

BOUNDS FOR HEIGHTS OF INTEGER POLYNOMIAL FACTORS

Laurențiu Panaitopol
University of Bucharest, Faculty of Mathematics,
79543 Bucarest, Romania.
Email: pan@math.math.unibuc.ro.

Doru Ștefănescu
University of Bucharest, Faculty of Physics, Department of Mathematics,
P. O. Box 39-95, Bucharest 39, Romania.
Email: stef@imar.ro.

Abstract: We describe new methods for the estimation of the bounds of the coefficients of proper divisors of integer polynomials in one variable. There exist classes of polynomials for which our estimates are better than those obtained using the polynomial measure or the 2-weighted norm.

1 Introduction

A main step in the process of factorization of integer polynomials in one variable is the estimation of the moduli of the coefficients of all possible divisors. Powerful methods are the consideration of estimations using the measure of a polynomial (cf. Mignotte [9]) and the use of weighted norms (cf. Beauzamy [3]).

We shall prove that there exist real polynomials for which sharper results may be obtained working directly with the upper bound of the roots instead of the measure. Such are, the polynomials with roots having moduli greater than one, for example Hurwitz polynomials. Alternative results are obtained for the lower bound.

We use the following standard notations:

\mathbb{N}	=	the natural numbers,
\mathbb{Z}	=	the integers,
\mathbb{Q}	=	the rational numbers,
\mathbb{R}	=	the real numbers
\mathbb{C}	=	the complex numbers,
$R[X]$	=	the univariate polynomials on the domain R ,
\mathbb{N}^*	=	the nonzero natural numbers,
\mathbb{R}_+^*	=	the nonzero positive real numbers.

Let us suppose that

$$P(X) = \sum_{i=0}^n a_i X^i \in \mathcal{C}[X] \setminus \mathcal{C},$$

and let $z_1, \dots, z_n \in \mathcal{C}$ be the roots of P .

There are several sizes associated with a polynomial $P \in \mathcal{C}[X]$. Among them we mention

$$\text{the measure} \quad M(P) = |a_n| \prod_{j=1}^n \max(1, |z_j|),$$

$$\text{the height} \quad H(P) = \max_{0 \leq i \leq n} |a_i|,$$

$$\text{the norm} \quad \|P\| = \sqrt{\sum_{i=0}^n a_i^2},$$

$$\text{the weighted } l_2 \text{-norm} \quad [P]_2 = \sqrt{\sum_{i=0}^n \frac{a_i^2}{\binom{n}{i}}}.$$

The measure was introduced by K. Mahler [8] (cf. also E. Landau [7]), the height was known to Cauchy [4], the norm corresponds to the euclidean norm of the vector given by the coefficients and the weighted norm was considered by Bombieri [2].

If $P \in \mathbb{Z}[X] \setminus \mathbb{Z}$ these sizes proved to be useful for finding bounds for the coefficients of the divisors. Let Q be a divisor of P from $\mathbb{Z}[X]$ and let $T \in \mathbb{R}_+^*$ be an upper bound for the coefficients of all possible divisors Q , i.e. T is a bound of the height of Q . A key step in factorization devices is the choice of a prime $p > T$ (or of a power of a prime $p^s > T$), which allows us to consider first the factorization of the image of P in a finite field. (See, for example ch. 7 from [10]).

Other sizes associated with P are

$$B = B(P) = \max\{|z_j|; 1 \leq j \leq n\}$$

and

$$A = A(P) = \min\{|z_j|; 1 \leq j \leq n\}$$

If Q is a proper divisor of P in $\mathbb{Z}[X]$, then the coefficients of Q are bounded by

$$\max_{0 \leq j \leq h} |a_n| \binom{h}{j} B^j, \quad (1)$$

where $h = \deg(Q) \in \{1, 2, \dots, n-1\}$. (See a proof, for example, in the monograph of A. G. Akritas [1].) We shall invoke this inequality for obtaining sharper estimates for the moduli of the coefficients of Q . For some classes of polynomials they are better than those obtained using the measure or the l_2 weighted norm. We also obtain other related evaluations of $H(Q)$ which depend on the size of a_0 and of an auxiliary parameter $\alpha > 0$.

2 Evaluation of the height of Q vs upper bounds of the roots

We first prove two results about binomial coefficients involved in the estimation of the moduli of the coefficients of Q .

Proposition 2.1 *Let $h \in \mathbb{N}^*$ and $B \in \mathbb{R}_+^*$, $B \geq 1$. Then*

$$\max_{0 \leq i \leq h} \binom{h}{i} B^i = \begin{cases} B^h & \text{if } h < B, \\ \max(B^h, \binom{h}{u} B^u), & \text{if } h \geq B, \end{cases}$$

where $u = \lfloor \frac{B(h+1)}{B+1} \rfloor$.

Proof. Because $B \geq 1$ one has

$$\binom{h}{0} B^0 = 1 \leq B^h = \binom{h}{h} B^h. \quad (2)$$

Therefore the maximum is equal to B^h or there exists $u \in \{1, 2, \dots, h-1\}$ such that

$$\max_{0 \leq i \leq h} \binom{h}{i} B^i = \binom{h}{u} B^u.$$

In this case we note that

$$\binom{h}{u} B^u \geq \binom{h}{u-1} B^{u-1} \quad (3)$$

and

$$\binom{h}{u+1} B^{u+1} \leq \binom{h}{u} B^u. \quad (4)$$

From (3) it follows that

$$\frac{B}{u} \geq \frac{1}{h-u+1},$$

therefore

$$u \leq \frac{(h+1)B}{B+1}. \quad (5)$$

On the other hand, from (4) it follows that

$$\frac{B}{u+1} \leq \frac{1}{h-u},$$

therefore

$$u \geq \frac{Bh-1}{B+1}. \quad (6)$$

From (5) and (6) it follows that

$$\frac{Bh-1}{B+1} \leq u \leq \frac{B(h+1)}{B+1}.$$

But $\frac{B(h+1)}{B+1} - 1 = \frac{Bh-1}{B+1}$. It follows that

$$\frac{B(h+1)}{B+1} - 1 \leq u \leq \frac{B(h+1)}{B+1}. \quad (7)$$

From (5) and (7) it follows that

$$u = \lfloor \frac{B(h+1)}{B+1} \rfloor. \quad (8)$$

From relations (2) and (8) it follows that

$$\max_{0 \leq i \leq h} \binom{h}{i} B^i = \max(B^h, \binom{h}{u} B^u).$$

We now observe that $h \geq \lfloor \frac{B(h+1)}{B+1} \rfloor$ if and only if $h \geq B$. Indeed

$$h - \frac{B(h+1)}{B+1} = \frac{h-B}{B+1} \geq 0 \iff h \geq B.$$

Now deal with case $H \geq B$.

If $h < B$, then $B^h > \binom{h}{s} B^s$ for all $s < h$. Actually, for $B > h$ and $s < h$ we have

$$B^h - \binom{h}{s} B^s = B^s (B^{h-s} - \prod_{i=0}^{h-s-1} \frac{h-i}{i+1}). \quad (9)$$

But $\frac{h-i}{i+1} < h-i < h < B$. Therefore

$$\prod_{i=0}^{h-s-1} \frac{h-i}{i+1} < B^{h-s}$$

and from (9) it follows that

$$B^h > \binom{h}{s} B^s.$$

Therefore if $h < B$, then

$$\max_{0 \leq i \leq h} \binom{h}{i} B^i = B^h. \quad \blacksquare$$

Theorem 2.2 Let $n \in \mathbb{N}$, $n \geq 2$ and $B \in \mathbb{R}_+^*$, $B \geq 1$. Then

$$\max_{1 \leq h \leq n-1} \left(\max_{0 \leq i \leq h} \binom{h}{i} B^i \right) = \begin{cases} B^{n-1} & \text{if } n < B+1, \\ \binom{n-1}{\lfloor \frac{Bn}{B+1} \rfloor} B^{\lfloor \frac{Bn}{B+1} \rfloor} & \text{if } n \geq B+1. \end{cases}$$

Proof. For fixed $h \in \{1, 2, \dots, n-1\}$ let

$$C(h) = \max_{0 \leq i \leq h} \binom{h}{i} B^i.$$

We have to evaluate

$$\max_{1 \leq h \leq n-1} C(h).$$

From Proposition 2.1 we know that

$$C(h) = \begin{cases} B^h & \text{if } h < B, \\ \max(B^h, \binom{h}{u} B^u), & \text{if } h \geq B, \end{cases} \quad (10)$$

where $u = \lfloor \frac{B(h+1)}{B+1} \rfloor$.

We first observe that $B^{n-1} = \max_{1 \leq i \leq n} B^i$ because $B \geq 1$.

On the other hand we compare $C(h)$ and $C(h-1)$ and we consider

$$u = \lfloor \frac{B(h+1)}{B+1} \rfloor \quad \text{and} \quad v = \lfloor \frac{Bh}{B+1} \rfloor.$$

to show that

$$\binom{h}{u} B^u \geq \binom{h-1}{v} B^v. \quad (11)$$

Indeed, we have

$$\frac{B(h+1)}{B+1} - \frac{Bh}{B+1} = \frac{B}{B+1} < 1,$$

so that

$$u - v \leq 1.$$

It follows that $u = v$ or $u = v + 1$.

First case: $u = v$.

We observe that $u \neq 0$ because $\frac{B(h+1)}{B+1} \geq 1$.

We have

$$\frac{\binom{h}{u}}{\binom{h-1}{u}} = \frac{h}{h-u} > 1$$

and therefore strict inequality in (11).

Second case: $u = v + 1$.
 In this case

$$\frac{\binom{h}{u}}{\binom{h-1}{u-1}} = \frac{h}{u} \geq 1,$$

and again (11) holds.

Now we note that

$$\frac{B(h+1)}{B+1} = h + \frac{B-h}{B+1} \leq h \quad \text{if} \quad h \geq B.$$

Hence

$$h \geq \left\lfloor \frac{B(h+1)}{B+1} \right\rfloor \quad \text{for} \quad h \geq B. \quad (12)$$

It now follows from relation (11) that $\max_{1 \leq h \leq n-1} C(h)$ is realized for $h = n - 1$.

If $n - 1 < B$, then

$$\max_h C(h) = B^{n-1}$$

by Proposition 2.1.

If $n - 1 \geq B$, then

$$\max_h C(h) = \binom{n-1}{\left\lfloor \frac{Bn}{B+1} \right\rfloor} B^{\left\lfloor \frac{Bn}{B+1} \right\rfloor}$$

again by Proposition 2.1. ■

In Proposition 2.1 and Theorem 2.2 we considered $B \geq 1$. But with slight modifications the same results hold for $0 < B < 1$.

Proposition 2.3 *Let $h \in \mathbb{N}^*$ and $B \in \mathbb{R}_+^*$, $0 < B < 1$. Then*

$$\max_{0 \leq i \leq h} \binom{h}{i} B^i = \begin{cases} 1 & \text{if } h < \frac{1}{B}, \\ \max(1, \binom{h}{u} B^u) & \text{if } h \geq \frac{1}{B}, \end{cases}$$

where $u = \left\lfloor \frac{B(h+1)}{B+1} \right\rfloor$.

Theorem 2.4 *Let $n \in \mathbb{N}$, $n \geq 2$ and $B \in \mathbb{R}_+^*$, $0 < B < 1$. Then*

$$\max_{1 \leq h \leq n-1} \left(\max_{0 \leq i \leq h} \binom{h}{i} B^i \right) = \begin{cases} 1 & \text{if } n < \frac{1}{B} + 1, \\ \binom{n-1}{\left\lfloor \frac{Bn}{B+1} \right\rfloor} B^{\left\lfloor \frac{Bn}{B+1} \right\rfloor} & \text{if } n \geq \frac{1}{B} + 1. \end{cases}$$

Now we consider an application of Theorems 2.2 and 2.4 to the estimation of the height of a proper divisor Q of P . Let $K > 0$ be a bound for $B(P)$.

Corollary 2.5 *If $1 \leq K \leq n - 1$ or $\frac{1}{n-1} < K < 1$ then*

$$H(Q) \leq |a_n| \binom{n-1}{\lfloor \frac{Kn}{K+1} \rfloor} K^{\lfloor \frac{Kn}{K+1} \rfloor}.$$

Proof. If $1 \leq K \leq n - 1$, we apply Theorem 2.2. For $\frac{1}{n-1} < K < 1$ the estimate follows from Theorem 2.4. ■

3 Limits for roots of polynomials with positive coefficients

We next show that knowledge of upper bounds for the sizes associated with a complex polynomial allows the determination of bounds of the coefficients of the divisors.

If we consider the bound (1) for the coefficients of a divisor of degree h of P , then we are interested in obtaining sharper estimates of B . The usual estimates relative to complex polynomials give evaluations that are too far from the best bound.

But for real polynomials with all the coefficients strictly positive the bound B can be evaluated in a more convenient way, thanks to a result of Eneström [5].

Theorem 3.1 *Let $P(X) = \sum_{i=0}^n a_i X^i \in \mathbb{R}_+^*[X]$. If $x_1, x_2, \dots, x_n \in \mathcal{C}$ are the roots of P then*

$$\min_{1 \leq i \leq n} \frac{a_{i-1}}{a_i} \leq |x_j| \leq \max_{1 \leq i \leq n} \frac{a_{i-1}}{a_i}, \quad \forall j = 1, 2, \dots, n.$$

Proof. We first recall the key result of Eneström about polynomials with positive real coefficients.

Let $Q(X) = \sum_{i=0}^n b_i X^i \in \mathbb{R}_+^*[X]$ and let $z_1, \dots, z_n \in \mathcal{C}$ be the roots of Q . Then

- i) If $b_0 \geq b_1 \geq \dots \geq b_n > 0$, then $|z_j| \geq 1 \quad \forall j = 1, \dots, n$.
- ii) If $0 < b_0 \leq b_1 \leq \dots \leq b_n$, then $|z_j| \leq 1 \quad \forall j = 1, \dots, n$.

Next, note that the coefficients of the polynomial

$$P_\beta(Y) = P(\beta Y) = \sum_{i=0}^n a_i \beta^i Y^i \in \mathbb{R}_+^*[Y],$$

where $\beta > 0$, satisfy

$$a_0 \geq a_1 \beta \geq a_2 \beta^2 \geq \dots \geq a_{i-1} \beta^{i-1} \geq a_i \beta^i \geq \dots \geq a_n \beta^n > 0$$

if and only if

$$\beta \leq \frac{a_{i-1}}{a_i} \forall i.$$

Taking

$$\beta = \min_{1 \leq i \leq n} \frac{a_{i-1}}{a_i}$$

and letting $y_1, \dots, y_n \in \mathcal{C}$ be the roots of P_β , we therefore have

$$|y_j| \geq 1, \quad (j = 1, \dots, n).$$

But $y_j = \frac{x_j}{\beta}$ and therefore

$$|x_j| \geq \min_{1 \leq i \leq n} \frac{a_{i-1}}{a_i}, \quad \forall j = 1, \dots, n.$$

A similar argument, based on ii), shows that

$$|x_j| \leq \max_{1 \leq i \leq n} \frac{a_{i-1}}{a_i}, \quad \forall j = 1, \dots, n$$

which ends the proof. ■

Remark: Let $P(X) = (-1)^n a_n X^n + \dots + a_2 x^2 - a_1 X + a_0 \in \mathbb{R}[X]$, where $a_0, a_1, \dots, a_n > 0$. If x_1, \dots, x_n are the roots of P then

$$\min_{1 \leq i \leq n} \left| \frac{a_{i-1}}{a_i} \right| \leq |x_j| \leq \max_{1 \leq i \leq n} \left| \frac{a_{i-1}}{a_i} \right|, \quad \forall j = 1, 2, \dots, n.$$

Indeed, the polynomial $P(-X)$ satisfies the hypotheses of Theorem 3.1 and $|x_j| = |-x_j|$ for all j .

4 Height estimates vs lower bounds of the roots

Eliminating X from the relations $P(X) = 0, Y = \alpha X$ (where $\alpha > 0$), one obtains a new polynomial $P_\alpha(Y)$. From the study of factors of P_α it is possible to derive new evaluations for the heights of factors of P .

Proposition 4.1 *Let $P \in \mathbb{Z}[X] \setminus \mathbb{Z}$, $P(0) \neq 0$, $x_1, \dots, x_n \in \mathcal{C}$ the roots of P ,*

and $\alpha \geq \frac{1}{\min_{1 \leq j \leq n} |x_j|}$. If $Q(X) = \sum_{i=0}^h b_i X^i \in \mathbb{Z}[X] \setminus \mathbb{Z}$ is a proper divisor of P

then

$$|b_i| \leq |a_0| \binom{h}{i} \alpha^i \quad \text{for all } i = 0, 1, \dots, h-1.$$

Proof. Let $Y = \alpha X$. We notice that $y_j = \alpha x_j$ ($j = 1, \dots, n$) are the roots of the polynomial

$$P_\alpha(Y) = \alpha^n P\left(\frac{Y}{\alpha}\right) = a_n Y^n + a_{n-1} \alpha Y^{n-1} + a_{n-2} \alpha^2 Y^{n-2} + \dots + a_0 \alpha^n \in \mathcal{C}[Y]$$

and $|y_j| \geq 1$ for all j .

We may suppose that x_1, x_2, \dots, x_h are the roots of the divisor Q . Therefore y_1, y_2, \dots, y_h are the roots of the polynomial

$$Q_\alpha(Y) = \alpha^h Q\left(\frac{Y}{\alpha}\right) = \sum_{i=0}^h b'_i Y^i = b_h Y^h + \sum_{i=0}^{h-1} b_i \alpha^{h-i} Y^i \in \mathcal{C}[Y].$$

As each $|y_j| \geq 1$ it follows that

$$\left| \frac{b'_i}{b_h} \right| = \left| \sum y_{u_1} y_{u_2} \dots y_{u_i} \right| \leq \binom{h}{i} |y_1 y_2 \dots y_h| = \binom{h}{i} \left| \frac{b_0}{b_h} \right| \alpha^h. \quad (13)$$

But $b'_i = \alpha^{h-i} b_i$. Therefore from (13) it follows that

$$|b_i| \leq \binom{h}{i} |a_0| \alpha^i, \quad (14)$$

which ends the proof. ■

Corollary 4.2 *If all the roots of P are outside the unit disk then*

$$|b_i| \leq \binom{h}{i} |a_0|, \quad \text{for all } i.$$

Proof. Let

$$\alpha = \frac{1}{\min |x_j|},$$

where $x_1, \dots, x_n \in \mathcal{C}$ are the roots of P . But $|x_j| \geq 1$ for all j , therefore $\alpha \leq 1$. The previous result gives now the desired estimate. ■

Remark: We obtained in [11] necessary and sufficient conditions for a polynomial over the integers to have all roots outside the unit disk. Therefore it is possible to know to which polynomials our corollary 4.2 may be applied.

Now we are able to evaluate the height of a proper divisor Q of P . Let $L > 0$ be a lower bound for $A(P)$.

Corollary 4.3 *If $\frac{1}{n-1} \leq L \leq 1$ or $1 < L \leq n-1$, then*

$$H(Q) \leq |a_0| \binom{n-1}{\lfloor \frac{n}{L+1} \rfloor} L^{-\lfloor \frac{n}{L+1} \rfloor}.$$

Proof. This follows from Proposition 4.1, with reference to Theorem 2.2, Theorem 2.4, and the proof of Corollary 2.5. ■

5 Applications

Let $P \in \mathbb{Z}[X] \setminus \mathbb{Z}$, $P(0) \neq 0$. Let m_1, m_2, m_3, m_4 be the following estimates of bounds heights of a proper polynomial divisor of P :

$$m_1 = \binom{n}{\lfloor \frac{n}{2} \rfloor} M \quad (\text{Specht, 1949})$$

$$m_2 = \frac{3^{3/4} \cdot 3^{\frac{n}{2}}}{2\sqrt{\pi n}} [P]_2 \quad (\text{Beauzamy, 1992})$$

$$m_3 = |a_n| \binom{n-1}{\lfloor \frac{Kn}{K+1} \rfloor} K^{\lfloor \frac{Kn}{K+1} \rfloor} \quad (\text{Corollary 2.5 of this paper})$$

$$m_4 = |a_0| \binom{n-1}{\lfloor \frac{n}{L+1} \rfloor} L^{-\lfloor \frac{n}{L+1} \rfloor} \quad (\text{Corollary 4.3 of this paper}),$$

where M is the measure, $[P]_2$ the weighted l_2 -norm, K is an upper bound for the maxima of the moduli of the roots and L a lower bound for the minima of the moduli of the roots.

We consider the polynomials

$$P_1 = 2X^7 - 2X^6 + 3X^5 - 4X^4 + 5X^3 - 7X^2 + 9X - 12,$$

$$P_2 = 28X^7 + 19X^6 + 13X^5 + 9X^4 + 6X^3 + 4X^2 + 3X + 2,$$

$$P_3 = X^6 + 2X^5 + 4X^4 + 5X^3 + 6X^2 + 7X + 9,$$

$$P_4 = 3X^7 + 4X^6 + 6X^5 + 9X^4 + 13X^3 + 19X^2 + 13X + 19.$$

We notice that, for these polynomials, the estimates given by Corollary 2.5 (respectively Corollary 4.3) are given by m_3 , respectively m_4 .

In the following table we compare the upper bounds of $H(Q)$ obtained from the four previous estimates, where Q is a possible proper divisor of P . The first four columns contain the sizes involved in the estimates, and the other four give the values of the estimates.

P	M	$[P]_2$	K	L	m_1	m_2	m_3	m_4
P_1	6	11.369	1.5	1	420	145.627	151.875	420
P_2	1	20.534	0.75	0.666	980	233.680	236.25	151.875
P_3	9	9.775	2	1.666	180	69.302	80	66.122
P_4	≥ 19	29.206	1.5	0.684	≥ 1995	332.046	227.812	1300.426

We note that the estimate m_1 gives better results for polynomials with small measure and small leading coefficients. The estimate m_2 gives good results for broader classes of polynomials. The estimates m_3 and m_4 apply to polynomials with strictly positive or non-zero alternate coefficients. They are useful, for example, in the study of polynomials with ‘small distances’ between consecutive coefficients.

Remark: In the original problem of factorization of a non-constant polynomial P from $\mathbb{Z}[X]$ it is necessary to find a bound which exceeds not only $H(Q)$, with Q a proper divisor of P , but also $|a_n|$.

Acknowledgment

We are grateful to Professors Douglas Bridges and Cris Calude who read and criticised previous versions of this paper.

References

1. A. G. AKRITAS: *Elements of Computer Algebra with Applications*, Wiley& Sons (1989).
2. B. BEAUZAMY, E. BOMBIERI, P. ENFLO, H. MONTGOMERY: Products of polynomials in many variables, *J. Number Theory*, **36**, 219-245 (1990).
3. B. BEAUZAMY: Products of polynomials and a priori estimates for coefficients in polynomial decompositions: A sharp result, *J. Symb. Comp.* **13**, 463-472 (1992).
4. A.-L. CAUCHY: *Exercices de Mathématiques*, 4^{ème} année, De Bure Frères, Paris (1829).
5. G. ENESTRÖM: Händelning af en allmän formel för antalet pensionärer, som vid en tidpunkt förefinns inom en sluten pension kassa, *Öfversigt af velinskapsakademiens förhandlingar* (Stockholm) **50**, 405-415 (1893).
6. D. E. KNUTH: *The Art of Computer Programming*, vol. 2, *Seminumerical Algorithms*, Addison-Wesley (1981).
7. E. LANDAU: Sur quelques théorèmes de M. Petrovitch relatifs aux zéros des fonctions algébriques, *Bull. Soc. Math. France*, **33**, 251-261 (1905).
8. K. MAHLER: An application of Jensen's formulæ to polynomials. *Mathematica*, **7**, 98-100 (1960).
9. M. MIGNOTTE: An inequality about factors of polynomials, *Math. Comp.*, **28**, 1153 - 1157 (1974).
10. M. MIGNOTTE: *Mathematics for Computer Algebra*, Springer Verlag (1991).
11. L. PANAITOPOL, D. ȘTEFĂNESCU: Some polynomial factorizations over the integers, *Bull. Math. Soc. Sc. Math. Roumanie*, **37 (85)**, n. 3-4 (1993). [to appear]
12. W. SPECHT: Abschätzungen der Wurzeln algebraischer Gleichungen, *Math. Z.* **52**, 310-321 (1949).