THE MINIMAL EUCLIDEAN NORM OF AN ALGEBRAIC NUMBER IS EFFECTIVELY COMPUTABLE

Michael Filaseta[†]
M. L. Robinson[‡]
Ferrell S. Wheeler[‡]

[†]University of South Carolina
Columbia, South Carolina

[‡]Supercomputing Research Center
Bowie, Maryland

January 1992

ABSTRACT. For $P \in \mathbb{Z}[x]$, let $\|P\|$ denote the Euclidean norm of the coefficient vector of P. For an algebraic number α, with minimal polynomial A, define the Euclidean norm of α by

$$\|\alpha\| = \|kA\|,$$

where k is the smallest positive integer for which $kA \in \mathbb{Z}[x]$. Define the minimal Euclidean norm of α by

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

Given an algebraic number α, we show there exists a $P \in \mathbb{Z}[x]$ with $P(\alpha) = 0$ and $\|P\| = \|\alpha\|_{min}$ such that the degree of P is bounded above by an explicit function of $\deg \alpha$, $\|\alpha\|$, and $\|\alpha\|_{min}$. As a result, we are able to prove that both P and $\|\alpha\|_{min}$ can be effectively computed using a suitable search procedure. As an indication of the difficulties involved, we show that the determination of P is equivalent to finding a shortest nonzero vector in an infinite union of certain lattices. After introducing several techniques for reducing the search space, a practical algorithm is presented which has been successful in computing $\|\alpha\|_{min}$ provided the degree and Euclidean norm of α are both sufficiently small. We also obtain the following unusual characterization of the roots of unity: An algebraic number α is a root of unity if and only if the set

$$\{P : P \in \mathbb{Z}[x],\ P(\alpha) = 0,\ P(0) \neq 0,\ \|P\| = \|\alpha\|_{min}\}$$

contains infinitely many polynomials. We show how to extend the above results to other l_p norms. Some related open problems are also discussed.

Key words and phrases. Minimal Euclidean norm, Algebraic numbers, Shortest vector in a lattice.

Typeset by $\mathcal{A}_\mathcal{M}\mathcal{S}$-TEX

§1 Introduction

Throughout this paper, let $\mathbb{Z}$, $\mathbb{Z}^+$, $\mathbb{Z}[x]$, $\mathbb{C}$, and $\mathbb{C}[x]$ denote the ring of integers, the set of positive integers, the ring of univariate polynomials over $\mathbb{Z}$, the field of complex numbers, and the ring of univariate polynomials over $\mathbb{C}$, respectively. If $A \in \mathbb{C}[x]$ and

$$A(x) = \sum_{j=0}^{d} a_j x^j = a_d \prod_{j=1}^{d} (x - \alpha_j), \tag{1.1}$$

define the height, Euclidean norm, and Mahler measure of A by

$$H(A) = \max_{0 \le j \le d} |a_j|,$$

$$\|A\| = \left(\sum_{j=0}^{d} |a_j|^2 \right)^{1/2},$$

and

$$M(A) = |a_d| \prod_{j=1}^{d} \max\{1, |\alpha_j|\},$$

respectively. Sometimes elements of $\mathbb{Z}[x]$ will be referred to as integer polynomials. We call an integer polynomial $A(x)$ irreducible when it has no factors in $\mathbb{Z}[x]$ other than $\pm A(x)$ and ± 1.

Let α be an algebraic number, and let A be an irreducible polynomial in $\mathbb{Z}[x]$ of smallest degree such that $A(\alpha) = 0$. Therefore, if $A(x)$ is as in (1.1), then $a_j \in \mathbb{Z}$ for $j \in \{0, 1, \dots, d\}$ and $\gcd(a_0, a_1, \dots, a_d) = 1$. We define the height, Euclidean norm, and Mahler measure of α by $H(\alpha) = H(A)$, $\|\alpha\| = \|A\|$, and $M(\alpha) = M(A)$, respectively. A function $F(\alpha)$ is called effectively computable if there is an algorithm for computing $F(\alpha)$ from the degree and coefficients of A. If the real number ξ satisfies $\xi \le F(\alpha)$, where $F(\alpha)$ is effectively computable, we say that $F(\alpha)$ is an effective upper bound for ξ and that ξ is effectively bounded above.

The central concern of this paper is finding, among all nonzero integer polynomials which vanish at α, a polynomial whose Euclidean norm is minimal. This extremal problem arose in part from a desire to find succinct ways to represent algebraic numbers on a computer. Indeed, it is easy to produce examples where the polynomial A has large Euclidean norm while an obvious integer polynomial multiple of A has decidedly lower Euclidean norm. For instance, a spectacular example of this decrease in Euclidean norms occurs when α is a primitive p^{th} root of unity for some prime p. Here $A(x) = \sum_{n=0}^{p-1} x^n$ has Euclidean norm $\sqrt{p}$. On the other hand, $(x-1)A(x) = x^p - 1$ has Euclidean norm $\sqrt{2}$.

Suppose now that $P \in \mathbb{Z}[x]$ is a solution to the above extremal problem. If $\deg P$ is large compared with $\|P\|^2$, then P must be a sparse polynomial since the number of nonzero terms in P is at most $\|P\|^2$. This situation is in stark contrast to the analogous extremal problem in which minimal Euclidean norm is replaced by minimal height. For example, when α is a primitive p^{th} root of unity, the polynomial $A(x)$ solves the minimal height problem but has no sparseness whatsoever.

Motivated by such considerations we define the minimal Euclidean norm of an algebraic number α by

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

For example, it is easy to see that

$$\|\alpha\|_{min} = 1 \iff \alpha = 0,$$

and

$$\|\alpha\|_{min} = \sqrt{2} \iff \alpha \text{ is a root of unity.}$$

Clearly, the function $\|\cdot\|_{min}$ is well defined on the algebraic numbers because a non-empty set of positive square roots of natural numbers always has a least element. It should be noted that $\|\cdot\|_{min}$ is not a norm on the one-dimensional vector space of algebraic numbers defined over the field of algebraic numbers. In fact, we now show that all three of the defining relations of a norm are not satisfied. We have just noted that $\|0\|_{min} \neq 0$. Let $\beta = \sqrt{2}$, so that $\|\beta\|_{min} = \sqrt{5}$ and $\|2\beta\|_{min} = \sqrt{65}$. Clearly,

$$\|2\beta\|_{min} \neq 2\,\|\beta\|_{min}\,.$$

Furthermore,

$$\|\beta+\beta\|_{min} > \|\beta\|_{min} + \|\beta\|_{min}\,,$$

and the triangle inequality fails as well.

With α and A as above, let $\mathcal{P}_\alpha$ denote the following set of polynomials:

$$\mathcal{P}_\alpha = \{QA : Q \in \mathbb{Z}[x],\ Q(0) \neq 0,\ \|QA\| = \|\alpha\|_{min}\}. \tag{1.2}$$

Note that $\left\|x^k P\right\| = \|P\|$ for any $k \in \mathbb{Z}^+$ and any $P \in \mathbb{Z}[x]$. Thus, from the perspective of minimal Euclidean norms, we have excluded from $\mathcal{P}_\alpha$ those polynomials with artificially high powers of x as factors. Furthermore, for any $P \in \mathcal{P}_\alpha$, it is easy to see that P must have the form

$$P(x) = \sum_{j=1}^{n} c_j x^{d_j}, \tag{1.3}$$

where $0 = d_1 < \cdots < d_n = \deg P$ and $c_j \neq 0$ for $1 \le j \le n$.

It is convenient to note that the following useful inequalities, valid for any algebraic number α, hold:

$$M(\alpha) \le \|\alpha\|_{min} \le \|\alpha\|\,. \tag{1.4}$$

The second inequality is trivial, while the first can be proved as follows. Let $P \in \mathcal{P}_\alpha$, so that $P = AQ$ for some $Q \in \mathbb{Z}[x]$. Noting that $M(Q) \ge 1$, we have

$$M(\alpha) \le M(A)M(Q) = M(P),$$

since the Mahler measure is multiplicative. Now $M(P) \leq \|P\|$ by Landau's inequality (see, e.g., [12]). Since $\|P\| = \|\alpha\|_{min}$, the first inequality in (1.4) is true.

Given a nonzero algebraic number α, our goal in §2 is to prove the existence of a $P \in \mathcal{P}_\alpha$ such that the degree of P is bounded above by an explicit function of $\deg \alpha$, $\|\alpha\|$, and $\|\alpha\|_{min}$. We first consider nonzero algebraic numbers with at least one conjugate not on the unit circle. In this case, well-known properties of resultants are used to show in Theorem 1 that if $P \in \mathcal{P}_\alpha$, then $\deg P$ is bounded above by an explicit function of $\deg \alpha$ and $\|\alpha\|_{min}$. Next we look at those algebraic numbers α which are roots of unity. In this case, inequalities for the Euler ϕ-function are used in Theorem 2 to show that there exists a $P \in \mathcal{P}_\alpha$ whose degree is bounded above by an explicit function of $\deg \alpha$ alone. Finally in §2, we consider those nonzero algebraic numbers α which are not roots of unity but have either no conjugates inside the unit circle or have no conjugates outside the unit circle. This time, results from the theory of linear recursive sequences are combined with resultants to show in Theorem 3 that if $P \in \mathcal{P}_\alpha$, then $\deg P$ is bounded by an explicit constant depending only on $\deg \alpha$, $\|\alpha\|$, and $\|\alpha\|_{min}$.

In §3 we combine the results of Theorems 1, 2, and 3 to prove that if the polynomial $A(x)$ corresponding to an algebraic number α is known, then a $P \in \mathcal{P}_\alpha$ can be effectively computed. In this way, we prove in Theorem 4 that the minimal Euclidean norm of an algebraic number is effectively computable. In §3 we use Theorems 1 and 3 to determine those algebraic numbers α whose corresponding $\mathcal{P}_\alpha$ is finite. In fact, in Theorem 5 we obtain the following unusual characterization of the roots of unity: an algebraic number α is a root of unity if and only if $\mathcal{P}_\alpha$ contains infinitely many polynomials.

In §4 we consider the computation of minimal Euclidean norms in practice. An algorithm for effectively computing $\|\alpha\|_{min}$ is presented which contains several techniques for reducing the size of the search space needed to find a $P \in \mathcal{P}_\alpha$. For example, one key idea is to use upper bounds, already obtained in Lemmas 1 and 2 of §2, for the gaps between the degrees of successive monomials which make up a polynomial in $\mathcal{P}_\alpha$ of the form (1.3).

The algorithm in §4 has been used successfully to compute the minimal Euclidean norm of certain algebraic numbers. A representative example is given in §5. As an indication of the difficulties involved, we prove that the determination of a $P \in \mathcal{P}_\alpha$ is equivalent to finding a shortest vector in an infinite union of certain lattices. Thus it is not surprising that the algorithm in §4 is feasible only when the degree and Euclidean norm of α are both sufficiently small. The algorithm in §4 can be viewed as a search over plausible multiples of A. We also discuss in §5 the possibility of searching over plausible multipliers of A. We indicate how results on the reducibility of lacunary polynomials (due to Selmer, Ljunggren, Jonassen, and Schinzel) can be used to reduce the search space in special situations.

Before continuing, we note that our results can be extended from the Euclidean norm to other l_p norms. For example, if A is a non-cyclotomic irreducible polynomial in $\mathbb{Z}[x]$, then the methods of §2 imply that a multiple P of A in $\mathbb{Z}[x]$ of large degree and bounded norm has the form $P = g(x)x^k + h(x)$ for some positive integer k and some $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ satisfying $\deg h < k$, $A(x)|g(x)$, and $A(x)|h(x)$. In other words, regardless of the norm being used, if P is a multiple of A in $\mathbb{Z}[x]$ with $P(0) \neq 0$ and $\deg P$ is large, then there must exist a multiple of A in $\mathbb{Z}[x]$ having smaller norm than P. Alternatively, we observe that the results obtained here can be generalized directly to other l_p norms by taking advantage of well known inequalities for making comparisons between different norms (cf. [4, Theorems 16,19]).

§2 Preliminary Degree Bounds

The theorems proved in this section collectively provide an affirmative answer to the following question: If α is a nonzero algebraic number, does there exist a $P \in \mathcal{P}_\alpha$ such that the degree of P is bounded above by an explicit function of $\deg \alpha$, $\|\alpha\|$, and $\|\alpha\|_{min}$? Recall that $\mathcal{P}_\alpha$ was defined in (1.2). First, however, we collect some useful facts concerning reciprocal polynomials. For nonzero $P \in \mathbb{Z}[x]$, define the reciprocal polynomial P^* of P by

$$P^*(x) = x^{\deg P} P(1/x) \in \mathbb{Z}[x].$$

For all nonzero algebraic numbers, it is clear that

$$P \in \mathcal{P}_\alpha \implies P^* \in \mathcal{P}_{1/\alpha}. \tag{2.1}$$

Furthermore, $\deg P = \deg P^*$ when $P(0) \neq 0$, $\|P\| = \|P\|^*$, and $M(P) = M(P^*)$. A polynomial P is said to be a reciprocal polynomial if $P = \pm P^*$, and an algebraic number α is reciprocal if $1/\alpha$ is a conjugate of α.

Besides helping prove Theorem 1, the lemma below will play an important role in §4 in our practical algorithm for computing minimal Euclidean norms.

Lemma 1. *Let α be a nonzero algebraic number, and let $A(x)$ be an irreducible polynomial in $\mathbb{Z}[x]$ of smallest possible degree with $A(\alpha) = 0$. Write $A(x)$ in the form (1.1). Let $P \in \mathcal{P}_\alpha$ have the form (1.3). If α has $\lambda \geq 1$ conjugates inside the unit circle, then for $1 \leq J \leq n-1$,*

$$d_{J+1} \leq \frac{\log M(\alpha)}{\log\big(M(\alpha)/|a_0|\big)}\, d_J + \frac{\log\left\{\left(\sum_{h=J+1}^{n} |c_h|\right)^{\lambda} \left(\sum_{i=1}^{J} |c_i|\right)^{d-\lambda}\right\}}{\log\big(M(\alpha)/|a_0|\big)}. \tag{2.2}$$

If α has $\nu \geq 1$ conjugates outside the unit circle, then for $1 \leq J \leq n-1$,

$$d_n - d_J \leq \frac{\log M(\alpha)}{\log\big(M(\alpha)/|a_d|\big)}\, \big(d_n - d_{J+1}\big) + \frac{\log\left\{\left(\sum_{h=1}^{J} |c_h|\right)^{\nu} \left(\sum_{i=J+1}^{n} |c_i|\right)^{d-\nu}\right\}}{\log\big(M(\alpha)/|a_d|\big)}. \tag{2.3}$$

Proof. Suppose first that α has $\lambda \geq 1$ conjugates inside the unit circle. For $1 \leq J \leq n-1$, define P_J by

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

Since $P \in \mathcal{P}_\alpha$, we know that $\|\alpha\|_{min} = \|P\| > \|P_J\|$. Hence, P_J and A must be relatively prime. Let R_J denote the resultant of A and P_J. Using well-known properties of the resultant, (see [19]) we have

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

If A has no roots lying outside or on the unit circle, the empty product occurring above is understood to equal 1. Noting that $M(\alpha) = M(1/\alpha)$ and that the latter trivially exceeds $|a_0|$, inequality (2.2) follows.

Suppose next that α has $\nu \ge 1$ conjugates outside the unit circle. Then $1/\alpha$ has ν conjugates inside the unit circle. Apply inequality (2.2) to $1/\alpha$ and the reciprocal polynomials of $A(x)$ and $P(x)$. Using (2.1) and $M(1/\alpha) = M(\alpha)$ we get inequality (2.3). $\square$

Theorem 1. *Let α be a nonzero algebraic number of degree d. Suppose at least one conjugate of α does not lie on the unit circle. If $P \in \mathcal{P}_\alpha$, then*

$$\deg P \le 2d \|\alpha\|_{min}^2 \left(\frac{2 \log \|\alpha\|_{min}}{\log \left(1 + 1/(2^{d(d-1)/2} \|\alpha\|_{min}^{2d}) \right)} \right)^{\|\alpha\|_{min}^2} .$$

Proof. Define $A(x)$ as in Lemma 1. We can assume that $P \in \mathcal{P}_\alpha$ has the form (1.3). We first treat the case in which α has $\lambda \ge 1$ conjugates inside the unit circle. Trivially, we have for $1 \le J \le n-1$,

$$\sum_{h=J+1}^{n} |c_h| \le \sum_{h=J+1}^{n} |c_h|^2 \le \|\alpha\|_{min}^2 .$$

Similarly,

$$\sum_{i=1}^{J} |c_i| \le \|\alpha\|_{min}^2 .$$

Hence, by (2.2) we have that

$$d_{J+1} \le \frac{\log M(\alpha)}{\log(M(\alpha)/|a_0|)} d_J + \frac{2d \log \|\alpha\|_{min}}{\log(M(\alpha)/|a_0|)} .$$

Using (1.4) we have

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

where

$$C = \frac{\log \|\alpha\|_{min}}{\log(M(\alpha)/|a_0|)}.$$

By induction on J and the fact that $d_1 = 0$, we have

$$\deg P = d_n \le 2d \sum_{j=1}^{n} C^j \le 2dnC^n.$$

Since $n \le \|\alpha\|_{min}^2$, we see at once that

$$\deg P \le 2d \|\alpha\|_{min}^2 \left(\frac{\log \|\alpha\|_{min}}{\log(M(\alpha)/|a_0|)} \right)^{\|\alpha\|_{min}^2}.$$

Hence, to prove the theorem when α has a conjugate inside the unit circle, it suffices to show

$$\log(M(\alpha)/|a_0|) \ge 1/2 \log \left(1 + 1 \,/\, \left(2^{d(d-1)/2} \|\alpha\|_{min}^{2d}\right)\right). \tag{2.4}$$

By a relabeling of the conjugates, we can assume, without loss of generality, that $|\alpha| < 1$. Hence,

$$\begin{aligned} \log(M(\alpha)/|a_0|) &= \log\Big(\prod_{|\alpha_j|<1} 1/|\alpha_j|\Big) \\ &\ge \log(1/|\alpha|) \\ &= 1/2 \log\big(1 + (1/|\alpha|^2 - 1)\big). \end{aligned} \tag{2.5}$$

Now if $\beta \ne 1$ is an algebraic number, we know from [16, equation (11.1)] that

$$|1 - \beta| > \left(2^{\deg \beta} M(\beta)\right)^{-1}.$$

Letting $\beta = 1/|\alpha|^2 = 1/(\alpha\overline{\alpha})$, an algebraic number of degree at most $d(d-1)/2$, we see that

$$\frac{1}{|\alpha|^2} - 1 > \left(2^{d(d-1)/2} M\left(\frac{1}{\alpha} \cdot \frac{1}{\overline{\alpha}}\right)\right)^{-1}. \tag{2.6}$$

From [2, equation (M2)] we know that if β and γ are algebraic numbers, then

$$M(\beta\gamma) \le M(\beta)^{\deg \gamma} M(\gamma)^{\deg \beta}.$$

Letting $\beta = 1/\alpha$ and $\gamma = 1/\overline{\alpha}$ yields

$$M\big(1\ /\ |\alpha|^2\big) \le M(1/\alpha)^{2d} \le \|\alpha\|_{min}^{2d},$$

using (1.4) and the fact that $\|\alpha\|_{min} = \|1/\alpha\|_{min}$. Thus from (2.6) we see that

$$\frac{1}{|\alpha|^2} - 1 \ge \frac{1}{2^{d(d-1)/2}\,\|\alpha\|_{min}^{2d}}.$$

Using this inequality in (2.5) immediately gives (2.4). Thus, Theorem 1 is proved when α has a conjugate lying inside the unit circle.

We now consider the remaining case for which α has $\nu \ge 1$ conjugates outside the unit circle. Then $1/\alpha$ has ν conjugates inside the unit circle. Apply the result just proved to $1/\alpha$ and the reciprocals of A and P. Theorem 1 follows from (2.1) upon noting that $\|1/\alpha\|_{min} = \|\alpha\|_{min}$ and $\deg(1/\alpha) = \deg\alpha = d$. $\square$

We now consider the case in which α is a root of unity. The next result is due to Loxton and Van der Poorten ([20], Lemma 6).

Theorem 2. *If α is a root of unity of degree d, then there exists an $n \le 4d\log\log 6d$ such that $x^n - 1 \in \mathcal{P}_\alpha$.*

Proof. We know there is an $n \in \mathbb{Z}^+$ such that $A(x)$ is simply the n^{th} cyclotomic polynomial $\Phi_n(x)$. Furthermore, $\Phi_n(x)$ divides $x^n - 1$ and $d = \phi(n)$ where ϕ is the Euler ϕ-function. Hence, to prove Theorem 2, it suffices to show that

$$n \le 4\phi(n)\log\log 6\phi(n).$$

This is easy to check by direct calculation if $1 \le n \le 100$. For $n > 100$ it follows by some easy manipulations of an inequality of Rosser and Schoenfeld [13, Theorem 15]. $\square$

The next lemma, needed in the proof of Theorem 2, will also play an important role in our practical algorithm for computing minimal Euclidean norms given in §4.

Lemma 2. *Let α be a nonzero algebraic number, and let $A(x)$ be an irreducible polynomial in $\mathbb{Z}[x]$ of smallest possible degree with $A(\alpha) = 0$. Write $A(x)$ in the form (1.1). Assume that α is not a root of unity. Let $P \in \mathcal{P}_\alpha$ have the form (1.3). If α has no conjugates inside the unit circle, then*

$$d_{J+1} - d_J \le \left(2\sum_{j=1}^{J}|c_j|\sum_{i=1}^{d}\frac{1}{|\alpha_i A'(\alpha_i)|} + 1\right)^d. \tag{2.7}$$

If α has no conjugates outside the unit circle, then

$$d_{J+1} - d_J \le \left(2\sum_{j=J+1}^{n}|c_j|\sum_{i=1}^{d}\frac{|\alpha_i|^{d-1}}{|A'(\alpha_i)|} + 1\right)^d \tag{2.8}$$

Proof. Since $P \in \mathcal{P}_\alpha$ we have $P(x) = Q(x)A(x)$ for some integer polynomial Q of the form

$$Q(x) = \sum_{j=0}^{m} q_j x^j$$

where $q_0 \neq 0$ and $q_m \neq 0$. Also, let $q_j = 0$ for $j < 0$ and $j > m$. As done in Lemma 1, fix J with $1 \leq J < n$ and let

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

Now, for all k such that $d_J < k < d_{J+1}$ we have

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

so that the sequence $\{q_i\}_{d_J - d < i < d_{J+1}}$ is a linear recurrence sequence of order d. In order to bound the elements of this sequence, write $Q(x) = P(x)/A(x)$ and expand $1/A(x)$ in a power series. Since all the roots of $A(x)$ are distinct, for $|x| < 1 \leq \min\limits_{1 \leq i \leq d} |\alpha_i|$ 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,

$$q_k = \sum_{j=1}^{d} \frac{-P_J(\alpha_j)}{\alpha_j A'(\alpha_j)} \alpha_j^{-k} \qquad (d_J \leq k < d_{J+1})$$

and, since $|\alpha_j| \geq 1$ for all $1 \leq j \leq d$,

$$|q_k| \leq \sum_{i=1}^{J} |c_i| \sum_{j=1}^{d} \frac{1}{|\alpha_j A'(\alpha_j)|} \qquad (k < d_{J+1}). \tag{2.9}$$

Let B_J denote the right hand side of (2.9). Note that within 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

$$d_{J+1} - d_J > (2B_J + 1)^d. \tag{2.10}$$

Inequality (2.10) implies that there are two d-vectors $v_1 = \langle q_{k_1-d+1}, \ldots, q_{k_1}\rangle$ and $v_2 = \langle q_{k_2-d+1}, \ldots, q_{k_2}\rangle$ with $d_J \le k_1 < k_2 < d_{J+1}$ such that $v_1 = v_2$. Thus, $\{q_i\}_{k_1-d<i<d_{J+1}}$ is cyclic with cycle length $\omega \le k_2 - k_1$. Now, we can form an infinite number of multipliers $Q_t(x)$ such that $Q_t(x)A(x) \in \mathcal{P}_\alpha$. 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

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

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

$$\|Q_t A\| = \|\alpha\|_{min}$$

and

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

There are no roots of unity among $\alpha_1, \ldots, \alpha_d$; therefore

$$A(x) \,\Bigg|\, \sum_{j=J+1}^{n} c_j x^{d_j}.$$

This is a contradiction since

$$\left\|\sum_{j=J+1}^{n} c_j x^{d_j}\right\| < \|P\| = \|\alpha\|_{min}.$$

Hence the assumption (2.10) is false, and inequality (2.7) is proved.

Now, consider the case when α has no conjugate outside the unit circle. Since $P \in \mathcal{P}_\alpha$ and $\alpha \ne 0$ we may appeal to (2.1). Apply inequality (2.7) to both $P^*(x) = x^{\deg P}P(1/x) \in \mathcal{P}_{1/\alpha}$ and to $1/\alpha$, which has degree d and norm $\|\alpha\|$. Here, $A^*(x) = x^d A(1/x)$ is an irreducible polynomial in $\mathbb{Z}[x]$ of smallest degree having $1/\alpha$ as a root. Note that

$$A^{*\prime}(x) = dx^{d-1}A(1/x) - x^{d-2}A'(1/x)$$

Thus, for any conjugate $1/\alpha_i$ of $1/\alpha$ we have

$$\left|A^{*\prime}(1/\alpha_i)\right| = \left|\alpha_i^{-(d-2)}A'(\alpha_i)\right|$$

and inequality (2.8) follows. $\square$

Theorem 3. *Let α be a nonzero algebraic number of degree d. Assume that α is not a root of unity. Suppose that either no conjugates of α lie outside the unit circle or no conjugates of α lie inside the unit circle. If $P \in \mathcal{P}_\alpha$, then*

$$\deg P \leq 2^d d^{d^2+d} \|\alpha\|_{min}^{2d+2} \|\alpha\|^{2d^2-2d}. \tag{2.11}$$

Proof. We use the notation of Lemma 2. First, consider the case for which α has no conjugates outside the unit circle. Arguing as in the proof of Theorem 1, inequality (2.8) implies

$$d_{J+1} - d_J \leq \left(2\left(\|\alpha\|_{min}^2 - 1\right) \sum_{i=1}^{d} \frac{1}{|A'(\alpha_i)|} + 1\right)^d$$

for $1 \leq J \leq n-1$. Since all of the roots of A are distinct, A and A' are relatively prime. Let R denote the resultant of A and A'. Using a well-known resultant argument (see [19] or [6, Proposition 1.6]), since $|\alpha_i| \leq 1$, we have

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

Since $\|A'\| \leq d\,\|A\|$, we have

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

which implies

$$\begin{aligned} d_{J+1} - d_J &\leq \left(2\left(\|\alpha\|_{min}^2 - 1\right) d^{d+1} \|\alpha\|^{2d-2} + 1\right)^d \\ &\leq 2^d d^{d^2+d} \|\alpha\|_{min}^{2d} \|\alpha\|^{2d^2-2d}. \end{aligned} \tag{2.12}$$

Iterating this inequality on J and noting that $n \leq \|\alpha\|_{min}^2$ proves (2.11) in the case where α has no conjugate outside the unit circle. For the case when α has no conjugate inside the unit circle, we apply inequality (2.11) to $1/\alpha$ by appealing to (2.1) and the result follows. $\square$

§3 Effective Computation of $\|\alpha\|_{min}$

Having done so much preliminary work in §2, we are now in a position to give a relatively simple proof of the the main result of this paper.

Theorem 4. *If α is an algebraic number, then $\|\alpha\|_{min}$ is effectively computable.*

Proof. Let $A(x)$ be as in Lemma 1 and Lemma 2. We shall prove the theorem by showing that a $P \in \mathcal{P}_\alpha$ can be computed in finite time given only a knowledge of the degree and coefficients of A. We first check if $\|\alpha\|_{min} = 1$. This is easy to do because $A(x) = x$ if and only if $\|\alpha\|_{min} = 1$. Of course if $\|\alpha\|_{min} = 1$, we are done. Otherwise, note that $\|\alpha\|_{min} = \sqrt{2}$ if and only if α is a root of unity. If $A(x)$ divides $x^j - 1$ in $\mathbb{Z}[x]$ for some $j = 1, 2, \ldots, \lfloor 4d \log\log 6d \rfloor$, then $\|\alpha\|_{min} = \sqrt{2}$, and we are done. Otherwise, by Theorem

2, $\|\alpha\|_{min} > \sqrt{2}$. Next, successively let $k = 3, 4, \ldots, \|\alpha\|^2 - 1$. For each value of k, search over the finite set of polynomials $P \in \mathbb{Z}[x]$ satisfying $P(0) \neq 0$, $\|P\|^2 = k$ and

$$\deg P \leq \max\left\{ 2dk \left(\frac{\log k}{\log\left(1 + 1/(2^{d(d-1)/2} k^d)\right)} \right)^k,\ 2^d d^{d^2+d} k^{d+1} \|\alpha\|^{2d^2-2d} \right\}.$$

By Theorems 1 and 3, the first such polynomial found such that $A|P$ satisfies $P \in \mathcal{P}_\alpha$ and $\|\alpha\|_{min} = \|P\| = \sqrt{k}$. If no such polynomial is found, then $A \in \mathcal{P}_\alpha$ and $\|\alpha\|_{min} = \|\alpha\|$. $\square$

The main virtue of the algorithm occurring in the proof of Theorem 4 is its simplicity. In §4 we shall suggest some techniques that can significantly speed up performance, but the resulting algorithm will be decidedly more complicated.

First, however, we determine those algebraic numbers α whose corresponding $\mathcal{P}_\alpha$ is finite. As we shall see in the following theorem, the solution to this problem gives rise to an interesting characterization of the roots of unity.

Theorem 5. *An algebraic number α is a root of unity if and only if $\mathcal{P}_\alpha$ contains infinitely many polynomials.*

Proof. Suppose first that α is an n^{th} root of unity. Then $x^{jn} - 1$ belongs to $\mathcal{P}_\alpha$ for all $j \in \mathbb{Z}^+$. Hence $\mathcal{P}_\alpha$ contains infinitely many polynomials. On the other hand, if α is a not a root of unity, then α satisfies the hypotheses of at least one of Theorems 1 and 3. In either case, if $P \in \mathcal{P}_\alpha$, then there are only finitely many choices for $\deg P$. Furthermore,

$$\|P\| = \|\alpha\|_{min} \leq \|\alpha\|,$$

so there are only finitely many choices for $\|P\|$. Hence, $\mathcal{P}_\alpha$ contains finitely many polynomials. Theorem 5 is proved. $\square$

§4 Computing Minimal Euclidean Norms in Practice

Let α be an algebraic number, and let $A(x)$ be as in the introduction. Suppose that only $A(x)$ is known. Throughout this section we will be concerned with how best to calculate $\|\alpha\|_{min}$ in practice. It should be noted that our approach contains several key observations that can significantly reduce the search space occurring in the proof of Theorem 4. In some of the steps of this algorithm several options are available. The most notable difference between certain options is the use of numerical approximations to the roots of A. It has been shown by Schönhage [17] (or see [6]) that approximations to all of the roots of A can be computed in time polynomial in $\deg A$, $\log H(A)$ and the number of bits needed. It is possible, in each of the steps below, to entirely avoid these approximations, but they can be used advantageously at times. In order to avoid cumbersome notations, we will use $\alpha_1, \ldots, \alpha_d$ to denote either the roots of A or sufficiently accurate approximations to the roots of A. We shall give an indication of the accuracy required for each occasion in which numerical approximations to the roots of A can be used.

Algorithm: MinEuclideanNorm

Input: $A(x) = \sum_{j=0}^{d} a_j x^j = a_d \prod_{j=1}^{d} (x - \alpha_j)$ where A is an irreducible integer polynomial with root α, and $a_d > 0$

Output: $P \in \mathcal{P}_\alpha$

Step 1: If A is monomial or binomial.

If $A(x) = a_d x^d + a_0$, then $P = A$. In other words, if the number of nonzero coefficients of any polynomial A is 2 or less, then $\|\alpha\|_{min} = \|\alpha\|$. This is easy to see from the general fact that if

$$a_d x^d + \cdots + a_0 \big| c_m x^m + \cdots + c_0$$

where $a_d, a_0, c_m, c_0 \neq 0$ and $d, m > 0$, then $a_d | c_m$ and $a_0 | c_0$.

Step 2: Determine if $\|\alpha\|_{min} = \sqrt{2}$.

Arguing as in the proof of Theorem 4, we need to decide if A is equal to Φ_n, the n^{th} cyclotomic polynomial, for some $n \geq 3$ (Step 1 accounts for $n = 1, 2$). Note first that if d is odd, then A could not be cyclotomic because $\deg \Phi_n = \phi(n)$ is even for $n \geq 3$. Of course, if A is cyclotomic, then it must satisfy $|a_d| = |a_0| = 1$ and $A(x) = \pm x^d A(1/x)$, i.e., α is reciprocal and both α and $1/\alpha$ are algebraic integers. Now, from Dobrowolski [3] we know that if

$$\max_{1 \leq i \leq d} |\alpha_i| < 1 + \frac{\log d}{6d^2},$$

then α is a root of unity. Hence, using only $O(\log d)$ bits of accuracy in the roots, we can determine if the $|\alpha_i|$ are sufficiently close to 1 to force the α_i to be roots of unity. If $A = \pm\Phi_n$, then all the conjugates of α have the form $e^{2\pi i a/n}$ where $(a, n) = 1$. Thus, after we determine that $A = \pm\Phi_n$, we can determine n by using that

$$n = \left(2\pi / \min\left\{|\arg(\alpha_1)|, \ldots, |\arg(\alpha_d)|\right\}\right).$$

These numerical calculations also require only $O(\log d)$ bits of accuracy in the roots. We can then take $P = x^n - 1$. Alternatively, once we have determined that α is a root of unity, Theorem 2 implies that we can take $P = x^m - 1$, where $m = [4d \log\log(6d)]!$, so that n need not be determined.

A more elegant procedure to determine if A is cyclotomic is discussed in Bradford and Davenport [1] using a "Graeffe" method. Define the Graeffe operator by

$$\operatorname{graeffe}(A(x)) = g(x)^2 - x h(x)^2 \quad \text{where} \quad A(x) = g(x^2) + x h(x^2).$$

The roots of $\operatorname{graeffe}(A)$ are exactly the squares of the roots of A. Let $A_1 = \operatorname{graeffe}(A)$. The following three tests can be applied repeatedly (at most $O(\log d)$ iterations) to determine if A is cyclotomic. If they fail, A is not cyclotomic. (1) If $A_1 = \pm A$, then A is cyclotomic. (2) If $A_1(x) = \pm A(-x)$, and $A(-x)$ is cyclotomic, then A is cyclotomic. (3) If $A_1 = \pm A_2^2$, where A_2 is cyclotomic, then A is cyclotomic. This procedure does not determine n, but methods for determining n are discussed in [1]. Of course, a straightforward algebraic algorithm to determine n (and to determine if A is cyclotomic) is simply to trial divide $A(x)$ into $x^n - 1$ (or compute $\gcd(A(x), x^n - 1)$) for all $d < n \leq 4d \log\log 6d$ (using Theorem 2).

Step 3: Compute configuration of conjugates.

In order to apply Lemma 1 efficiently we need to know the location of the zeros with respect to the unit circle. In order to use numerical approximations to the roots to determine their location we need to know how much accuracy is required in order to differentiate $|\alpha|$ from 1. From [16, equation (11.1)], if $\beta \neq 1$ is algebraic, then

$$|1-\beta| \geq 2^{-\deg \beta} M(\beta)^{-1}.$$

Let $\beta = \alpha\overline{\alpha} = |\alpha|^2$. Since $\deg \beta \leq d(d-1)/2$, $M(\alpha\overline{\alpha}) \leq M^{2d}(\alpha)$ (see [2, equation (M2)]), and $M(\alpha) \leq \|\alpha\|$ (see, e.g., [12]), we have

$$\left||\alpha|^2 - 1\right| \geq 2^{-d(d-1)/2} \|\alpha\|^{-2d}.$$

Thus, $|\alpha|$ can be differentiated from 1 with only $O(d^2 \log H(\alpha))$ bits of accuracy. Therefore, using sufficiently accurate numerical approximations to the roots of A we can determine λ, the number of conjugates inside the unit circle; ν, the number of conjugates outside the unit circle; and $s = d - \lambda - \nu$, the number of conjugates on the unit circle.

There are also several algebraic methods that can be used for computing λ and ν which we will briefly touch on. Recall that A is an irreducible integer polynomial and we can assume, without loss of generality, that $A(\pm 1) \neq 0$ by Step 1. This allows us to make certain simplifications that cannot be made in general. First, consider the case in which A is not a reciprocal polynomial. In this case, $s = 0$ and there is no root β of A such that $1/\beta$ is also a root. Thus, the Schur-Cohn method (see [11, p. 204] or [2, p. 30]) is guaranteed to compute λ (and ν). Other methods are discussed in both [11] and [2], where a method using the Graeffe transform is presented. The second case is when A is a reciprocal polynomial. In this case, $\lambda = \nu = (d-s)/2$ so all we need do is compute s, the number of roots on the unit circle. One method to compute s is to form the resultant $R(x)$ of $A(z)$ and $z^2 - 2xz + 1$. Now, s is the number of real roots in $[-1, 1]$ of $R(x)$. This, of course, can be computed using Sturm's rule (see [7] or [11]).

Step 4: Check if A has a binomial multiple.

Assume this to be the case and let

$$Q(x)A(x) = a_d v x^{d+m} \pm a_0 u$$

where $Q \in \mathbb{Z}[x]$ has degree m, and u and v are the absolute values of the constant and leading coefficients, respectively, in Q. First, this implies that $|\alpha_1| = \cdots = |\alpha_d|$ and so by comparing the smallest root α_1 with the largest root α_d to the accuracy for which they were computed, we can check if this can possibly be the case. This check can be skipped if root approximations are not used. But, it must be the case that either $\lambda = d$ or $\nu = d$. Recall that the product of all the roots of A has absolute value equal to $|a_0/a_d|$ and the product of all the roots of Q has absolute value equal to u/v. Since Step 2 ruled out the possibility that α is a root of unity, we know that $|a_0| \neq |a_d|$ and $u \neq v$. The roots of QA all lie on the same circle with radius

$$\left|\frac{a_0}{a_d}\right|^{1/d} = \left(\frac{u}{v}\right)^{1/m} \tag{3.1}$$

which immediately leads to

$$m = \frac{d \log(u/v)}{\log |a_0/a_d|}.$$

We note that $a_0^2 + a_d^2 \neq ||QA||^2$ because this would imply $u = v = 1$, contradicting that $u \neq v$. Thus, we simply search over all $(u, v) \in \mathbb{Z}^+ \times \mathbb{Z}^+$ such that $a_0^2 + a_d^2 < \|QA\|^2 = a_0^2u^2 + a_d^2v^2 < \|A\|^2$ and such that there exists a positive integer m satisfying (3.1). Two obvious observations that can be made are if k is a putative value for $\|QA\|^2$ then $\gcd(a_0^2, a_d^2)|k$, and (u, v) must also pass the test that each of $A(1)$ and $A(-1)$ divides one of $a_dv + a_0u$ and $a_dv - a_0u$. For every such (u, v) we check if A divides either $a_dvx^{d+m} + a_0u$ or $a_dvx^{d+m} - a_0u$. If a binomial multiple is found, then we can only claim that $\|\alpha\|_{min} \leq \|QA\|$ which can be used in the steps below.

Step 5: Search for a $P \in \mathcal{P}_\alpha$.

Similar to the proof of Theorem 4, we shall fix k and search over all $P \in \mathbb{Z}[x]$ of the form (1.3) satisfying $\|P\|^2 = k$ and conditions governed by either Lemma 1, Theorem 1, Lemma 2, or Theorem 3. The decision between the lemmas and the theorems is based on whether or not approximations (to α_i or $M(\alpha)$) are to be used. The decision between Lemma 1/Theorem 1 versus Lemma 2/Theorem 3 is based on the following criteria depending on the computations made in Step 3. We assume that approximations are available. If $|a_d| = 1$ or $|a_0| = 1$ (α or $1/\alpha$ is an algebraic integer), then use Lemma 1 since the multiplicative factor in either (2.2) or (2.3) is 1 and the resulting bound on $d_{J+1} - d_J$ is almost certainly better than Lemma 2 in the chance that it could be used. If $s = d$, then only Lemma 2 is applicable. If $\lambda \neq 0$ and $\nu \neq 0$, then use Lemma 1. Lastly, if $s \neq d$ and either $\lambda = 0$ or $\nu = 0$, then we can use either Lemma 1 or Lemma 2 (or both simultaneously). For a discussion of computing $A'(\alpha_i)$ in Lemma 2 see [6, Lemma 1.5].

In order to use Lemma 1 we need to compute upper and lower bounds for $M(\alpha)$ and be able to distinguish $M(\alpha)/|a_0|$ and $M(\alpha)/|a_d|$ from 1. This is a straightforward computation given approximations to the roots of A. But, (2.4) implies that $O(d^2)$ bits of accuracy might be required. On the other hand, good approximations to $M(\alpha)$ can be had without direct computation of the roots. An elegant method using the Graeffe transform is as follows. Let $A_0 = A$ and $A_{m+1} = \text{graeffe}(A_m)$. Note that $M(A_m) = M(A)^{2^m}$ and $M(A_m) \leq \|A\|_m \leq 2^d M(A_m)$. Thus, as stated in [2, Proposition 1], we have

$$2^{-d2^{-m}} \|A_m\|^{2^{-m}} \leq M(\alpha) \leq \|A_m\|^{2^{-m}}.$$

Other methods for computing $M(\alpha)$ are also discussed in [2]. An easy special case is when one of λ, ν, or s is equal to d. Then, $M(\alpha) = \max\{|a_0|, |a_d|\}$.

We now would like to give one possible way of partitioning the search space. We will assume that we are in a situation in which both (2.2) and (2.3) apply. Other cases are similar and somewhat simpler. (1) Loop over integers k from $\max\{a_0^2 + a_d^2 + 1, M^2(\alpha)\}$ to $\|\alpha\|^2 - 1$ (or $a_0^2u^2 + a_d^2v^2 - 1$ if a binomial multiple was found in Step 4 and $a_0^2u^2 + a_d^2v^2 < \|\alpha\|^2$). Here, we assume that $k = \|\alpha\|_{min}^2$ and if $P \in \mathcal{P}_\alpha$, then $P = QA$ for some integer polynomial Q. Since P has the form (1.3), $a_d|c_n$, $a_0|c_1$. We have already seen in Step 4 that if $P \neq A$, then $P \neq a_dx^{d+m} \pm a_0$. Hence, we have $k \geq a_0^2 + a_d^2 + 1$. Also,

$M(\alpha) \leq M(Q)M(A) = M(P) \leq \|P\| = \sqrt{k}$. (2) Loop over integers r from $a_0^2 + a_d^2$ to $k-1$ in steps of $\gcd(a_0^2, a_d^2)$. Here, r denotes $c_1^2 + c_n^2 = a_0^2u^2 + a_d^2v^2$ where u and v are the constant and leading coefficients, respectively, of Q in $P = QA$. (3) Loop over all pairs $(u,v) \in \mathbb{Z}^+ \times \mathbb{Z}^+$ satisfying $a_0^2u^2 + a_d^2v^2 = r$. (4) Loop over all square partitions $\{s_2, \ldots, s_{n-1}\}$ of $k-r$, i.e., $s_2^2 + \cdots + s_{n-1}^2 = k - r$ where $s_j \in \mathbb{Z}^+$. (5) Loop over all distinct permutations $(\sigma_2, \ldots, \sigma_{n-1})$ of the square partition $\{s_2, \ldots, s_{n-1}\}$. (6) Loop over the 2^{n-1} sign combinations $(\epsilon_1, \ldots, \epsilon_{n-1})$ where $\epsilon_j = \pm 1$. Now, set

$$(c_1, c_2, \ldots, c_{n-1}, c_n) = (\epsilon_1 u a_0, \epsilon_2 \sigma_2, \ldots, \epsilon_{n-1}\sigma_{n-1}, v a_d),$$

which is the vector of nonzero coefficients of P as in (1.3). Before searching over possible degree sequences (the degrees of the monomials in P), we can perform a test independent of the degree sequence. Proceed only if $A(1) | \sum_{j=1}^{n} c_j$. Indeed if $|A(-1)| > |A(1)|$, then we should perform the entire algorithm with $-\alpha$ and $A(-x)$ since $P(x) \in \mathcal{P}_\alpha$ if and only if $P(-x) \in \mathcal{P}_{-\alpha}$. (7) Loop over all degree sequences $(d_1, \ldots, d_n)$ satisfying (2.2) and (2.3) simultaneously (we assumed they both apply). We can work from "both ends" of $(d_1, \ldots, d_n)$, meeting in the middle, in order to minimize the accumulation of the multiplicative factors in the inequalities. Another method, assuming that an approximation to α is available, is work with only one of the inequalities, (2.2) say, depending on which has the smallest multiplicative factor. Then, loop over degree sequences $(d_1, \ldots, d_{n-1})$, and let d_n equal the integer nearest to $\log |R(\alpha)/c_n| / \log |\alpha|$, where $R(x) = \sum_{j=1}^{n-1} c_j x^{d_j}$. (8) If d_n satisfies both $d_n > d$ and (2.2), check by trial division to see if $A(x)$ divides $P(x) = \sum_{j=1}^{n} c_j x^{d_j}$. If so, then $P \in \mathcal{P}_\alpha$ and $\|\alpha\|_{min} = \sqrt{k}$. If no such P is found during this combinatorial search procedure, then $\|\alpha\|_{min} = \|\alpha\|$ and $A \in \mathcal{P}_\alpha$.

§5 Conclusions and Connections

The algorithm in §4 has been used to successfully compute the minimal Euclidean norm of certain algebraic numbers. For example, let β be a root of the irreducible integer polynomial

$$B(x) = x^9 - x^8 + x^7 - x^6 + x^5 - x^4 + x^3 - x^2 + 2x - 1,$$

so that $\|\beta\| = \sqrt{13}$. It is easy to see that $\|\beta\|_{min} \leq \sqrt{4}$ by considering $(x+1)B(x)$. Since $B(x)$ has a real root between 0 and 1, $B(x)$ is not cyclotomic and $\|\beta\|_{min} \neq \sqrt{2}$. In the absence of further argument, one would be compelled to continue searching for other elements $P \in \mathcal{P}_\beta$ satisfying $\|P\|_{min} = \sqrt{3}$. However, such a search would be fruitless and never terminate because an implementation of the algorithm in §4 certified that $\|\beta\|_{min} = \sqrt{4}$ and that

$$(x+1)B(x) = x^{10} + x^2 + x - 1 \in \mathcal{P}_\beta.$$

Suppose now that α is an algebraic number with $A(x)$ as in the introduction. Motivated by the preceding example, it is worth noting, as an indication of the difficulties involved, that the determination of a $P \in \mathcal{P}_\alpha$ yields a shortest nonzero vector in an infinite union of certain lattices. Indeed, if v and w are in $\mathbb{C}^n$, let $v \cdot w$ denote the dot product of v and w. Given any subset W of $\mathbb{C}^n$, we let

$$W^\perp = \{v \in \mathbb{C}^n : v \cdot w = 0 \ \forall\, w \in W\}.$$

If α is algebraic, consider the lattice L_n defined by

$$L_n = \left\{(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})\right\}^{\perp} \cap \mathbb{Z}^n.$$

Then a polynomial $P \in \mathbb{Z}[x]$ satisfies both

$$P(\alpha) = 0 \text{ and } \|P\| = \|\alpha\|_{min}$$

if and only if the coefficient vector of P is a shortest nonzero vector in $\cup_{n=1}^{\infty} L_n$. In light of such difficulties, it is not surprising that the algorithm in §4 is not feasible unless the degree and Euclidean norm of α are both sufficiently small. In fact, even when α is an algebraic integer and Lemma 1 is used to bound the number of plausible multiples of A, it is easy to see that the number of elements in the search space is at least exponential in $\|\alpha\|^2$, provided $\|\alpha\|_{min} = \|\alpha\|$.

The algorithm in §4 can be thought of as a "search-over-multiples" approach in that we exhaust over plausible multiples of A for one of least Euclidean norm. However, there is also the possibility of a "search-over-multipliers" approach. Here we search over plausible polynomial multipliers of A for one which, when multiplied with A, yields an element of $\mathcal{P}_\alpha$. We shall now show that the "search-over-multipliers" approach has a finite search space of plausible multipliers. Suppose that $Q \in \mathbb{Z}[x]$ is any multiplier of A for which $\|QA\| = \|\alpha\|_{min}$. An upper bound, say $D(\alpha)$, on $\deg Q$ follows immediately from Theorems 1-3. Furthermore, using a result of Mignotte [12, Theorem 2], we know that

$$|q_j| \le \binom{\deg Q}{j} \|\alpha\|_{min} \le \binom{D(\alpha)}{j} \|\alpha\|_{min},$$

where $Q(x) = \sum_{j=0}^{\deg Q} q_j x^j$. At first glance, the "search-over-multipliers" approach sounds more appealing than the "search-over-multiples" approach because each multiplier requires a polynomial multiplication operation, while each plausible multiple requires a polynomial division operation. However, there are usually significantly more multipliers to search over than multiples. Also, Lemmas 1 and 2 can be used in the "search-over-multiples" approach to drastically cut down the number of multiples. These savings do not seem possible in the "search-over-multipliers" approach outlined above.

Nonetheless, in special situations, known results on the reducibility of lacunary integer polynomials can be used to reduce the search space occurring in the algorithm in §4. As an example, let q be an odd prime and let ϵ_1, ϵ_2, and ϵ_3 take the values ± 1. Suppose we are checking to see if $\|\alpha\|_{min}^2 = 3 + q^2$ by determining if a polynomial of the form

$$P(x) = x^{d_3} + \epsilon_1 x^{d_2} + \epsilon_2 x^{d_1} + \epsilon_3 q \tag{5.1}$$

belongs to $\mathcal{P}_\alpha$. If $q > 3$, then there is no further work to be done because Ljunggren [10] has shown that any P of the form (5.1) is irreducible. If $q = 3$, then Ljunggren [10] proved that any P of the form (5.1) is either irreducible or the product of an irreducible integer polynomial and a polynomial of the form $x^j \pm 1$ for some $j \in \mathbb{Z}^+$. It is easy to see that such severe constraints on the factors of P can sometimes be used to drastically reduce the number of plausible multiples of A that need to be considered. Other relevant results on the reducibility of lacunary integer polynomials can be found in the the papers of Selmer [18]; Ljunggren [9], [10]; Jonassen [5]; and Schinzel [14], [15]. We note that the second paper of Schinzel's is in fact the first in his monumental series of 11 papers on the subject of lacunary integer polynomials.

Acknowledgment

The authors would like to thank H. R. P. Ferguson for pointing out the connection between minimal Euclidean norms and shortest vectors in lattices which was discussed in §5.

References

[1] R. J. Bradford and J. H. Davenport, *Effective tests for cyclotomic polynomials*, Symbolic and Algebraic Computation (P. Gianni, ed.), Proceedings of ISSAC in Rome, Italy, 1988, Springer-Verlag, Lecture Notes in Computer Science Vol. 358, pp. 244–251.

[2] L. Cerlienco, M. Mignotte, and F. Piras, *Computing the measure of a polynomial*, J. Symbolic Computation **4** (1987), 21–33.

[3] E. Dobrowolski, *On the maximal modulus of conjugates of an algebraic integer*, Bull. Acad. Polon. Sci. **26** (1978), 291–292.

[4] G. H. Hardy, J. E. Littlewood and G. Pólya, *Inequalities*, 2nd Edition, Cambridge University Press, Cambridge, 1952.

[5] A.T. Jonassen, *On the irreducibility of the trinomials $x^m \pm x^n \pm 4$*, Math. Scand. **21** (1969), 177–189.

[6] R. Kannan, A. Lenstra, and L. Lovász, *Polynomial factorization and nonrandomness of bits of algebraic and some transcendental numbers*, Math. Comp. **50** no. 181 (1988), 235–250.

[7] D. Knuth, *The Art of Computer Programming, Volume 2, Seminumerical Algorithms*, 2nd Edition, Addison-Wesley, Reading, Massachusetts, 1981.

[8] L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*, J. Reine Angew. Math. **53** (1857), 133–175.

[9] W. Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*, Math. Scand. **8** (1960), 287–302.

[10] W. Ljunggren, *On the irreducibility of certain lacunary polynomials*, Norske. Vid. Selsk. Forh. (Trondheim) **36** (1963), 159–164.

[11] M. Marden, *Geometry of Polynomials*, Mathematical Surveys, Number 3, American Mathematical Society, Providence, Rhode Island, 1966.

[12] M. Mignotte, *An inequality about factors of polynomials*, Math. Comp. **28** no. 128 (1974), 1153–1157.

[13] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. of Math. **6** (1962), 64–94.

[14] A. Schinzel, *On the reducibility of polynomials and in particular trinomials*, Acta. Arith. **11** (1965), 1–34.

[15] A. Schinzel, *Reducibility of lacunary polynomials. I.*, Acta. Arith. **16** (1969/70), 123-159.

[16] W. M. Schmidt, *Diophantine Approximation*, Lect. Notes in Math. 785, Springer-Verlag, New York, 1980.

[17] A. Schönhage, *The Fundamental Theorem of Algebra in terms of computational complexity*, Preliminary report, Math. Inst. Univ. Tübingen (1982).

[18] E. S. Selmer, *On the irreducibility of certain trinomials*, Math. Scand. (1956).

[19] J. Uspensky, *Theory of Equations*, McGraw-Hill, New York, 1948.
[20] A. J. van der Poorten and J. H. Loxton, *Multiplicative relations in number fields*, Bull. Austrl. Math. Soc. **16** (1974), 83–98.

Mathematics Department, University of South Carolina, Columbia, South Carolina 29208

Supercomputing Research Center, 17100 Science Drive, Bowie, MD 20715-4300