Astérisque

FELICE RONGA

Recherche de solutions d'inéquations polynomiales

Astérisque, tome 192 (1990), p. 11-16

<http://www.numdam.org/item?id=AST_1990__192__11_0>

Recherche de solutions d'inéquations polynomiales

FELICE RONGA

Soit $P(X) \in \mathbf{Z}[X_1, \ldots, X_n]$ un polynôme à coefficients entiers de degré d, R un entier positif et soit $\Omega_R^+(P) = \{x \in \mathbf{R}^n | P(x) > 0, \|x\| \leq R\}$, où sur $\mathbf{R}^n$ l'on prend la norme $\|x\| = sup\{|x_i|, i = 1 \ldots n\}$. Si $P(X) = \sum_{\alpha \in S} a_\alpha X^\alpha$, supposons que $|a_\alpha| \leq H$, $\alpha \in S$ et que $\#S \leq N$. Nous allons montrer que toute solution de l'inéquation $P(x) > 0$ avec $\|x\| \leq R$ est dans la même composante qu'une solution qui appartient au sommets du maillage obtenu en partageant les cotés du cube $\{x | \|x\| < R\}$ en T parties, où T est un entier qui dépend de n, d, N, et H et qui sera donné explicitement (voir le corollaire du théorème I).

J'aimerais remercier le referee inconnu qui a relevé que les resultats de ce travail ne sont valables que si l'on travaille avec des polynômes à coefficients entiers, alors que dans des versions intermédiaires une partie des résultats étaient énoncés pour des polynômes à coefficients réels.

REMARQUES

1. Le cas de plusieurs inéquations se ramène à celui d'une seule. En effet, si $P_1(X), \ldots, P_n(X) \in \mathbf{Z}[X_1, \ldots, X_n]$ les composantes connexes de l'ensemble

$$\Omega_R^+(P_1, \ldots, P_k) = \{x \in \mathbf{R}^n | P_i(x) > 0, i = 1 \ldots k, \|x\| \leq R\}$$

sont parmi les composantes connexes de $\Omega_R^+(P)$, où $P = P_1 \cdot \ldots \cdot P_k$. Il suffit donc d'ecarter, parmi les solutions de $P(x) > 0$, celles pour lesquelles il existe i avec $P_i(x) < 0$.

2. Le théorème II nous dit que toute solution dans $\mathbf{R}^n$ tout entier de l'inéquation $P(x) > 0$ est dans la même composante connexe de $\{x | P(x) > 0\}$ qu'une solution se trouvant dans le cube centré à l'origine de demi-côté R, où $R = R(n, d, N, H)$ est donné explicitement.

3. Ainsi que le referee me l'a fait remarquer, des résultats analogues, bien que moins explicites, ont été obtenus dans [1].

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

LEMME 1. *Soit* $P(Y) = \sum_{i=0}^{d} a_i Y^i$, $a_i \in \mathbf{R}$ *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 $\alpha \in \mathbf{R}$ *est tel que* $\alpha \neq 0$ *et* $P(\alpha) = 0$ *on a:*

$$\frac{m}{m+M} \leq |\alpha| \leq \frac{m+M}{m}$$

Dans la suite nous travaillerons essentiellement avec des polynômes à coefficients entiers, car ainsi nous n'aurons pas à nous occuper de la borne inférieure de la valeur absolue des coefficients, qu'il serait trop compliqué d'estimer lors d'opérations d'addition et de multiplication. Pour la borne supérieure, le lemme suivant, dont la preuve est laissée au lecteur, sera utile dans la preuve de la proposition 1.1. Adoptons la notation suivante: si $P(X_1, \dots, X_n)$ désigne un polynôme à coefficients réels, $H(P)$ désignera le maximum des valeurs absolues de ses coefficients.

LEMME 2. *Soient* $P_i(Y) = \sum_{0 \leq h \leq q} a_h^i Y^h$, $i = 1 \dots k$ *des polynômes de degré au plus* q *à coefficients dans* $\mathbf{R}$ *et supposons que* $|a_h^i| \leq H$, $\forall i, h$. *Alors, si* $P(Y) = P_1(Y) \cdot \dots \cdot P_k(Y)$ *et* $Q(Y) = P_1(Y) + \dots + P_k(Y)$ *on a:*

$$H(P) \leq (q+1)^{k-1} M^k \quad , \quad H(Q) \leq kM \ .$$

LEMME 3. *Soit* $P(X) = \sum_{\alpha \in S} a_\alpha X^\alpha \in \mathbf{R}[X_1, \dots, X_n]$, *avec* $|a_\alpha| \leq H$, $\#S \leq N$. *Soit* $b \in \mathbf{R}^n$ *tel que* $P(b) > 0$, $R = sup\{1, \|b\|\}$, *et soit* $v \in \mathbf{R}^n$, $\|v\| = \varepsilon R$, $0 < \varepsilon \leq 1$. *Alors on a:*

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

PREUVE:

$$\begin{aligned} |P(b+v) - P(b)| &= \Big| \sum_{\substack{\alpha \in S \\ \beta < \alpha}} a_\alpha \binom{\alpha}{\beta} b^\beta v^{\alpha-\beta} \Big| \leq H \Big| \sum_{\substack{\alpha \in S \\ \beta < \alpha}} \binom{\alpha}{\beta} R^{|\beta|} R^{|\alpha-\beta|} \varepsilon^{\alpha-\beta} \Big| \\ &= H \sum_{\alpha \in S} R^{|\alpha|} \left((1+\varepsilon)^{|\alpha|} - \varepsilon^{|\alpha|} \right) \leq NHR^d \left((1+\varepsilon)^d - \varepsilon^d \right) \\ &\leq NHR^d d (1+\varepsilon)^{d-1} \varepsilon \leq NHR^d d 2^{d-1} \varepsilon \end{aligned}$$

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

PROPOSITION 1.1. *Soient* $F_1, \ldots, F_p \in \mathbf{Z}[X_1, \ldots, X_p]$ *des polynômes de degré respectivement* $m_1, \ldots, m_p$, $F_i(X) = \sum_{\alpha \in S_i} a_\alpha^i X^\alpha$, *avec* $|a_\alpha^i| \leq H$ *et* $\#S_i \leq N$, *et supposons que les* F_i *soient de degré au plus* q *en* X_p. *Soit*

$$\Sigma_p = \{x_p \in \mathbf{C} \mid \exists x_1, \ldots, x_{p-1} \in \mathbf{C} \text{ t.q. } F_i(x_1, \ldots, x_p) = 0,\ i = 1 \ldots p\}$$

et supposons que $\Sigma_p \neq \mathbf{C}$. *Alors si* $x_p \in \Sigma_p$ *et* $x_p \neq 0$, *on a:*

$$\frac{1}{1 + (q+1)^{\rho-1}(NH)^\rho \cdot \rho!} \leq |x_p| \leq 1 + (q+1)^{\rho-1}(NH)^\rho \cdot \rho! \quad \text{où} \quad \rho = \binom{\sum m_i}{p-1}$$

PREUVE: Soit $V_m = (\mathbf{Z}[X_p])[X_1, \ldots, X_{p-1}]_{\leq m}$ l'espace des polynômes de degré $\leq m$ en $X_1, \ldots, X_{p-1}$, à coefficients dans les polynômes en X_p. V_m est un $\mathbf{Z}[X_p]$–module libre avec base les X'^α, où $\alpha = (\alpha_1, \ldots, \alpha_{p-1})$, $|\alpha| \leq m$ et $X' = (X_1, \ldots, X_{p-1})$. Posons $D = 1 + \sum_{i=1}^p (m_i - 1)$ et considérons l'application $\mathbf{Z}[X_p]$–linéaire:

$$\phi : V_{D-m_1} \oplus \cdots \oplus V_{D-m_p} \to V_D \quad , \quad \phi(A_1, \ldots, A_p) = \sum A_i F_i \ .$$

On montre (voir [2] ou [3]) que:

$$rang(\phi) < dim(V_D) \iff \exists x^* = (x_0, \ldots, x_p) \subset \mathbf{C}^{n+1} - \{0\} \text{ t.q. } F_i^*(x^*) = 0,\ i = 1 \ldots p \ ,$$

où $F_i^*(X_0, \ldots, X_p)$ est l'homogénéisé de F_i, et on montre aussi que le diviseur commun des mineurs de rang maximal de ϕ est le résultant $R(X_p)$ de $F_1, \ldots, F_p$ par rapport à X_p. Puisque l'on a supposé que $\Sigma_p \neq \mathbf{C}$, il existe un mineur d'ordre maximal $\mu(X_p)$ de ϕ qui n'est pas identiquement nul, et qui s'annulle forcémment en x_p. On peut donc appliquer le lemme 1 à ce mineur, et pour cela nous allons estimer les coefficients de $\mu(X_p)$. Ecrivons: $F_i(X_1, \ldots, X_p) = \sum_{\alpha \in S_i'} b_\alpha^i(X_p) \cdot X'^\alpha$. Si $X'^\beta \in V_{m_i}$, on aura: $\phi(X'^\beta) = \sum_{\alpha \in S_i'} b_\alpha^i(X_p)\, X'^{\alpha+\beta}$ et si $\mu_{\gamma,(\beta,i)}(X_p)$ designe le coefficient de μ correspondant aux éléments de la base $X'^\beta \in V_{D-m_i}$ et $X'^\gamma \in V_D$:

$$\mu_{\gamma,(\beta,i)}(X_p) = \sum_{\substack{\alpha \in S_i' \\ \alpha+\beta=\gamma}} b_\alpha^i(X_p) \ ,$$

d'où l'on voit que les coefficients des puissances de X_p dans $\mu_{\alpha,\beta}(X_p)$ sont majorés par NH. Puisque $dim(V_D) = \binom{D+p-1}{p-1} = \binom{\sum m_i}{p-1} = \rho$, le mineur $\mu(X_p)$ est une somme de $\rho!$ termes de la forme:

$$\prod_{h=1\ldots\rho} \mu_{(\gamma_h,(\beta_h,i_h))}(X_p)$$

et les $\mu_{\gamma,(\beta,i)}(X_p)$ sont de degré au plus q. Donc, d'après le lemme 2 on a: $H(\mu(X_p)) \leq \rho!(q+1)^{\rho-1}(NH)^{\rho}$.

COROLLAIRE 1.2. *Soit $P(X) \in \mathbb{Z}[X_1,\ldots,X_n]$ un polynôme de degré d, $P(X) = \sum_{\alpha\in S} a_\alpha X^\alpha$, avec $|a_\alpha| \leq H$, pour tout $\alpha \in S$ et $\#S \leq N$. Soit c une valeur critique de P, $c \neq 0$. Alors:*

$$\frac{1}{1+2^{r-1}(dNH)^r \cdot r!} \leq |c| \leq 1 + 2^{r-1}(dNH)^r \cdot r! \quad , \text{où} \quad r = \binom{d+n(d-1)}{n}.$$

PREUVE: On considère le système d'équations:

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

On y applique la proposition 1.1, dans laquelle Y jouera le rôle de X_p, $p = n+1$, H sera remplacé par dH et q=1.

On pose $\mu(n,d,N,H) = 2^{r-1}(dNH)^r \cdot r!$, que l'on notera aussi (abusivement) $\mu(P)$.

PROPOSITION 1.3. *Soit $P(X) \in \mathbb{Z}[X_1,\ldots,X_n]$, $P(X) = \sum_{\alpha\in S} a_\alpha X^\alpha$ 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*

$$P(b) \geq \frac{1}{1+\mu(n,d,N,NR^dH)}$$

PREUVE: 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 $\|b\| < R$, alors $P(b)$ est une valeur critique de $P(X)$ et on applique le corollaire 1.2. Sinon, $\exists i_1,\ldots,i_k \in \{1,\ldots,n\}$, $i_1 < \cdots < i_k$ tels que $|b_j| = R \Leftrightarrow j \in \{i_1,\ldots,i_k\}$. On remplace $P(X)$ par le polynôme à $n-k$ variables obtenu en remplaçant X_j par b_j, $j \in \{i_1,\ldots,i_k\}$ et on remarque que H peut être remplacé par NR^dH. Si $k < n$ on applique le corollaire 1.2, sinon $P(b) \geq 1$ puisque $P(X)$ est à coefficients entiers.

THÉORÈME I. *Soit $P(X) = \sum_{\alpha\in S} a_\alpha X^\alpha \in \mathbb{Z}[X_1,\ldots,X_n]$, $|a_\alpha| \leq H$, pour tout $\alpha \in S$ et $\#S \leq N$. Si $\exists a \in \mathbb{R}^n$, $\|a\| \leq R$, 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:*

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

où

$$\rho = \frac{1}{dNHR^d 2^{d-1}} \cdot \frac{1}{1+\mu(P)}$$

COROLLAIRE. *Sous les hypothèses du théorème, dans toute composante connexe de* Ω_R^+ *il y a un point* Λ *de la forme* $\Lambda = (\lambda_1, \ldots, \lambda_n)$, *avec* $\lambda_i = \frac{k_i}{T}$, $k_i \in \mathbf{Z}$ *et* $T = \left[\frac{1}{\rho}\right] + 1$, *où* [ ] *denote la partie entière.*

Ce théorème et son corollaire sont des conséquences immédiates de la proposition 1.3 et du lemme 3.

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

PROPOSITION 1.5. *Soit* $P(X) \in \mathbf{Z}[X_1, \ldots, X_n]$ *un polynôme pour lequel* $0 \in \mathbf{C}$ *est une valeur régulière du complexifié:* $P(x) = 0$, $x \in \mathbf{C}^n \Rightarrow dP_x \neq 0$. *Soit*

$$\Omega^+(P) = \left\{x \in \mathbf{R}^n \mid P(x) > o\right\}$$

Alors si:

$$R > 1 + 3^{s-1}\left(dH(P)(N(P)+1)\right)^s s!$$

où $s = \binom{2+d+n(d-1)}{n+1}$ *l'inclusion* $\Omega_R^+ \subset \Omega^+(P)$ *induit une bijection sur les composantes connexes.*

PREUVE: Considérons le système de $n+2$ équations:

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

Si (x, λ, r) est une solution, 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, le résultant de ce système d'équations par rapport à r n'est pas identiquement nul. On peut donc lui appliquer la proposition 1.1, avec H remplacé par dH, N par $N(P)+1$, $q = 2$, $p = n+2$. Il en suit 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.

THÉORÈME II. *Soit* $P(X) \in \mathbb{Z}[X_1, \ldots, X_n]$. *Si:*

$$R > 1 + 3^{s-1}\left(d\tilde{H}(N(P)+2)^s\right) s!$$

où $\tilde{H} = 2(1+\mu(P))(H(P)+1)$ *et* $s = \binom{2+d+n(d-1)}{n+1}$ *alors toute composante connexe de* $\Omega^+(P)$ *rencontre* $\Omega^+_R(P)$.

PREUVE: Nous allons passer de P à un polynôme Q à coefficients entiers dont $0 \in \mathbb{C}$ est une valeur régulière, auquel on appliquera la proposition 1.5.

Si $a \in \Omega^+(P)$, soit $\eta = inf\left\{P(a), \frac{1}{1+\mu(P)}\right\}$ et posons $P_\eta(X) = \frac{1}{\eta}P(X) - 1$. Alors $a \in \Omega^+(P_\eta)$, et $0 \in \mathbb{C}$ est une valeur régulière de P_η. Remarquons que si $n' \leq n$, $d' \leq d$, alors $\mu(n', d', N, M) \leq \mu(n, d, N, M)$; donc $0 \in \mathbb{C}$ est aussi une valeur régulière de la partie homogène de degré maximum de P_η. Posons $Q(X) = 2(1+\mu(P))P(X) - 1$. Pour $t \in [2(1+\mu(P)), \frac{1}{\eta}]$, le polynôme $P_t(X) = tP(X) - 1$, ainsi que sa partie homogène de degré maximum, admettent $0 \in \mathbb{C}$ comme valeur régulière. Il s'en suit que l'inclusion $\Omega^+(Q) \subset \Omega^+(P_\eta)$ est une équivalence d'homotopie. On a que $H(Q) = 2(1+\mu(P))(H(P)+1)$, $N(Q) = N(P)+1$ et le résultat suit alors de la proposition 1.5.

BIBLIOGRAPHIE

[1] D. Yu Grigor'ev and N.N. Vorobjov (Jr), Solving Systems of Polynomial Inequalities in Subexponential Time, J. Symbolic Computation (1988) **5**, 37-64.

[2] D. Lazard, Algèbre linéaire sur $K[X_1, \ldots, X_n]$ et élimination, Bull. Soc. Math. de France **105** (1977), 165-190.

[3] F.S. Macaulay, Some Formulæ in Elimination, Proceedings of the London Math. Soc. **XXXV**, 3-27.

Université de Genève
Faculté des Sciences
Section de Mathématiques
2-4, rue du Lièvre, Case Postale 240
CH-1211 Genève 24