

# Journal of Inequalities in Pure and Applied Mathematics

## NEW INEQUALITIES ON POLYNOMIAL DIVISORS

LAURENȚIU PANAITOPOL AND DORU ȘTEFĂNESCU

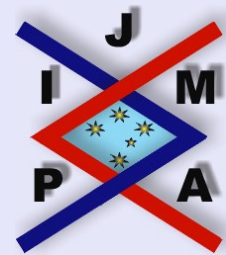
University of Bucharest  
010014 Bucharest 1  
Romania.

*EMail:* [pan@al.math.unibuc.ro](mailto:pan@al.math.unibuc.ro)

University of Bucharest  
P.O. Box 39–D5  
Bucharest 39  
Romania.

*EMail:* [stef@fpcm5.fizica.unibuc.ro](mailto:stef@fpcm5.fizica.unibuc.ro)

©2000 Victoria University  
ISSN (electronic): 1443-5756  
131-04



---

volume 5, issue 4, article 89,  
2004.

*Received 06 May, 2004;  
accepted 27 June, 2004.*

*Communicated by: L. Toth*

---

Abstract

Contents



Home Page

Go Back

Close

Quit

## Abstract

In this paper there are obtained new bounds for divisors of integer polynomials, deduced from an inequality on Bombieri's  $l_2$ -weighted norm [1]. These bounds are given by explicit limits for the size of coefficients of a divisor of given degree. In particular such bounds are very useful for algorithms of factorization of integer polynomials.

*2000 Mathematics Subject Classification:* 12D05, 12D10, 12E05, 26C05

*Key words:* Inequalities, Polynomials

## Contents

1	Introduction .....	3
2	Inequalities on Factors of Complex Polynomials .....	5
3	Bounds for Divisors of Integer Polynomials .....	7
4	Examples .....	11
4.1	Prescribed coefficients .....	11
4.2	Divisors of prescribed degree .....	13
4.3	Arbitrary divisors .....	15

References



### New Inequalities on Polynomial Divisors

Laurențiu Panaitopol and  
Doru Ștefănescu

Title Page

Contents



Go Back

Close

Quit

Page 2 of 16

# 1. Introduction

Let  $P$  be a nonconstant polynomial in  $\mathbb{Z}[X]$  and suppose that  $Q$  is a nontrivial divisor of  $P$  over  $\mathbb{Z}$ . In many problems it is important to have a priori information on  $Q$ . For example in polynomial factorization a key step is the determination of an upper bound for the coefficients of such a polynomial  $Q$  in function of the coefficients and the degree finding (see J. von zur Gathen [3], M. van Hoeij [4]). Throughout this paper we will consider inequalities involving the quadratic norm, Bombieri's norm and the height of a polynomial.

We derive upper bounds for the coefficients of a divisor in function of the weighted  $l_2$ -norm of E. Bombieri. Our main result is Theorem 3.1 in which we obtain upper bounds for the size of polynomial coefficients of prescribed degree of a given polynomial over the integers. This may lead to a significant reduction of the factorization cost. In particular we obtain bounds for the heights which are an improvement on an inequality of B. Beuzamy [2].

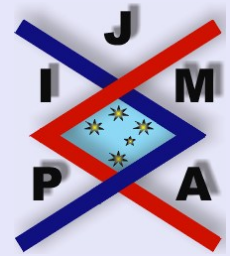
We first present some definitions.

**Definition 1.1.** Let  $P(X) = \sum_{j=0}^n a_j X^j \in \mathbb{C}[X]$ . The quadratic norm of  $P$  is

$$\|P\| = \sqrt{\sum_{j=0}^n |a_j|^2}.$$

The weighted  $l_2$ -norm of Bombieri is

$$[P]_2 = \sqrt{\sum_{j=0}^n \frac{|a_j|^2}{\binom{n}{j}}}.$$



---

## New Inequalities on Polynomial Divisors

Laurențiu Panaitopol and  
Doru Ștefănescu

---

Title Page

Contents



Go Back

Close

Quit

Page 3 of 16

The height of  $P$  is

$$H(P) = \max\{|a_0|, |a_1|, \dots, |a_n|\}.$$

The measure of  $P$  is

$$M(P) = \exp \left\{ \int_0^1 \log |P(e^{2i\pi t})| dt \right\}.$$

Note that

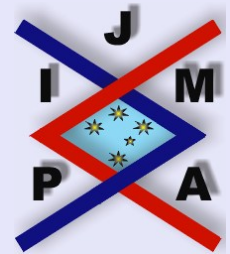
$$H(P) \leq \binom{n}{\lfloor n/2 \rfloor} \cdot M(P), \quad \|P\| \leq \binom{2n}{n}^{\frac{1}{2}} \cdot M(P), \quad H(P) \leq 2^n \cdot M(P).$$

Bombieri's norm and the height are used in estimations of the absolute values of the coefficients of polynomial divisors of integer polynomials. This reduces to the evaluation of the height of the divisors. We mention the evaluation of B. Beauzamy:

- If  $P(X) = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$ ,  $n \geq 1$  and  $Q$  is a divisor of  $P$  in  $\mathbb{Z}[X]$ , then

$$(1.1) \quad H(Q) \leq \frac{3^{3/4} \cdot 3^{n/2}}{2(\pi n)^{1/2}} [P]_2.$$

(B. Beauzamy [2]).



## New Inequalities on Polynomial Divisors

Laurențiu Panaitopol and  
Doru Ștefănescu

Title Page

Contents



Go Back

Close

Quit

Page 4 of 16

## 2. Inequalities on Factors of Complex Polynomials

We derive inequalities on the coefficients of divisors of complex polynomials, using a well-known inequality on Bombieri's norm [1] and an idea of B. Beauzamy [2].

**Proposition 2.1.** *If*

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{C}[X] \setminus \mathbb{C},$$

$P(0) \neq 0$ ,  $n \geq 3$  and

$$Q(X) = b_d X^d + b_{d-1} X^{d-1} + \cdots + b_1 X + b_0 \in \mathbb{C}[X]$$

is a nontrivial divisor of  $P$  of degree  $d \geq 2$ , then

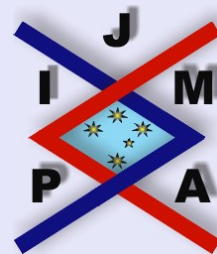
$$\begin{aligned} \left( \frac{|a_0|^2}{|b_0|^2} + \frac{|a_n|^2}{|b_d|^2} \right) \left( |b_0|^2 + |b_d|^2 + \frac{|b_i|^2}{\binom{d}{i}} \right) \\ \leq \binom{n}{d} [P]_2^2, \quad \text{for all } i = 1, 2, \dots, d-1. \end{aligned}$$

*Proof.* By an inequality of B. Beauzamy, E. Bombieri, P. Enflo and H. Montgomery [1] (cf. also B. Beauzamy [2]), it is known that if  $P = QR$  in  $\mathbb{C}[X]$ , then

$$(2.1) \quad \binom{n}{d}^{\frac{1}{2}} [P]_2 \geq [Q]_2 [R]_2.$$

Note that

$$[R]_2^2 \geq |R(0)|^2 + |lc(R)|^2 = \frac{|a_0|^2}{|b_0|^2} + \frac{|a_n|^2}{|b_d|^2}.$$



New Inequalities on Polynomial Divisors

Laurențiu Panaitopol and  
Doru Ștefănescu

Title Page

Contents



Go Back

Close

Quit

Page 5 of 16

Therefore, by (2.1),

$$(2.2) \quad [P]_2 \geq \frac{\left(\frac{|a_0|^2}{|b_0|^2} + \frac{|a_n|^2}{|b_d|^2}\right) [Q]_2}{\binom{n}{d}^{\frac{1}{2}}}.$$

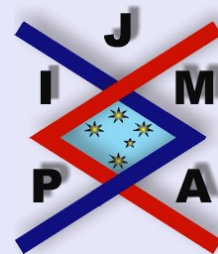
But a lower bound for  $[Q]_2$  is  $\sqrt{|b_0|^2 + |b_d|^2 + \frac{|b_i|^2}{\binom{d}{i}}}$ . Therefore

$$\left(\frac{|a_0|^2}{|b_0|^2} + \frac{|a_n|^2}{|b_d|^2}\right) \left(|b_0|^2 + |b_d|^2 + \frac{|b_i|^2}{\binom{d}{i}}\right) \leq \binom{n}{d} [P]_2^2.$$

□

**Corollary 2.2.** For all  $i \in \{1, 2, \dots, d-1\}$  we have

$$|b_i| \leq \sqrt{\binom{d}{i} \binom{n}{d} \left(\frac{|a_0|^2}{|b_0|^2} + \frac{|a_n|^2}{|b_d|^2}\right)^{-1} [P]_2^2 - \binom{d}{i} (|b_0|^2 + |b_d|^2)}.$$




---

**New Inequalities on Polynomial Divisors**

Laurențiu Panaitopol and  
Doru Ștefănescu

---

Title Page

Contents



Go Back

Close

Quit

Page 6 of 16

### 3. Bounds for Divisors of Integer Polynomials

For polynomials with integer coefficients Corollary 2.2 allows us to give upper bounds for the heights of polynomial divisors.

**Theorem 3.1.** *Let  $P(X) = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X] \setminus \mathbb{Z}$  and let  $Q(X) = \sum_{i=0}^d a_i X^i \in \mathbb{Z}[X]$  be a nontrivial divisor of  $P$  in  $\mathbb{Z}[X]$ , with  $1 \leq d \leq n-1$ . If  $n = \deg(P) \geq 4$  and  $P(0) \neq 0$ , then*

$$(3.1) \quad |b_i| \leq \sqrt{\binom{d}{i} \left( \frac{1}{2} \binom{n}{d} [P]_2^2 - a_0^2 - a_n^2 \right)} \quad \text{for all } i.$$

*Proof.* We consider first the case  $d = 1$ . We have  $\binom{d}{i} = 1$  and  $i = 0$  or  $i = 1$ . Therefore  $b_i$  divides  $a_0$  or  $a_n$ , so

$$b_i^2 \leq a_0^2 + a_n^2.$$

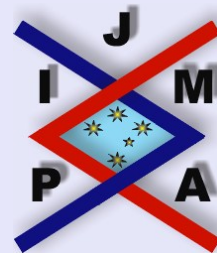
As  $n \geq 4$  it follows that

$$b_i^2 \leq 2(a_0^2 + a_n^2) - (a_0^2 + a_n^2) \leq \frac{1}{2}n[P]_2^2 - a_0^2 - a_n^2.$$

Consider now  $d \geq 2$ .

For  $i = 0$  we have

$$\begin{aligned} b_0^2 &\leq a_0^2 \leq a_0^2 + a_n^2 = \frac{1}{2}4(a_0^2 + a_n^2) - a_0^2 - a_n^2 \\ &\leq \frac{1}{2}n(a_0^2 + a_n^2) - a_0^2 - a_n^2 \end{aligned}$$



New Inequalities on Polynomial Divisors

Laurențiu Panaitopol and  
Doru Ștefănescu

Title Page

Contents



Go Back

Close

Quit

Page 7 of 16

$$\begin{aligned} &\leq \frac{1}{2} \binom{n}{d} (a_0^2 + a_n^2) - a_0^2 - a_n^2 \\ &\leq \binom{d}{i} \left( \frac{1}{2} \binom{n}{d} (a_0^2 + a_n^2) - a_0^2 - a_n^2 \right). \end{aligned}$$

The same argument holds for  $i = d$ .

We suppose now  $1 \leq i \leq d - 1$ . First we consider the case

$$\left| \frac{a_0}{b_0} \right| = \left| \frac{a_n}{b_d} \right| = 1.$$

We have

$$\left( \frac{a_0}{b_0} \right)^2 + \left( \frac{a_n}{b_d} \right)^2 = 2$$

and the inequality follows from Corollary 2.2.

If

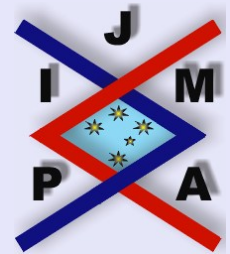
$$\left| \frac{a_0}{b_0} \right| > 1 \quad \text{or} \quad \left| \frac{a_n}{b_d} \right| > 1,$$

we have

$$\left( \frac{a_0}{b_0} \right)^2 + \left( \frac{a_n}{b_d} \right)^2 \geq 5$$

and by Proposition 2.1 we have

$$b_i^2 \leq \binom{d}{i} \left( \frac{1}{5} \binom{n}{d} [P]_2^2 - b_0^2 - b_d^2 \right).$$




---

**New Inequalities on Polynomial Divisors**

Laurențiu Panaitopol and  
Doru Ștefănescu

---

Title Page

Contents



Go Back

Close

Quit

Page 8 of 16



To conclude, it is sufficient to prove that

$$\frac{1}{5} \binom{n}{d} [P]_2^2 - b_0^2 - b_d^2 \leq \frac{1}{2} \binom{n}{d} [P]_2^2 - a_0^2 - a_n^2,$$

i.e.

$$\left(\frac{1}{2} - \frac{1}{5}\right) \binom{n}{d} [P]_2^2 \geq a_0^2 + a_n^2 - b_0^2 - b_d^2,$$

which follows from

$$\frac{3}{10} n [P]_2^2 \geq \frac{12}{10} (a_0^2 + a_n^2) > a_0^2 + a_n^2 - b_0^2 - b_d^2.$$

□

**Corollary 3.2.** *If  $n = \deg(P) \geq 4$  and  $d = \deg(Q)$  we have*

$$H(Q) \leq \sqrt{\binom{d}{\lfloor d/2 \rfloor}} \cdot \sqrt{\frac{1}{2} \binom{n}{d} [P]_2^2 - a_0^2 - a_n^2}.$$

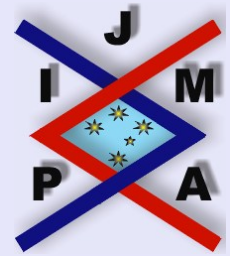
**Corollary 3.3.** *If  $n = \deg(P) \geq 6$  we have*

$$H(Q) \leq \sqrt{\frac{1}{2} \binom{d}{\lfloor d/2 \rfloor} \cdot \binom{n}{d} [P]_2^2 - 2(a_0^2 + a_n^2)}.$$

*Proof.* For  $d = \deg(Q) = 1$  we put  $Q(X) = b_0 + b_1X$ . Then  $b_0$  divides  $a_0$  and  $b_1$  divides  $a_n$ . So

$$H(Q)^2 < a_0^2 + a_n^2 \leq \frac{n-4}{2} (a_0^2 + a_n^2).$$

But this is equivalent to the statement.



## New Inequalities on Polynomial Divisors

Laurențiu Panaitopol and  
Doru Ștefănescu

Title Page

Contents



Go Back

Close

Quit

Page 9 of 16

For  $d \geq 2$  we have  $\binom{d}{\lfloor d/2 \rfloor} \geq 2$  and the inequality follows by Corollary 3.2.  $\square$

**Corollary 3.4.** For  $n = \deg(P) \geq 6$  we have

$$H(Q) \leq \sqrt{\frac{3^{(2n+3)/2}}{4\pi n} [P]_2^2 - a_0^2 - a_n^2}.$$

*Proof.* By a B. Beauzamy result we have

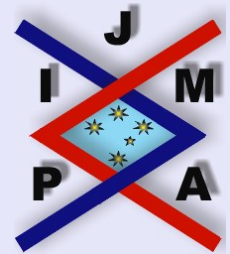
$$\frac{1}{2} \binom{d}{\lfloor d/2 \rfloor} \leq \frac{3^{(2n+3)/2}}{4\pi n}.$$

$\square$

**Corollary 3.5.** If  $\deg(P) \geq 6$  we have

$$H(Q) \leq \sqrt{\frac{3^{(2n+3)/2}}{4\pi n} [P]_2^2 - 2(a_0^2 + a_n^2)}.$$

*Proof.* We use Corollary 3.3 and the proof of Corollary 3.4.  $\square$




---

**New Inequalities on Polynomial Divisors**

Laurențiu Panaitopol and  
Doru Ștefănescu

Title Page

Contents



Go Back

Close

Quit

Page 10 of 16

## 4. Examples

We compare now the various results throughout the paper. We also compare them with estimates of B. Beauzamy [2]. The computations are done using the `gp`-package.

### 4.1. Prescribed coefficients

In polynomial factorization we are ultimately interested in knowing the size of coefficients of an arbitrary divisor of prescribed degree. We consider the following bounds for the  $i$ th coefficient of a divisor of degree  $d$  of the polynomial  $P$ :

$$B_1(P, d, i) = \sqrt{\frac{1}{2} \binom{d}{i} \cdot \binom{n}{d} [P]_2} \quad (\text{B. Beauzamy [2]}),$$

$$B_2(P, d, i) = \sqrt{\binom{d}{i} \cdot \sqrt{\frac{1}{2} \binom{n}{d} [P]_2^2 - a_0^2 - a_n^2}} \quad (\text{Theorem 3.1}).$$

Let

$$Q_1 = x^4 + x + 1,$$

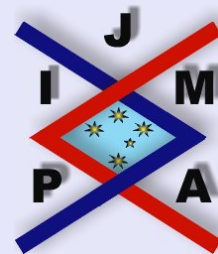
$$Q_2 = 7x^5 + 12x^4 + 11,$$

$$Q_3 = 11x^7 - x^5 + x + 1,$$

$$Q_4 = 111x^7 - x^5 + x^3 + x + 2,$$

$$Q_5 = 3x^7 + 12x^6 - x + 37,$$

$$Q_6 = 4x^{11} + x^8 + 8x^7 - x^5 + x^3 + x + 2,$$



---

New Inequalities on Polynomial Divisors

Laurențiu Panaitopol and  
Doru Ștefănescu

---

Title Page

Contents



Go Back

Close

Quit

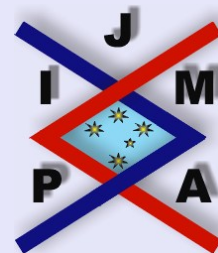
Page 11 of 16

$$Q_7 = 113x^{11} + 2x^9 - 13x^8 + x^7 - x^4 + 3x^2 + 2x + 91,$$

$$Q_8 = x^{15} + 30x^4 + 5x^3 + 2x^2 + 5x + 2.$$

$P$	$d$	$i$	$B_1(P, d, i)$	$B_2(P, d, i)$
$Q_1$	3	0	2.12	1.58
$Q_1$	3	1	3.67	2.73
$Q_1$	3	2	3.67	2.73
$Q_1$	3	3	2.12	1.58
$Q_2$	3	0	31.52	28.70
$Q_2$	3	1	54.60	49.71
$Q_3$	5	0	35.81	34.07
$Q_3$	5	1	80.09	76.19
$Q_3$	5	2	113.26	107.79
$Q_3$	6	0	20.68	17.48
$Q_3$	6	1	50.65	42.82
$Q_3$	6	2	80.09	67.71
$Q_3$	6	3	92.48	78.18
$Q_4$	6	5	508.75	429.97
$Q_5$	6	1	171.38	145.27
$Q_6$	9	1	70.88	69.59
$Q_6$	9	3	216.54	212.62
$Q_6$	10	1	33.41	30.27
$Q_6$	10	4	153.11	138.72

Table 1



**New Inequalities on Polynomial Divisors**

Laurențiu Panaitopol and  
Doru Ștefănescu

Title Page

Contents



Go Back

Close

Quit

Page 12 of 16

$Q_7$	8	2	6973.46	6931.07
$Q_7$	10	2	2282.60	2064.71
$Q_8$	13	1	71.15	70.70
$Q_8$	13	5	708.01	703.45
$Q_8$	14	2	71.15	67.88
$Q_8$	14	3	142.31	135.77
$Q_8$	14	6	408.77	389.97

Table 1 continued

## 4.2. Divisors of prescribed degree

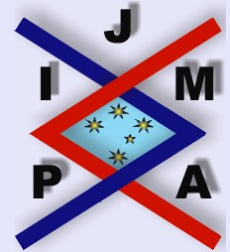
We consider now bounds for divisors of given degree  $d$ . Let

$$B_1(P, d) = \sqrt{\frac{1}{2} \binom{d}{\lfloor d/2 \rfloor} \binom{n}{d}} \cdot [P]_2 \quad (\text{B. Beauzamy [2]}),$$

$$B_2(P, d) = \sqrt{\binom{d}{\lfloor d/2 \rfloor}} \cdot \sqrt{\frac{1}{2} \binom{n}{d} [P]_2^2 - a_0^2 - a_n^2} \quad (\text{Corollary 3.2}),$$

$$B_3(P, d) = \sqrt{\frac{1}{2} \binom{d}{\lfloor d/2 \rfloor} \cdot \binom{n}{d} [P]_2^2 - 2(a_0^2 + a_n^2)} \quad (\text{Corollary 3.3})$$

We have  $B_3(P, d) < B_2(P, d) < B_1(P, d)$ . The bounds  $B_2(P, d)$  and  $B_3(P, d)$  are better for polynomials with large leading coefficients and and large free terms.



New Inequalities on Polynomial Divisors

Laurențiu Panaitopol and  
Doru Ștefănescu

Title Page

Contents



Go Back

Close

Quit

Page 13 of 16

Considering the polynomials

$$R_1 = x^5 + 13x^4 + x + 101,$$

$$R_2 = 11x^7 - x^5 + x + 1,$$

$$R_3 = 11x^7 - x^5 + x + 34,$$

$$R_4 = 14x^{11} - 3x^2 + x + 29,$$

$$R_5 = 12x^{15} - x^{14} + x^{12} - x^{11} + 2x^9 + 5x^4 + 5x^3 + 2x^2 + 5x + 16,$$

we obtain

$P$	$d$	$B_1(P, d)$	$B_2(P, d)$	$B_3(P, d)$
$R_1$	1	159.96	143.96	—
$R_1$	2	319.93	303.57	—
$R_1$	3	391.84	371.80	—
$R_1$	4	391.84	350.61	—
$R_2$	4	113.26	111.64	109.99
$R_2$	5	113.26	110.54	107.74
$R_3$	4	366.20	360.93	355.58
$R_4$	2	238.84	236.66	234.46
$R_4$	9	1895.80	1878.49	1861.02
$R_4$	10	1199.01	1143.22	1084.57
$R_5$	1	54.89	53.04	51.12
$R_5$	2	205.41	204.43	203.45
$R_5$	12	9190.89	9180.83	9170.76
$R_5$	13	6016.85	5988.26	5959.54
$R_5$	14	3216.14	3107.60	2995.12

Table 2



**New Inequalities on Polynomial Divisors**

Laurențiu Panaitopol and  
Doru Ștefănescu

Title Page

Contents



Go Back

Close

Quit

Page 14 of 16

### 4.3. Arbitrary divisors

Finally we consider bounds for an arbitrary divisor of a polynomial  $P$ . We put

$$B_1(P) = \frac{3^{3/4} \cdot 3^{n/2}}{2(\pi n)^{1/2}} \cdot [P]_2 \quad (\text{B. Beauzamy [2]}),$$

$$B_2(P) = \sqrt{\frac{3^{(2n+3)/2}}{4\pi n} [P]_2^2 - a_0^2 - a_n^2} \quad (n \geq 4, \text{ Corollary 3.4}),$$

$$B_3(P) = \sqrt{\frac{3^{(2n+3)/2}}{4\pi n} [P]_2^2 - 2(a_0^2 + a_n^2)} \quad (n \geq 6, \text{ Corollary 3.5}).$$

We always have  $B_3(P) < B_2(P) < B_1(P)$ .

If we consider

$$R_6 = 12x^6 - 2x^4 + x + 11,$$

$$R_7 = x^6 - x^3 + 11,$$

$$R_8 = 2x^6 - x^3 + 114,$$

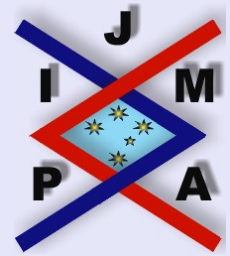
$$R_9 = 2x^9 + x^5 + 11,$$

$$R_{10} = 2x^{11} - x^6 + x^5 + 119.$$

we get

$P$	$B_1(P)$	$B_2(P)$	$B_3(P)$
$R_6$	115.47	114.33	113.16
$R_7$	78.30	77.52	76.73
$R_8$	808.15	800.07	791.90
$R_9$	336.22	336.02	335.85
$R_{10}$	9712.13	9711.41	9710.68

Table 3



Title Page

Contents



Go Back

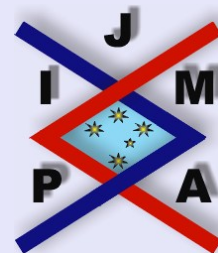
Close

Quit

Page 15 of 16

## References

- [1] B. BEAUZAMY, E. BOMBIERI, P. ENFLO AND H. MONTGOMERY, Products of polynomials in many variables, *J. Number Theory*, **36** (1990), 219–245.
- [2] B. BEAUZAMY, Products of polynomials and a priori estimates for coefficients in polynomial decompositions: A sharp result, *J. Symb. Comp.*, **13** (1992), 463–472.
- [3] J. VON ZUR GATHEN AND J. GERHARD, *Modern Computer Algebra*, Cambridge University Press (1999).
- [4] M. VAN HOEIJ, Factoring polynomials and the knapsack problem, preprint (2001).
- [5] M. MIGNOTTE, An inequality about factors of polynomials, *Math. Comp.*, **28** (1974), 1153–1157.
- [6] L. PANAITOPOL AND D. ȘTEFĂNESCU, Height bounds for integer polynomials, *J. Univ. Comp. Sc.*, **1** (1995), 599–609.



---

### New Inequalities on Polynomial Divisors

Laurențiu Panaitopol and  
Doru Ștefănescu

---

Title Page

Contents



Go Back

Close

Quit

Page 16 of 16