Mh. Math. 109, 271—277 (1990)

Monatshefte für
Mathematik

Bounding the Coefficients of a Divisor of a Given Polynomial

By

Andrew Granville*, Princeton, NJ

(Received 2 January 1989)

Abstract. We find bounds for the coefficients of a divisor $g(X)$ of a given polynomial $f(X)$.

1. Introduction

Algorithms that factor a given polynomial $f(X) \in \mathbb{Z}[X]$ in polynomial time use bounds for the coefficients of any possible divisor g of f (see [1]). Currently the most practical such bounds are both due to MIGNOTTE: In [3] he proved that if g is irreducible then

$$\|g\| \leqslant e^{\sqrt{d}}(d + 2\sqrt{d} + 2)^{1+\sqrt{d}} \|f\|^{1+\sqrt{d}} \tag{1}$$

where d is the degree of g and, for any arbitrary polynomial, $P(X) = \sum_{i \geqslant 0} p_i X^i$, we define $\|P\| := \left(\sum_{i \geqslant 0} |p_i|^2 \right)^{1/2}$. In [2] MIGNOTTE proved that for any divisor g of f,

$$\|g\| \leqslant 2^d \|f\|. \tag{2}$$

(See Section 2 of [3] for lots of other related inequalities.)

As the smallest factor of a polynomial f is irreducible and has degree $\leqslant n/2$ (where $n =$ degree of f) we see that the factoring algorithm described in [1] can be implemented under the assumption that there exists a factor g of f with

* Supported in part by NSF Grant No. DMS-8610730.

$$\|g\| \leqslant \min\left\{2^{n/2}\|f\|,\ e^{-1}\left(\frac{e}{2}\|f\|(n+\sqrt{8n}+4)\right)^{1+\sqrt{n/2}}\right\}.$$

MIGNOTTE has also shown that for a given integer polynomial g, there exists an integer polynomial f, of degree around $d^2 \log d$, such that the 2^d in (2) cannot be replaced by $(2-\varepsilon)^d$. However a careful examination of (2) leads one to realize that the inequality is probably not sharp if the degree of g is greater than, say, two-thirds of the degree of f. For, if $f = gh$ then one should expect a bound on the coefficients of g of roughly the same order of magnitude as the bound on the coefficients of h. This indeed follows from our main result:

Theorem. *If $f(X)$ and $g(X)$ are polynomials with complex coefficients, of degree n and d respectively, such that* (i) *$g(X)$ divides $f(X)$, and* (ii) *$|f(0)| = |g(0)| \neq 0$, then*

$$\|g\| \leqslant \left(\sum_{j=0}^{n-d}\binom{d}{j}^2\right)^{1/2}\|f\|. \tag{3}$$

Remark. That $f(0) \neq 0$ in (ii) simply means that we have removed any powers of X dividing $f(X)$ — clearly this does not affect the result. That $|f(0)| = |g(0)|$ in (ii) prohibits one from artificially multiplying g by a large constant.

As a consequence of the theorem we have

Corollary. *If $f(X)$ and $g(X)$ are polynomials with integer coefficients such that g divides f then*

$$\|g\| \leqslant \left(\frac{\sqrt{5}+1}{2}\right)^n \|f\|, \tag{4}$$

where n is the degree of f.

For an arbitrary divisor g of f, (4) improves on (2). It is thus of interest to determine the smallest β such that the estimate

$$\|g\| \leqslant \beta^{n\{1+o(1)\}}\|f\|, \quad n = \deg f$$

holds uniformly as $n \to \infty$, for all g dividing f. By (2), $\beta \leqslant 2$ and (4) improves this to $\beta \leqslant \left(\frac{1+\sqrt{5}}{2}\right) \approx 1.61803\ldots$. We use the following lemma to find a non-trivial lower bound on β:

Lemma. *If $f(X)$ and $g(X)$ are polynomials satisfying* (i) *and* (ii) *of the Theorem, and the coefficients of g are all non-negative, then*

$$\beta \geq (|g|/|f|)^{1/\deg f}, \tag{5}$$

where, for an arbitrary polynomial $P(X) = \sum_{i \geqslant 0} p_i X^i$, we define $|P|: = \sum_{i \geqslant 0} |p_i|$.

If we choose $g(X) = 1 + cX + c^2 X^2 + \ldots + c^{d-1} X^{d-1}$ and $f(X) = 1 - c^d X^d$ for some positive real number c and integer $d \geqslant 1$, then $\beta \geqslant ((1 - c^d)/(1 - c)(1 + c^d))^{1/d}$ by the Lemma. The choice $d = 5$, $c = 0.8846$ leads to $\beta \geqslant 1.208\ldots$.

Acknowledgements: This paper forms part of the author's doctoral thesis completed under the supervision of Dr. PAULO RIBENBOIM at Queen's University in 1987. I would like to thank Professor RIBENBOIM, as well as GREG FEE and MIKE MONAGAN, with whom I had relevant discussions.

2. The Proof of the Theorem

Define a map Φ: $\mathbb{C}[X] \to \mathbb{C}[X]$ by

$$\Phi(f(X)) = f(X) \prod_{\substack{f(\alpha) = 0 \\ |\alpha| < 1}} \alpha \left(\frac{\bar{\alpha} X - 1}{X - \alpha} \right)$$

where the product counts each of any multiple roots. In [2], MIGNOTTE observed that

$$\|(\bar{\alpha} X - 1) P(X)\| = \|(X - \alpha) P(X)\|$$

for any polynomial $P(X)$ and complex number α, and so

$$\|g\|/\|f\| = \left(\prod_{\substack{(f/g)(\alpha) = 0 \\ |\alpha| < 1}} |\alpha| \right) \|\phi(g)\|/\|\phi(f)\|, \tag{6}$$

for any polynomials f and g satisfying (i) and (ii). Clearly (3) will follow from this equation if (3) holds with f replaced by $\Phi(f)$ and g replaced by $\Phi(g)$. Thus we may henceforth assume

(iii) All roots of $f(X)$ lie on or outside the unit circle.

So suppose that f and g satisfy (i), (ii) and (iii) above. The coefficient of X^{d-j} in $g(X)$ is given by the leading coefficient of g times the sum, over all j-subsets of the d roots of $g(X)$, of the product of those j roots. Now, as each root of $g(X)$ lies on or outside the unit circle, this has magnitude less than or equal to $\binom{d}{j}$ times the leading coefficient of g times the absolute value of the product of all the roots of $g(X)$, which equals $\binom{d}{j}|g(0)|$. Therefore, by (ii),

$$g(X) \quad \text{is majorized by} \quad |f(0)|\,(1+X)^d. \tag{7}$$

(The power series $\sum_{i\geq 0} u_i X^i$ is said to be *majorized* by $\sum_{i\geq 0} v_i X^i$ if $|u_i| \leq v_i$ for each i.)

Remark. (2) follows immediately from (7), as $|f(0)| \leq \|f\|$ and $\sum_{j=0}^{d} \binom{d}{j}^2 = \binom{2d}{d} \leq 2^{2d}$.

We now use a different method to majorize $g(X)$: Define

$$h(X) = f(X)/g(X) = c \prod_{i=1}^{n-d} (X - \alpha_i).$$

Thus

$$1/h(X) = 1\bigg/\left(h(0) \prod_{i=1}^{n-d} (1 - X\alpha_i^{-1})\right).$$

Now, as each α_i^{-1} lies on or inside the unit circle (by (iii)), thus the power series $1/(1 - X\alpha_i^{-1})$ is majorized by $1/(1-X)$. Therefore, as $|h(0)| = 1$ (by (ii)), we see that $1/h(X)$ is majorized by $1/(1-X)^{n-d}$. Now, by definition, $g(X) = (1/h(X))f(X)$ and so

$$g(X) \quad \text{is majorized by} \quad \left(\sum_{j=0}^{n} |f_j|\, X^j\right)\bigg/(1-X)^{n-d} \tag{8}$$

where $f(X) := \sum_{j=0}^{n} f_j X^j$. By expanding this product we deduce that

$$|g_m| \leq \sum_{j=0}^{m} |f_j| \binom{m-j+n-d-1}{m-j} \tag{9}$$

for each $m = 0, 1, \ldots, d$ where $g(X) := \sum_{m=0}^{d} g_m X^m$.

Now, from (7), as $|f(0)| \leqslant \|f\|$,

$$\sum_{m=2d-n+1}^{d} |g_m|^2 \leqslant \|f\|^2\left(\sum_{m=2d-n+1}^{d} \binom{d}{m}^2\right) = \|f\|^2\left(\sum_{j=0}^{n-d-1} \binom{d}{j}^2\right)$$

using the change of variable $j = d - m$. So in order to prove (3) we need only show

$$\sum_{m=0}^{2d-n} |g_m|^2 \leqslant \|f\|^2\binom{d}{n-d}^2. \tag{10}$$

For convenience write $u = 2d - n$ and $v = n - d - 1$. For each $0 \leqslant i, j \leqslant u$ define

$$d_{i,j} = \sum_{r=0}^{u-j} \binom{r+v}{v}\binom{r+v+j-i}{v}$$

and

$$e_i = \sum_{j=0}^{u} d_{i,j}.$$

Note that $d_{i,j} \leqslant d_{0,j}$ for each i and j and so $e_i \leqslant e_0$. Therefore, by (9),

$$\begin{aligned}\sum_{m=0}^{u} |g_m|^2 \leqslant \sum_{m=0}^{u}\left(\sum_{i=0}^{m} |f_i|\binom{m-i+v}{v}\right)^2 = \\ = \sum_{i=0}^{u} d_{i,i}|f_i|^2 + 2\sum_{0\leqslant i<j\leqslant u} d_{i,j}|f_i|\,|f_j| \leqslant \\ \leqslant \sum_{i=0}^{u} e_i|f_i|^2 \leqslant e_0\,\|f\|^2\end{aligned}$$

as $2|f_i|\,|f_j| \leqslant |f_i|^2 + |f_j|^2$. But then (10) follows as

$$\begin{aligned}e_0 &= \sum_{r=0}^{u}\binom{v+r}{v}\sum_{j=0}^{u-r}\binom{v+r+j}{v} \leqslant \\ &\leqslant \binom{v+u+1}{v+1}\sum_{r=0}^{u}\binom{v+r}{v} = \binom{v+u+1}{v+1}^2 = \binom{d}{n-d}^2.\end{aligned}$$

3. Upper and Lower Bounds for β

Proof of the Lemma: For an arbitary polynomial P, we note the inequalities

$$\|P\| \leqslant |P| \leqslant (1 + \deg P)\,\|P\|$$

which are given in [3]; also that $|P^k| \leqslant |P|^k$, with equality whenever the coefficients of P are all non-negative.

So suppose that f and g satisfy (i) and (ii) above, and that the coefficients of g are all non-negative. Then, for any positive integer k,

$$\|g^k\|/\|f^k\| \geqslant |g^k|/|f^k|\,(1 + \deg(g^k)) \geqslant (|g|/|f|)^k\,(1 + k\,\deg(g)).$$

and so

$$\log\beta \geqslant \lim_{k\to\infty} \frac{1}{\deg f^k} \log(\|g^k\|/\|f^k\|) \geqslant \frac{1}{\deg f}\log(|g|/|f|).$$

Sketch of the proof of the Corollary: After dividing f and g by any powers of X that divide them, and multiplying g through by $f(0)/g(0)$, the resulting polynomials, f and g, satisfy (i) and (ii) of the Theorem. The result thus follows from proving the inequality

$$\sum_{j=0}^{n-d} \binom{d}{j}^2 \leqslant \left(\frac{\sqrt{5}+1}{2}\right)^{2n} \tag{11}$$

for all positive $n > d \geqslant 1$.

To prove (11) we make repeated use of Stirling's formula in the form

$$1 < n!\,(2\pi n)^{-1/2}\,(n/e)^{-n} < e^{1/12n}:$$

If $d \leqslant 2n/3$ then the left-hand side of (11) is bounded above by $\sum_{j=0}^{d} \binom{d}{j}^2 = \binom{2d}{d}$, and (11) follows from an easy application of Stirling's formula. If $2n/3 < d < n$ then the left-hand side of (11) is bounded above by $(n - d + 1)\binom{d}{n-d}^2$, and this expression is maximized when $d = \left(\frac{1 + 1/\sqrt{5}}{2}\right)n + O(1)$; (11) then follows from Stirling's formula.

References

[1] LANDAU, S.: Factoring polynomials quickly. Notices Amer. Math. Soc. **34**, 3—8 (1987).

[2] MIGNOTTE, M.: Some useful bounds. In: BUCHBERGER, B., et al. (eds.). Computer Algebra, Symbolic and Algebraic Computation, 259—263. Wien – New York: Springer 1982.

[3] Mignotte, M.: An inequality about irreducible factors of integer polynomials. J. Number Theory **30**, 156—166 (1988).

A. Granville
School of Mathematics
The Institute for Advanced Study
Princeton, NJ 08540, U.S.A.

Printed in Austria