Bull. Math. Soc. Sci. Math. Roumanie
Tome 65 (113), No. 2, 2022, 213–231

**Sur la hauteur des transformées de Graeffe d'un polynôme à coefficients entiers**

par

Mihai Cipu(1), Gérard Kientega(2), Maurice Mignotte(3), Salifou Nikiema(4)

*À la mémoire de Doru Ştefănescu*

**Résumé**

Le problème de la relation entre la hauteur d'un polynôme et de ses puissances se pose. John Abbott, en recherchant les polynômes dont les hauteurs des carrés sont plus petites que celle du polynôme initial, a conjecturé que la hauteur du carré d'un polynôme à coefficients entiers est au moins égale au double de celle du polynôme initial. Dans le présent travail, nous considérons l'étude d'un analogue de la conjecture d'Abbott dans le cas de la transformation de Graeffe–Dandelin.

**Key Words** : Polynômes, hauteur de polynômes, transformation de Dandelin-Graeffe.
**2010 Mathematics Subject Classification** : Primary : 11D09, 11B37, 11J86.

# 1 Introduction

La méthode de Graeffe ou méthode de Dandelin–Lobachevsky–Graeffe est un algorithme pour déterminer toutes les racines d'un polynôme. Elle a été élaborée indépendamment par Germinal Pierre Dandelin en 1826 et Nikolai Ivanovich Lobachevsky en 1834. En 1837 Karl Heinrich Graeffe découvrit aussi l'idée principale de cette méthode. (L'histoire n'aime pas les noms de plus d'une syllabe, on parle maintenant de méthode de Graeffe, autre exemple analogue l'équation de Fermat est devenue celle de Pell.) La méthode conduit à une séparation des racines en les élevant au carré à chaque étape. Ce résultat est obtenu en modifiant seulement les coefficients du polynôme. Finalement, les formules de Viète permettent de trouver des valeurs approchées des racines. De nos jours cette méthode ne sert plus pour trouver des valeurs approchées des racines mais possède un intérêt théorique lié à la mesure de Mahler.

La mesure de Mahler est multiplicative : pour tout polynôme $P$ et tout entier positif $n$, on a $\mathrm{M}(P^n) = \mathrm{M}(P)^n$. La hauteur d'un polynôme ne possède pas cette propriété et le problème de la relation entre la hauteur d'un polynôme et de ses puissances se pose. John Abbott, en recherchant les polynômes dont les hauteurs des carrés sont plus petites que celle du polynôme initial, a conjecturé que la hauteur du carré d'un polynôme est au moins égale au double de celle du polynôme initial, c'est la *conjecture initiale d'Abbott.* Ici nous considérons l'étude d'un analogue de la conjecture initiale d'Abbott dans le cas de la transformation de Graeffe-Dandelin.

## 2 Notations et généralités

Tous les polynômes considérés dans cet article sont à coefficients entiers. Pour un polynôme $P = \sum_{i=0}^{d} a_i X^i$ de degré $d$, on pose

$$\mathrm{ht}(P) = \max_{0 \le i \le d} |a_i|, \quad \|P\| = \left( \sum_{i=0}^{d} |a_i|^2 \right)^{1/2}, \qquad \mathrm{L}(P) = \sum_{i=0}^{d} |a_i|$$

et

$$|P|_\infty = \max\{|P(z)| \,:\, |z| = 1\},$$

que l'on nomme respectivement la *hauteur*, la *norme*, la *longueur* et la *norme infinie* de $P$. Et on sait (Parseval) que

$$\frac{1}{2\pi} \int_0^{2\pi} |P(e^{it})|^2 dt = \|P\|^2.$$

On sait aussi que (voir [8]), si $\mu > \lambda > 0$, alors

$$\left( \frac{1}{2\pi} \int_0^{2\pi} |P(e^{it})|^\lambda dt \right)^{1/\lambda} \le \left( \frac{1}{2\pi} \int_0^{2\pi} |P(e^{it})|^\mu dt \right)^{1/\mu},$$

avec inégalité stricte si $P$ n'est pas un monôme. Enfin nous utiliserons librement les inégalités [6]

$$\mathrm{ht}(P) \le \|P\| \le |P|_\infty \le \mathrm{L}(P).$$

De plus, si $k = \mathrm{Card}\{0 \le i \le d \,:\, a_i \ne 0\}$, on posera $k = \# P$, le nombre de coefficients non nuls de $P$, alors, clairement,

$$\|P\| \le \sqrt{k}\, \mathrm{ht}(P), \qquad \mathrm{L}(P) \le k\, \mathrm{ht}(P).$$

La conjecture d'Abbott [1] qui a motivé notre étude est la suivante :

- Si $P$ est un polynôme à coefficients entiers qui n'est pas un monôme alors

$$\mathrm{ht}(P^2) \ge 2\, \mathrm{ht}(P).$$

Etant donnée la similitude qu'il y a entre la transformation de Graeffe et l'élévation au carré d'un polynôme nous étudions la question, l'inégalité

$$\mathrm{ht}(\mathcal{G}P) \ge 2\, \mathrm{ht}(P), \tag{I}$$

où $\mathcal{G}P$ désigne la transformée de Graeffe de $P$, a-t-elle lieu ?

L'exemple du polynôme $X - 1$ pour lequel $\mathcal{G}(X-1) = 1 - X$ montre que la réponse à cette question n'est pas toujours positive. Plus généralement, si $\mathcal{G}P = \pm P$ il est facile de voir que $\mathrm{M}(P) = 1$. Inversement si $P$ est de degré $d$ et si $\mathrm{M}(P) = 1$ alors $\mathrm{L}(P) \le 2^d$ et les éléments de la suite $\mathcal{G}^n P$, $n \ge 0$, parcourent un ensemble fini si bien que cette suite est soit ultimement périodique soit ultimement stationnaire.

En fait dans tous les cas la suite des $\mathcal{G}^n P$ est ultimement stationnaire comme le montre la petite démonstration qui suit. Soit $P$ un polynôme de mesure 1 et soit $\zeta$ une racine de $P$, alors $\zeta$ est une racine de l'unité disons d'ordre $k$. Alors $\zeta^2$ est une racine de $\mathcal{G}P$ et son ordre est $k$ si $k$ est impair et $k/2$ sinon. On pose $k = 2^\nu k'$ où $k'$ est impair. Soit $\Omega = \Omega_0 \cup \Omega_1 \cup \cdots \cup \Omega_w$ la décomposition de l'ensemble des racines de $P$ où $\Omega_0$ est l'ensemble des racines pour lesquelles $\nu = 0$, où $\Omega_1$ est l'ensemble des racines pour lesquelles $\nu = 1, \ldots$ et où $w$ est le maximum des $\nu$ (chaque racine est répétée autant de fois que sa multiplicité). Alors l'ensemble des racines de $\mathcal{G}P$ est décomposé, avec des notations évidentes, en $\Omega' = \Omega'_0 \cup \Omega'_1 \cup \cdots \cup \Omega'_{w-1}$, où $\Omega'_0$ est égal à $\Omega_0$ augmenté de l'image de $\Omega_1$, et où $\Omega'_i$ est l'image de $\Omega_{i+1}$ pour tout $i = 1, 2, \ldots, w-1$. Il en résulte que l'on a $\mathcal{G}^{w+1}P = \mathcal{G}^w P$ et que $\mathcal{G}^u P \neq \mathcal{G}^v P$ lorsque $0 \leq u < v \leq w$.

Dans le cas où $\mathrm{M}(P) > 1$ il est clair que $M(\mathcal{G}^n P)$ tend vers l'infini avec $n$, ainsi que $\mathrm{ht}(\mathcal{G}^n P)$. Il existe donc un entier $k > 0$ tel que $\mathrm{ht}(\mathcal{G}^k P) \geq 2\mathrm{ht}(P)$, mais – comme on le verra plus bas – la valeur $k = 1$ ne convient pas toujours. L'essentiel du travail qui suit consiste à donner des conditions suffisantes pour que $k = 1$ soit valable.

## 3 La transformation de Graeffe-Dandelin

Si $P$ est un polynôme non constant on pose

$$\mathcal{G}P(X) = P(Y) \cdot P(-Y), \quad \text{où } Y^2 = X,$$

et, plus généralement, pour $m \geq 2$,

$$\mathcal{G}_m P(X) = \prod_{i=1}^{m} P(\varepsilon^i Y),$$

où $\varepsilon$ est une racine primitive $m$-ième de l'unité et où $Y^m = X$. Ainsi $\mathcal{G}_2(P) = \mathcal{G}P$ et les racines de $\mathcal{G}_m(P)$ sont les puissances $m$-ièmes de celles de $P$.

On utilise la *mesure de Mahler* : si $P$ est un polynôme non constant de degré $d$, de coefficient dominant $a$ et de racines $\alpha_1, \ldots, \alpha_d$ alors sa mesure est

$$\mathrm{M}(P) = |a| \prod_{i=1}^{d} \max\{1, |\alpha_i|\}.$$

Il est bien connu que (inégalité de Landau)

$$\mathrm{M}(P) \leq \|P\|,$$

où l'inégalité est stricte lorsque $P$ n'est pas un monôme, et les formules de Viète conduisent aussitôt à la majoration

$$\mathrm{L}(P) \leq 2^d \mathrm{M}(P).$$

Pour ce qui nous intéresse ici, notons aussi que

$$\mathrm{M}(P^m) = \mathrm{M}(\mathcal{G}_m P) = \mathrm{M}(P)^m.$$

Comme vu plus haut, la conjecture d'Abbott ne se généralise pas dans le cas de la transformation de Graeffe-Dandelin. Par contre, la question se pose pour $P$ à coefficients entiers lorsque $\mathrm{M}(P) > 1$. Même pour certains polynômes tels que $\mathrm{M}(P) > 1$ l'inégalité

$\mathrm{ht}(\mathcal{G}P) \geq 2\mathrm{ht}(P)$ peut ne pas avoir lieu. Voici un tel exemple. Prenons pour $P$ le polynôme qui, à ce jour, a la mesure de Mahler $> 1$ minimale connue, il s'agit de

$$P = X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1,$$

pour lequel $\mathrm{M}(P) = 1.17628081\ldots$. On vérifie alors que

$$\mathcal{G}P = X^{10} - X^9 - X^7 + X^6 - X^5 + X^4 - X^3 - X + 1$$

est encore de hauteur 1. Ensuite on obtient successivement

$$\begin{aligned}
\mathcal{G}_4(P) &= X^{10} - X^9 - X^7 - 3\,X^6 - X^5 - 3\,X^4 - X^3 - X + 1,\\
\mathcal{G}_8(P) &= X^{10} - X^9 - 8\,X^8 - 9\,X^7 + 5\,X^6 + 15\,X^5 + 5\,X^4 - 9\,X^3 - 8\,X^2 - X + 1,\\
\mathcal{G}_{16}(P) &= X^{10} - 17\,X^9 + 56\,X^8 - 121\,X^7 + 181\,X^6 - 209\,X^5 + 181\,X^4\\
&\qquad - 121\,X^3 + 56\,X^2 - 17\,X + 1,\\
\mathcal{G}_{32}(P) &= X^{10} - 177\,X^9 - 616\,X^8 - 1113\,X^7 - 1547\,X^6 - 1745\,X^5 - 1547\,X^4\\
&\qquad - 1113\,X^3 - 616\,X^2 - 177\,X + 1.
\end{aligned}$$

Le polynôme $P$ est le polynôme minimal d'un nombre de Salem $\alpha$, avec $\alpha > 1$ réel, dont les conjugués autres que $1/\alpha$ sont complexes de module 1. Donc $\mathrm{M}(P) = \alpha$ et la formule de Viète appliquée au coefficient de $X^9$ de $\mathcal{G}_{32}(P)$ montre que

$$1.173656\ldots = 168^{1/32} < \alpha < 186^{1/32} = 1.177395\ldots,$$

ce qui illustre la méthode initiale de Dandelin pour le calcul des valeurs approchées des racines d'un polynôme.

Si on poursuit cette transformation, on trouve

$$\begin{aligned}
\mathcal{G}_{64}(P) &= X^{10} - 32561\,X^9 - 17640\,X^8 + 46311\,X^7 + \cdots,\\
\mathcal{G}_{128}(P) &= X^{10} - 1060254001\,X^9 + 3327073560\,X^8 + \cdots
\end{aligned}$$

Ce qui permet alors d'obtenir l'approximation

$$1.176280818209108 < \alpha < 1.176280818365\ldots.$$

Remarquons aussi que la transformation de Dandelin est facile à calculer : si on décompose le polynôme en sa partie paire plus sa partie impaire,

$$P(X) = Q(X^2) + XR(X^2),$$

alors, au signe près,

$$\mathcal{G}P(X) = Q^2(X) - XR^2(X),$$

ce qui montre bien que $\mathcal{G}P$ se calcule directement à partir des coefficients de $P$.

**Exemple 1.** *Si $P = X^n - 1$ avec $n$ impair alors $\mathcal{G}P = -P$.*

**Réductions .**

– On voit aussitôt que $\mathcal{G}_m(XP) = -X \cdot \mathcal{G}(P)$, on peut se ramener au cas où $P$ ne s'annule pas à l'origine, dans la suite on supposera donc toujours — sans le rappeler systématiquement — $P(0) \neq 0$.

– Si $P$ est de degré $d$, son polynôme réciproque est $\tilde{P}(X) = X^d \cdot P(1/X)$, alors $\mathcal{G}_m \tilde{P}$ est le polynôme réciproque de $\mathcal{G}_m P$.

– Si les polynômes $P$ et $Q$ vérifient $Q(X) = P(-X)$ alors $\mathcal{G}_m Q = (-1)^m \mathcal{G}_m P$ pour tout $m$.

– S'il existe un entier $e \geq 3$ impair tel que $P(X) = Q(X^e)$ alors, encore, $\mathcal{G}_m P(X) = \mathcal{G}_m Q(X^e)$, pour tout $m$. On pourra donc toujours supposer que, si $P = \sum a_i X^i$, alors le pgcd des indices $i$ tels que $a_i \neq 0$ est égal à une puissance de 2. Notons aussi que si $P = Q(X^2)$ alors $\mathcal{G}P = Q^2$.

– Si le polynôme $P$ n'est pas primitif, c'est-à-dire si $P = bP_1$ pour un certain entier $b$, avec $|b| > 1$ et $P_1$ à coefficients entiers, alors $\mathcal{G}_m P = b^m \mathcal{G}_m(P_1)$. On pourra donc se limiter au cas où $P$ est primitif.

– Terminons cette liste par une remarque triviale : $\mathcal{G}_m(-P) = (-1)^m \mathcal{G}_m P$ pour tout $m$.

Grâce à ces réductions on voit que l'on peut se limiter à considérer des polynômes unitaires primitifs pour lesquels $a_d > 0$, $a_{d-1} \geq 0$ et $0 < |a_0| \leq a_d$, la preuve est laissée en exercice au lecteur.

Voici maintenant un premier résultat facile.

**Théorème 1.** *Posons* $H = \mathrm{ht}(P)$. *Si* $\mathrm{lcf}(P)^2 \geq 2H$ *alors le polynôme* $\mathcal{G}P$ *vérifie*

$$\mathrm{ht}(\mathcal{G}P) \geq 2\,\mathrm{ht}(P).$$

En effet, on a $|\mathrm{lcf}(\mathcal{G}P)| = \mathrm{lcf}(P)^2$.

Pour le cas général on a le résultat suivant.

**Théorème 2.** *Soit* $P$ *de hauteur* $H$ *tel que* ${a_d}^2 \geq 2H$, *alors ce polynôme vérifie*

$$\mathrm{ht}(\mathcal{G}_m P) \geq \binom{m}{\lfloor m/2 \rfloor} \mathrm{ht}(P) \qquad \textit{pour tout} \quad m \geq 2.$$

*Démonstration.* Ceci vient d'être démontré pour $m = 2$. Considérons $m \geq 3$. Alors $\mathcal{G}_m P = {a_d}^m X^d + \cdots$ et donc $\mathrm{ht}(\mathcal{G}_m P)) \geq |a_d|^m \geq {a_d}^2 \cdot 2^{m-2} \geq 2^{m-1} H$, ce qui implique le résultat puisque $\binom{m}{\lfloor m/2 \rfloor} \leq 2^{m-1}$ d'après un lemme démontré en [2]. □

Si on applique le Théorème 1 au polynôme réciproque de $P$, on aboutit au résultat suivant.

**Théorème 3.** *Soit* $P$ *un polynôme à coefficients entiers qui n'est pas un monôme et qui vérifie* $\mathrm{ht}(\mathcal{G}P) < 2\,H$, *où* $H = \mathrm{ht}(P) > 1$. *Alors* $\max\{|a_0|, |a_d|\} < \sqrt{2\,\mathrm{ht}(P)}$. *Donc* $P$ *possède au moins trois termes non nuls.*

Examinons le cas des trinômes. Pour simplifier on pose

$$P = aX^d + bX^e + c, \quad d > e > 0, \quad d' = \lfloor d/2 \rfloor,\ e' = \lfloor e/2 \rfloor.$$

On pose à nouveau $P(X) = Q(X^2)+XR(X^2)$. Il y a quatre cas à distinguer selon les parités de $d$ et $e$. Si on note I pour impair et P pour pair les quatre cas sont PP, II, IP et PI. Posons $H_2 = \mathrm{ht}(\mathcal{G}P)$. Dans le cas PP, on a $\mathcal{G}P = Q^2$ et donc $H_2 = \mathrm{ht}(Q^2)$ et $\mathrm{ht}(P) = \mathrm{ht}(Q)$. Dans [2] on a montré que la conjecture initiale de Abbott est vraie pour le polynômes avec au plus six termes, donc $H_2 \geq 2\,\mathrm{ht}(P)$. Dans le cas II, $Q = c$, $R = aX^{d'} + bX^{e'}$ et

$$\mathcal{G}P = -a^2X^d - 2abX^{d'+e'+1} - b^2X^e + c^2$$

et on a toujours

$$H_2 = \max\{a^2, 2|ab|, b^2, c^2\} \geq 2\,\mathrm{ht}(P).$$

Dans le cas IP, $Q = bX^{e'} + c$, $R = aX^{d'}$ et

$$\mathcal{G}P = -a^2X^d + b^2X^e + 2bcX^{e'} + c^2$$

et alors

$$H_2 = \max\{a^2, 2|bc|, b^2, c^2\} \geq 2\,\mathrm{ht}(P).$$

Enfin, dans le cas PI, $Q = aX^{d'} + c$, $R = bX^{e'}$ et

$$\mathcal{G}P = a^2X^d + 2acX^{d'} - b^2X^e + c^2.$$

Ainsi, dans le cas PI, si $d \neq 2e$ on a

$$H_2 = \max\{a^2, 2|ac|, b^2, c^2\} \geq 2\,\mathrm{ht}(P)$$

et la condition (I) a lieu. Par contre, si $d' = e$ on a

$$H_2 = \max\{a^2, |b^2 - 2ac|, c^2\}.$$

Quitte à effectuer un certain nombre de réductions, on peut supposer que $P = aX^2+bX+c$ avec $a > 0$, $b \geq 0$ et $|c| \geq a$. De plus, si $ac < 0$ alors $H_2 = \max\{b^2 + 2a|c|, c^2\} \geq 2\mathrm{ht}(P)$. On supposera donc en plus $c > 0$. Enfin si $c^2 \geq 2b$ on a encore $H_2 \geq 2\mathrm{ht}(P)$, on supposera donc $b > c^2/2$. Alors $\mathrm{ht}(P) = b$ et

$$H_2 - 2b \geq b^2 - 2b - 2c^2 > c^4/4 - 3c^2,$$

ce qui montre que (I) a lieu pour $c \geq 4$. Restent les cas $1 \leq c \leq 3$.

– Si $c = 3$ alors $b \geq 5$ et $H_2 - 2b \geq b^2 - 2b - 6a$, ce qui montre que le seul cas où (I) n'a pas lieu est $b = 5$ avec $a = 3$, soit pour le polynôme

$$T_1 = 3X^2 + 5X + 3,$$

pour lequel $H_2 = 9$ et $\mathrm{ht}(T_1) = 5$ et $\mathrm{M}(T_1) = 3$.

– Si $c = 2$ alors $b \geq 3$ et $H_2 - 2b \geq b^2 - 2b - 4a$, ce qui montre que le seul cas où (I) n'a pas lieu est $b = 3$ avec $a = 1$ ou 2, soit pour les polynômes

$$T_2 = 2X^2 + 3X + 2, \qquad T_3 = X^2 + 3X + 2,$$

dont la hauteur est 3 et pour lequels $H_2 = 4$ et $H_2 = 5$, respectivement, avec $\mathrm{M}(T_2) = \mathrm{M}(T_3) = 2$.

– Si $c = 1$ alors $a = 1$, $b \geq 1$ et $H_2 - 2b \geq b^2 - 2b - 2$, ce qui montre que les seuls cas où (I) n'a pas lieu sont $b = 2$ et $b = 1$, soit pour les polynômes

$$T_4 = X^2 + 2X + 1, \qquad T_5 = X^2 + X + 1,$$

dont la hauteur est $b$ et pour lequels $H_2 = 2$ et $H_2 = 1$, respectivement, avec $\mathrm{M}(T_2) = \mathrm{M}(T_3) = 1$.

En résumé, nous avons obtenu le résultat suivant.

**Théorème 4.** *Soit $P$ un trinôme à coefficients entiers, $P = aX^d + bX^e + c$, avec $d > e > 0$ et $abc \neq 0$, alors $\mathrm{ht}(\mathcal{G}P) \geq 2\,\mathrm{ht}(P)$ sauf si $P$ est réductible à l'un des cinq polynômes suivants*

$$3X^2 + 5X + 3, \quad 2X^2 + 3X + 2, \quad X^2 + 3X + 2, \quad X^2 + 2X + 1, \quad X^2 + X + 1.$$

# 4 Les polynômes cubiques

Commençons par des remarques très élémentaires.

**Proposition 1.** *Soit $P = aX^n + bX^{n-1} + cX^{n-2} + \cdots$ un polynôme à coefficients entiers de degré $n$ avec $a > 0$. Posons $h = \mathrm{ht}(P)$ et supposons $h = \max\{a, |b|, |c|\}$. Alors, l'une quelconque des conditions suivantes*

*(i)* $b = 0$ *et* $c \neq 0$,

*(ii)* $h \geq 2$ *et* $c = 0$,

*(iii)* $c < 0$,

*implique*

$$\mathrm{ht}(\mathcal{G}P) \geq 2\mathrm{ht}(P).$$

*Démonstration.* Posons $H = \mathcal{G}P$. On a le développement

$$\mathcal{G}P = (-1)^n \big(a^2 X^n + (2ac - b^2) X^{n-1} + \cdots\big).$$

Donc, si $b = 0$ alors $|2ac - b^2| = 2a|c| \geq 2h$, ainsi (i) implique bien $H \geq 2h$.

Si $c = 0$ alors $H \geq \max\{a^2, b^2\} \geq 2h$ si $h \geq 2$.

Enfin, si $c < 0$ alors $H \geq b^2 + 2a|c| \geq 2h$. Ce qui achève la démonstration. $\square$

On peut compléter la proposition précédente par un lemme technique mais facile à démontrer.

**Lemme 1.** *Soit $P = aX^n + bX^{n-1} + cX^{n-2} + \cdots + k$ un polynôme à coefficients entiers avec $a > 0$, $b \geq 0$ et $k \neq 0$. Soient $h = \mathrm{ht}(P)$ et $H = \mathrm{ht}(\mathcal{G}P)$. Supposons $H < 2h$ alors $\max\{a, |k|\} < \sqrt{2h}$. De plus, si $h = b$ alors $b = 9$ ou $b \leq 7$.*

*Si $b = 9$ alors* (I) *a lieu sauf peut-être si $a = 4$ et $8 \leq c \leq 9$.*

*Si* $b = 7$ *alors* (I) *a lieu sauf peut-être si* $a = 3$ *et* $6 \leq c \leq 7$.
*Si* $b = 6$ *alors* (I) *a lieu sauf peut-être si* $a = 3$ *et* $5 \leq c \leq 6$.
*Si* $b = 5$ *alors* (I) *a lieu sauf peut-être si* $a = 3$ *avec* $3 \leq c \leq 5$ *ou si* $a = 2$ *avec* $4 \leq c \leq 5$.
*Si* $b = 4$ *alors* (I) *a lieu sauf peut-être si* $a = 2$ *avec* $3 \leq c \leq 4$.
*Si* $b = 3$ *alors* (I) *a lieu sauf peut-être si* $a = 2$ *avec* $1 \leq c \leq 3$ *ou si* $a = 1$ *et* $2 \leq c \leq 3$.
*Si* $b = 2$ *alors* (I) *a lieu sauf peut-être si* $a = 1$ *avec* $1 \leq c \leq 2$.

*Démonstration.* Le point de départ consiste à noter que si $a^2 \geq 2h$ alors (I) a clairement lieu. Supposons maintenant $h = b$. On note que $2b > H \geq b^2 - 2ac \geq b(b - 2a)$ implique $b \leq 2a + 1$. Avec $a^2 \leq 2b - 1$, cette inégalité donne $a \leq 2 + \sqrt{5}$ et $b \leq 5 + 2\sqrt{5}$, soit $b \leq 9$. A partir de là, on considère chaque valeur de $b$ comprise entre 2 et 9 et pour chacun de ces $b$ on calcule les valeurs possibles pour l'expression $b^2 - 2ac$ pour $1 \leq a < \sqrt{2b}$ et $1 \leq c \leq b$ (noter que si $c \leq 0$ alors $b^2 - 2ac \geq b^2 \geq 2b$). Le résultat s'ensuit. ∎

Nous pouvons maintenant appliquer cette proposition au cas des polynômes cubiques. Soit $P = aX^3 + bX^2 + cX + d$ un polynôme cubique à coefficients entiers de hauteur $h$ avec $d = P(0) \neq 0$. On a

$$\mathcal{G}P = -a^2X^3 + (b^2 - 2ac)X^2 + (2bd - c^2)X + d^2.$$

Après des réductions convenables on peut supposer $a > 0$, $b \geq 0$, $d \neq 0$ et $h = \max\{a, |b|\}$. Posons $H = \mathrm{ht}(\mathcal{G}P)$. Si $h = 1$ alors (I) a lieu sauf si $P = X^3 + X^2 + X + 1$ ou si $P = X^3 \pm 1$.

Nous supposons maintenant $h \geq 2$. On a $H \geq \max\{a^2, d^2\}$. On peut donc aussi supposer $b = h$, $a < \sqrt{2b}$ et $d < \sqrt{2b}$. D'après le Lemme ci-dessus on peut aussi supposer $c > 0$ et $b = 9$ ou $2 \leq b \leq 7$. En analysant chaque cas on aboutit finalement au résultat suivant.

**Théorème 5.** *Soit* $P$ *un polynôme cubique à coefficients entiers avec* $P(0) \neq 0$, $h = \mathrm{ht}(P)$ *et* $H = \mathrm{ht}(\mathcal{G}P)$ *alors on a* $H \geq 2h$ *sauf si* $P$ *se réduit à l'un des cas suivants :*

$$\begin{array}{lll}
P = 4X^3 + 9X^2 + 9X + 4, & & \textit{alors} \quad H = 16, \\
P = 4X^3 + 9X^2 + 8X + d, & 3 \leq d \leq 4, & \textit{alors} \quad H = 17, \\
P = 3X^3 + 7X^2 + 7X + 3, & & \textit{alors} \quad H = 9, \\
P = 3X^3 + 7X^2 + 6X + d, & 2 \leq d \leq 3, & \textit{alors} \quad H = 13, \\
P = 3X^3 + 6X^2 + 5X + d, & 2 \leq d \leq 3, & \textit{alors} \quad H = 2d + 5, \\
P = 3X^3 + 5X^2 + 3X + 1, & & \textit{alors} \quad H = 9, \\
P = 3X^3 + 5X^2 + 4X + d, & 1 \leq d \leq 2, & \textit{alors} \quad H = 9, \\
P = 3X^3 + 5X^2 + 5X + 3, & & \textit{alors} \quad H = 9, \\
P = 2X^3 + 5X^2 + 4X + d, & 1 \leq d \leq 2, & \textit{alors} \quad H = 9,
\end{array}$$

$$
\begin{array}{lll}
P = 2X^3 + 4X^2 + 3X + d,\ 1 \le d \le 2, & \textit{alors} & H = 3d + 1,\\
P = 2X^3 + 3X^2 + 3X + d,\ 1 \le d \le 2, & \textit{alors} & H = 4,\\
P = 2X^3 + 3X^2 + 2X + 1, & \textit{alors} & H = 4,\\
P = 2X^3 + 3X^2 + X + 1, & \textit{alors} & H = 5,\\
P = X^3 + 3X^2 + cX + 1,\ 2 \le c \le 3, & \textit{alors} & H = 9 - 2c,\\
P = X^3 + 3X^2 + 3X + 2, & \textit{alors} & H = 4,\\
P = X^3 + 2X^2 + cX + 1,\ 1 \le c \le 2, & \textit{alors} & H = 5 - 2c,\\
P = X^3 \pm 1, & \textit{alors} & H = 1,\\
P = X^3 + X^2 + X + 1, & \textit{alors} & H = 1.
\end{array}
$$

## 5 Inégalité de Landau

Soit maintenant $P = \sum_{i=0}^{d} a_i X^i$ non nul, non monôme. Pour tout entier $m \ge 2$ on a

$$\mathrm{L}(P) \le 2^d \mathrm{M}(P) = 2^d \big(\mathrm{M}(P)^m\big)^{1/m},$$

de plus $\mathrm{M}(P^m) = \mathrm{M}(\mathcal{G}_m P) = \mathrm{M}(P)^m$, et l'inégalité de Landau implique

$$\mathrm{L}(P) \le 2^d \mathrm{M}(P) < 2^d \big(\min\{\|P^m\|, \|\mathcal{G}_m P\|\}\big)^{1/m}.$$

En particulier,

**Théorème 6.** *Soit $P$ un polynôme à coefficients entiers de degré $d \ge 1$ qui n'est pas un monôme alors, pour tout entier $m \ge 2$ on a*

$$\|\mathcal{G}_m P\| > 2^{-md}\, \mathrm{L}(P)^m$$

*et donc*

$$\mathrm{ht}(\mathcal{G}_m P) > 2^{-md} (d+1)^{-1/2}\, \mathrm{L}(P)^m.$$

On en déduit aussitôt le résultat suivant.

**Corollaire 1.** *Soit $P$ un polynôme à coefficients entiers de degré $d$ qui n'est pas un monôme alors il existe un nombre $L_0$ tel que pour $\mathrm{L}(P) \ge L_0$ et pour tout entier $m \ge 2$ on a*

$$\mathrm{ht}(\mathcal{G}_m P) \ge 2^m\, \mathrm{ht}(P).$$

*On peut prendre $L_0 = 2\,\left(4^{d+1} \lceil \sqrt{d+1}\, \rceil\right)^2$.*

**Corollaire 2.** *Pour tout $d \ge 1$ fixé il n'existe qu'un nombre fini de polynômes à coefficients entiers de degré $d$ pour lesquels $\mathrm{ht}(\mathcal{G}P) < 2\mathrm{ht}(P)$. De plus pour un $P$ donné avec $\mathrm{M}(P) > 1$, il existe un entier $m_0$ tel que si $m \ge m_0$ et $Q = \mathcal{G}_m(P)$ alors on a $\mathrm{ht}(\mathcal{G}Q) \ge 2\mathrm{ht}(Q)$.*

# 6 Polynômes lacunaires

On appelle *valuation* d'un polynôme $P$, et on note $\mathrm{val}(P)$, le plus grand entier $r$ tel que $X^r$ divise $P$, ainsi $\mathrm{val}(X^3 - X^2) = 2$. Dans [4] le résultat suivant est démontré.

**Théorème B.** *Soit $P = a_d X^d + a_r X^r + Q$ un polynôme à coefficients entiers de degré $d$ où $Q$ est un polynôme à coefficients $\geq 0$ de degré $s$ avec $r > 2s$, alors $P$ vérifie la conjecture d'Abbott.*

Ici nous démontrons la variante suivante.

**Théorème 7.** *Soit $P = a_d X^d + a_r X^r + Q$ un polynôme à coefficients entiers de degré $d$ où $Q$ est un polynôme à coefficients $\geq 0$ de degré $s$ avec $r > (d+s)/2$ et $\max\{a_d^2, a_r^2\} \geq 2\,\mathrm{ht}(P)$ alors $\mathcal{G}P$ vérifie l'inégalité* (I).

*Démonstration.* Il faut distinguer quatre cas suivant les parités de $d$ et $r$. On constate, avec les hypothèse ci-dessus, que l'on a toujours

$$\mathrm{ht}(\mathcal{G}P) \geq \max\{a_d^2, a_r^2\},$$

d'où la conclusion. □

# 7 Utilisation des racines des polynômes

## 7.1 Polynômes admettant un nombre de Pisot-Salem comme racine

**Définition 1.** *Un* nombre de Pisot-Salem *est un entier algébrique réel strictement supérieur à 1 dont tous les conjugués sont de module au plus égal à 1.*

**Exemple 2.** *Le polynôme $P$ de degré dix considéré plus haut est un polynôme de Pisot-Salem (en fait de Salem).*

**Théorème 8.** *Soit $\alpha$ un nombre de Pisot-Salem de polynôme minimal $P$ de degré $d$, ou plus généralement un polynôme qui a une seule racine de module $> 1$, disons $\alpha$. Si $\alpha \geq 2\binom{d}{\lfloor d/2 \rfloor}$ alors $P$ vérifie l'inégalité* (I).

*Démonstration.* Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire de degré $d$, de racines $\alpha$, $\beta$, $\gamma$, … avec $\alpha > 1$ réel et $|\beta| \leq 1$, $|\gamma| \leq 1$, … alors

$$\mathrm{ht}(P) \leq \binom{d}{\lfloor d/2 \rfloor} \mathrm{M}(P) = \binom{d}{\lfloor d/2 \rfloor} \alpha.$$

Par ailleurs, les racines de $\mathcal{G}P$ sont $\alpha^2$, $\beta^2$, $\gamma^2$, … donc

$$\mathcal{G}P = X^d - (\alpha^2 + \beta^2 + \gamma^2 + \cdots) X^{d-1} + \cdots .$$

Ce qui montre que

$$\mathrm{ht}(\mathcal{G}P) \geq \alpha^2 - (d-1).$$

D'où le résultat. □

**Supplément**

On utilise le résultat suivant.

**Lemme 2.** *Soit* $P = (X - \zeta_1) \cdots (X - \zeta_m) Q(X)$ *un polynôme à coefficients complexes, alors*

$$\mathrm{ht}(P) \geq ||\zeta_1| - 1| \cdots ||\zeta_m| - 1| \cdot \mathrm{ht}(Q)$$

*ainsi que*

$$\mathrm{ht}(P) \leq (|\zeta_1| + 1) \cdots (|\zeta_m| + 1) \cdot \mathrm{ht}(Q).$$

*Démonstration.* La première inégalité est le Théorème 1 de [1], la seconde est triviale. □

On en déduit facilement.

**Théorème 9.** *Soit* $P = a_d X^d + \cdots + a_1 X + a_0$ *un polynôme à coefficients entiers avec* $a_d a_0 \neq 0$ *dont les racines* $\zeta_1, \ldots, \zeta_d$ *sont telles que*

$$||\zeta_1| - 1| \cdots ||\zeta_d| - 1| \cdot |a_d| \geq 2,$$

*alors* $P$ *vérifie l'inégalité* (I).

*Démonstration.* D'après le Lemme 2 , on obtient l'inégalité

$$\mathrm{ht}(\mathcal{G}P) \geq |a_d|^2 \left|(|\zeta_1|^2 - 1) \cdots (|\zeta_d|^2 - 1)\right| = |a_d|^2 \left|(|\zeta_1| - 1) \cdots (|\zeta_d| - 1)\right| (|\zeta_1| + 1) \cdots (|\zeta_d| + 1)$$

et la conclusion s'ensuit grâce au Lemme 2. □

**Corollaire 3.** *Soit* $P = a_d X^d + \cdots + a_1 X + a_0$ *un polynôme à coefficients entiers avec* $a_d a_0 \neq 0$ *dont les racines* $\zeta_1, \ldots, \zeta_d$ *sont telles que* $\mu = \min_{1 \leq i \leq d} \{|\zeta_i|\} \geq 1 + (2/|a_d|)^{1/d}$, *alors* $P$ *vérifie l'inégalité* (I).

*Démonstration.* L'hypothèse $\mu \geq 1 + (2/|a_d|)^{1/d}$ conduit à l'inégalité

$$||\zeta_1| - 1| \cdots ||\zeta_d| - 1| \, |a_d| \geq 2$$

et le résultat découle du Théorème 9. □

Si on considère la mesure, on voit que

$$\sqrt{d+1}\, \mathrm{ht}(\mathcal{G}P) \geq \mathrm{M}(\mathcal{G}P) = \mathrm{M}(P)^2 \geq \mathrm{M}(P) \cdot \mathrm{ht}(P)/2^d.$$

Par conséquent

$$\mathrm{M}(P) \geq \left(2\sqrt{d+1}\, \mathrm{ht}(P)\right)^{1/2} \implies \mathrm{ht}(\mathcal{G}P) \geq 2\mathrm{ht}(P).$$

Mais ce résulat ne semble pas très facile à appliquer.

# 8 Polynômes asymétriques

Dans cette section, nous considérons un polyñome *asymétrique* si un des coefficients est trés grand par rapport aux autres. Chaque fois on va préciser les sens à donner à l'expression "trés grand par rapport aux autres". Voici un résultat pour de tels polynômes.

**Théorème 10.** *Soit* $P = \sum_{i=0}^{d} a_i X^i \in \mathbb{Z}[X]$ *un polynôme non nul tel qu'il existe un indice* $\ell$ *pour lequel*

$$|a_\ell| \geq 1 + \sqrt{1 + S_1^2 + S_2^2} \quad \textit{où} \quad S_1 = \sum_{i \equiv \ell \pmod 2,\, i \neq \ell} |a_i| \quad \text{et} \quad S_2 = \sum_{i \not\equiv \ell \pmod 2} |a_i| \,.$$

*Alors* $\mathrm{ht}(\mathcal{G}P) \geq 2\,\mathrm{ht}(P)$.

*Démonstration.* On minore la hauteur de $\mathcal{G}P$ par le module du coefficient qui contient $a_\ell^2$ en notant qu'il n'y a pas d'autre terme du développement de ce coefficient qui contient $a_\ell$ et on obtient

$$\mathrm{ht}(\mathcal{G}P) \geq |a_\ell|^2 - S_1^2 - S_2^2.$$

Et l'hypothèse de l'énoncé implique

$$\mathrm{ht}(\mathcal{G}P) \geq 2\,|a_\ell|,$$

ce qu'il fallait démontrer. ∎

Le résultat que nous venons de démontrer est utile dans l'étude des polynômes quartiques avec le double de la hauteur strictement plus grande que la hauteur de la transformée de Graeffe–Dandelin.

**Théorème 11.** *Soit* $P \in \mathbb{Z}[X]$ *un polynôme primitif de degrée* $4$ *avec* $P(0) \neq 0$. *Si* $\mathrm{ht}(\mathcal{G}P) < 2\mathrm{ht}(P)$ *alors* $P$ *se réduit à l'un de* $362$ *cas qu'on peut explicitement déterminer.*

*Démonstration.* Soit $P = aX^4 + bX^3 + cX^2 + dX + e$, avec tous les coefficients entiers. Après des réductions convenables on peut supposer $a > 0$, $b \geq 0$. Notons $h = \mathrm{ht}(P)$ et $H = \mathrm{ht}(\mathcal{G}P)$. Puisque

$$\mathcal{G}P = a^2X^4 + (2ac - b^2)X^3 + (c^2 + 2ae - 2bd)X^2 + (2ce - d^2)X + e^2,$$

on a

$$H = \max\{a^2, |2ac - b^2|, |c^2 + 2ae - 2bd|, |2ce - d^2|, e^2\}.$$

Dans le cas où $h = b \geq |c|$ on applique le Lemme 1. Le raisonnement de la preuve du Théorème 5 conduit rapidement à la conclusion que $P$ se réduit à l'un des 81 cas possibles.

Dans la suite de cette preuve on suppose qu'on a $h = |c| > b$. On note que l'hypothèse $2|c| > b^2 - 2ac$ implique

$$c > 0 \qquad \text{et} \qquad b^2 \leq 2c(a+1) - 1.$$

De l'inégalité $2c > d^2 - 2ce$ on déduit

$$e \geq 1 \qquad \text{et} \qquad d^2 \leq 2c(e+1) - 1,$$

tandis que $2c > c^2 + 2ae - 2bd$ implique

$$ae < bd.$$

D'après le Théorème 10 on a $c < 1 + \sqrt{1 + (a+e)^2 + (b+|d|)^2}$, donc

$$\begin{aligned}(c-1)^2 &\leq 2(a^2+e^2) + 2(b^2+d^2) \leq 2(4c-2) + 4c(a+e-2) - 4 \\ &< 16c - 8 + 8c\sqrt{2c}.\end{aligned}$$

(Ici on a tenu aussi compte de Théorème 1.) L'inégalité en $c$ qui en résulte est satisfaite seulement pour $c \leq 161$.

Maintenant tous les coefficients de $P$ sont bornés et un programme écrit en PARI/GP [7] donne dans une minute la liste de 281 polynômes satisfaisant toutes les restrictions imposées. ∎

Notons qu'il y a aussi 8 polynômes quartiques non-primitifs satisfaisant $\mathrm{ht}(\mathcal{G}P) < 2\,\mathrm{ht}(P)$.

Dans la notation de la preuve précédente, on constate que $H$ pour les quartiques dont le coefficient de valeur maximale est $b$ prend une des valeurs 1 à 9, 11 à 13, 16, 17. Ces nombres sont des termes consecutifs dans les suites A326643 (dont le $n$-ième terme donne le nombre des sous-ensembles de $\{1, 2, \ldots, n\}$ ayant la moyenne arithmétique et celle géometrique entière) et A222030 (dont les termes sont soit des nombres premiers soit de la forme $\lfloor n^2/4 \rfloor$) listées dans [9]. La hauteur des autres polynômes mentionnés dans le Théorème 11 est égale à 1, 3 à 30, 32, 33, 35 à 37, 41, 45, 49, 53, 57 ou 65. Cette suite ne figure pas dans [9].

Le Lemme 2 montre que la hauteur $h$ d'un tel polynôme est une des valeurs 1 à 7, 9 si $h = b$. En examinant la liste produite par notre programme, on constate que $h$ peut être n'importe quel nombre de 1 à 29 ou 33 si $h = c$.

**Théorème 12.** *Soit $P \in \mathbb{Z}[X]$ de la forme $P = Q + R$, où les polynômes $Q$ et $R$ sont de parités différentes. On suppose que $a$ est un coefficient extrémal de $Q$ (c'est-à-dire relatif au degré maximal ou minimal de $Q$) et que $a \geq 1 + \sqrt{1 + \mathrm{L}(R)^2}$, alors*

$$\mathrm{ht}(\mathcal{G}P) \geq 2\,a.$$

*Si, de plus, $a = \mathrm{ht}(P)$ alors*

$$\mathrm{ht}(\mathcal{G}P) \geq 2\,\mathrm{ht}(P).$$

*Démonstration.* Comme $a$ est le coefficient d'un terme de degré extrémal de $Q$, dans la formule qui fournit $\mathcal{G}P$ la contribution de $Q$ contient un terme dont le coefficient est exactement $a^2$. Il en résulte que

$$\mathrm{ht}(\mathcal{G}P) \geq a^2 - \mathrm{L}(R)^2.$$

La conclusion de la proposition est alors évidente. ∎

Voici une variante du Théorème 12 vu plus haut.

**Théorème 13.** *Soit $P = Q + R$ un polynôme à coefficients entiers de degré $d$ tel que $Q$ soit impair, $R$ pair et que* $\mathrm{val}(Q) > \deg(R)$ *et on suppose en outre que $Q$ et $R$ vérifient* $\mathrm{ht}(Q^2) \geq c\,\mathrm{ht}(Q)$ *et* $\mathrm{ht}(R^2) \geq c\,\mathrm{ht}(R)$ *pour un certain nombre $c > 0$ alors* $\mathrm{ht}(\mathcal{G}P) \geq c\,\mathrm{ht}(P)$.

La preuve est immédiate compte tenu des hypothèses et de la formule qui exprime $\mathcal{G}P$ en fonction des polynômes $Q$ et $R$.

# 9 Un complément

**Notation 1.** *Soit $P$ un polynôme à coefficients entiers de degré $d$ de la forme $P = aX^s + R$, avec $|a| = \mathrm{ht}(P)$ et $P(0) \neq 0$. On pose $R = \sum_{i=0}^{\ell} c_i X^{r_i}$, où $r_0 < r_1 < \ldots < r_\ell$. Quitte à remplacer $P$ par son polynôme réciproque, on peut supposer que $s \leq d/2$.*

**Théorème 14.** *Soit $P(X) = R(X) + aX^s$ un polynôme pour lequel $R$ ne contient pas de terme en $X^s$. On suppose que $R$ est un polynôme en $X^\delta$ avec $\delta > 1$. Si l'une des conditions suivantes a lieu*

– *d'une part $a^2 \geq 2\mathrm{ht}(R)$ et d'autre part $s$ n'est pas divisible par $\delta$,*

– *d'une part $a \geq \mathrm{ht}(R)$ et d'autre part $s$ n'est pas divisible par $\delta$,*

*alors $P$ vérifie l'inégalité* (I).

*Si $P(X) = R(X) + aX^s + bX^t$, avec $s \neq t$, est un polynôme pour lequel $R$ ne contient pas de terme en $X^s$, ni en $X^t$ tel que $|ab| \geq \mathrm{ht}(P)$ et que $R$ est un polynôme en $X^\delta$ avec $\delta > 1$ avec de plus $s + t$ pair et non divisible par $\delta$, alors* $\mathrm{ht}(\mathcal{G}P) \geq 2\mathrm{ht}(P)$.

*Démonstration.* Dans le cas où $P(X) = R(X) + aX^s$, on a

$$\mathcal{G}P = \mathcal{G}R + a^2(-1)^s X^s + \Big(R(\sqrt{X}) + (-1)^s R(-\sqrt{X})\Big)\, a(\sqrt{X})^s.$$

On remarque d'abord qu'il n'y a aucune simplification entre $a^2(-1)^s X^s$ et $\Big(R(\sqrt{X}) + (-1)^s R(-\sqrt{X})\Big)\, a(\sqrt{X})^s$.

– Sous la première hypothèse, il n'y a pas de simplification entre $\mathcal{G}R$ et $a^2(-1)^s X^s$ (puisque les exposants du développement de $\mathcal{G}R$ sont tous des multiples de $\delta$ tandis que $s$ n'est pas divisible par $\delta$). Donc

$$\mathrm{ht}(\mathcal{G}P) \geq a^2 \geq 2\mathrm{ht}(P).$$

– Si la seconde propriété a lieu, il n'y a pas de simplification entre $\mathcal{G}R$ et $\Big(R(\sqrt{X}) + (-1)^s R(-\sqrt{X})\Big)\, a(\sqrt{X})^s$ (puisque les exposants du développement de $\mathcal{G}R$ sont tous des multiples de $\delta$ et que $\delta$ ne divise pas $s$). Donc

$$\mathrm{ht}(P^2) \geq 2\,|a| \geq 2\mathrm{ht}(P).$$

Dans le dernier cas, on a

$$\begin{aligned}\mathcal{G}P =& \mathcal{G}R + a^2(-1)^s X^s + b^2(-1)^t X^t + \big((-1)^s + (-1)^t\big)\, abX^{\frac{s+t}{2}} + \\ & \Big((-1)^s R(\sqrt{X}) + R(\sqrt{X})\Big)\, a(\sqrt{X})^s + \Big((-1)^t R(\sqrt{X}) + R(\sqrt{X})\Big)\, b(\sqrt{X})^t\end{aligned}$$

quand on regarde le développement de $\mathcal{G}P$ on voit que les hypothèses impliquent qu'il n'y a aucune simplification portant sur le terme $((-1)^s + (-1)^t)\, abX^{\frac{s+t}{2}}$ et donc que

$$\mathrm{ht}(\mathcal{G}P) \geq 2|ab| \geq 2\mathrm{ht}(P).$$

□

## 10 Une question

Dans l'introduction nous avons montré que les polynômes $P$ tels que $\mathrm{M}(P) = 1$, c'est-à-dire les produits de polynômes cyclomiques, devaient être mis de côté quand on étudie les coefficients de la transformé de Graeffe. Notons aussi que si $h$ est un nombre impair et si $P(X) = Q(X^h)$ alors $\mathcal{G}P = \mathcal{G}Q(X^h)$, ce qui conduit à considérer, pour $P = \sum_{i=0}^{d} a_i X^i$, la quantité

$$\delta = \delta(P) = \text{p.g.c.d.}\{i; a_i \neq 0\}.$$

Nous sommes maintenant en mesure de poser la question qui nous intéresse.

**Question 1.** *Existe-t-il une infinité de polynômes $P$ de hauteur égale à 1, avec $\mathrm{M}(P) > 1$ et $\delta(P) = 1$ tels que la hauteur de la transformée $\mathcal{G}P$ soit aussi égale à 1 ?*

Nous avons cherché des exemples par des calculs sur ordinateurs. Quand le degré augmente de 1, le temps de calcul est multiplié par 3, en conséquence nous n'avons pu mener les essais que pour $d \leq 27$. Pour $d = 27$, nous avons trouvé l'exemple

$$P = x^{27} - x^{24} + x^{21} + x^{20} - x^{18} - x^{17} + x^{15} + x^{14} - x^{12} - x^{11} + x^8 + x^7 + x^6 - x^5 - x^4 - x^3 + x^2 + x + 1$$

qui se factorise en

$$P = (x^2 + x + 1)(x^{25} - x^{24} + x^{19} - x^{17} + x^{13} - x^{11} + x^6 - x^3 + 1)$$

et qui vérifie

$$1.718825 < \mathrm{M}(P) < 1.718827.$$

Pour qu'un polynôme $P$ de hauteur 1 ait un transformée de Dandelin-Graeffe aussi de hauteur 1 il doit vérifier de nombreuses contraintes. Le résultat qui suit montre en particulier que ses parties paire et impaire doivent être assez bien “intercalées”.

**Proposition 2.** *Soit $P$ un polynôme de la forme $P = (\pm X^i \pm X^{i'} + \cdots) + (\pm X^j \pm X^{j'} + \cdots)$, de hauteur 1, avec $i > i' > \cdots$, $j > j' > \cdots$ et où les $i$, $i'$, … sont tous pairs tandis que tous les $j$, $j'$, … sont impairs. On suppose que $i + i' \neq 2j$ ainsi que $i + i' > j + j'$ ou bien que $j + j' \neq 2i$ ainsi que $j + j' > i + i'$, alors la hauteur du transformé $\mathcal{G}P$ est $\geq 2$.*

*Démonstration.* D'après les notations, on a

$$\begin{aligned}\mathcal{G}P &= (\pm X^{i/2} \pm X^{i'/2} + \cdots)^2 - X(\pm X^{(j-1)/2} \pm X^{(j'-1)/2} + \cdots)^2 \\ &= (X^i \pm 2X^{(i+i')/2} + \cdots) + (-X^j \pm 2X^{(j+j')/2} + \cdots).\end{aligned}$$

Et on voit que la première hypothèse implique que le terme $2X^{(i+i')/2}$ ne subit aucune simplification tandis que la seconde implique que le terme $2X^{(j+j')/2}$ ne subit aucune simplification. D'où la conclusion. ∎

**Corollaire 4.** *Soit $P$ un polynôme comme dans la Proposition 2 on suppose que $\mathcal{G}P$ est de hauteur 1, alors*

- *si $i = d$ est pair*
  - *si $i' = d-2$ alors $j = d-1$,*
  - *si $i' = d-4$ alors $j = d-1$ et $j' = d-3$,*
  - *si $i' = d-6$ alors $j = d-3$ ou $(j, j') = (d-1, d-5)$,*

  *et on a toujours $d > j > i'$,*
- *si $j = d$ est impair*
  - *si $j' = d-2$ alors $i = d-1$,*
  - *si $j' = d-4$ alors $i = d-1$ et $i' = d-3$,*
  - *si $j' = d-6$ alors $i = d-3$ ou $(i, i') = (d-1, d-5)$,*

  *et on a toujours $d > i > j'$.*

*Démonstration.* D'abord il est clair que les $i$ et les $j$ jouent des rôles similaires, on déduit donc le cas $j = d$ du cas $i = d$ en échangeant les lettres $i$ et $j$.

Soit donc $P$ comme dans la Proposition 2 avec $i = d$ et $\mathrm{ht}(\mathcal{G}P) = 1$. D'après la proposition on a nécessairement $i + i' = 2j$ ou $i + i' \leq j + j'$.

– Si $i' = d-2$ alors $(i+i')/2 = d-1$ et la seule possibilité est $j = d-1$,

– si $i' = d-4$ alors $(i+i')/2 = d-2$ et la seule possibilité est $j + j' = 2d-4$, ce qui impose $j = d-1$ et $j' = d-3$,

– si $i' = d-6$ alors $(i+i')/2 = d-3$ et les seules possibilités sont $j = d-3$ ou $(j, j') = (d-1, d-5)$.

La preuve de la dernière remarque est laissée au lecteur. ∎

Prenons l'exemple du polynôme $P$ trouvé pour $d = 26$,

$$x^{26}+x^{25}+x^{24}+x^{23}+x^{22}+x^{21}-x^{17}-x^{16}-x^{13}-x^{12}-x^{11}-x^{10}-x^9-x^6-x^5+x^3+x^2+x+1,$$

on est dans le cas $i = d$, $i' = d-2$ et on a bien $j = d-1$.

Et pour l'exemple du polynôme $P$ trouvé pour $d = 27$,

$$x^{27}-x^{24}+x^{21}+x^{20}-x^{18}-x^{17}+x^{15}+x^{14}-x^{12}-x^{11}+x^8+x^7+x^6-x^5-x^4-x^3+x^2+x+1$$

on est dans le cas $j = d$, $j' = d-6$ et on a bien $i = d-3$.

**Remarque 1.** *En appliquant le corollaire au polynôme réciproque de $P$, on obtient des conditions sur les termes de bas degré de $P$. Dans les deux exemples précédents la partie de plus bas degré est $x^2+x+1$ ce qui correspond au premier cas du corrolaire, plus généralement un polynôme $P$ pour lequel $\mathrm{ht}(\mathcal{G}P)=1$ ne se termine jamais par $\pm x^{2k}\pm 1$.*

Si $P=\sum_{i=0}^{d} a_i X^i$ on définit le *support* de $P$ par $\mathrm{S}(P)=\{i : a_i \neq 0\}$ et on pose $\#(P)=\mathrm{Card}(P)$. Nous utiliserons les notations $\mathrm{S}(P)=\{e_1,e_2,\dots,e_k\}$ où $e_1<e_2<\cdots<e_k=d$. Nous limitons notre étude aux polynômes $P$ de hauteur 1, de mesure $>1$, unitaires, avec $P(0)\neq 0$ (donc $e_1=0$) et tels que $\delta(P)=1$ et $h=\mathrm{ht}(\mathcal{G}P)=1$. On pose $P=\sum_{\ell=1}^{k}\varepsilon_\ell X^{e_\ell}$, où $\varepsilon_\ell=\pm 1$, $\varepsilon_k=1$.

Examinons les petites valeurs de $k$. Mais notons d'abord que la valeur $k=5$ est atteinte pour le polynôme $P=x^5-x^4+x^2-x+1$. Nous nous limiterons donc à $1\le k\le 4$.

Les cas $k\le 2$ sont triviaux, il n'y a aucun $P$. On note aussi que pour $k\ge 3$ l'exposant $e_2$ est nécessairement impair.

- $k=3$ : Alors $P=X^d+\varepsilon_2 X^{e_2}+\varepsilon_1$

– si $d$ est pair alors $\mathcal{G}P=X^d+2\varepsilon_1 X^{d/2}+1-X^{e_2}$ donc $h=1$ implique $\varepsilon_1=1$ et $d=2e_2$, comme $\delta=1$ on a $P=X^2+X+1$, polynôme cyclotomique, cas exclu.

– le cas $d$ impair est impossible d'après la Proposition 2.

- $k=4$ : Alors $P=X^d+\varepsilon_3 X^{e_3}+\varepsilon_2 X^{e_2}+\varepsilon_1$. Nécessairement $e_2$ est impair. Pour $d$ il y a deux cas : soit $d$ est impair et alors $e_3$ est pair, soit $d$ est pair et alors $e_3$ est impair.

– Si $d$ est impair, alors $\mathcal{G}P=-X^d-2\varepsilon_2 X^{(d+e_2)/2}-X^{e_2}+X^{e_3}+2\varepsilon_1\varepsilon_3 X^{e_3/2}+1$. Donc $h=1$ implique $e_3=2e_2$, $\varepsilon_1=\varepsilon_3=\varepsilon$ (disons) et $d+e_2=2e_3$, $\varepsilon_2=1$, donc $d=3e_2$ et de plus $e_2=2e_3$. Comme $\delta=1$, le polynôme $P$ est de la forme $P=X^3+\varepsilon X^2+X+\varepsilon=(X^2+1)(X+\varepsilon)$ et $\mathrm{M}(P)=1$, cas exclu.

– Si $d$ est pair, alors $\mathcal{G}P=X^d+2\varepsilon_1 X^{d/2}+1-X^{e_3}-2\varepsilon_2\varepsilon_3 X^{(e_3+e_2)/2}-X^{e_2}$. On a $d>e_3>(e_3+e_2)/2>e_2$ donc la condition $h=1$ implique $d=e_3+e_2$ et de plus $\varepsilon_2\varepsilon_3=\varepsilon_1$. Le seul cas possible est donc $P=X^d+X^{d-e}+\varepsilon X^e+\varepsilon$, où $e<d/2$ est impair. Mais alors $P=(X^{d-e}+\varepsilon)(X^e+1)$ et $\mathrm{M}(P)=1$, cas exclu.

D'où le corollaire suivant.

**Corollaire 5.** *Soit $P$ un polynôme comme dans la Proposition 2 on suppose que $\mathcal{G}P$ est de hauteur 1, alors $\#(P)\ge 5$.*

Posons $P=P_0+P_1$, où $P_0$ désigne la partie paire de $P$ et $P_1$ sa partie impaire et

$$P_0=\pm X^{e_{0,1}}\pm X^{e_{0,2}}\pm\cdots\pm X^{e_{0,k_0}},\quad P_1=\pm X^{e_{1,1}}\pm X^{e_{1,2}}\pm\cdots\pm X^{e_{1,k_1}},$$

où $0=e_{0,1}<e_{0,2}<\cdots<e_{0,k_0}$ et $e_{1,1}<e_{1,2}<\cdots<e_{1,k_1}$. Le transformé de Dandelin-Graeffe est $Q=\mathcal{G}P=P_0(\sqrt{X})^2-P_1(\sqrt{X})^2$.

Bien sûr les termes constants et $\pm X^d$ de $Q$ n'entrent dans aucune simplification. De plus le terme $\pm 2X^{e_{0,2}/2}$ de $Q$ doit se simplifier soit avec $\pm X^{e_{1,1}}$ soit avec $\pm 2X^{(e_{1,1}+e_{1,2})/2}$, ce qui correspond respectivement à $e_{0,2}=2e_{1,1}$ ou à $e_{2,0}=e_{1,1}+e_{1,2}$. En passant au polynôme réciproque on voit que si $d$ est pair alors le terme $\pm 2X^{(e_{0,k_0-1}+e_{0,k_0})/2}$ doit se simplifier soit avec $\pm X^{e_{1,k_1}}$ soit avec $\pm 2X^{(e_{1,k_1-1}+e_{1,k_1})/2}$ tandis que si $d$ est impair on a des résultats analogues.

**Remarque 2.** *Si $P_0 = X^d \pm 1$ et si $k \geq 5$ (donc $k_1 \geq 3$) on voit que $Q = X^d \pm 2X^{d/2} \pm 1 - P_1(\sqrt{X})^2$ et qu'au moins un des deux termes $\pm 2X^{(e_{1,1}+e_{1,2})/2}$ ou $\pm 2X^{(e_{1,k_1-1}+e_{1,k_1})/2}$ ne sera pas simplifié.*

**Notation 2.** *Si $\mathrm{S}(P) = \{e_1, e_2, \ldots, e_k\}$ avec $0 = e_1 < e_2 < \cdots < e_k = d$ on dit que $P$ est de type $(e_1, e_2, \ldots, e_k) \mod 2$, ainsi par exemple $P = X^5 - X^4 + X^2 - X + 1$ est de type 01001.*

Supposons maintenant $k = 5$.

D'après la Remarque 2 $P$ n'est pas de type 01110. Rappelons aussi qu'on a vu que $\deg P \geq 5$ et que pour le degré 5 le seul $P$ avec $\mathrm{ht}(P) = \mathrm{ht}(Q) = 1$ et $\mathrm{M}(P) > 1$ est, à une réduction près, $P = X^5 - X^4 + X^2 - X + 1$.

Si $P$ est de type 01010, alors $P_0 = X^d \pm X^{e_3} \pm 1$ et $P_1 = \pm X^{e_4} \pm X^{e_2}$, d'après les remarques plus haut, on a $e_3 = 2e_2$ et $d + e_3 = 2e_4$ et, pour les termes restants on a $d = e_2 + e_4$ ou $d = 2e_3$. Dans tous les cas on obtient $e_3 = 3e_2$, $e_4 = 3e_2$, $d = 4e_2$ et comme $\delta(P) = 1$ on conclut que $P$ se réduit à un polynôme de degré 4, cas exclu.

Si $P$ est de type 01001, en passant au polynôme réciproque on aboutit au type 01101.

Si $P$ est de type 01001 alors $P_0 = \pm X^{e_4} \pm X^{e_3} \pm 1$ et $P_1 = X^d \pm X^{e_1}$. On voit successivement que $e_3 = 2e_2$, $e_4 = 2e_3 = 4e_2$, $e_3 + e_4 = d + e_2$ donc $d = 5e_2$ et $\delta(P) = 1$ impose $P = X^5 \pm X^4 \pm X^2 \pm X \pm 1$ et finalement $P$ équivalent à $X^5 - X^4 + X^2 - X + 1$.

Donc,

**Corollaire 6.** *Si $\#(P) = 5$ avec $\mathrm{ht}(P) = \mathrm{ht}(\mathcal{G}P) = 1$, $\delta(P) = 1$ et $\mathrm{M}(P) > 1$ alors $P$ se réduit au polynôme $X^5 - X^4 + X^2 - X + 1$.*

Remarquons enfin que si $P$ est un polynôme de degré $d$ avec $\mathrm{ht}(P) = \mathrm{ht}(\mathcal{G}P) = 1$, $\delta(P) = 1$ et $\mathrm{M}(P) > 1$ et si $d'$ est un entier impair $> d$ alors le polynôme $\bar{P} = (X^d \pm 1)P$ vérifie encore $\mathrm{ht}(\bar{P}) = \mathrm{ht}(\mathcal{G}\bar{P}) = 1$, $\delta(\bar{P}) = 1$ et $\mathrm{M}(\bar{P}) > 1$. En effet $\bar{P} = X^d \cdot P \pm P$, comme il n'y a pas de simplification $\mathrm{ht}(\bar{P}) = 1$ et $\delta(\bar{P}) = 1$, d'autre part $\mathcal{G}\bar{P} = \mathcal{G}(X^d \pm 1) \cdot \mathcal{G}P = (-X^d + 1) \cdot \mathcal{G}P$ est aussi de hauteur 1 et enfin $\mathrm{M}(\bar{P}) = \mathrm{M}(X^d \pm 1) \cdot \mathrm{M}(P) = \mathrm{M}(P) > 1$. On note que le degré de $\bar{P}$ est arbitrairement grand. La même conclusion vaut en prenant $\bar{P} = (X^{2d'} + X^{d'} + 1)P$. On peut aussi prendre un polynôme, disons $F$, qui est une solution et poser $\bar{P} = F(X^d) \cdot P$, alors $\bar{P}$ est encore une solution et $\mathrm{M}(\bar{P}) = \mathrm{M}(F) \cdot \mathrm{M}(P) > \mathrm{M}(P)$, ce qui montre que la mesure d'une solution peut être arbitrairement grande. La question 1 admet donc une réponse positive. Ce qui nous amène à renforcer cette question par exemple en :

**Question 2.** *Existe-t-il une infinité de polynômes irréductibles $P$ de hauteur égale à 1, avec $\mathrm{M}(P) > 1$ et $\delta(P) = 1$ tels que la hauteur de la transformée $\mathcal{G}P$ soit aussi égale à 1 ?*

Question plus difficile que la précédente.

**Remerciements**. Le travail de M. Cipu et M. Mignotte a bénéficié d'un soutien d'un projet du GRDI ECO-Math.

## Références

[1] J. Abbott, Bounds on factors in $\mathbb{Z}[x]$, *J. Symbolic Comput.*, **50**, 532–563 (2013).

[2] M. Cipu, G. Kientega, M. Mignotte, S. Nikiema, Sur la hauteur des puissances d'un polynôme à coefficients entiers, *soumis African Diaspora Journal of Mathematics* (2020).

[3] G. Kientega, S. Nikiema, Inequalities involving the coefficients of a polynomial, *International Journal of Mathematics and Computation*, **25**, 8–17 (2014).

[4] G. Kientega, S. Nikiema, Croissance de la hauteur des puissances d'un polynôme, *Annales de l'Université de Ouagadougou, Série C*, **10**, 105–115 (2014).

[5] M. Mignotte, On the product of the largest roots of a polynomial, *J. Symbolic Computation*, **13**, 605–611 (1992).

[6] M. Mignotte, D. Ştefănescu, *Polynomials : an Algorithmic Approach*, Springer-Verlag, Singapore (1999).

[7] The PARI Group, PARI/GP, version `2.9.2`, Bordeaux (2017), available from http ://pari.math.u-bordeaux.fr/.

[8] W. Rudin, *Real and Complex Analysis (Third Edition)*, McGraw-Hill Book Company (1987).

[9] N. J. A. Sloane et al., On-Line Encyclopedia of Integer Sequences, *http ://oeis.org.*

Received : 27.01.2022
Accepted : 27.03.2022

(1) Simion Stoilow Institute of Mathematics of the Romanian Academy,
Research Unit 7, P.O. Box 1-764, Bucharest 014700, Romania
E-mail : `Mihai.Cipu@imar.ro`

(2) Université Joseph Ki-Zerbo, U. F. R. des Sciences Exactes et Appliquées,
03 BP 7021 Ouagadougou 03, Burkina Faso
E-mail : `kientdia@yahoo.fr`

(3) Université de Strasbourg, U. F. R. de Mathématiques,
67084 Strasbourg, France
E-mail : `Maurice.Mignotte@math.unistra.fr`

(4) Université de Ouahigouya, U. F. R. des Sciences et Technologies,
01 BP 346 Ouahigouya 01, Burkina Faso
E-mail : `salifouabdoul01@gmail.com`