Polynômes à coefficients entiers prenant des valeurs positives aux points réels

Yann Bugeaud & Maurice Mignotte, Université de Strasbourg

À la mémoire de Laurentiu Panaitopol

Résumé. Étant donné un polynôme F à coefficients entiers qui ne prend que des valeurs positives sur les réels, nous cherchons à minorer sa valeur minimale sur les réels, en fonction de son degré et de sa hauteur.

I. Introduction.

Étant donné un polynôme F à coefficients entiers qui ne prend que des valeurs positives sur les réels, nous cherchons à minorer sa valeur minimale sur les réels, en fonction de son degré et de sa hauteur. Une question voisine est considérée en [2], où les auteurs cherchent des *certificats de positivité*. On peut aussi citer l'article [1], dans lequel sont données des conditions nécessaires et suffisantes pour qu'un polynôme du quatrième degré soit positif (par élimination de quantificateurs). Ce type de recherches présente un intérêt en robotique. Ici, notre préoccupation sera une question d'approximation diophantienne.

Dans le présent texte, la hauteur d'un polynôme F à coefficients réels, notée $H(F)$, est le maximum des valeurs absolues de ses coefficients. La notation $a \ll_d b$ (resp. $a \gg_d b$) signifie que a est inférieur (resp. supérieur) à b multiplié par une constante ne dépendant que de d.

Soit F un polynôme de degré $d \geq 2$, à coefficients entiers et qui reste positif sur les réels. Ce polynôme admet donc un minimum m, noté $\mathrm{m}(F)$, atteint en un zéro β de sa dérivée. Ce zéro est un nombre algébrique de degré au plus $d-1$ et de hauteur majorée par dH, où H est la hauteur de F.

II. Minorations du minimum.

Nous démontrons d'abord un petit lemme général qui donne des informations sur le cas des polynômes à coefficients réels.

Lemme. — *Soit F un polynôme non constant à coefficients réels qui ne prend que des valeurs positives sur les réels, dont la hauteur vaut H et de coefficient dominant égal à a. Soit z un point réel où F atteint son minimum, alors*

$$|z| \leq 1 + \sqrt{H/a}.$$

Démonstration. Soit m le minimum de F. Comme le polynôme $F-m$ est de hauteur $\leq H$ — puisque $0 < m \leq F(0)$ — et possède une racine double en z, il s'écrit

$$F - m = a(X-z)^2 G,$$

où G est unitaire.

Nous affirmons que si $P(X) = (X - \alpha)Q(X)$ est un polynôme à coefficients complexes, avec $|\alpha| \geq 1$, alors

$$H(Q)(|\alpha| - 1) < H(P).$$

En effet, si $P(X) = \sum_{i=0}^{d} a_i X^i$ et $Q(X) = \sum_{j=0}^{d-1} b_j X^j$, avec $b_{-1} = b_d = 0$, alors $a_i = b_{i-1} - \alpha b_i$ pour $0 \leq i \leq d$. Notons j l'indice minimal tel que $|b_j| = H(Q)$, alors

$$(|\alpha| - 1)H(Q) < |\alpha b_j| - |b_{j-1}| \leq |a_j| \leq H(P).$$

On peut supposer $|z| > 1$, sinon il n'y a rien à démontrer. Si H' la hauteur de G, on déduit de l'affirmation ci-dessus que

$$a(|z| - 1)^2 H' \leq H,$$

d'où le résultat puisque $H' \geq 1$. $\square$

Par la transformation $x \mapsto 1/x$, on obtient aussitôt le corollaire suivant.

Corollaire. — *Soit F un polynôme non constant à coefficients réels qui ne prend que des valeurs positives, et dont la hauteur vaut H. Soit z un point réel où F atteint son minimum. Si z est non nul, on a alors*

$$|z| \geq \left(1 + \sqrt{H/F(0)}\right)^{-1}.$$

Remarque. Supposons que F admette un minimum en un point β avec $|\beta| > 1$ et soit $F^*(X) = X^d F(1/X)$ le polynôme réciproque de F. Alors

$$F^*(1/\beta) = \beta^{-d} F(\beta) < F(\beta),$$

ce qui montre que — pour notre problème — on peut supposer que le minimum est atteint en un point β avec $|\beta| \leq 1$ (et même, si on le souhaite, $0 \leq \beta \leq 1$).

Revenons au cas d'un polynôme F à coefficients entiers. Rappelons tout d'abord une estimation à la Liouville, qui se déduit du Theorem A.1 de [3].

Proposition. — *Soient P et Q des polynômes non constants à coefficients entiers, de degré n et m, respectivement. Si β est une racine de Q telle que $P(\beta)$ est non nul, on a*

$$|P(\beta)| \geq (n+1)^{1-m} (m+1)^{-n/2} H(P)^{1-m} H(Q)^{-n}.$$

En appliquant la proposition ci-dessus, on obtient la minoration $F(\beta) \gg_d H^{-2d+2}$, où H est la hauteur de F et d son degré. Le fait que β annule F' nous permet d'améliorer légèrement cette estimation.

Théorème. — *Soit $F = \sum_{i=0}^{d} a_i X^{d-i}$ un polynôme à coefficients entiers non constant et qui reste strictement positif sur les réels. On désigne par H sa hauteur et par $m = \mathrm{m}(F)$ sa valeur minimale. Alors*

$$m \geq d^{(9-7d)/2} H^{-2d+3}.$$

Cette minoration est plus précise que celle du Theorem 6 de [2].

Démonstration. La valeur minimale de F est atteinte en un point β racine de la dérivée F'. On veut minorer m. On a la relation

$$F_1 := dF - XF' = \sum_{i=1}^{d} i a_i X^{d-i} \qquad \text{et} \qquad dm = F_1(\beta).$$

Notant que $H(F_1) \leq dH$ et $H(F') \leq dH$, la proposition ci-dessus entraîne que

$$\begin{aligned} dm &\geq d^{1-(d-1)}\, d^{-(d-1)/2}\, H(F_1)^{-d+2}\, H(F')^{-d+1} \\ &\geq d^{(11-7d)/2} H^{-2d+3}, \end{aligned}$$

d'où le résultat annoncé. ∎

Remarque. Si les coefficients $a_1, \ldots, a_h$ de F sont nuls, alors F_1 est de degré au plus $d-1-h$ et on obtient alors, avec les notations du théorème,

$$m \gg_d H^{-2d+3+h}.$$

De manière analogue, on a aussi une amélioration de la minoration de m si $a_{d-1} = \cdots = a_{d-k} = 0$; c'est également le cas si on suppose F' réductible sur les entiers.

III. Des exemples.

Le cas $d = 2$ se traite très simplement et on voit que l'estimation du théorème est alors optimale du point de vue de la dépendance en la hauteur. Il suffit par exemple de considérer la famille de polynômes

$$F_a(X) := (a^2 + a + 1)X^2 + (2a + 1)X + 1,$$

où $a \geq 1$ est entier. Un rapide calcul montre que F_a a deux racines complexes conjuguées et ne prend donc que des valeurs positives sur les réels. En outre, on vérifie que $F_a(1/a) = 1/a^2 \leq 3H(F_a)^{-1}$.

Pour le polynôme

$$P = X^d + (aX - 1)^2$$

avec $d \geq 4$ pair et $a \geq 2$, on a

$$\mathrm{m}(P) \leq P(1/a) = a^{-d} = H(P)^{-d/2}.$$

Dans cet exemple, les coefficients $a_1, \ldots, a_{d-3}$ de P sont tous nuls, et la remarque qui clôt la partie II montre que $\mathrm{m}(P) \gg_d H(P)^{-d}$.

On peut aussi construire d'une manière élémentaire et tout à fait différente des polynômes F de hauteur H vérifiant l'estimation $\mathrm{m}(F) \ll_d H^{-d/2}$. Considérons un nombre algébrique irrationnel réel ξ, avec $0 < \xi < 1/2$, de degré δ, de hauteur H et dont le polynôme minimal est noté Q. Grâce au théorème de Minkowski on voit qu'il existe un polynôme R non nul, à coefficients entiers, de hauteur $< H$ (donc $R(\xi) \neq 0$) et de degré $\leq \delta$, qui vérifie

$$|R(\xi)| \leq 4H^{-\delta}.$$

Alors le polynôme

$$P(X) = Q^2(X) + R^2(X)$$

est clairement positif, de degré $d = 2\delta$, de hauteur $\ll_d H^2$ et on a

$$0 < P(\xi) = R^2(\xi) \ll_d H(P)^{-d/2}.$$

Cette méthode conduit à un meilleur résultat dès lors que l'on peut garantir que $|R(\xi)|$ est très petit. Soit $a \geq 1$ un entier et posons

$$Q_a(X) = X^n - aX + 1, \quad R_a(X) = (a+1)X^n - X^{n-1} - aX + 1.$$

Nous avons observé [4] que le résultant de Q_a et R_a est égal à ± 1, et que Q_a et R_a ont une racine proche de $a^{-1} + a^{-n-1}$. Notant β_a la racine de R_a proche de $a^{-1} + a^{-n-1}$, un rapide calcul montre que

$$|R_a(\beta)| \ll a^{-2n+1}.$$

Par conséquent, le polynôme $P_a := Q_a^2 + R_a^2$, de degré $d = 2n$ et de hauteur $\ll a^2$, vérifie

$$0 < P_a(\beta) \ll a^{-4n+2} \ll H(P_a)^{-d+1}.$$

Cet exemple montre que la minoration de m obtenue dans la Proposition est essentiellement la meilleure possible, dans la mesure où l'exposant de H est nécessairement inférieur ou égal à $-d + 1$.

En reprenant l'article [4] on peut construire d'autres exemples de même qualité. Considérons les polynômes

$$P_{a,n}(X) = (X^n - aX + 1)^2 + X^{2n-2}(aX - 1)^2, \quad a \geq 3,$$

pour $n \geq 2$. Il est clair qu'ils restent positifs sur les réels. De plus, la hauteur de $P_{a,n}$ est majorée par $2a^2$ et on vérifie facilement que

$$P_{a,n}(a^{-1} + a^{-n-1}) \leq 2n^2 a^{-4n+2} \ll_d H(P_{a,n})^{-d+1}$$

pour a assez grand, où $d = 2n$ est le degré de $P_{a,n}$.

Par conséquent, si, pour $d \geq 2$ pair, on pose

$$\pi(d) = \limsup \frac{-\log(\mathrm{m}(P))}{\log(\mathrm{H}(P))},$$

où la limite porte sur les polynômes positifs à coefficients entiers de degré d, alors nous avons montré que

$$d - 1 \leq \pi(d) \leq 2d - 3, \quad \text{si } d \geq 2.$$

En particulier, $\pi(2)=1$ et
$$3 \le \pi(4) \le 5.$$

Les familles de polynômes que nous construisons pour minorer $\pi(d)$ ont des coefficients polynomiaux en le paramètre a. Nous obtenons ainsi “beaucoup” de polynômes. Il est vraisemblable qu'il existe des familles de polynômes à coefficients exponentiels en le paramètre a qui permettraient d'améliorer la minoration de $\pi(d)$. Cette remarque est étayée par la construction de Danilov [5], au moyen des solutions d'une équation de Pell, d'une infinité de paires d'entiers positifs (x,y) vérifiant $|x^3-y^2| \ll x^{1/2}$.

Remarque. Considérons un polynôme F à coefficients entiers qui ne s'annule pas sur les réels et qui admet deux racines complexes conjuguées α et $\bar\alpha$ avec $|\alpha| \le 1$, donc $\varepsilon := (\alpha-\bar\alpha)/2$ vérifie $|\varepsilon| \le 1$. Posons $\gamma = (\alpha+\bar\alpha)/2$. Alors
$$F(\gamma) = F(\alpha) + \varepsilon F'(\gamma) + \frac{\varepsilon^2}{2!}F''(\gamma) + \cdots$$
et aussi
$$F(\gamma) = F(\bar\alpha) - \varepsilon F'(\gamma) + \frac{\varepsilon^2}{2!}F''(\gamma) - \cdots,$$
si bien que
$$2F(\gamma) = \frac{\varepsilon^2}{2!}F''(\gamma) + \frac{\varepsilon^4}{4!}F^{(4)}(\gamma) + \cdots,$$
ce qui implique aussitôt
$$|F(\gamma)| \le d^3\varepsilon^2 H,$$
où H est la hauteur de F. En conséquence, si on sait construire des polynômes de ce type avec ε très petit, alors ces polynômes auront un minimum lui aussi très petit. **Mais** il semble difficile de démontrer une quelconque “réciproque” de ce fait, la difficulté consistant à minorer la valeur $F''(\gamma)$.

Références bibliographiques

[1] D. S. Arnon, M. Mignotte. — *On Mechanical Quantifier Elimination for Elementary Algebra and Geometry*, J. Symb. Comput. **5** (1988), 237–259.

[2] F. Boudaoud, F. Caruso, M.-F. Roy. — *Certificates of Positivity in the Bernstein Basis*, Discrete Comput. Geom. **39** (2008), 639–655.

[3] Y. Bugeaud. — Approximation by algebraic numbers. Cambridge Tracts in Mathematics 160, Cambridge University Press, 2004.

[4] Y. Bugeaud, M. Mignotte. — *On the distance between roots of integer polynomials*, Proc. Edinburgh Math. Soc. **47** (2004), 553–556.

[5] L. V. Danilov. — *The Diophantine equation $x^3-y^2=k$ and a conjecture of M. Hall*, Mat. Zametki **32** (1982), 273–275, 425 (en russe); trad. en anglais : Math. Notes **32** (1982), 617–618.

Yann Bugeaud, Maurice Mignotte
Université de Strasbourg
Mathématiques
7, rue René Descartes
67084 STRASBOURG Cedex

e-mail : {bugeaud,mignotte}@math.unistra.fr