ANNALES DE LA FACULTÉ DES SCIENCES DE TOULOUSE

PHILIPPE GLESSER

Majoration de la norme des facteurs d'un polynôme

Annales de la faculté des sciences de Toulouse 5^e série, tome 11, n° 1 (1990), p. 67-74

<http://www.numdam.org/item?id=AFST_1990_5_11_1_67_0>

Annales de la Faculté des Sciences de Toulouse Vol. XI, n° 1, 1990

Majoration de la norme des facteurs d'un polynôme

PHILIPPE GLESSER[1]

RÉSUMÉ. — Le but de cet article est de donner une nouvelle majoration de la norme des facteurs d'un polynôme à coefficients complexes. Outre son intérêt théorique, une telle majoration est utile pour les algorithmes de factorisation des polynômes.

ABSTRACT. — The object of this paper is to give a new upper bound for the norm of factors of a polynomial with complex coefficients. Besides its theoretical interest, this kind of bound is useful in algorithms for polynomial factorisation.

1. Introduction

Dans cet article on utilise les définitions suivantes :

Soit F un polynôme à coefficients complexes, $F = \sum_{i=0}^{n} a_i X^i$, on note :

$$H(F) = \max_{i=0,1,\ldots,n} |a_i|\,, \text{ la hauteur de } F\,,$$

$$L(F) = \sum_{i=0}^{n} |a_i|\,, \text{ la longueur de } F\,,$$

$$\text{et} \quad \|F\|_2 = \left(\sum_{i=0}^{n} |a_i|^2\right)^{\frac{1}{2}}\,, \text{la norme de } F\,.$$

Dans la suite on considère deux polynômes P et Q à coefficients complexes,

$$P = a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0\,,$$
$$Q = b_n X^n + b_{n-1} X^{n-1} + \cdots + b_0\,,$$

P étant un diviseur de Q.

[1] Ph. Glesser, Université Louis-Pasteur, 7, rue René-Descartes 67084 Strasbourg

Le but de cet article est de majorer la longueur, la norme et la hauteur de P, en fonction de la norme de Q. On utilisera pour cela un lemme dû à A. Granville.

2. Résultats intermédiaires

Cette partie comprend l'énoncé et la démonstration de deux lemmes et de deux corollaires nécessaires à la démonstration du résultat principal de cet article qui se trouve, sous forme de théorème, dans la troisième partie du papier.

LEMME 1. — *Soit P un polynôme à coefficients dans* $\mathbf{C}$:

$$P(X) = a_0 + a_1X + \cdots + a_mX^m .$$

On pose : $(X+\alpha)P(X) = b_0 + b_1X + \cdots + b_{m+1}X^{m+1}$,
et $(\overline{\alpha}X+1)P(X) = c_0 + c_1X + \cdots + c_{m+1}X^{m+1}$.
Alors : $\|(X+\alpha)P(X)\|_2 = \|(\overline{\alpha}X+1)P(X)\|_2$,

et de plus si $|\alpha| \leq 1$, *alors :*

$$\sum_{i=0}^{k} |c_i|^2 \geq \sum_{i=0}^{k} |b_i|^2 \quad (0 \leq k \leq m).$$

Preuve. — Ayant posé $a_{-1} = 0$ et $a_{m+1} = 0$, on a :

$$b_i = a_{i-1} + \alpha a_i \text{ et } c_i = \overline{\alpha}a_{i-1} + a_i, \quad \text{pour } 0 \leq i \leq m+1.$$

Donc : $$\sum_{i=0}^{k} |c_i|^2 = \sum_{i=0}^{k} (\overline{\alpha}a_{i-1} + a_i)(\alpha\overline{a_{i-1}} + \overline{a_i})$$
$$= \sum_{i=0}^{k} \left(|\alpha|^2 |a_{i-1}|^2 + \overline{\alpha}\,\overline{a_i}a_{i-1} + \alpha a_i\overline{a_{i-1}} + |a_i|^2\right).$$

Tandis que : $$\sum_{i=0}^{k} |b_i|^2 = \sum_{i=0}^{k} \left(|a_{i-1}|^2 + \alpha a_i\,\overline{a_{i-1}} + \overline{\alpha a_i}a_{i-1} + |\alpha|^2 |a_i|^2\right).$$

Ainsi :
$$\sum_{i=0}^{k} |c_i|^2 - \sum_{i=0}^{k} |b_i|^2 = |a_k|^2 - |\alpha|^2 |a_k|^2$$
$$= (1 - |\alpha|^2)|a_k|^2 .$$

Ceci démontre la première assertion en faisant $k = m + 1$, et la seconde pour $0 \leq k \leq m$, lorsque $|\alpha| \leq 1$.

Le corollaire suivant est une conséquence immédiate du lemme 1.

COROLLAIRE 1. — *Soit P un polynôme à coefficients dans* C :

$$P(X) = a_m(X + \alpha_1)\dots(X + \alpha_m) = a_0 + a_1 X + \dots + a_m X^m .$$

On pose : $\widetilde{P}(X) = a_m \prod_{S}(\overline{\alpha_i}X + 1) \prod_{\overline{S}}(X + \alpha_i)$, *où S est un sous-ensemble de* $\{1, 2, \dots, m\}$ *tel que si* $i \in S$, $|\alpha_i| \leq 1$, $\overline{S}$ *étant son complémentaire dans* $\{1, 2, \dots, m\}$.

Alors : $\|P\|_2 = \|\widetilde{P}\|_2$ *et* $\sum_{i=0}^{k} |\widetilde{a}_i|^2 \geq \sum_{i=0}^{k} |a_i|^2$, $(0 \leq k \leq m)$

(les $\widetilde{a}_i$ sont les coefficients de $\widetilde{P}$).

LEMME 2 (A. Granville). — *Soit P et Q deux polynômes à coefficients complexes :*

$$P = a_m(X + \alpha_1)\dots(X + \alpha_m) = a_m X^m + \dots + a_0 .$$
$$Q = b_n(X + \alpha_1)\dots(X + \alpha_n) = b_n X^n + \dots + b_0 , \quad n > m , \ b_0 \neq 0$$

(autrement dit P divise Q).

On suppose que $|\alpha_i| \geq 1$ $(m + 1 \leq i \leq n)$. *Alors :*

$$|a_j| \leq \sum_{i=0}^{j} |b_i| \binom{j - i + n - m - 1}{j - i} \left|\frac{a_0}{b_0}\right| \quad (0 \leq j \leq m).$$

Preuve. — On a : $P = \dfrac{a_m}{b_n} \dfrac{1}{(X + \alpha_{m+1})} \cdots \dfrac{1}{(X + \alpha_n)} Q.$

Or $\dfrac{1}{X+\alpha_i} = \dfrac{1}{\alpha_i(X/\alpha_i+1)} = \dfrac{1}{\alpha_i}\left(1-\dfrac{X}{\alpha_i}+\left(\dfrac{X}{\alpha_i}\right)^2+\cdots\right)$,

ce qui entraîne que :

$$\frac{1}{X+\alpha_i} \ll \frac{1}{|\alpha_i|}(1+X+X^2+X^3+\cdots)$$

(si $U = \sum_{n\geq 0} u_n X^n$ est une série formelle à coefficients complexes et $V = \sum_{n\geq 0} v_n X^n$ une série formelle à coefficients réels positifs ou nuls, on dit que V majore U et on note $U \ll V$, si $|u_n| \leq v_n$ pour tout n positif ou nul). Donc :

$$P \ll \left|\frac{a_0}{b_0}\right|(1+X+X^2+X^3+\cdots)^{n-m}(|b_0|+\cdots+|b_n|X^n),$$

ce qui entraîne que :

$$P \ll \left|\frac{a_0}{b_0}\right|\left(\sum_{i\geq 0}\binom{n-m+i-1}{i}X^i\right)(|b_0|+\cdots+|b_n|X^n),$$

et par conséquent que :

$$P \ll \left|\frac{a_0}{b_0}\right|\sum_{j\geq 0}\left(\sum_{i=0}^{j}|b_i|\binom{n-m+j-i-1}{j-i}\right)X^j,$$

d'où l'on déduit finalement que :

$$|a_j| \leq \left|\frac{a_0}{b_0}\right|\sum_{i=0}^{j}|b_i|\binom{n-m+j-i-1}{j-i}.$$

COROLLAIRE 2. — *Soient P et Q deux polynômes à coefficients complexes :*

$$P = a_m(X+\alpha_1)\ldots(X+\alpha_m) = a_m X^m+\cdots+a_0$$
$$Q = b_n(X+\alpha_1)\ldots(X+\alpha_n) = b_n X^n+\cdots+b_0, \quad n>m,\ b_0\neq 0.$$

Alors : $$|a_j| \leq \left|\frac{a_0}{b_0}\right|\binom{j+n-m}{j}\|Q\|_2 \quad (0\leq j\leq m).$$

Preuve. — Soit :

$$\widetilde{Q} = b_n \prod_{\substack{|\alpha_i|\geq 1 \\ \text{ou} \\ i\leq m}} (X+\alpha_i) \prod_{\substack{|\alpha_i|<1 \\ \text{et} \\ i>m}} (\overline{\alpha}_i X + 1).$$

D'après le lemme 2 : $|a_j| \leq \left|\dfrac{a_0}{\widetilde{b}_0}\right| \sum_{i=0}^{j} |\widetilde{b}_i| \binom{j-i+n-m-1}{j-i}$,

où les $\widetilde{b}_i$ sont les coefficients de $\widetilde{Q}$.

On vérifie que $|b_0| \leq |\widetilde{b}_0|$, d'où l'on déduit que :

$$|a_j| \leq H(\widetilde{Q}) \left|\frac{a_0}{b_0}\right| \sum_{i=0}^{j} \binom{j-i+n-m-1}{j-i}.$$

Donc : $$|a_j| \leq \left|\frac{a_0}{b_0}\right| \binom{j+n-m}{j} \|\widetilde{Q}\|_2$$

et par conséquent :

$$|a_j| \leq \left|\frac{a_0}{b_0}\right| \binom{j+n-m}{j} \|Q\|_2,$$

d'après le corollaire 1.

3. Énoncé et démonstration du théorème

THÉORÈME. — *Soient P et Q deux polynômes à coefficients complexes :*

$$P = a_m(X+\alpha_1)\dots(X+\alpha_m) = a_m X^m + \dots + a_0,$$
$$Q = b_n(X+\alpha_1)\dots(X+\alpha_n) = b_n X^n + \dots + b_0, \quad n \geq m,\ b_0 \neq 0.$$

Alors :

$$L(P) \leq \left(\left|\frac{a_0}{b_0}\right| + \left|\frac{a_m}{b_n}\right|\right) \binom{n - \left[(m-1)/2\right]}{[m/2]} \|Q\|_2,$$

$$\|P\|_2 \leq \sqrt{\left|\frac{a_0}{b_0}\right|^2 + \left|\frac{a_m}{b_n}\right|^2} \left(\sum_{j=0}^{[m/2]} \binom{j+n-m}{j}^2\right)^{\frac{1}{2}} \|Q\|_2,$$

et $$H(P) \leq \max\left\{\left|\frac{a_0}{b_0}\right|, \left|\frac{a_m}{b_n}\right|\right\} \binom{n - \left[(m+1)/2\right]}{[m/2]} \|Q\|_2.$$

Preuve. — D'après le corollaire 2 :

$$|a_j| \leq \left|\frac{a_0}{b_0}\right| \binom{j+n-m}{j} \|Q\|_2\,, \quad \text{pour } 0 \leq j \leq [m/2]\,.$$

En regardant les polynômes réciproques de P et Q, c'est-à-dire respectivement $a_0X^m + \cdots + a_m$ et $b_0X^n + \cdots + b_n$, on constate de même que :

$$|a_{m-j}| \leq \left|\frac{a_m}{b_n}\right| \binom{j+n-m}{j} \|Q\|_2\,, \quad \text{pour } 0 \leq j \leq [m/2]\,.$$

Donc : $$L(P) = \sum_{j=0}^{m} |a_j| \leq \left(\left|\frac{a_0}{b_0}\right| + \left|\frac{a_m}{b_n}\right|\right) \sum_{j=0}^{[m/2]} \binom{j+n-m}{j} \|Q\|_2\,,$$

d'où l'on déduit : $$L(P) \leq \left(\left|\frac{a_0}{b_0}\right| + \left|\frac{a_m}{b_n}\right|\right) \binom{n-m+[m/2]+1}{[m/2]} \|Q\|_2\,.$$

Les deux autres inégalités se démontrent de la même manière.

Ce théorème a, pour le cas particulièrement intéressant des polynômes à coefficients entiers, la conséquence immédiate suivante.

COROLLAIRE 3. — *Soient P et Q deux polynômes à coefficients entiers tels que P divise Q (m = degré de P et n = degré de Q, $n \geq m$), alors :*

$$L(P) \leq 2 \binom{n - \left[(m-1)/2\right]}{[m/2]} \|Q\|_2\,,$$

$$\|P\|_2 \leq \left(2 \sum_{j=0}^{[m/2]} \binom{j+n-m}{j}^2\right)^{\frac{1}{2}} \|Q\|_2\,,$$

et $$H(P) \leq \binom{n - \left[(m+1)/2\right]}{[m/2]} \|Q\|_2\,.$$

COROLLAIRE 4. — *Soient P et Q deux polynômes à coefficients complexes :*

$$P = a_mX^m + \cdots + a_0\,,$$
$$Q = b_nX^n + \cdots + b_0\,.$$

On suppose que P divise Q et que $|a_0| \leq |b_0|$ et $|a_m| \leq |b_n|$, alors :

$$L(P) \leq 2^{2n/3} \|Q\|_2\,, \quad \textit{lorsque } n \textit{ est assez grand.}$$

Preuve. — 1) On suppose que $m \geq 2n/3$.

D'après le théorème : $L(P) \leq 2 \binom{n - \left[(m-1)/2\right]}{[m/2]} \|Q\|_2$.

Or comme $m \geq \frac{2n}{3}$: $L(P) \leq 2 \binom{2n/3+2}{n/3+1} \|Q\|_2$.

Enfin : $2 \binom{2n/3+2}{n/3+1} \sim \frac{8}{\sqrt{\pi(n/3+1)}} 2^{2n/3}$, lorsque n tend vers l'infini.

2) On suppose que $m \leq 2n/3$: La majoration classique $L(P) \leq 2^m \|Q\|_2$ montre que :

$$L(P) \leq 2^{2n/3} \|Q\|_2 .$$

4. Conclusion

L'intérêt du théorème est de fournir une bonne majoration de la taille du facteur P de degré m d'un polynôme Q de degré $m+k$, lorsque le rapport du degré de P par le degré de Q est proche de 1.

Une telle majoration peut être utile pour comparer la mesure et la hauteur d'un polynôme donné (cf. [3] et [6]). La majoration utilisée dans [3] était la suivante :

$$H(P) \leq \frac{(m+k)^{m+k}}{m^m k^k} L(Q) \tag{1}$$

(remarque : d'autres inégalités de ce type sont données dans [1], [2] et [5]).

Comparons-la avec la majoration induite par le théorème dans le cas où $|a_0| \leq |b_0|$ et $|a_m| \leq |b_{m+k}|$:

$$H(P) \leq \binom{[m/2]+k}{[m/2]} L(Q) . \tag{2}$$

On suppose que $k = O(m^{2/3})$ en l'infini. On montre que :

$$\frac{(m+k)^{m+k}}{m^m k^k} \sim \left(\frac{em}{k}\right)^k e^{\frac{k^2}{2m}} ,$$

alors que :

$$\binom{[m/2]+k}{[m/2]} \sim \frac{1}{\sqrt{2\pi k}} \left(\frac{e}{k}\left[\frac{m}{2}\right]\right)^k e^{\frac{k^2}{2[m/2]}} \quad \text{lorsque } m \text{ tend vers l'infini.}$$

Donc, lorsque m est assez grand, l'inégalité (2) est meilleure que l'inégalité (1).

Exemples numériques

En testant différentes valeurs de m et de k, on obtient les tableaux suivants :

@1	10	20	30	50	100
1	25,8	53,0	80,2	134,5	270,5
3	449,7	4695	17197	84827	710850
6		202255	$3{,}31 \cdot 10^6$	$9{,}28 \cdot 10^7$	$7{,}19 \cdot 10^9$
10			$1{,}96 \cdot 10^8$	$7{,}35 \cdot 10^{10}$	$1{,}31 \cdot 10^{14}$

@1	10	20	30	50	100
1	5	10	15	25	50
3	20	165	560	2600	20825
6		1716	18564	376740	$2{,}296 \cdot 10^7$
10			184756	$3{,}005 \cdot 10^7$	$2{,}29 \cdot 10^{10}$

Le premier tableau donne les valeurs de : $\dfrac{(m+k)^{m+k}}{m^m k^k}$,

le second donne les valeurs de : $\binom{[m/2]+k}{[m/2]}$.

Remerciements.
Je remercie M. Mignotte pour ses nombreuses remarques.

Références

[1] J.D. DONALDSON and Q.I. RAHMAN . — *Inequalities for polynomials whith a prescribed zero*, Pacific J. Math. **41** (1983) pp. 375-378

[2] A. DURAND . — *A Propos d'un théorème de S. Bernstein sur la dérivée d'un polynôme*, C.R. Acad. Sci. Paris Sér. **I** Math. **290** (1980) pp. 523-525

[3] PH. GLESSER . — *Inégalités sur la mesure des polynômes*, Rendiconti-Cagliari (à paraître)

[4] A. GRANVILLE Ph. D thesis (manuscrit)

[5] R. GÜTING . — *Polynomials whith multiple zeroes*, Mathematika **14** (1967) pp. 181-196

[6] M. MIGNOTTE . — *An inequality about irreducible factors of integer polynomials*, Journal of number theory (1988) pp. 156-166