ANNALES DE L'INSTITUT FOURIER

FELICE RONGA

Un procédé d'élimination effective et quelques applications

Annales de l'institut Fourier, tome 45, n° 2 (1995), p. 421-435

<http://www.numdam.org/item?id=AIF_1995__45_2_421_0>

© Annales de l'institut Fourier, 1995, tous droits réservés.

L'accès aux archives de la revue « Annales de l'institut Fourier » (http://annalif.ujf-grenoble.fr/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Ann. Inst. Fourier, Grenoble
45, 2 (1995), 421-435

UN PROCÉDÉ D'ÉLIMINATION EFFECTIVE ET QUELQUES APPLICATIONS

par Felice RONGA

Soient $F_1(X,Y),\ldots,F_k(X,Y) \in \mathbb{C}[X_1,\ldots,X_n,Y]$ des polynômes et posons

$$Z_Y = \{y \in \mathbb{C} \mid \exists x_1,\ldots,x_n \in \mathbb{C}\,,\ F_i(x_1,\ldots,x_n,y) = 0\,,\ i = 1,\ldots,k\}\,.$$

Le résultat principal de ce travail est une estimation explicite en termes des coefficients des F_i des éléments de Z_Y, dans le cas où Z_Y est un ensemble fini de points (voir §1, théorème I). Cette estimation est basée sur le Nullstellensatz effectif, tel qu'il est démontré dans [5] ou [1].

Comme première application, on donne des bornes explicites des valeurs critiques non nulles d'un polynôme $P(X)$, d'où l'on peut déduire par exemple une valeur explicite $\varepsilon_0 \in \mathbb{R}^+$ telle que $0 \in \mathbb{C}$ ne soit pas valeur critique de $P(X) - \varepsilon$, $\forall \varepsilon$ tel que $0 < |\varepsilon| \leq \varepsilon_0$ (voir corollaire 1.3).

Au §2 on donne une méthode pour résoudre explicitement des inéquations polynomiales strictes. Soit $P(X) \in \mathbb{R}[X_1,\ldots,X_n]$ un polynôme à coefficients réels de degré d, R un entier positif et soit $\Omega_R^+(P) = \{x \in \mathbb{R}^n | P(x) > 0, \|x\| \leq R\}$, où sur $\mathbb{R}^n$ l'on prend la norme $\|x\| = \sup\{|x_i|\,,\ i = 1\ldots n\}$. On montrera que tout $x \in \Omega_R^+(P)$ est dans la même composante qu'une solution qui appartient aux sommets du maillage obtenu en partageant les côtés du cube $\{x \mid \|x\| \leq R\}$ en T parties, où T est un entier qui dépend des coefficients de P et qui sera donné explicitement (voir le corollaire 2.3 du théorème II). Le théorème III montre que toute solution dans $\mathbb{R}^n$ de l'inéquation $P(x) > 0$ est dans la même composante connexe de $\Omega^+(P) = \{x | P(x) > 0\}$ qu'une solution se trouvant

Mots-clés : Estimation explicite – Valeurs critiques.
Classification math. : 14Q20 – 68Q40.

dans $\Omega_R^+(P)$, où R est donné explicitement à partir des coefficients de P. Enfin, le théorème IV montre que si a et $b \in \Omega^+(P)$ sont sur le sommet d'un maillage de $\mathbb{R}^n$, ils sont dans la même composante connexe de $\Omega^+(P)$ si et seulement si ont peut les joindre par des arêtes appartenant à un raffinement explicite du maillage, dans un cube explicite.

Au §3 nous construisons à partir de l'estimation explicite des valeurs critiques un algorithme qui permet d'isoler et approcher de façon certaine les racines réelles (multiples ou non) d'un polynôme à coefficients réels à une variable $P(t) \in \mathbb{R}[t]$. Nous obtenons en particulier une borne inférieure de la distance minimale entre racines distinctes de P, en termes des coefficients et du degré de P, valable même si P a des racines multiples.

Les résultats de ce travail reprennent en partie ceux de [6], où le cas des polynômes à coefficients entiers était considéré : l'estimation donnée dans l'énoncé principal (proposition 1.1) de [6] n'est pas correcte, et tous les énoncés qui le suivent doivent être modifiés en conséquence.

L'ingrédient qui permet de travailler avec des polynômes à coefficients complexes est la donnée d'une procédure permettant, à partir d'un ensemble fini $A \subset \mathbb{C}$ de nombres complexes et d'un entier naturel m de fournir une borne inférieure $\lambda(A, m) > 0$ des valeurs absolues des nombres non nuls obtenus à partir de A en itérant m fois l'opération qui consiste à ajouter à A l'ensemble des nombres obtenus par addition, soustraction et multiplication des éléments de A.

On trouve dans [2] et [3] des résultats dans la même direction et souvent plus ambitieux que ceux de ce travail. Cependant, nos résultats sont tout à fait explicites et peuvent en principe être utilisés directement pour faire des calculs, bien que les nombres avec lesquels on est amené à travailler peuvent devenir excessivement grand lorsque le degré des polynômes et le nombre de variables augmente.

Dans [4], on utilise le résultant de 2 polynômes à une variable pour obtenir toutes sortes d'estimations sur les racines, même multiples, d'un polynôme.

1. Élimination effective.

Le lemme suivant est bien connu (voir A.L. Cauchy, Œuvres Complètes, Série II, tome IX, De Bure Frères, Paris, (1829), page 122) :

1.1. LEMME. — *Soit* $P(Y) = \sum_{i=0}^{d} a_i Y^i$, $a_i \in \mathbb{C}$ *un polynôme non identiquement nul et posons :*

$$m = \inf\{|a_i|\,,\ i = 0 \dots d,\ a_i \neq 0\}\,, \quad M = \sup\{|a_i|\,,\ i = 0 \dots d\}\,.$$

Si $\alpha \in \mathbb{C}$ *est tel que* $\alpha \neq 0$ *et* $P(\alpha) = 0$ *on a :*

$$\frac{m}{m+M} < |\alpha| < \frac{m+M}{m}\,.$$

Preuve. — Quitte à diviser P par m on peut supposer que $m = 1$. Si $P(Y) = Y^h \cdot Q(Y)$, avec $Q(0) \neq 0$, on peut remplacer P par Q. On peut donc supposer que $a_0 \neq 0$, $a_d \neq 0$ et $a_i \neq 0 \Rightarrow 1 \leq |a_i| \leq M$. Si $|\alpha| < 1$, évidemment $|\alpha| < 1 + M$ et d'autre part :

$$0 = |P(\alpha)| = \Big|a_0 + \sum_{1}^{d} a_i\,\alpha^i\Big| \geq |a_0| - \sum_{1}^{d} |a_i|\,|\alpha|^i$$

$$> 1 - M \sum_{1}^{\infty} |\alpha|^i = 1 - M\,\frac{|\alpha|}{1-|\alpha|}$$

d'où l'on tire que $|\alpha| > \dfrac{1}{1+M}$. Si $|\alpha| > 1$ on applique ce qui précède à $Q(Y) = Y^d \cdot P\left(\dfrac{1}{Y}\right)$ et $\dfrac{1}{\alpha}$. Si $|\alpha| = 1$ les inégalités énoncées sont évidentes.

□

DÉFINITION. — *Soient* $A \subset \mathbb{C}$ *un sous-ensemble fini et* $m > 0$ *un entier naturel. Définissons le sous-ensemble* $\Lambda(A, m)$, $m \geq 1$, *par induction sur* m *:*

$$\Lambda(A, 1) = A$$

$$\Lambda(A, m) = \Lambda(A, m-1) \cup \{x + a \mid x\,,\ a \in \Lambda(A, m-1)\}$$
$$\cup \{x - a \mid x\,,\ a \in \Lambda(A, m-1)\} \cup \{x \cdot a \mid x\,,\ a \in \Lambda(A, m-1)\}\,.$$

On pose

$$\lambda(A) = \begin{cases} \inf\{|a| \mid a \in A\,,\ a \neq 0\} & \text{si } A \cap (\mathbb{C} \setminus \{0\}) \neq \varnothing \\ 0 & \text{sinon} \end{cases}$$

et

$$\lambda(A, m) = \lambda(\Lambda(A, m))\,.$$

Si $P(X) = \sum_{\alpha \in S} a_\alpha X^\alpha \in \mathbb{C}[X_1, \ldots, X_n]$, on pose $A(P) = \{a_\alpha\,,\ \alpha \in S\}$ et $\Lambda(P, m) = \Lambda(A(P), m)$. Si $P_1(X), \ldots, P_n(X) \in \mathbb{C}[X_1, \ldots, X_n]$, on pose :

$$A(P_1, \ldots, P_n) = \bigcup_{i=1}^{n} A(P_i) \quad , \quad \Lambda(P_1, \ldots, P_n, m) = \Lambda(A(P_1, \ldots, P_n), m)$$
$$\lambda(P_1, \ldots, P_n, m) = \lambda(\Lambda(P_1, \ldots, P_n, m))\,.$$

□

Notons que si les P_i sont à coefficients entiers, on a $\lambda(P_1, \ldots, P_n) \geq 1$.

Soit $P(X_1, \ldots, X_n) = \sum_{\alpha \in S} a_\alpha X^\alpha$; on pose :

$$H(P) = \sup\{|a_\alpha|\ ,\ \alpha \in S\}\,.$$

1.2. Lemme. — *Soient* $P_i(Y) = \sum_{h=0\ldots q} a_h^i Y^h$, $i = 1 \ldots k$ *des polynômes de degré au plus* q *en une variable* Y *à coefficients dans* $\mathbb{C}$ *et supposons que* $|a_h^i| \leq H$, $\forall i, h$, *avec* $H \geq 1$. *Alors on a :*

(1) $H(P_1(Y) + \cdots + P_k(Y)) \leq kH$

(2) $H(P_1(Y) \cdot \ldots \cdot P_k(Y)) \leq (q+1)^{k-1} H^k$

(3) $A(P_1 + \cdots + P_k) \subset A(P_1, \ldots, P_k, k)$

(4) $A(P_1 \cdot \ldots \cdot P_k) \subset A\big(P_1, \ldots, P_k, k + (1+q)^{k-1}\big)$.

Preuve. — Les inégalités et inclusions énoncées suivent facilement des deux égalités suivantes :

$$P_1 + \cdots + P_k = \sum_{i=0}^{q} \left(\sum_{h=0}^{k} a_h^i \right) Y^h$$

$$\text{et} \quad P_1 \cdot \ldots \cdot P_k = \sum_{h=0}^{kq} \Big(\sum_{\substack{i_1 = 0 \ldots q, \ldots, i_k = 0 \ldots q \\ i_1 + \cdots + i_k = h}} a_{i_1}^1 \cdots a_{i_k}^k \Big) Y^h.$$

□

Nous reprenons quelques notations de [5]. Soient n, k et $d_1, \ldots, d_k$ des entiers naturels. On pose :

$$N(n, d_1, \ldots, d_k) = \min\Big\{ s \;\Big|\; \forall f_1, \ldots, f_k \in \mathbb{C}[X_1, \ldots, X_n] \text{ avec degré} f_i = d_i,\ i = 1, \ldots, k, \text{ les } f_i \text{ étant sans zéros communs dans } \mathbb{C}^n, \text{ il existe } g_1, \ldots, g_k \in \mathbb{C}[X_1, \ldots, X_n] \text{ avec degré}(f_i \cdot g_i) \leq s \text{ et } \sum_{i=1}^{k} f_i \cdot g_i = 1 \Big\}.$$

On montre dans [5] que si $d_1 \geq \ldots \geq d_k$ et $d_i \neq 2$, $i = 1, \ldots, k$, alors

$$N(n, d_1, \ldots, d_k) = \begin{cases} d_1 \cdot \ldots \cdot d_k & \text{si } k \leq n \\ d_1 \cdot \ldots \cdot d_{k-1} \cdot d_n & \text{si } k > n \\ d_1 + d_k - 1 & \text{si } k > n = 1 \end{cases}$$

le cas $n = 1$ étant élémentaire. Dans [1] on montre sans hypothèse sur les d_i que si les $f_i \in \mathbb{C}[X_1, \ldots, X_n]$, $i = 1, \ldots, n$ sont sans zéros communs, alors il existe g_i, $i = 1, \ldots, n$, tels que $\sum_{i=1}^{n} f_i g_i = 1$ avec

$$\text{degré}(g_i) \leq n \cdot \min(k, n) \cdot D^{\min(k,n)} + \min(k, n) \cdot D$$

où $D = \max\{d_1, \ldots, d_k\}$, et donc dans tous les cas

$$N(n, d_1, \ldots, d_k) \leq n \cdot \min(k, n) \cdot D^{\min(k,n)} + (\min(k, n) + 1) \cdot D.$$

THÉORÈME I. — *Soient $F_1, \ldots, F_k \in \mathbb{C}[X_1, \ldots, X_n, Y]$ des polynômes de degré respectivement $d_1, \ldots, d_k$ en $(X_1, \ldots, X_n)$ et de degré au plus q en Y. Si on écrit $F_i(X) = \sum_{\alpha \in S_i} a_\alpha^i (X, Y)^\alpha$, avec $S_i \subset \mathbb{N}^{n+1}$, on suppose que $\forall \alpha \in S_i, i = 1, \ldots, k$, $|a_\alpha^i| \leq H$, où $H \geq 1$. Supposons que l'ensemble*

$$Z_Y = \Big\{ y \in \mathbb{C} \;\Big|\; \exists x_1, \ldots, x_n \in \mathbb{C} \text{ t.q. } F_i(x_1, \ldots, x_n, y) = 0,\ i = 1 \ldots p \Big\}$$

consiste en un nombre fini de points. Alors si $y \in Z_Y$ et $y \neq 0$, on a :

$$\frac{\lambda}{\lambda + N!(q+1)^N H^N} < |y| < \frac{\lambda + N!(q+1)^N H^N}{\lambda}$$

où $N = N(n, d_1, , \ldots, d_k)$
et $\lambda = \lambda\left(\{a_\alpha^i,\ \alpha \in S^i,\ i = 1, \ldots, p\}, N + N! + (1+q)^{N-1}\right)$.

Preuve. — Soit $V_m = \mathbb{C}[X_1, \ldots, X_n]_{\leq m}$ l'espace des polynômes de degré $\leq m$ en $X_1, \ldots, X_n$; on le munit de la base $\{X^\alpha\}_{|\alpha| \leq m}$. Pour tout $y \in \mathbb{C}$ définissons l'application linéaire

$$\Phi(y) : V_{N-d_1} \oplus \cdots \oplus V_{N-d_k} \to V_N,$$

$$\Phi(y)(g_1(X), \ldots, g_k(X)) = \sum_{i=1}^{k} g_i(X) F_i(X, y).$$

Cela définit une application polynomiale

$$\Phi : \mathbb{C} \to \mathrm{Hom}\,(V_{N-d_1} \oplus \cdots \oplus V_{N-d_k}, V_N)$$

où $\mathrm{Hom}(V, W)$ désigne l'espace des applications linéaires de V dans W. Il résulte du Nullstellensatz et de la définition de N que

$$y \in Z_Y \iff 1 \in \mathrm{Im}(\Phi(y)).$$

Soit $\rho = \sup\{\mathrm{rang}(\Phi(y)),\, y \in \mathbb{C}\}$ et $\Sigma = \{y \in \mathbb{C} \mid \mathrm{rang}(\Phi(y)) < \rho\}$. Si $y \in \mathbb{C} \setminus \Sigma$ le rang de $\Phi(y')$ est égal à ρ pour y' dans un voisinage de y, et il existe donc un voisinage de y sur lequel $\mathrm{Im}(\Phi)$ varie continûment. Si on avait $y \in Z_Y$, on aurait aussi $y' \in Z_Y$ pour y' dans un voisinage de y, ce qui est contraire à l'hypothèse que Z_Y est un ensemble fini. On a donc :

$$Z_Y \subset \Sigma.$$

Il existe alors un mineur $M(Y)$ d'ordre $\rho \leq N$ de la matrice de Φ qui n'est pas identiquement nul et qui s'annule sur Z_Y.

Nous allons estimer les coefficients de $M(Y)$ pour lui appliquer le lemme 1.1 afin d'établir les inégalités énoncées. Ecrivons :

$$F_i(X_1, \ldots, X_n, Y) = \sum_{\alpha \in S_i'} b_\alpha^i(Y) X^\alpha$$

où $S_i' \subset \mathbb{N}^n$ et $b_\alpha^i \in \mathbb{C}[Y]$, de degré au plus q. Soit $\nu_{\beta,(\alpha,i)}(Y)$ le coefficient de Φ correspondant aux éléments de la base $X^\alpha \in V_{N-d_i}$ et $X^\beta \in V_N$; on a :

$$\nu_{\beta,(\alpha,i)}(Y) = \begin{cases} b_{\beta-\alpha}^i(Y) & \text{si } \beta - \alpha \in S_i' \\ 0 & \text{sinon.} \end{cases}$$

Donc $M(Y)$ est la somme d'au plus $N!$ termes de la forme :

$$\pm \prod_{h=1,\ldots,\rho} b_{\alpha_h}^{i_h}(Y)$$

et avec le lemme 1.2 on voit que

$$H(M(Y)) \leq N!(q+1)^{N-1}H^N$$
$$\text{et } A(M(Y)) \subset \Lambda\left(\{a_\alpha^i,\ \alpha \in S_i,\ i=1,\ldots,n\},\ N+N!+(1+q)^{N-1}\right).$$

Les inégalités énoncées suivent du lemme 1.1 appliqué à $M(Y)$. □

1.3 COROLLAIRE. — *Soit $P(X) \in \mathbb{C}[X_1,\ldots,X_n]$ un polynôme de degré $d \geq 2$. Soit c une valeur critique de P, $c \neq 0$. Alors :*

$$\frac{\lambda}{\lambda + N!2^{N-1}(dH)^N} < |c| < \frac{\lambda + N!2^{N-1}(dH)^N}{\lambda}$$

où $N = N(n, d, \underbrace{d-1,\ldots,d-1}_{n})$, $H = H(P)$

et $\lambda = \lambda\left(\left\{Y - P(X), \frac{\partial P}{\partial X_i}, i = 1,,\ldots,,n\right\}, N + N! + 2^{N-1}\right)$.

Preuve. — On considère le système d'équations :

$$Y - P(X) = 0, \quad \frac{\partial P}{\partial X_i}(X) = 0,\ i = 1\ldots n.$$

Comme l'on sait qu'il n'y a qu'un nombre fini de valeurs critiques, on peut appliquer le théorème I, avec les substitutions $H \to dH$ et $q = 1$. □

On pose

$$\mu(n,d,H) = N!2^{N-1}(dH)^N \quad \text{et} \quad \kappa(P) = \frac{\lambda}{\lambda + \mu(P)}.$$

2. Application aux inéquations polynomiales.

2.1. LEMME. — *Soit $P(X) = \sum_{\alpha \in S} a_\alpha X^\alpha \in \mathbb{R}[X_1,\ldots,X_n]$, avec $|a_\alpha| \leq H$, $\#S \leq s$. Soit $b \in \mathbb{R}^n$ tel que $P(b) > 0$, $R = \sup\{1, \|b\|\}$, et soit $v \in \mathbb{R}^n$, $\|v\| = \varepsilon R$, $0 < \varepsilon \leq 1$. Alors on a :*

$$\varepsilon < \frac{P(b)}{dsHR^d 2^{d-1}} \quad \Rightarrow \quad P(b+v) > 0.$$

Preuve.

$$|P(b+v)-P(b)| = \Big|\sum_{\substack{\alpha\in S\\ \beta<\alpha}} a_\alpha \binom{\alpha}{\beta} b^\beta v^{\alpha-\beta}\Big| \le H\Big|\sum_{\substack{\alpha\in S\\ \beta<\alpha}} \binom{\alpha}{\beta} R^{|\beta|}R^{|\alpha-\beta|}\varepsilon^{\alpha-\beta}\Big|$$
$$= H\sum_{\alpha\in S} R^{|\alpha|}\left((1+\varepsilon)^{|\alpha|}-1\right) \le sHR^d\left((1+\varepsilon)^d-1\right)$$
$$\le sHR^d d(1+\varepsilon)^{d-1}\varepsilon \le sHR^d d\,2^{d-1}\varepsilon$$

où l'avant-dernière inégalité est une conséquence du théorème des accroissements finis. De là le résultat suit immédiatement. □

2.2. PROPOSITION. — *Soit* $P(X) \in \mathbb{R}[X_1,\dots,X_n]$ *de degré* $d \ge 2$, $P(X) = \sum_{\alpha\in S} a_\alpha X^\alpha$, $\#S \le s$ *et soit* $R \in \mathbb{N} - \{0\}$. *Alors si* $a \in \Omega_R^+$, $\exists b \in \Omega_R^+$ *dans la même composante connexe de* Ω_R^+ *que* a *tel que*

$$P(b) \ge \frac{\lambda}{\lambda + \mu(n,d,sR^dH)}$$

où $\lambda = \lambda\left(\{1\}\cup\{\pm a_\alpha R^h \mid \alpha\in S,\, h=0,\dots,d\}, s+d+N+N!+2^{N-1}\right)$, $N = N(n,d,\underbrace{d,d-1,\dots,d-1}_{n})$.

Preuve. — Soit $k \in \{1,\dots,n\}$ et $j = \{j_1 < \dots < j_k\} \subset \{1,\dots,n\}$, $\varepsilon = (\varepsilon_1,\dots,\varepsilon_n)$, $\varepsilon_h \in \{-1,+1\}$. Soit $P_{j,\varepsilon}$ le polynôme à $n-k$ variables obtenu en remplaçant X_h par $\varepsilon_h R^h$ dans $P(X)$. On remarque que $H(P_{j,\varepsilon}) \le sR^dH(P)$ et que les coefficients des polynômes $Y - P_{j,\varepsilon}(X)$, $\frac{\partial P_{j,\varepsilon}}{X_i}$ appartiennent à $\Lambda\left(\{1\}\cup\{\pm a_\alpha R^h \mid \alpha\in S, h=0,\dots,d\}, s+d\right)$. Soit Ω_a la composante connexe de a dans Ω_R^+ et soit $b \in \Omega_a$ tel que $P(b) = \sup\{P(x), x\in\Omega_a\}$. Si $\exists j_1,\dots,j_k \in \{1,\dots,n\}$ tels que $|b_j| = R \Leftrightarrow j \in \{j_1,\dots,j_k\}$ avec $k<n$, alors $P(b)$ est une valeur critique d'un $P_{j,\varepsilon}$ et on applique le corollaire 1.3. Sinon $P(b) \in \Lambda\left(\{\pm a_\alpha R^h \mid \alpha\in S, h=0\dots d\}, s\right)$ et donc $P(b) \ge \lambda > \frac{\lambda}{\lambda+\mu}$. □

THÉORÈME II. — *Soit* $P(X) = \sum_{\alpha\in S} a_\alpha X^\alpha \in \mathbb{R}[X_1,\dots,X_n]$, $|a_\alpha| \le H$, *pour tout* $\alpha\in S$ *et* $\#S \le s$. *S'il existe* $a\in\mathbb{R}^n$, $\|a\| \le R$, *où* R *est un entier positif, tel que* $P(a) > 0$, *alors il existe* b *dans la même composante connexe de* Ω_R^+ *que* a *tel que :*

$$\left\{x\in\mathbb{R}^n \;\middle|\; \|x\| \le R,\ \|x-b\| < \rho\right\} \subset \Omega_R^+$$

où

$$\rho = \frac{1}{dsHR^d 2^{d-1}} \cdot \frac{\lambda}{\lambda + \mu(n, d, sR^d H)}$$

avec $\lambda = \lambda\left(\{1\} \cup \{\pm a_\alpha R^h \mid \alpha \in S,\ h = 0 \dots d\}, s + d + N + N! + 2^{N-1}\right)$, $N = N(n, d, \underbrace{d, d-1, \dots, d-1}_{n})$.

2.3. COROLLAIRE. — *Sous les hypothèses du théorème II, dans toute composante connexe de* Ω_R^+ *il y a un point* a *de la forme* $a = (a_1, \dots, a_n)$, *avec* $a_i = \dfrac{k_i}{T}$, $k_i \in \mathbb{Z}$ *et* $T = \left[\dfrac{1}{\rho}\right] + 1$, *où* [ ] *désigne la partie entière.*

Ce théorème et son corollaire sont des conséquences immédiates de la proposition 2.2 et du lemme 2.1.

Nous allons montrer maintenant que la recherche des solutions d'une inéquation polynomiale dans $\mathbb{R}^n$ tout entier se ramène à la recherche de solutions dans un cube de côté R, pour un R qui sera donné explicitement.

2.4. PROPOSITION. — *Soit* $P(X) \in \mathbb{R}[X_1, \dots, X_n]$ *un polynôme pour lequel* $0 \in \mathbb{C}$ *est une valeur régulière du complexifié (i.e. :* $P(x) = 0$, $x \in \mathbb{C}^n \Rightarrow dP_x \neq 0$*). Soit*

$$\Omega^+(P) = \left\{x \in \mathbb{R}^n \mid P(x) > 0\right\}.$$

Alors si

$$R \geq \frac{\lambda + N! 3^{N-1} (dH)^N}{\lambda}$$

où $\lambda = \lambda\left(\{1, -1\} \cup A(P) \cup A\left(\dfrac{\partial P}{\partial X_i}\right), N + N! + 3^{N-1}\right)$, $N = N(n + 1, d, \underbrace{d-1, \dots, d-1}_{n}, 2)$, *l'inclusion* $\Omega_R^+ \subset \Omega^+(P)$ *induit une bijection sur les composantes connexes.*

Preuve. — Considérons le système de $n + 2$ équations :

$$P(x) = 0 \quad , \quad \frac{\partial P}{\partial X_i} - z\, x_i = 0\,,\ i = 1 \dots n, \quad \sum x_i^2 - r^2 = 0.$$

Si (x, z, r) est une solution, avec $r > 0$, alors la sphère centrée à l'origine de rayon r est tangente en x à l'hypersurface $P^{-1}(0)$. Comme $P^{-1}(0)$ est non singulière, il n'y a qu'un nombre fini de telles sphères. On peut donc appliquer le théorème I à ce système d'équations, avec les substitutions

$Y \to r$, $H \to dH$, $q \to 2$, $k \to n+2$, $n \to n+1$, $d_1 \to d$, $d_2, , \ldots, d_{n+1} \to d$, $d_{n+2} \to 2$. Il s'ensuit que si R satisfait l'inégalité de l'énoncé, toute sphère de rayon $r \geq R$ est transverse à $P^{-1}(0)$. On en déduit facilement le résultat.

□

Notons que pour la proposition précédente il aurait suffit de supposer que les singularités de $P^{-1}(0)$ soient isolées.

Rappelons que $\kappa(P)$ désigne la borne inférieure des valeurs absolues des valeurs critiques non nulles de P donnée par le corollaire 1.3.

THÉORÈME III. — *Soit* $P(X) \in \mathbb{R}[X_1, \ldots, X_n]$ *et supposons que :*

$$R > \frac{\tilde{\lambda} + N! 3^{N-1} (d\tilde{H})^N}{\tilde{\lambda}}$$

où $\tilde{H} = \dfrac{1}{\kappa(P)} \cdot H(P) + 1$, $N = N(n+1, d, \underbrace{d-1, \ldots, d-1}_{n}, 2)$, $\tilde{\lambda} = \lambda\left(\{1, -1\} \cup A(Q) \cup A\left(\dfrac{\partial Q}{\partial X_i}\right), N + N! + 3^{N-1}\right)$, *avec* $Q(X) = \dfrac{1}{\kappa(P)} \cdot P(X) - 1$. *Alors toute composante connexe de* $\Omega^+(P)$ *rencontre* $\Omega_R^+(P)$ *; de plus, si* $a, b \in \Omega_R^+(P)$, *alors ils sont dans une même composante de* $\Omega^+(P)$ *si et seulement si ils sont dans une même composante de* $\Omega_R^+(P)$.

Preuve. — Nous allons passer de P à un polynôme Q dont $0 \in \mathbb{C}$ est une valeur régulière, auquel on appliquera la proposition 2.4.

Si $a \in \Omega^+(P)$, soit $\eta = \inf\left\{\dfrac{1}{2} P(a), \kappa(P)\right\}$ et posons $P_\eta(X) = \dfrac{1}{\eta} P(X) - 1$. Alors $a \in \Omega^+(P_\eta)$, et $0 \in \mathbb{C}$ est une valeur régulière de P_η. Remarquons que si $n' \leq n$, alors $\mu(n', d, H) \leq \mu(n, d, H)$; il s'ensuit que $0 \in \mathbb{C}$ est aussi une valeur régulière de la partie homogène de degré maximum de P_η. Pour $t \in [\dfrac{1}{\kappa(P)}, \dfrac{1}{\eta}]$, le polynôme $P_t(X) = tP(X) - 1$, ainsi que sa partie homogène de degré maximum, admettent $0 \in \mathbb{C}$ comme valeur régulière. Puisque $Q(X) = P_1(X)$, l'inclusion $\Omega^+(Q) \subset \Omega^+(P_\eta)$ est une équivalence d'homotopie. On a que $H(Q) \leq \dfrac{1}{\kappa(P)} H(P) + 1$ et le résultat suit alors de la proposition 2.4. □

THÉORÈME IV. — *Soit* $P(X) \in \mathbb{R}[X_1, \ldots, X_n]$ *et soit* R *satisfaisant l'inégalité du théorème III. Soient* a, b *des sommets d'un maillage de taille*

ε_0 du cube de demi-côté R centré en 0. Alors si a et b sont dans $\Omega^+(P)$, ils sont dans la même composante connexe si et seulement si on peut les joindre par un chemin dans $\Omega_R^+(P)$ constitué d'arêtes du maillage, pourvu que

$$\varepsilon_0 \leq \frac{\tilde{\lambda}}{\tilde{\lambda} + N!2^{N-1}\tilde{H}^n}$$

où $\tilde{H} = \frac{1}{\kappa(P)} \cdot d \cdot H(P) + 2$, $N = N(2n+2, d, d, \underbrace{d-1, \ldots, d-1}_{2n}, 2)$, $Q(X) = \frac{1}{\kappa(P)} \cdot P(X) - 1$ *et* $\tilde{\lambda} = \lambda\left(\{\pm 1, \pm 2\} \cup A(Q) \cup A\left(\frac{\partial Q}{\partial X_i}\right), N + N! + 2^{N-1}\right)$.

Preuve. — On considère le système d'équations :

$$Q(x) = 0, \quad Q(y) = 0, \quad z_1 dQ_x - (x - y) = 0,$$
$$z_2 dQ_y - (x - y) = 0, \quad \varepsilon - \sum_{i=1}^{n} (x_i - y_i)^2 = 0$$

où dQ_x désigne le gradient de Q en x. Il y a $2n + 3$ équations et autant d'inconnues : $x, y \in \mathbb{R}^n$, z_1 , z_2 , $\varepsilon \in \mathbb{R}$. Si $Q(x) = Q(y) = 0$, $x \neq y$ et la distance de x à y est extrémale, alors il existe $\varepsilon > 0$ et z_1, z_2 tels que $(x, y, z_1, z_2, \varepsilon)$ est solution du système d'équations. Il suffit donc d'appliquer le théorème I avec les substitutions $Y \to \varepsilon$, $k \to 2n+3$, $n \to 2n+2$, $H \to \tilde{H}$, $q \to 1$, $d_1, d_2 \to d$, $d_3, \ldots, d_{2n+2} \to d - 1$, $d_{2n+3} \to 2$. □

3. Isolation et approximation des racines d'un polynôme réel.

Dans tout ce paragraphe, on utilisera les notations suivantes :

$P(t) = \sum_{i \in S} a_i t^i$, $a_i \in \mathbb{R}$, d = degré de $P(t)$, $\#S \leq s$, $|a_i| \leq H$, $H \geq 1$

$R \in \mathbb{R}^+$ un nombre tel que $R \geq 1$ et $P(\alpha) = 0 \Rightarrow |\alpha| \leq R$

$\kappa = \kappa(P) = \frac{\lambda}{\lambda + N!2^{N-1}(dH)^N}$,

où $N = 2d - 2$, $\lambda = \lambda\left(\{Y - P(t), P'(t)\}, N + N! + 2^{N-1}\right)$ désigne la borne inférieure de la valeur absolue de la plus petite valeur critique non nulle de $P(t)$ donnée par le corollaire 1.3.

3.1. LEMME. — *Si* $P(t_0) = 0$ *alors*

$$|t| \leq R \text{ et } |t - t_0| \leq r \Rightarrow |P(t)| \leq dHsR^d r.$$

Preuve.

$$|P'(t)| = \left| \sum_{i \in S} i a_i t^i \right| \leq dHsR^d.$$

Par le théorème des accroissements finis :

$$|P(t)| = |P(t) - P(t_0)| \leq \sup \{|P'(\theta)| \mid 0 \leq \theta \leq 1\} \cdot |t - t_0| \leq dHsR^d r.$$

□

THÉORÈME V. — *Si* $r > 0$ *satisfait l'inégalité :*

$$r \leq \frac{\kappa}{dHsR^d}$$

alors si α, β *sont des racines distinctes de* $P(t)$ *on a :*

$$|\alpha - \beta| > r.$$

Preuve. — On peut supposer que $\alpha < \beta$ et qu'il n'y a pas d'autre racine de $P(t)$ entre α et β. Puisque $P(\alpha) = P(\beta) = 0$ il doit exister $\gamma \in]\alpha, \beta[$ tel que $P'(\gamma) = 0$, et donc $P(\gamma)$ est une valeur critique (non nulle puisqu'il P n'a pas de racine dans $]\alpha, \beta[$) de $P(t)$. Si $|\alpha - \beta| \leq r$, alors par le lemme 3.1 :

$$|P(\gamma)| \leq dHsR^d r \leq \kappa$$

ce qui est impossible. □

Remarque. — Une estimation semblable peut être déduite de [4], corollaire du théorème 7'.

La proposition suivante va nous permettre de construire un algorithme pour isoler et approcher les racines de $P(t)$.

3.2. PROPOSITION. — *Soit* $n \in \mathbb{N}$ *vérifiant :*

$$n \geq \frac{dHsR^d}{\kappa} R \quad , \text{ i.e. : } \frac{R}{n} \leq \frac{\kappa}{dHsR^d}$$

et soit $\left\{ x_i = i\frac{R}{n}\,,\ i = -n, \ldots, n \right\}$ *le partage de* $[-R, R]$ *en* $2n$ *intervalles de longeur* $\frac{R}{n}$. *Alors :*

i) *tout intervalle* $[x_i, x_{i+1}]$ *contient au plus une racine.*

ii) *si* $P(x_i) > 0$ *et* $P(x_{i+1}) < 0$, *ou bien* $P(x_i) < 0$ *et* $P(x_{i+1}) > 0$, *alors* $[x_i, x_{i+1}]$ *contient exactement une racine.*

iii) *si* $|P(x_i)| \leq \kappa$ *et*

$$P(x_i)\,,\ P(x_{i+1}) > 0\,,\ P'(x_i) < 0\,,\ P'(x_{i+1}) > 0$$

ou bien

$$P(x_i)\,,\ P(x_{i+1}) < 0\,,\ P'(x_i) > 0\,,\ P'(x_{i+1}) < 0$$

l'intervalle $[x_i, x_{i+1}]$ *contient exactement une racine.*

iv) *Si* $\alpha \in [-R, R]$ *est une racine de* $P(t)$, *ou bien* $\exists i$ *tel que* $\alpha = x_i$, *ou bien* α *appartient à un intervalle satisfaisant ii) ou iii).*

Preuve. — i) suit du théorème V et ii) du théorème de Bolzano-Weierstrass.

iii) : On se place dans le cas $P(x_i) > 0$. La dérivée de $P(t)$ doit s'annuler dans $]x_i, x_{i+1}[$; soit $\alpha \in]x_i, x_{i+1}[$ la plus petite racine de $P'(t)$ dans cet intervalle. Alors $P(\alpha) \geq 0$ (sans quoi il y aurait une racine de $P'(t)$ plus petite que α dans l'intervalle) et $P(\alpha)$ est une valeur critique de $P(t)$. Puisque $P'(x_i) > 0$, il résulte du lemme 3.1 que :

$$P(\alpha) < P(x_i) \leq \kappa$$

et donc $P(\alpha) = 0$.

iv) Si $\alpha \in [-R, R]$ est une racine de $P(t)$, supposons que l'on ne soit ni dans le cas ii) ni dans le cas où $\exists i$ tel que $\alpha = x_i$. Il existe $i \in [-n, n-1]$ tel que $\alpha \in]x_i, x_{i+1}[$ et on peut supposer sans perte de généralité que $P(x_i) > 0$, et donc $P(x_{i+1}) > 0$ puisqu'on n'est pas dans le cas ii). Si $x \in [x_i, x_{i+1}]$, on a, d'après le lemme 3.1. :

$$|P(x)| \leq dHsR^d \frac{R}{n} \leq \kappa$$

donc $P(x)$ ne peut être une valeur critique non nulle de $P(t)$. Puisque α est l'unique racine de P dans $[x_i, x_{i+1}]$, il s'ensuit que α est l'unique racine

aussi de $P'(t)$ dans cet intervalle. Donc $P(t)$ décroît de x_i à α, puis croît de α à x_{i+1}, et alors $P'(x_i) < 0$, $P'(x_{i+1}) > 0$. □

Le lemme suivant est une reformulation du lemme 3.1 :

3.3. LEMME. — *Si*

$$(\#) \qquad |P(t_0)| > dHsR^d r$$

alors $P(t) \neq 0$, $\forall t$ *tel que* $|t - t_0| \leq r$. □

Nous dirons que la condition $\sigma(t_0, r)$ est satisfaite si $\#$ est vraie; on dira qu'un intervalle $[a, b]$ satisfait σ si $\sigma(a, b-a)$ ou $\sigma(b, b-a)$ est satisfaite.

Algorithme d'isolation et approximation des racines. On commence par prendre R tel que toute racine de $P(t)$ soit dans $[-R, R]$ (par exemple en utilisant le lemme 1.1).

Si $\sigma(-R, 2R)$ ou $\sigma(R, 2R)$ sont satisfaites, on termine : il n'y a pas de racine. Sinon on partage $[-R, R]$ en 2 intervalles égaux.

A la n-ième étape on aura partagé $[-R, R]$ en un certain nombre d'intervalles dont les extrémités sont de la forme $iR/2^n$, $i \in [-2^n, 2^n]$. Certains intervalles satisfont la condition σ; les autres seront de longueur $R/2^n$. On partage ces derniers en 2 et l'on teste avec σ, jusqu'à ce que :

$$2^n \geq \frac{dHsR^{d+1}}{\kappa}.$$

A ce stade, on teste les intervalles restant avec la proposition 3.2 pour voir s'ils contiennent une (et alors une seule) racine. On peut continuer à subdiviser et tester avec 3.2 jusqu'à obtenir une précision voulue.

BIBLIOGRAPHIE

[1] W.D. BROWNAWELL, Bounds for the degrees in the Nullstellensatz, Ann. of Math., 126 (1987), 577–591.

[2] J. HEINTZ, M.-F. ROY, P. SOLERNÓ, Sur la complexité du principe de Tarsky-Seidenberg, Bulletin de la Société Mathématique de France, 118 (1990), 101–126.

[3] D. Yu GRIGOR'EV and N.N. VOROBJOV (Jr), Solving Systems of Polynomial Inequalities in Subexponential Time, J. Symbolic Computation, 5 (1988), 37–64.

[4] R. GÜTING, Polynomials with multiple zeros, Mathematika, 14 (1967), 181–196.

[5] J. KOLLÁR, Sharp effective Nullstellensatz, Journal of the American Math. Soc., 1 (1988), 963–975.

[6] F. RONGA, Recherche de solutions d'inéquations polynomiales, Astérisque, 192 (1990), 11–16.

Manuscrit reçu le 17 octobre 1994.

Felice RONGA,
Section de Mathématiques
Université de Genève
C.P. 240
CH-1211 Genève 24.
E-mail address : Ronga@ibm.unige.ch