NORMS OF FACTORS OF POLYNOMIALS

Michael Filaseta and Ikhalfani Solan*

1. Introduction

Let $\alpha_1, \alpha_2, \dots, \alpha_d$ be the roots, appearing as many times as their multiplicity, of a non-zero polynomial $A(x) \in \mathbb{Z}[x]$. Thus, we may write

$$A(x) = \sum_{j=0}^{d} a_j x^j = a_d \prod_{j=1}^{d} (x - \alpha_j) \tag{1}$$

where the a_j are integers with $a_d \neq 0$. We define the Euclidean norm of A to be $\|A\| = \left(\sum_{j=0}^{d} |a_j|^2 \right)^{1/2}$. With a positive integer N and a polynomial A fixed, we will be interested in bounding the size of $\|Q(x)\|$ given that $Q(x) \in \mathbb{Z}[x]$ and $\|AQ\| \leq N$. Such a bound on $\|Q\|$ is not always possible. In fact, if $A(x)$ is divisible by a cyclotomic polynomial $\Phi_m(x)$, then by considering $w(x) \in \mathbb{Z}[x]$ for which $w(x)\Phi_m(x) = x^m - 1$, we deduce that the Euclidean norm of

$$A(x)w(x)(x^{km} + x^{(k-1)m} + \cdots + x^m + 1)$$

for any positive integer k is bounded above by a quantity that is independent of k. Hence, whenever $A(x)$ is divisible by a cylcotomic polynomial and N is sufficiently large, there will be $Q(x) \in \mathbb{Z}[x]$ with arbitrarily large Euclidean norm and with $\|AQ\| \leq N$. It is reasonable, however, to expect that the Euclidean norm of $Q(x)$ is bounded whenever $A(x)$ is free of cyclotomic factors. This in fact is the main result of this paper.

Theorem 1. *Let $A(x) \in \mathbb{Z}[x]$ be a polynomial having no cyclotomic factors. Let $N \geq 1$. If $Q(x) \in \mathbb{Z}[x]$ and $\|A(x)Q(x)\| \leq N$, then $\|Q\|$ is bounded by a function depending only on $A(x)$ and N.*

The bound on $\|Q\|$ can be made explicit, and this will be clear from the arguments. There are special cases where such a bound follows from the

*Both authors were supported by NSF Grant DMS-9400937. Research of the second author was done as partial fulfillment of the Ph.D. requirement at the University of South Carolina.

literature. In particular, if $A(\alpha)Q(\alpha) = 0 \implies A(1/\alpha)Q(1/\alpha) \neq 0$, then Theorem 1 follows from the main result of Schinzel in [9]. More generally, if $A(x)$ has no roots with absolute value 1, then a theorem of Donaldson and Rahman [2] would imply Theorem 1. Furthermore, in this case, the bound on $\|Q\|$ takes a nice form. We explain this use of Donaldson and Rahman's work in more detail in Section 4.

As a consequence of a more general conjecture of Schinzel [10], it would follow that if $A(x)Q(x)$ has no cyclotomic factors and $\|AQ\| \leq N$, then $\|Q\|$ is bounded by a function depending only on N. On the other hand, Schinzel (private communication) has supplied us with the following example which shows that the dependence of the bound for $\|Q\|$ on the polynomial $A(x)$ is necessary in Theorem 1. Let p and q be odd primes with $p > q$. Let $A(x) = \Phi_{pq}(x) + x - 1$ and $Q(x) = (x^p - 1)(x^q - 1)/(x - 1)$. Then

$$A(x)Q(x) = x^{pq} + x^{p+q} - x^p - x^q.$$

Thus, $\|AQ\| = 2$, but $\|Q\|$ can be arbitrarily large. It can be shown that $A(x)$ is x^q times an irreducible polynomial which is not cyclotomic. Thus, the bound on $\|Q\|$ in Theorem 1 must depend on $A(x)$. By applying classical bounds on norms of factors of polynomials, it is not difficult to see that the bound on $\|Q\|$ can be made a function of only the degree of $A(x)$ and N. Whether the bound on $\|Q\|$ can be made a function of only $\|A\|$ and N is unclear.

A second problem we consider in this paper is that of finding among all nonzero integer polynomials which are divisible by a given polynomial $A(x)$, a polynomial with minimum Euclidean norm. Thus, we want a nonzero element of the principal ideal $(A(x))$ in $\mathbb{Z}[x]$ with smallest possible Euclidean norm. Similar to our discussion above, it is not difficult to produce examples where the polynomial $A(x)$ has a large Euclidean norm while an obvious multiple of $A(x)$ has decidedly lower Euclidean norm.

We will make use of the notation:

$$M(A) = |a_d| \prod_{j=1}^{d} \max\{1, |\alpha_j|\} \text{ (the Mahler measure of } A),$$

$$\|A\|_{\min} = \min\{\|P\| : P(x) \in \mathbb{Z}[x], A(x)|P(x), P(x) \not\equiv 0\},$$

$$\mathcal{P}_A = \{QA : Q \in \mathbb{Z}[x], Q(0) \neq 0, ||QA|| = \|A\|_{\min}\}.$$

Thus, we are interested in an algorithm for finding an element of $\mathcal{P}_A$. We will not be able to resolve this problem in general, but an answer to the problem does follow from Theorem 1 in the case that $A(x)$ has no cyclotomic factors. In fact, in this case, $\mathcal{P}_A$ has a finite number of elements and they can all be determined. Previously, the first author together with

Robinson and Wheeler [4] found such an algorithm in the case that $A(x)$ is irreducible. The more general problem considered here was posed at the end of that paper.

Similar to their approach, the idea is to find an upper bound B on the degree of the elements of $\mathcal{P}_A$. Once this has been accomplished, then the task of finding the elements of $\mathcal{P}_A$ can be seen to be effectively computable as follows. We observe that A is in the ideal $(A(x))$ so $\|A\|$ is an upper bound on $\|A\|_{\min}$. This means that the coefficients of any element of $\mathcal{P}_A$ are each bounded in absolute value by $\|A\|$. Thus, the elements of $\mathcal{P}_A$ can be determined by considering all the polynomials in $\mathbb{Z}[x]$ with coefficients bounded in absolute value by $\|A\|$ and with degree at most B. Those which are divisible by $A(x)$ and have the smallest Euclidean norm are then the elements of $\mathcal{P}_A$.

Theorem 2. *Let $A(x) \in \mathbb{Z}[x]$ be a polynomial having no cyclotomic factors. Let $P(x) \in \mathcal{P}_A$. Then $\deg P$ is bounded by a function depending only on A.*

The bound on $\deg P$ can be made explicit. Indeed, the method described above for finding the elements of $\mathcal{P}_A$ depends on having more than an existence proof of a bound on $\deg P$.

The bounds in this paper will be functions of other known bounds in the literature. To be explicit, we will need a quantity $B(m, N)$ satisfying the following condition:

(C) For any non-zero $P(x) \in \mathbb{Z}[x]$ of degree $\leq m$ with $\|P\| \leq N$ and any $Q(x) \in \mathbb{Z}[x]$ such that $Q(x)|P(x)$, we have $\|Q\| \leq B(m, N)$.

We may take, for example, $B(m, N)$ of the form $\beta^m N$ for some appropriate β (cf. [1], [5], [6], [8]; $\beta = 2$ will suffice), but we allow for the possibility that a different estimate may be used. We also note that in (C) we may suppose that $B(m, N)$ is increasing with respect to each of m and N, and we do so.

2. Preliminaries and Lemmas

Let $P \in \mathbb{Z}[x]$ with $P(0) \neq 0$. We define the reciprocal polynomial of P to be $P^*(x) = x^{\deg P} P(1/x) \in \mathbb{Z}[x]$. It is clear that if $P \in \mathcal{P}_{\mathcal{A}}$, then $P^* \in \mathcal{P}_{\mathcal{A}^*}$. Furthermore, $\deg P = \deg P^*$ and $\|P\| = \|P^*\|$. By considering reciprocal polynomials when necessary, we will be able to suppose that a polynomial under consideration either has a root inside the unit circle or has all its roots on the unit circle.

We begin with some lemmas which may be viewed as extensions of two lemmas appearing in [4]. We define $A(x)$ as in (1). Observe that for any polynomial $f(x)$, we have $\|f(x)\| = \|xf(x)\|$. It follows that we may suppose $a_0 \neq 0$ in Theorem 1 and Theorem 2. Set

$$P(x) = \sum_{j=1}^{n} c_j x^{d_j}$$

with $0 = d_1 < d_2 < \cdots < d_n = \deg P(x)$ and each c_j non-zero. For fixed J with $1 \leq J \leq n$, set

$$P_J(x) = \sum_{j=1}^{J} c_j x^{d_j}. \tag{2}$$

Lemma 1. *Suppose $A(x)$ is irreducible and has a root with absolute value < 1. Let N be such that $\|P\| \leq N$, and let $J \in \{1, 2, \ldots, n-1\}$. If $A(x)|P(x)$ and $A(x) \nmid P_J(x)$, then*

$$d_{J+1} \leq C(d_J + 2d)$$

where $C = \log N / \log(M(A)/|a_0|)$.

Here, $A(x)|P(x)$ and $P(0) \neq 0$, so that $a_0 \neq 0$ follows. Observe that the condition $A(x)$ has a root with absolute value < 1 implies

$$M(A) > |a_d| \prod_{j=1}^{d} |\alpha_j| = |a_0|.$$

Thus, the definition of C above makes sense.

For the proof of Lemma 1, we let R_J denote the resultant of $A(x)$ and $P_J(x)$. Let λ denote the number of roots of $A(x)$ having absolute value < 1. We use well known properties of resultants [11] to obtain

$$\begin{aligned}
1 \leq |R_J| &= |a_d|^{d_J} \prod_{j=1}^{d} |P_J(\alpha_j)| \\
&= |a_d|^{d_J} \prod_{|\alpha_j|<1} |P(\alpha_j) - P_J(\alpha_j)| \prod_{|\alpha_k|\geq 1} |P_J(\alpha_k)| \\
&\leq |a_d|^{d_J} \prod_{|\alpha_j|<1} \left(|\alpha_j|^{d_{J+1}} \sum_{h=J+1}^{n} |c_h| \right) \prod_{|\alpha_k|\geq 1} \left(|\alpha_k|^{d_J} \sum_{i=1}^{J} |c_i| \right) \\
&\leq \left(\frac{|a_0|}{M(A)} \right)^{d_{J+1}} \left(\sum_{h=J+1}^{n} |c_h| \right)^{\lambda} M(A)^{d_J} \left(\sum_{i=1}^{J} |c_i| \right)^{d-\lambda}.
\end{aligned}$$

Dividing by $(|a_0|/M(A))^{d_{J+1}}$ and taking logarithms of both sides gives

$$d_{J+1} \leq \frac{\log M(A)}{\log\left(M(A)/|a_0|\right)} d_J + \frac{\log\left(\left(\sum_{h=J+1}^{n} |c_h|\right)^{\lambda} \left(\sum_{i=1}^{J} |c_i|\right)^{d-\lambda} \right)}{\log\left(M(A)/|a_0|\right)}. \tag{3}$$

Now

$$\sum_{h=J+1}^{n} |c_h| \leq \sum_{h=J+1}^{n} |c_h|^2 \leq N^2.$$

Similarly,

$$\sum_{i=1}^{J} |c_i| \leq N^2.$$

Hence, it is clear by (3) that

$$d_{J+1} \leq \frac{\log M(A)}{\log\left(M(A)/|a_0|\right)} d_J + \frac{2d \log N}{\log\left(M(A)/|a_0|\right)}.$$

By well known properties of Mahler measure, we obtain $M(A) \leq M(P) \leq \|P\| \leq N$. Since

$$C = \frac{\log N}{\log\left(M(A)/|a_0|\right)} \geq \frac{\log M(A)}{\log\left(M(A)/|a_0|\right)} \geq 1,$$

we deduce

$$d_{J+1} \leq C d_J + 2dC$$

as required.

Lemma 2. *Let $N \geq 1$, and let $A(x) \in \mathbb{Z}[x]$ as in (1). Assume that $A(x)$ is irreducible and has at least one root inside the unit circle. If there exists $Q(x) \in \mathbb{Z}[x]$ such that $\|AQ\| \leq N$, then $\|Q\|$ is bounded above by a constant depending only on $A(x)$ and N (and independent of Q and its degree). More specifically,*

$$\|Q\| \leq NB(2dN^4 C^{N^2}, N),$$

where $C = \log N / \log\left(M(A)/|a_0|\right)$.

Proof. We may suppose that $Q(0) \neq 0$ and do so. We set $P(x) = A(x)Q(x)$. We consider 3 cases.

CASE 1: $A(x) \nmid P_J(x)$ for all $J \in \{1, 2, \dots, n-1\}$.

We may apply Lemma 1 for each $J \in \{1, 2, \dots, n-1\}$ to obtain that

$$d_{J+1} \leq C(d_J + 2d).$$

Recall that $d_1 = 0$ and, as shown above, $C \geq 1$. By induction on J, we have

$$\text{(4)} \qquad \deg\ P = d_n \leq 2d \sum_{j=1}^{n} C^j \leq 2dnC^n.$$

But then $n \le \|P\|^2 \le N^2$ implies that $\deg P \le 2dN^2C^{N^2}$. By Condition (C), we obtain

$$\|Q\| \le B(2dN^2C^{N^2}, N).$$

The right side is less than the bound given in the lemma, so in this case we are through.

CASE 2: $A(x)|P_J(x)$ for some J and $d_{J+1} - d_J \le 2dN^2C^{N^2}$ for all $J \le n-1$.

Since $n \le N^2$, summing the inequality on J and using that $d_1 = 0$, we obtain $\deg(A(x)Q(x)) \le 2dN^4C^{N^2}$. Here, we deduce that

$$\|Q\| \le B(2dN^4C^{N^2}, N),$$

completing the argument in this case.

CASE 3: For some $J \le n-1$, $d_{J+1} - d_J > 2dN^2C^{N^2}$.

Let r be the number of J's for which $d_{J+1} - d_J$ exceeds $2dN^2C^{N^2}$. Let $1 \le J_1 < J_2 < \cdots < J_r \le n-1$ be such that $J \in \{J_1, J_2, \ldots, J_r\}$ if and only if $d_{J+1} - d_J > 2dN^2C^{N^2}$. We show that $A(x)|P_J(x)$ for each $J \in \{J_1, J_2, \ldots, J_r\}$. Assume otherwise, and let $i \in \{1, 2, \ldots, r\}$ be minimal such that $A(x) \nmid P_{J_i}(x)$. Let $J' \in \{1, 2, \ldots, J_i - 1\}$ be maximal such that $A(x)|P_{J'}(x)$; if no such J' exists, we set $J' = 0$ and $P_{J'}(x) = P_0(x) = 0$. We consider the polynomial $(P(x) - P_{J'}(x))/x^{d_{J'+1}}$. This polynomial is a multiple of $A(x)$ and has norm $\le \|P\| \le N$. By Lemma 1 with this polynomial in the place of $P(x)$, we deduce

$$d_{J+1} - d_{J'+1} \le C(d_J - d_{J'+1} + 2d) \quad \text{for } J' < J \le J_i.$$

We appeal to the argument we gave for (4) to obtain

$$d_{J_i+1} - d_{J'+1} \le 2dN^2C^{N^2}.$$

This contradicts that

$$d_{J_i+1} - d_{J'+1} \ge d_{J_i+1} - d_{J_i} > 2dN^2C^{N^2}.$$

Therefore, we obtain that $A(x)|P_J(x)$ for each $J \in \{J_1, J_2, \ldots, J_r\}$.

Let $k_0 = 0$, and let $k_j = d_{J_j+1}$ for each $j \in \{1, 2, \ldots, r\}$. Replacing these d_{J_j+1} with their respective k_j's in $A(x)Q(x)$ we get

$$A(x)Q(x) = \sum_{j=1}^{n} c_j x^{d_j} = \sum_{j=0}^{r} h_j(x) x^{k_j},$$

for some $h_j(x) \in \mathbb{Z}[x]$ with $\deg h_j(x) = d_{J_{j+1}} - d_{J_j+1}$ for $j \in \{1, 2, \ldots, r-1\}$, $\deg h_0(x) = d_{J_1}$ and $\deg h_r(x) = d_n - d_{J_r+1}$. Now $k_{L+1} - (k_L +$

$\deg h_L(x)) > 2d\,N^2\,C^{N^2}$ as L varies over $\{0, 1, \ldots, r-1\}$. Also, since $A(x)|P_J(x)$ for each $J \in \{J_1, J_2, \ldots, J_r\}$ and since $A(x)|P(x)$, we obtain that $A(x)|h_j(x)$ for all $j \in \{0, 1, \ldots, r\}$. Therefore, for each $j \in \{0, 1, \ldots, r\}$, there exists $w_j(x) \in \mathbb{Z}[x]$ satisfying

$$h_j(x) = A(x)w_j(x).$$

Thus,

$$Q(x) = \sum_{j=0}^{r} w_j(x)x^{k_j}.$$

For each $j \in \{0, 1, \ldots, r\}$, the coefficients of $A(x)w_j(x)$ are among the coefficients of $A(x)Q(x)$. Hence,

$$\|h_j(x)\| = \|A(x)w_j(x)\| \le \|A(x)Q(x)\| \le N.$$

By the choice of the k_j's, we note that if $h_j(x) = \sum_{i=1}^{k} b_i x^{n_i}$, then $n_{J+1} - n_J \le 2d\,N^2\,C^{N^2}$ for all $J \in \{1, 2, \ldots k-1\}$. Since each $h_j(x)$ is a polynomial with norm $\le N$, we are in a position to apply Case 1 or 2 to each $h_j(x)$. We deduce that

$$\|w_j(x)\| \le B(2dN^4C^{N^2}, N) \quad \text{ for } j \in \{0, 1, \ldots, r\}.$$

Now $r + 1 \le n \le N^2$ implies that

$$\|Q\|^2 = \sum_{j=0}^{r} \|w_j\|^2 \le N^2 B^2(2dN^4C^{N^2}, N).$$

Thus, in this case, we also get that the lemma follows.

If $A(x)$ has a root with absolute value > 1, one can still apply Lemma 2 by considering reciprocal polynomials. In other words, one considers $A^*(x)$ and notes that $\|A(x)Q(x)\| = \|A^*(x)Q^*(x)\|$. The bound is the same as that given in Lemma 1 except that A needs to be replaced by A^* in the definition of C. Lemma 2, however, does not handle the case when $A(x)$ has roots only on the unit circle. In order to deal with this case, we introduce two new lemmas.

Lemma 3. *Suppose the roots of $A(x)$ are distinct and have absolute value ≥ 1. Suppose further that no root of $A(x)$ is a root of unity. Let N be such that $\|P\| \le N$, and let $J \in \{1, 2, \ldots, n-1\}$. If $A(x)|P(x)$ and $A(x) \nmid P_J(x)$, then*

$$d_{J+1} - d_J \le 2^d d^{d^2+d} N^{2d} \|A\|^{2d^2-2d}.$$

Proof. Let $Q(x) = P(x)/A(x)$ and write

$$Q(x) = \sum_{j=0}^{m} q_j x^j \qquad \text{with } q_0 q_m \neq 0.$$

We define $q_j = 0$ for $j \notin [0, m]$. Recall from (2) that $P_J(x) = \sum_{j=1}^{J} c_j x^{d_j}$. Now for all k such that $d_J < k < d_{J+1}$, we have

$$0 = a_0 q_k + a_1 q_{k-1} + \cdots + a_d q_{k-d} \tag{5}$$

since the right-hand side is simply the coefficient of x^k in the product $A(x)Q(x) = P(x)$. Thus, the sequence $\{q_i\}_{d_J - d < i < d_{J+1}}$ is a linear recurrence of order d. In order to bound the elements of this sequence we expand $1/A(x)$ in a formal power series. Since all the roots of $A(x)$ are distinct, we have

$$\begin{aligned}
Q(x) &= P(x) \sum_{j=1}^{d} \left(\frac{-1}{\alpha_j A'(\alpha_j)} \right) \frac{1}{1 - x/\alpha_j} \\
&= P(x) \sum_{h=0}^{\infty} x^h \sum_{j=1}^{d} \frac{-\alpha_j^{-h}}{\alpha_j A'(\alpha_j)} \\
&= \sum_{k=0}^{\infty} x^k \sum_{\substack{i \\ d_i \leq k}} c_i \sum_{j=1}^{d} \frac{-\alpha_j^{-(k-d_i)}}{\alpha_j A'(\alpha_j)} \\
&= \sum_{k=0}^{\infty} x^k \sum_{j=1}^{d} \frac{-\alpha_j^{-k}}{\alpha_j A'(\alpha_j)} \sum_{\substack{i \\ d_i \leq k}} c_i \alpha_j^{d_i}.
\end{aligned}$$

Thus,

$$q_k = \sum_{j=1}^{d} \frac{-P_{J'}(\alpha_j)}{\alpha_j A'(\alpha_j)} \alpha_j^{-k} \qquad \text{for } 1 \leq J' \leq n-1 \text{ and } d_{J'} \leq k < d_{J'+1}.$$

Since $|\alpha_j| \geq 1$ for each j, we deduce that

$$|q_k| \leq \sum_{i=1}^{J} |c_i| \sum_{j=1}^{d} 1/|A'(\alpha_j)| \qquad \text{for all } k < d_{J+1}. \tag{6}$$

Let B_J denote the right-hand side of (6). In the sequence $\{q_i\}_{d_J - d < i < d_{J+1}}$ there are $d_{J+1} - d_J$ contiguous subsequences of length d. And, there are at most $(2B_J + 1)^d$ distinct $d-$vectors $\langle q_{k-d+1}, \ldots, q_k \rangle$ satisfying $|q_i| \leq B_J$ for $k - d + 1 \leq i \leq k$. Assume that

$$d_{J+1} - d_J > (2B_J + 1)^d. \tag{7}$$

Then there are two d-vectors

$$\vec{v}_1 = \langle q_{k_1-d+1}, \ldots, q_{k_1} \rangle \quad \text{and} \quad \vec{v}_2 = \langle q_{k_2-d+1}, \ldots, q_{k_2} \rangle$$

with $d_J \le k_1 < k_2 < d_{J+1}$ such that $\vec{v}_1 = \vec{v}_2$. From (5), we see that for $d_J < k < d_{J+1}$, the value of q_k is determined by the previous d values of q_j. Thus, $\{q_j\}_{k_1-d<j<d_{J+1}}$ is cyclic with cycle length $\omega \le k_2 - k_1$. Now, we form an infinite number of multipliers $Q_t(x)$ such that $\|Q_t(x)A(x)\| = \|Q(x)A(x)\|$. This is done by splicing in t copies of the vector $\langle q_{d_{J+1}-\omega}, \ldots, q_{d_{J+1}-1} \rangle$ into the coefficient vector for Q between $q_{d_{J+1}-1}$ and $q_{d_{J+1}}$. More precisely, we have

$$Q_t(x) = \sum_{j=0}^{d_{J+1}-\omega-1} q_j x^j + \left(\sum_{j=d_{J+1}-\omega}^{d_{J+1}-1} q_j x^j \right) (1 + x^\omega + \cdots + x^{\omega t}) + x^{\omega t} \sum_{j=d_{J+1}}^{m} q_j x^j$$

and

$$Q_t(x)A(x) = \sum_{j=1}^{J} c_j x^{d_j} + x^{\omega t} \sum_{j=J+1}^{n} c_j x^{d_j}.$$

Note that $\|Q_t A\| = \|QA\| \le N$ and

$$(Q_t(x) - Q(x))A(x) = (x^{\omega t} - 1) \sum_{j=J+1}^{n} c_j x^{d_j}.$$

There are no roots of unity among $\alpha_1, \ldots, \alpha_d$. Hence, $A(x) | \sum_{j=J+1}^{n} c_j x^{d_j}$. But $A(x)|P(x)$ implies now that $A(x)|P_J(x)$, a contradiction. Thus (7) does not hold so that

$$d_{J+1} - d_J \le (2B_J + 1)^d.$$

One easily gets that

$$d_{J+1} - d_J \le \left(2(N^2 - 1) \sum_{j=1}^{d} \frac{1}{|A'(\alpha_j)|} + 1 \right)^d.$$

Since all the roots of A are distinct, A and A' are relatively prime. Let R denote the resultant of A^* (the reciprocal polynomial for $A(x)$) and A'^* (the reciprocal polynomial for $A'(x)$). The roots of A^* are $1/\alpha_j$ for $1 \le j \le d$. If for some j, $1/\alpha_j$ is a root of A'^*, then α_j is a root of A', contradicting that A and A' are relatively prime. Thus, A^* and A'^* are relatively prime, and the resultant is non-zero. We consider a value of $i \in \{1, 2, \dots, d\}$. Then by an argument of resultants (cf. [7, Proposition 1.6]) and the fact that $|\alpha_i| \geq 1$, we have

$$1 \leq |R| \leq d|A'^*(1/\alpha_i)| \|A'^*\|^{d-1} \|A^*\|^{d-1} \leq d|A'(\alpha_i)| \|A'\|^{d-1} \|A\|^{d-1}.$$

We use that $\|A'\| \leq \left(\sum_{j=1}^{d} d^2 |a_j|^2\right)^{1/2} \leq d\|A\|$. Then

$$\frac{1}{|A'(\alpha_i)|} \leq d^d \|A\|^{2d-2}.$$

This holds for each $i \in \{1, 2, \dots, d\}$ so that

$$\begin{aligned} d_{J+1} - d_J &\leq \left(2(N^2-1)d^{d+1}\|A\|^{2d-2} + 1\right)^d \\ &\leq 2^d d^{d^2+d} N^{2d} \|A\|^{2d^2-2d}. \end{aligned}$$

This completes the proof of the lemma.

Lemma 4. *Let $N \geq 1$, and suppose $A(x)$ has distinct roots with each of absolute value ≥ 1. Suppose further that no root of $A(x)$ is a root of unity. If $Q(x) \in \mathbb{Z}[x]$ is such that $\|AQ\| \leq N$, then*

$$\|Q\| \leq N\, B(2^d d^{d^2+d} N^{2d+2} \|A\|^{2d^2-2d},\ N).$$

Proof. Again we view $P(x)$ as the product of the polynomials $A(x)$ and $Q(x)$. As in Lemma 2, we consider 3 cases.

CASE 1: $A(x) \nmid P_J(x)$ for all $J \in [1, n-1]$.

We use Lemma 3 and sum over J. Noting that $n \leq N^2$, we obtain

$$\deg P \leq 2^d d^{d^2+d} N^{2d+2} \|A\|^{2d^2-2d}.$$

Therefore $Q(x)$ satisfies condition (C) with $m = 2^d d^{d^2+d} N^{2d+2} \|A\|^{2d^2-2d}$. Hence,

$$\|Q\| \leq B(2^d d^{d^2+d} N^{2d+2} \|A\|^{2d^2-2d},\ N).$$

CASE 2: $A(x)|P_J$ for some J, and for all $J \in [1, n-1]$, $d_{J+1} - d_J \leq 2^d d^{d^2+d} N^{2d} \|A\|^{2d^2-2d}$.

As above we get here that

$$\|Q(x)\| \leq B(2^d d^{d^2+d} N^{2d+2} \|A\|^{2d^2-2d},\ N).$$

CASE 3: For some J, $d_{J+1} - d_J > 2^d d^{d^2+d} N^{2d} \|A\|^{2d^2-2d}$.

By Lemma 3, we get $A(x)|P_J(x)$ for any such J. We appeal to the argument given in Lemma 2, Case 3. Here the situation is somewhat simpler as the corresponding $h_j(x)$ are clearly divisible by $A(x)$ (since $A(x)|P_J(x)$ whenever $d_{J+1} - d_J > 2^d d^{d^2+d} N^{2d} \|A\|^{2d^2-2d}$). We deduce that

$$\|Q\| \le N\, B(2^d d^{d^2+d} N^{2d+2} \|A\|^{2d^2-2d},\ N),$$

and Lemma 4 follows.

The following lemma can be considered as a characterization of the multipliers of $A(x)$ which give minimum norm. This lemma is also useful in reducing the search space of multipliers in the implementation of the algorithm to find the elements of $\mathcal{P}_A$.

Lemma 5. *Let $A(x)$ be as in (1) of degree d. Let $Q(x) = \sum_{j=1}^{r} q_j x^{m_j}$ with $0 = m_1 < m_2 < \cdots < m_r$ and each $q_j \neq 0$. If $||A(x)Q(x)|| = ||A(x)||_{\min}$, then $m_{J+1} - m_J \le d$ for each $J \in \{1, 2, \ldots, r-1\}$. Furthermore,*

$$\deg Q(x) \le (||Q||^2 - 1)d.$$

Proof. Let $P(x) = A(x)Q(x)$. Then $\|P\| = \|A\|_{\min}$. Assume $m_{J+1} - m_J > d$ for some $J \in \{1, 2, \ldots, r-1\}$. Let $Q_J = \sum_{j=1}^{J} q_j x^{m_j}$. Then $Q(x) = \sum_{j=J+1}^{r} q_j x^{m_j} + Q_J(x)$ implies

$$A(x)Q(x) = A(x) \sum_{j=J+1}^{r} q_j x^{m_j} + A(x)Q_J(x).$$

Now $\deg(A(x)Q_J(x)) = d + m_J < m_{J+1}$. Therefore, the coefficients of $A(x)Q(x)$ are the disjoint union of the coefficients of $A(x)\sum_{j=J+1}^{r} q_j x^{m_j}$ and the coefficients of $A(x)Q_J(x)$. Hence, $||A(x)Q_J(x)|| < \|P\|$, giving a contradiction. Thus, $m_{J+1} - m_J \le d$.

It is clear that $r \le ||Q||^2$. Now, $m_{J+1} - m_J \le d$ for each $J \in \{1, 2, \ldots, r-1\}$ and $m_1 = 0$ imply that

$$\deg Q(x) = \sum_{J=1}^{r-1} (m_{J+1} - m_J) \le \sum_{J=1}^{r-1} d = (r-1)d \le (||Q||^2 - 1)d,$$

establishing the lemma.

3. Proofs of the Theorems

Proof of Theorem 1. We use Lemmas 2 and 4 where a bound was given for $\|Q\|$ when $\|AQ\| \le N$. Observe that one of these two lemmas will apply if $A(x)$ is an irreducible non-cyclotomic polynomial. We write $\tilde{B}(A,N)$ to denote a bound given from these two lemmas for $\|Q\|$.

Write $A(x) = \prod_{j=1}^{m} f_j(x)$ with each $f_j(x)$ irreducible and where repeated factors appear as many times as their multiplicity. By the conditions in the theorem, no $f_j(x)$ is cyclotomic. For each $j \in \{1, 2, \ldots, m\}$, we consider $A(x) = f_j(x)$ and apply either Lemma 2 or Lemma 4. Applying these lemmas repeatedly on each f_j, we get

$$\begin{aligned} ||f_2 f_3 \cdots f_m Q|| &\leq \tilde{B}(f_1, N) \\ ||f_3 f_4 \cdots f_m Q|| &\leq \tilde{B}(f_2, \tilde{B}(f_1, N)) \\ ||f_4 f_5 \cdots f_m Q|| &\leq \tilde{B}(f_3, \tilde{B}(f_2, \tilde{B}(f_1, N))) \\ &\vdots \end{aligned}$$

and the required bound on $\|Q\|$ follows.

Proof of Theorem 2. Let $N = \|A\|$. We set $Q(x) = P(x)/A(x)$. The polynomial $P(x)$ is a multiple of $A(x)$ with minimal Euclidean norm so that $\|A(x)Q(x)\| \leq N$. By Theorem 1, $||Q||$ is bounded by a function of $A(x)$ and N. Since $N = \|A\|$, we deduce that $||Q||$ is bounded by a function which depends only on $A(x)$. Also, Lemma 5 implies that $\deg Q$ is bounded by a function of $||Q||$ and $d = \deg A$. Thus, $\deg Q$ is bounded by a function depending only on $A(x)$. The result now follows from $\deg P = \deg Q + \deg A$.

4. Further Remarks

As mentioned in the introduction, there are also results in the literature which would help give estimates of the type we have been considering. One such result which can be found in [2] and [3] is as follows.

Lemma 6. *Let $Q(x)$ be a complex polynomial of degree n and α any complex number. Then*

$$\|Q\| \leq \left(1 + |\alpha|^2 - 2|\alpha| \cos\left(\frac{\pi}{n+2}\right)\right)^{-1/2} \|Q(x)(x-\alpha)\|.$$

From this result, we can obtain the following revision of Theorem 1.

Theorem 3. *Let $A(x) \in \mathbb{Z}[x]$ be a polynomial of the form (1) having no roots on the unit circle. Let $N \geq 1$. If $Q(x) \in \mathbb{Z}[x]$ and $\|A(x)Q(x)\| \leq N$, then*

$$\|Q\| \leq \frac{N}{|A^{+}(1)|},$$

where $A^+(x) = a_d \prod_{i=1}^{d}(x - |\alpha_i|)$.

Proof. By Lemma 6, we have

$$\begin{aligned}\|a_d Q(x)\| &\le \left(1 + |\alpha_1|^2 - 2|\alpha_1| \cos\left(\frac{\pi}{\deg Q + 2}\right)\right)^{-1/2} \|a_d Q(x)(x - \alpha_1)\| \\ &\le \left(1 + |\alpha_1|^2 - 2|\alpha_1|\right)^{-1/2} \|a_d Q(x)(x - \alpha_1)\| \\ &\le \frac{\|a_d Q(x)(x - \alpha_1)\|}{|1 - |\alpha_1||}.\end{aligned}$$

If we replace $a_d Q(x)$ with $a_d Q(x)(x - \alpha_1)$ above and use α_2 in place of α_1, we get that

$$\frac{\|a_d Q(x)(x - \alpha_1)\|}{|1 - |\alpha_1||} \le \frac{\|a_d Q(x)(x - \alpha_1)(x - \alpha_2)\|}{|(1 - |\alpha_1|)(1 - |\alpha_2|)|}$$

so that

$$\|a_d Q(x)\| \le \frac{\|a_d Q(x)(x - \alpha_1)(x - \alpha_2)\|}{|(1 - |\alpha_1|)(1 - |\alpha_2|)|}.$$

Continuing in this manner, we obtain

$$\begin{aligned}|a_d| \ \|Q(x)\| = \|a_d Q(x)\| &\le \frac{\|a_d Q(x) \ \prod_{i=1}^{d}(x - \alpha_i)\|}{\prod_{i=1}^{d} |1 - |\alpha_i||} \\ &= \frac{\|A(x)Q(x)\|}{\prod_{i=1}^{d} |1 - |\alpha_i||}.\end{aligned}$$

Hence,

$$\|Q(x)\| \le \frac{\|A(x)Q(x)\|}{|a_d| \prod_{i=1}^{n} |1 - |\alpha_i||} \le \frac{N}{|A^+(1)|},$$

completing the proof.

Observe that if $|\alpha_1| = 1$, the expression

$$\left(1 + |\alpha_1|^2 - 2|\alpha_1| \cos\left(\frac{\pi}{\deg Q + 2}\right)\right)^{-1/2}$$

gets large as $\deg Q$ increases. This would cause the bound on $\|Q(x)\|$ obtained directly from Lemma 6 to tend to infinity as $\deg Q$ tends to infinity. Under the condition that $A(x)$ has no roots with absolute value 1, this situation is avoided.

References

1. D. Boyd, *Two sharp inequalities for the norm of a factor of a polynomial*, Mathematika **39** (1992), 341–349.
2. J. Donaldson and Q. Rahman, *Inequalities for polynomial with a prescribed zero*, Pacific J. Math. **41** (1972), 375–378.

3. A. Durand, *Quelques aspects de la théorie analytique des polynômes I, II;* Cinquante ans de polynômes (Paris, 1988), Lecture Notes in Math. 1415, Springer-Verlag, Berlin, 1990, pp. 1–42, 43–85.
4. M. Filaseta, M. Robinson and F. Wheeler, *The minimal Euclidean norm of an algebraic number is effectively computable*, J. Algorithms **16** (1994), 309–333.
5. P. Glesser, *Nouvelle majoration de la norme des facteurs d'un polynôme*, C.R. Math. Rep. Acad. Sci. Canada **12** (1990), 224–228.
6. A. Granville, *Bounding the coefficients of a divisor of a given polynomial*, Monatsh. Math. **109** (1990), 271–277.
7. R. Kannan, A. Lenstra, and L. Lovász, *Polynomial factorization and nonrandomness of bits of algebraic and some transendental numbers*, Math. Comp. **50** (1988), 235–250.
8. M. Mignotte, *An inequality about factors of polynomials*, Math. Comp. **28** (1974), 1153–1157.
9. A. Schinzel, *Reducibility of lacunary polynomials I*, Acta Arith. **16** (1969/70), 123–159.
10. A. Schinzel, *Proc. of Symposia in Pure Math. (edited by D.J. Lewis)*, vol. 20, American Math. Soc., Providence, 1971, pp. 135–149.
11. J. Uspensky, *Theory of Equations*, McGraw-Hill, New York, 1948.

Mathematics Department
University of South Carolina
Columbia, SC 29208

filaseta@math.sc.edu

Mathematics Department
U.W.I. mona
Jamaica, W.I.

solan@uwimona.jm.edu