et en chaque point $\zeta_i, i = 1, \ldots, k$ de $\mathcal{T}$ il existe un polynôme dans L de condition opposée à son signe dans $\mathcal{T}$ alors le système H est impossible.

Sur chaque intervalle ouvert $I =]\zeta_{i-1}, \zeta_i[$ on choisit un polynôme P de condition de signe contradictoire à son signe dans $\mathcal{T}$ sur cet intervalle. On prend un polynôme de plus bas degré possible dans L , pour ne pas grossir le degré final dans l'identité cherchée. Supposons le polynôme P de degré p. Soit $(\epsilon_0, \epsilon_1, \ldots, \epsilon_p)$ le p-uplet de signes de $P, P', \ldots, P^{(p)}$ sur I. D'après le corollaire 12, il existe une formule de Taylor généralisée qui manifeste l'évidence forte que P ait la condition de signe souhaitée sur I et donc l'incompatibilté $\downarrow [, \zeta_{i-1} < X < \zeta_i] \downarrow$. Cette formule de Taylor généralisée s'écrit sous la forme donnée dans la défintion 1 :

$$Q_{i-1}^{2n_{i,1}} Q_i^{2n_{i,2}} \alpha_i + S_{i,1} + Q_{i-1} S_{i,2} - Q_i S_{i,3} - Q_{i-1} Q_i S_{i,4} + Z_i = 0$$

avec $Q_{i-1} = X - \zeta_{i-1}, Q_i = X - \zeta_i, \alpha_i \in \mathbf{R}, S_{i,j}, j = 1, 2, 3, 4$ sont des sommes de carrés pondérées dans $\mathbf{R}[X]$ avec des poids positifs.
Sur les intervalles $]-\infty, \zeta_1[$ et $]\zeta_k, +\infty[$ l'incompatibilité $\downarrow (, X < \zeta_1) \downarrow$ (ou $\downarrow (, \zeta_k < X) \downarrow$) de est donnée par la formule de Taylor ordinaire d'un polynôme convenable dans L.
Maintenant en un point $\zeta_{\neg_i}, i = 1, \ldots, k$ l'incompatibilité $\downarrow [, X = \zeta_i] \downarrow$ est donnée par un polynôme de condition de signe contradictoire en ζ_i. Elle s'écrit à partir d'une égalité de la forme :

$$P(X) = P(\zeta_i) + (X - \zeta_i) Q(X)$$

On conclut en applicant le lemme 14 o

4. Quelques précisions sur l'implantation et le côut de l'algorithme en Axiom

Nous avons implanté l'algorithme décrit précédemment en Axiom, pour le cas où les polynômes de la liste L sont à coefficients entiers.
Soit P la famille (P_j) des polynômes de L et leurs dérivées successives. Soit s le nombre de polynômes dans L. Soit m le nombre de zéros réels de P et soient $\zeta_1 < \ldots, \zeta_m$ ces zéros réels. Soit d le degré maximum des polynômes de L. Soit enfin t la taille maximum des polynômes de P. Nous avons utilisé l'algorithme SI (cf [RS]) pour obtenir le tableau complet de signes des $P_j(\zeta_i)$. Nous pouvons majorer la complexité du calcul de ce tableau par : $O(smd^5(\log\ m)^3 t^2)$
En ce qui concerne l'identité algébrique qui donne le positivstellensatz, nous avons introduit pour chaque ζ_i une variable formelle Y_i qui le represente. Notre algorithme produit, à partir du tableau des signes des $P_j(\zeta_i)$ fournit par SI, une expression algébrique en X et les $P_j(Y_i)$, qui est une incompatibilité convenable, pour autant que les Y_i soient remplacés par les ζ_i. En conséquence cette expression represente une identité à coefficients dans $\mathbf{R}_{alg}$. Chaque fois que $P_j(\zeta_i) = 0$ nous avons remplacé le terme $P_j(Y_i)$ par 0 dans l'expression, qui en a été d'autant simplifiée. L'identité finale est donc une égalité dans $\mathbf{Z}[X, (Y_i)]/\mathcal{I}$ où $\mathcal{I}$ est l'idéal engendré par les $P_j(Y_i)$ correspondants aux $P_j(\zeta_i)$ nuls.
En pratique le temps de calcul de l'identité s'est toujours révélé inferieur au temps de calcul du tableau des signes de $P_j(\zeta_i)$.
Dans notre thèse, nous donnons tous les calculs sur les algorithmes et nous calculerons une majoration précise pour la complexité du seul calcul de l'identité algébrique (à partir du tableau de signes des $P_j(\zeta_i)$).
Remarquons aussi que l'identité algébrique calculée peut être representée sous une forme plus ou moins compacte. Pour en limiter la taille nous avons introduit quelques opérations formelles. Ces opérations apparaissent lorsqu'on élimine les $Q_i = X - \zeta_i$ en utilisant le point (iii) de la proposition 4. Le point (iii) consiste à élever à la puissance d'un entier positif pair, une identité du type (cf la démonstration de la proposition..) :

$$M + C + QY_1 + Y_2 = 0$$

après avoir isolé au second membre le terme QY_1. Nous écrirons cette manipultion simplement par

$$(-QY_1)^{2k} = M^{2k} + MC diffp1(M, C, 2k) + diffp_2(M, C, 2k) + Y_2 diffp0(M, C, Y_2, 2k)$$

avec $\quad diffp1(M, C, 2k) := \sum_{j=0}^{k-1} \binom{2k}{2i+1} M^{2(k-i-1)} C^{2i} \quad , \quad diffp2(M, C, 2k) := \sum_{j=1}^{k} \binom{2k}{2i} M^{2(k-i)} C^{2i},$

$diffp0(M, C, Y_2, 2k) := \sum_{j=1}^{2k} \binom{2k}{j}(M + C)^{2k-j} Y_2^{j-1}$. Les résultats de deux premières opérations sont des sommes de carrés " pondérés" dans $\mathbf{R}[X]$

Références

[BCR] J. Bochnak, M. Coste and M.F Roy "Géométrie algébrique réelle", Ergebnisse, Spinger-Verlag, 1987

[LOM1] H. Lombardi : MEGA 90 eds Mora, Traverso

[LOM2] H. Lombardi : Rennes 91 eds Coste, Mahe, Roy

[RS] M.F Roy and A. Szpirglass, *Complexity of computation on real algebraic numbers*, J. of Symb. comp., 1990, 10, 39-51

[CLGR] F. Cucker, L. Gonzalez, F. Rosselo *On algorithms for real algebraic plane curves*, Effective Methods in Algebraic Geomety - Progress in Math. vol 94 1991

[WAR] H. Warou "Thèse Univ. de Rennes1 en préparation".

WAROU HAROUNA

Institut de Recherche Mathématique de Rennes,
Université de Rennes I, Campus de Beaulieu,
F-35042 Rennes Cedex, France