Derandomization of Sparse Cyclotomic Integer Zero Testing

Qi Cheng*
School of Computer Science
The University of Oklahoma
Norman, OK 73019, USA.
Email: qcheng@cs.ou.edu.

Abstract

The zero testing and sign determination problems of real algebraic numbers of high extension degree are important in computational complexity and numerical analysis. In this paper we concentrate on sparse cyclotomic integers. Given an integer n and a sparse polynomial $f(x) = c_k x^{e_k} + c_{k-1}x^{e_{k-1}} + \cdots + c_1 x^{e_1}$ over $\mathbf{Z}$, we present a deterministic polynomial time algorithm to decide whether $f(\omega_n)$ is zero or not, where ω_n denotes the n-th primitive root of unity $e^{2\pi\sqrt{-1}/n}$. All previously known algorithms are either randomized, or do not run in polynomial time. As a side result, we prove that if n is free of prime factors less than $k+1$, there exist k field automorphisms $\sigma_1, \sigma_2, \cdots, \sigma_k$ in the Galois group $Gal(\mathbf{Q}(\omega_n)/\mathbf{Q})$ such that for any nonzero integers $c_1, c_2, \cdots, c_k$ and for any integers $0 \le e_1 < e_2 < \cdots < e_k < n$, there exists i so that $|\sigma_i(c_k\omega_n^{e_k} + c_{k-1}\omega_n^{e_{k-1}} + \cdots + c_1\omega_n^{e_1})| \ge 1/2^{(k^2\log n + k\log k)}$.

1 Introduction

In computational geometry and numerical analysis, we often need to know whether an algebraic number is zero or not. Furthermore, in case that a nonzero algebraic number is real, we sometimes need to determine its sign. We can usually compute the decimal expansion of the algebraic number up to a polynomial precision in polynomial time. The zero testing problem or sign determination problem become nontrivial if the algebraic number has high extension degree and its absolute value may be too small. These two problems are closely related to fundamental questions in computational complexity such as polynomial identity testing [4].

A cyclotomic integer can be represented as $f(\omega_n)$, where f is an integral polynomial. We call a cyclotomic integer sparse if f is given in its sparse representation. Can we decide in polynomial time whether a sparse cyclotomic integer is zero or not? In the other words, can we decide whether the primitive n-th root of unity ω_n is a root of $f(x)$ in time polynomial in $\log n$ and size of the sparse representation of $f(x)$? Note that $f(\omega_n)$ is zero iff $\Phi_n(x)|f(x)$, where $\Phi_n(x)$ is the n-th cyclotomic polynomial. The number of nonzero terms in $\Phi_n(x)$ can be exponential in $\log n$, thus it may not be possible to write it down. Nonetheless the zero testing problem of cyclotomic integers was proved to be in co-NP in [8, Theorem 4.3]. An algorithm to solve the problem was proposed recently [6, Theorem 3], whose time complexity is exponential in number of prime factors of n, thus if n has many distinct small prime factors then the algorithm does not run in polynomial time. In addition, the algorithm assumes that the prime factorization of n is known.

Even though the degree of a sparse integral polynomial $f(x)$ can be very high, we can approximately compute the decimal expansion of $f(\omega_n)$ up to any precision in time polynomial in the input size and the precision by using Taylor series

$$\omega_n^d = e^{2d\pi\sqrt{-1}/n} = \sum_{i=0}^{\infty} \frac{1}{i!}\left(\frac{2d\pi\sqrt{-1}}{n}\right)^i$$

for each term of $f(\omega_n)$. What is the the smallest possible absolute value of a nonzero sparse cyclotomic integer? Define

$$r(k,n,m) = \min\Big\{|\sum_{i=1}^{k} c_i\omega_n^{e_i}| \;\Big|\; c_i \in \mathbf{Z}, |c_i| \le m, 0 \le e_i < n, \sum_{i=1}^{k} c_i\omega_n^{e_i} \ne 0\Big\}.$$

If we can bound $-\log r(k,n,m)$ from above by a polynomial function in $k, \log n$ and $\log m$, then we can solve the zero testing problem in polynomial time. For any $\sigma \in Gal(\mathbf{Q}(\omega_n)/\mathbf{Q})$, $|\sigma(f(\omega_n))| \le km$. If $f(\omega_n)$ is not

*This research is supported in part by NSF career award CCR-0237845.

zero, we have

$$|Norm(f(\omega_n))| = \prod_{\sigma \in Gal(\mathbf{Q}(\omega_n)/\mathbf{Q})} |\sigma(f(\omega_n))| \geq 1. \quad (1)$$

Thus $|f(\omega_n)| \geq 1/(km)^{\phi(n)}$, where ϕ is Euler's phi function. This means that $r(k,n,m) \geq 1/(km)^{\phi(n)}$, which is known as the root separation bound. If the bound is close to be tight, it seems that we need exponential precision, i.e. $\phi(n)\log(km) = \Omega(n\log(km)/\log\log n)$, to tell whether a real sparse cyclotomic integer is zero or not. Numerical evidence suggests that the root separation bound is too pessimistic for sparse cyclotomic integers. However there is no significant improvement on the bound of $r(k,n,m)$ in recent years.

Definition 1 *The sparseness of a polynomial is the number of its nonzero terms. The height of an integral polynomial is the maximum absolute value of its coefficients. For an integral polynomial f, we use $sps(f)$ to denote its sparseness and use $ht(f)$ to denote its height.*

On the other hand, from the inequality (1) we can also conclude that absolute values of most of the conjugates of a nonzero $f(\omega_n)$ are not too small. In fact, it can be shown that if we randomly select an element $\sigma \in Gal(\mathbf{Q}(\omega_n)/\mathbf{Q})$, then with probability at least $1/2$, $|\sigma(f(\omega_n))| \geq 1/km$. So we can solve zero testing of sparse cyclotomic integers in randomized polynomial time. This idea has been used in [4, 3] to design randomized algorithm for polynomial identity testing and zero-test of expressions involving roots of rationals.

If $f(\omega_n)$ is known to be a real number, can we decide whether it is positive or negative? This is called sign determination problem of sparse real cyclotomic integers. The sign determination problem appears to be much harder than the zero testing problem for many types of algebraic numbers. The most famous one is the sum of square roots problem [7, 5], which asks to determine the sign of

$$\sqrt{a_1} + \cdots + \sqrt{a_k} - \sqrt{b_1} - \cdots - \sqrt{b_k} \qquad (2)$$

where a_i and b_i are positive integers. It is still open whether the problem is in NP or not, even in the case when a_i's and b_i's are bounded from above by a polynomial function on k. This type of problems have attracted attentions recently and they belong to the so called generic task of numerical analysis [1]. We comment that the zero testing problem of sum of square roots can be solved in deterministic polynomial time [2].

1.1 Our results

In this paper, we present the first deterministic polynomial time algorithm to test whether a sparse cyclotomic integer is zero or not. Our algorithm does not need to know the large prime factors of n, which may be hard to find. First observe that if n is a prime and $f(x)$ is a nonzero integral polynomial of sparseness less than n, then $f(\omega_n)$ cannot be zero. This fact can be derived from the following Chebotarev theorem.

Proposition 1 *If n is a prime, then any minor of the matrix $(\omega_n^{ij})_{1\leq i,j\leq n}$ is not zero.*

There are many proofs of the Chebotarev theorem. For an elementary one, see [9]. By studying selected minors of the matrix $(\omega_n^{ij})_{1\leq i,j\leq n}$ when n is not a prime, we show that if f is a nonzero integral polynomial and all the prime factors of n are greater than $sps(f)$, then the cyclotomic integer $f(\omega_n)$ can not be zero. If n has small prime factors, then from a sparse cyclotomic integer $f(\omega_n)$, our algorithm produces a list of sparse cyclotomic integers in *smaller* field, such that $f(\omega_n)$ is zero iff all the elements in the list are zero. The algorithm applies the procedure recursively on each cyclotomic integer in the list until we reach a field where the zero testing problem can be easily solved. The recursion can have many recursive levels. As the recursion goes deeper, the number of cyclotomic integers increases, and in some cases, the sum of their sparseness also increases, nonetheless we are able to show that the algorithm runs in polynomial time.

One can find an element σ in $Gal(\mathbf{Q}(\omega_n)/\mathbf{Q})$ in randomized polynomial time such that $|\sigma f(\omega_n)|$ is not too small whenever $f(\omega_n)$ is not zero, but can we derandomize the procedure? We answer it affirmatively in Section 4 when the prime factors of n are all greater than $sps(f)$. For other n's, this problem is likely to be harder than the derandomization of zero testing problem. From the numerical evidence, it is reasonable to conjecture that $|f(\omega_n)|$ is not too small whenever $f(\omega_n)$ is not zero and f is sparse. If the conjecture is true, then the sign determination problem of real sparse cyclotomic integer can be settled. We believe that finding a large conjugate in deterministic polynomial time is the first step towards proving the conjecture.

It has been proved that all abelian number fields are subfields of cyclotomic fields. For example, for a prime p, the square of the principle Gaussian sum $\sum_{i=1}^{p-1}(\frac{i}{p})\omega_p^i$ is p or $-p$. Hence $\sqrt{p} \in \mathbf{Q}(\omega_{4p})$. Applying this observation, we can write (2) as sum of at most $\sum_{i=1}^k a_i + \sum_{i=1}^k b_i$ many t-th roots of unity, where $t|(4\prod_{i=1}^k a_i \prod_{i=1}^k b_i)$. As a result, we obtain a *sparse* cyclotomic integer, assuming that a_i's and b_i's are bounded from above by a polynomial function on k. This means that we convert the problem of comparing sums of square roots to the sign determination problem of sparse cyclotomic integers when a_i's and b_i's are small. We believe that cyclotomic integers provide a uniform platform to study the problem of zero testing and sign determination of algebraic integers.

2 Key lemmas for derandomization

It is well known that the ring of integers in cyclotomic field $\mathbf{Q}(\omega_n)$ consists of all the elements in $\mathbf{Z}[\omega_n]$. The field automorphism of $\mathbf{Q}(\omega_n)$ is isomorphic to $(\mathbf{Z}/n\mathbf{Z})^*$. For an integer $i \in (\mathbf{Z}/n\mathbf{Z})^*$, let $\sigma^{(i)}$ denote the field automorphism which sends ω_n to ω_n^i. Then for any integral polynomial f, we have

$$\sigma^{(i)}(f(\omega_n)) = f(\omega_n^i).$$

First we prove a general lemma

Lemma 1 *Let E be a subfield of F. Let $\alpha_1, \alpha_2, \cdots, \alpha_k$ be elements in F. If there exist k field automorphisms $\sigma_1, \sigma_2, \cdots, \sigma_k \in Gal(F/E)$ such that the matrix*

$$V = \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_k) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_k) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_k(\alpha_1) & \sigma_k(\alpha_2) & \cdots & \sigma_k(\alpha_k) \end{pmatrix}$$

is nonsingular, then $\alpha_1, \alpha_2, \cdots, \alpha_k$ are linearly independent over E .

Proof: Suppose that $\alpha_1, \alpha_2, \cdots, \alpha_k$ are linearly dependent over E. Then there exist $a_1, a_2, \cdots, a_k \in E$ such that $\sum_{i=1}^k a_i\alpha_i = 0$ and $a_i \neq 0$ for at least one i. Hence $\sigma_j(\sum_{i=1}^k a_i\alpha_i) = \sum_{i=1}^k a_i\sigma_j(\alpha_i) = 0$ for all $1 \leq j \leq k$. This means that the vectors

$$\begin{pmatrix} \sigma_1(\alpha_1) \\ \sigma_2(\alpha_1) \\ \vdots \\ \sigma_k(\alpha_1) \end{pmatrix}, \begin{pmatrix} \sigma_1(\alpha_2) \\ \sigma_2(\alpha_2) \\ \vdots \\ \sigma_k(\alpha_2) \end{pmatrix}, \cdots, \begin{pmatrix} \sigma_1(\alpha_k) \\ \sigma_2(\alpha_k) \\ \vdots \\ \sigma_k(\alpha_k) \end{pmatrix}$$

are linearly dependent over $E \subseteq F$. Thus the matrix V is singular, which leads to a contradiction. □

Let k be positive integers and f be an integral polynomial given in sparse form with $sps(f) = k$. Write $n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_l^{\beta_l} r$, where $p_1, p_2, \cdots, p_l$ are distinct primes less than $k+1$ and r is free of prime factors less than $k+1$. Note that it may be hard to factor r. As observed in [8, 6], $f(\omega_n) = 0$ iff

$$x^n - 1 \text{ divides } f(x) \prod_{p|n} (x^{n/p} - 1).$$

If the expansion of the latter polynomial has a short sparse representation, then we can check quickly whether $x^n - 1$ divides it or not by replacing x^e in the expansion with $x^{e \mod n}$ and testing whether we have a zero polynomial or not. Thus if $r = 1$ and $l \leq 2$, then we can solve the zero testing problem of cyclotomic integers efficiently.

For $q \in \{p_1, p_2, \cdots, p_l, r\}$, since $\omega_n^e = \omega_n^{aq+b} = (\omega_n^q)^a \omega_n^b$ where a and b are quotient and remainder respectively of division of e by q, we can write $f(\omega_n)$ in the following form

$$g_t(\omega_n^q)\omega_n^{e_t} + g_{t-1}(\omega_n^q)\omega_n^{e_{t-1}} + \cdots + g_1(\omega_n^q)\omega_n^{e_1} \qquad (3)$$

such that exponents $e_t, e_{t-1}, \cdots, e_1$ fall in t different classes modulo q, and $g_i(x)$'s are sparse polynomials. We divide the zero testing problem of (3) into three cases:

1. $gcd(q, n/q) = 1$ and $t < q$, which includes the case that $q = r$; or
2. $gcd(q, n/q) = 1$ and $t = q$, which implies that q is a prime; or
3. $gcd(q, n/q) > 1$, which implies that $q^2|n$.

Each case will be handled by one of the following lemmas.

Lemma 2 *If $t < q$ and $gcd(q, n/q) = 1$, then the cyclotomic integer (3) is zero iff $g_i(\omega_{n/q})$ is zero for all $1 \leq i \leq t$.*

Proof: We shall show that $\omega_n^{e_1}, \omega_n^{e_2}, \cdots, \omega_n^{e_t}$ are linearly independent over $\mathbf{Q}(\omega_n^q) = \mathbf{Q}(\omega_{n/q})$. For $1 \leq i \leq t$, set $s_i = 1 + (i-1)Tn/q$, where T is an integer that is congruent to $(n/q)^{-1} \pmod q$. Since for every i, $s_i \mod n/q = 1$ and $s_i \mod q = i < q$, so $gcd(s_i, n) = 1$ and $\sigma^{(s_i)} \in Gal(\mathbf{Q}(\omega_n)/\mathbf{Q})$, which fixes $\mathbf{Q}(\omega_{n/q})$. We only need to prove the matrix V

$$= \begin{pmatrix} \sigma^{(s_1)}(\omega_n^{e_1}) & \sigma^{(s_1)}(\omega_n^{e_2}) & \cdots & \sigma^{(s_1)}(\omega_n^{e_t}) \\ \sigma^{(s_2)}(\omega_n^{e_1}) & \sigma^{(s_2)}(\omega_n^{e_2}) & \cdots & \sigma^{(s_2)}(\omega_n^{e_t}) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma^{(s_t)}(\omega_n^{e_1}) & \sigma^{(s_t)}(\omega_n^{e_2}) & \cdots & \sigma^{(s_t)}(\omega_n^{e_t}) \end{pmatrix}$$

$$= \begin{pmatrix} \omega_n^{e_1 s_1} & \omega_n^{e_2 s_1} & \cdots & \omega_n^{e_t s_1} \\ \omega_n^{e_1 s_2} & \omega_n^{e_2 s_2} & \cdots & \omega_n^{e_t s_2} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_n^{e_1 s_t} & \omega_n^{e_2 s_t} & \cdots & \omega_n^{e_t s_t} \end{pmatrix}$$

is nonsingular. In fact, $det(V)$

$$
\begin{aligned}
&= (\prod_{i=1}^{t} \omega_n^{e_i}) \times \\
&\begin{vmatrix}
\omega_n^{e_1(s_1-1)} & \omega_n^{e_2(s_1-1)} & \cdots & \omega_n^{e_t(s_1-1)} \\
\omega_n^{e_1(s_2-1)} & \omega_n^{e_2(s_2-1)} & \cdots & \omega_n^{e_t(s_2-1)} \\
\vdots & \vdots & \ddots & \vdots \\
\omega_n^{e_1(s_t-1)} & \omega_n^{e_2(s_t-1)} & \cdots & \omega_n^{e_t(s_t-1)}
\end{vmatrix} \\
&= (\prod_{i=1}^{t} \omega_n^{e_i}) \times \\
&\begin{vmatrix}
1 & 1 & \cdots & 1 \\
\omega_n^{\frac{e_1 Tn}{q}} & \omega_n^{\frac{e_2 Tn}{q}} & \cdots & \omega_n^{\frac{e_t Tn}{q}} \\
\vdots & \vdots & \ddots & \vdots \\
\omega_n^{\frac{e_1(t-1)Tn}{q}} & \omega_n^{\frac{e_2(t-1)Tn}{q}} & \cdots & \omega_n^{\frac{e_t(t-1)Tn}{q}}
\end{vmatrix}
\end{aligned}
$$

where the matrix in the last line is Vandermonde. Hence

$$det(V) = \prod_{i=1}^{t} \omega_n^{e_i} \prod_{1 \le i < j \le t} (\omega_n^{e_j Tn/q} - \omega_n^{e_i Tn/q}).$$

If $e_j \not\equiv e_i \pmod q$, then $e_j Tn/q \not\equiv e_i Tn/q \pmod n$. Hence $det(V) \neq 0$ and $\omega_n^{e_1}, \omega_n^{e_2}, \cdots, \omega_n^{e_t}$ are linearly independent over $\mathbf{Q}(\omega_{n/q})$ by Lemma 1.

□

Remark: The lemma implies that if n is free of prime factors less than $k+1$, then (3) cannot be zero.

Lemma 3 *If $q^2|n$, then the cyclotomic integer (3) is zero iff $g_i(\omega_{n/q})$ is zero for all $1 \le i \le t$.*

Proof: For $1 \le i \le t$, we define u_i to be $1 + (i-1)n/q$. Since for any prime dividing n, it must divide $(i-1)n/q$, we have that $gcd(u_i, n) = 1$. It is easy to see that $\sigma^{(u_i)}$ fixes $\mathbf{Q}(\omega_{n/q})$. Just like what we do in the proof of Lemma 2, we compute the determinant of the matrix $W = (\sigma_n^{(u_i)}(\omega_n^{e_j}))_{1 \le i,j \le t}$

$$
\begin{aligned}
&\begin{vmatrix}
\omega_n^{e_1 u_1} & \omega_n^{e_2 u_1} & \cdots & \omega_n^{e_t u_1} \\
\omega_n^{e_1 u_2} & \omega_n^{e_2 u_1} & \cdots & \omega_n^{e_t u_2} \\
\vdots & \vdots & \ddots & \vdots \\
\omega_n^{e_1 u_t} & \omega_n^{e_2 u_t} & \cdots & \omega_n^{e_t u_t}
\end{vmatrix} \\
&= (\prod_{i=1}^{t} \omega_n^{e_i}) \times \\
&\begin{vmatrix}
\omega_n^{e_1(u_1-1)} & \omega_n^{e_2(u_1-1)} & \cdots & \omega_n^{e_t(u_1-1)} \\
\omega_n^{e_1(u_2-1)} & \omega_n^{e_2(u_2-1)} & \cdots & \omega_n^{e_t(u_2-1)} \\
\vdots & \vdots & \ddots & \vdots \\
\omega_n^{e_1(u_t-1)} & \omega_n^{e_2(u_t-1)} & \cdots & \omega_n^{e_t(u_t-1)}
\end{vmatrix} \\
&= (\prod_{i=1}^{t} \omega_n^{e_i}) \times \\
&\begin{vmatrix}
1 & 1 & \cdots & 1 \\
\omega_n^{\frac{e_1 n}{q}} & \omega_n^{\frac{e_2 n}{q}} & \cdots & \omega_n^{\frac{e_t n}{q}} \\
\vdots & \vdots & \ddots & \vdots \\
\omega_n^{\frac{(t-1)e_1 n}{q}} & \omega_n^{\frac{(t-1)e_2 n}{q}} & \cdots & \omega_n^{\frac{(t-1)e_t n}{q}}
\end{vmatrix}
\end{aligned}
$$

where we need to compute the determinant of a Vandermonde matrix in the last line. Hence

$$det(W) = \prod_{i=1}^{t} \omega_n^{e_i} \prod_{1 \le i < j \le t} (\omega_n^{e_j n/q} - \omega_n^{e_i n/q}).$$

If $e_j \not\equiv e_i \pmod q$, then $e_j n/q \not\equiv e_i n/q \pmod n$. Hence $det(W) \neq 0$ and $\omega_n^{e_1}, \omega_n^{e_2}, \cdots, \omega_n^{e_t}$ are linearly independent over $\mathbf{Q}(\omega_{n/q})$ by Lemma 1.

□

The remaining case is that $t = q$ is a prime and $gcd(q, n/q) = 1$. In this case, the q integers $n/q, 2n/q, \cdots, (q-1)n/q$ and n fall in different classes modulo q, so we can rewrite (3) in the form

$$\begin{aligned} &\tilde{g}_1(\omega_n^q)\omega_n^{n/q} + \tilde{g}_2(\omega_n^q)\omega_n^{2n/q} + \cdots \\ &+\tilde{g}_{q-1}(\omega_n^q)\omega_n^{(q-1)n/q} + \tilde{g}_q(\omega_n^q) \end{aligned} \quad (4)$$

Lemma 4 *If q is a prime and $gcd(q, n/q) = 1$, then the cyclotomic integer (4) is zero iff $\tilde{g}_1(\omega_{n/q}) = \tilde{g}_2(\omega_{n/q}) = \cdots = \tilde{g}_q(\omega_{n/q})$.*

Proof: We have that

$$1 + \omega_n^{n/q} + \omega_n^{2n/q} + \cdots + \omega_n^{(q-1)n/q} = 0.$$

Hence $1 = -\omega_n^{n/q} - \omega_n^{2n/q} - \cdots - \omega_n^{(q-1)n/q}$. Plug it into (4), we obtain

$$\begin{aligned} &(\tilde{g}_1(\omega_n^q) - \tilde{g}_q(\omega_n^q))\omega_n^{n/q} + \\ &(\tilde{g}_2(\omega_n^q) - \tilde{g}_q(\omega_n^q))\omega_n^{2n/q} + \\ &\cdots + (\tilde{g}_{q-1}(\omega_n^q) - \tilde{g}_q(\omega_n^q))\omega_n^{(q-1)n/q}. \end{aligned} \quad (5)$$

Lemma 2 implies that (5) is zero iff $\tilde{g}_i(\omega_n^q) - \tilde{g}_q(\omega_n^q) = 0$ for all $1 \le i \le q-1$. That is equivalent to

$$\tilde{g}_1(\omega_{n/q}) = \tilde{g}_2(\omega_{n/q}) = \cdots = \tilde{g}_q(\omega_{n/q}).$$

□

3 Algorithm and time complexity analysis

Based on the lemmas in the previous section, we shall take a divide-and-conquer approach to design a zero testing algorithm for sparse cyclotomic integers. To guarantee polynomial time complexity, when Lemma 4 applies, we pick the $\tilde{g}_M(x)$ with fewest number of nonzero terms among all $\tilde{g}_i(x)$'s in (4), and test whether $\tilde{g}_i(\omega_{n/q}) - \tilde{g}_M(\omega_{n/q})$ equals to zero for all $i \neq M$, $1 \le i \le q$. The algorithm is described in Figure 1, whose inputs consist of an integral polynomial $f(x)$ given in sparse form and an integer n. The degree of f is less than n. The algorithm outputs "Yes" if $f(\omega_n) = 0$. Otherwise it outputs "No".

Theorem 1 *The algorithm* **zerotesting**$(f(x),\ n)$ *runs in time* $poly(k, \log n, \log m)$*, where* k *is the sparseness of* $f(x)$ *and* m *is the height of* $f(x)$*.*

The following lemma is useful in proving the theorem.

Lemma 5 *Let* $t \ge 4$ *be a positive integer. Let* $a_1 \le a_2 \le \cdots \le a_t$ *be positive integers. Then*

1. $(\sum_{i=1}^t a_i)^2 > \sum_{i=1}^t a_i^2$;
2. $(\sum_{i=1}^t a_i)^2 > \sum_{i=2}^t (a_i + a_1)^2$;

Proof: The first inequality is trivial. For the second one, we have

$$\begin{aligned}
& (\sum_{i=1}^t a_i)^2 - \sum_{i=2}^t (a_i + a_1)^2 \\
= & \sum_{i=1}^t a_i^2 + \sum_{1 \le i < j \le t} 2a_i a_j \\
& - \sum_{i=2}^t a_i^2 - (t-1)a_1^2 - \sum_{i=2}^t 2a_1 a_i \\
= & \sum_{2 \le i < j \le t} 2a_i a_j - (t-2)a_1^2 \\
> & \ 0
\end{aligned}$$

□

Now we are ready to prove Theorem 1.

Proof: This algorithm is recursive. There are at most $\sum_{i=1}^l \beta_i + 1$ many recursive levels. For $1 \le i \le \sum_{i=1}^l \beta_i +$

1. If $f(x)$ is a zero polynomial, then return "Yes".
2. Let k be the sparseness of $f(x)$. Write $n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_l^{\beta_l} r$, where $p_1, p_2, \cdots, p_l$ are primes less than $k+1$ and r does not have prime factors less than $k+1$.
3. If $r = 1$ and $l \le 2$, then if
$$(x^n - 1) | f(x) \prod_{p|n} (x^{n/p} - 1),$$
return "yes", else return "no".
4. Let $q = \max\{p_1, p_2, \cdots, p_l, r\}$. Write $f(\omega_n)$ as
$$g_t(\omega_n^q)\omega_n^{e_t} + \cdots + g_2(\omega_n^q)\omega_n^{e_2} + g_1(\omega_n^q)\omega_n^{e_1}$$
where $e_i \not\equiv e_j \pmod q$ for $1 \le i < j \le t$. If $q^2 | n$, or $t < q$, go to Step 6.
5. Rewrite $f(\omega_n)$ in the form:
$$\begin{aligned}
& \tilde{g}_1(\omega_n^q)\omega_n^{n/q} + \tilde{g}_2(\omega_n^q)\omega_n^{2n/q} + \cdots \\
& + \tilde{g}_{q-1}(\omega_n^q)\omega_n^{(q-1)n/q} + \tilde{g}_q(\omega_n^q);
\end{aligned}$$
Let $\tilde{g}_M(x)$ be the polynomial with minimum number of nonzero terms among all $\tilde{g}_i(x)$; Do
$$\begin{aligned}
g_1(x) &\leftarrow \tilde{g}_1(x) - \tilde{g}_M(x) \\
&\cdots \\
g_{M-1}(x) &\leftarrow \tilde{g}_{M-1}(x) - \tilde{g}_M(x) \\
g_M(x) &\leftarrow \tilde{g}_{M+1}(x) - \tilde{g}_M(x) \\
&\cdots \\
g_{t-1}(x) &\leftarrow \tilde{g}_t(x) - \tilde{g}_M(x) \\
t &\leftarrow t - 1.
\end{aligned}$$
6. If for all $1 \le i \le t$, **zerotesting**$(\ g_i(x), n/q\ )$ outputs "yes", then return "yes", else return "no".

Figure 1. Algorithm zerotesting($f(x)$, n)

1, let $[g_{i1}(x), g_{i2}(x), \cdots, g_{ih_i}(x)]$ be the list of polynomials that are inputs of **zerotesting** in the recursive level i. At the first level, there is only one polynomial $f(x)$. Namely, $h_1 = 1$ and $g_{1,1}(x) = f(x)$. We shall show that for $2 \leq i \leq \sum_{i=1}^{l} \beta_i + 1$,

$$\sum_{1 \leq j \leq h_i} sps^2(g_{ij}(x)) \leq \sum_{1 \leq j \leq h_{i-1}} sps^2(g_{(i-1)j}(x)). \quad (6)$$

W.l.o.g. consider the function call of **zerotesting**$(g_{(i-1)1}(x), n')$. Suppose that in Step 4, we write $g_{(i-1)1}(\omega_{n'})$ as

$$g_1(\omega_{n'/q})\omega_{n'}^{e_1} + g_2(\omega_{n'/q})\omega_{n'}^{e_2} + \cdots + g_\tau(\omega_{n'/q})\omega_{n'}^{e_\tau}$$

and that g_j has sparseness a_j for $1 \leq j \leq \tau$. Then $sps(g_{(i-1)1}(x)) = \sum_{j=1}^{\tau} a_i$. Again w.l.o.g., assume that $a_1 \leq a_2 \leq \cdots \leq a_\tau$. Suppose that $g_{i1}(x), g_{i2}(x), \cdots, g_{it}(x)$ are handled in Step 6 of **zerotesting**$(g_{(i-1)1}(x), n')$. The sparseness of $g_{i1}(x), g_{i2}(x), \cdots, g_{it}(x)$ are either $a_1, a_2, \cdots, a_\tau$ respectively, or are at most $a_2 + a_1, a_3 + a_1, \cdots, a_\tau + a_1$ respectively. In both cases, we have

$$\sum_{1 \leq j \leq t} sps^2(g_{ij}(x)) \leq sps^2(g_{(i-1)1}(x)).$$

Sum up for all $g_{(i-1)j}(x)$, $1 \leq j \leq h_{i-1}$, we prove (6).

Since at the first level, there is only one polynomial with sparseness k, the algorithm will never handle more than k^2 many sparse cyclotomic integers in any recursive level, and each cyclotomic integers will have sparseness no larger than k. This proves the theorem. □

4 Search for a large conjugate

First we review some facts about complex vector space. It is actually not much different from the commonly known vector space $\mathbf{R}^k$. For a complex number v, we denote its complex conjugate by $\overline{v}$. If $\mathbf{v} = (v_1, v_2, \cdots, v_k)$ and $\mathbf{u} = (u_1, u_2, \cdots, u_k)$ are two vectors in $\mathbf{C}^k$, the inner product of $\mathbf{v}$ and $\mathbf{u}$ can be defined as

$$< \mathbf{v}, \mathbf{u} >= \sum_{i=1}^{k} v_i \overline{u_i}.$$

The (2-)norm of a vector $\mathbf{v}$ is defined as $\sqrt{< \mathbf{v}, \mathbf{v} >}$ and is denoted by $|\mathbf{v}|$. Let $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_k$ be vectors in $\mathbf{C}^k$. It is well known that the Gram-Schmidt orthogonalization applies and it produces orthogonal vectors $\mathbf{v}_1^*, \mathbf{v}_2^*, \cdots, \mathbf{v}_k^*$ by the following procedure:

$$\begin{aligned} \mathbf{v}_i^* &= \mathbf{v}_i - \sum_{j=1}^{i-1} \mu_{i,j} \mathbf{v}_j^* \\ \mu_{i,j} &= \frac{< \mathbf{v}_i, \mathbf{v}_j^* >}{< \mathbf{v}_j^*, \mathbf{v}_j^* >} \end{aligned}$$

We have $|\mathbf{v}_i| \geq |\mathbf{v}_i^*|$ for all $1 \leq i \leq k$. Denote the $k \times k$ matrix $(\mathbf{v}_1^T, \mathbf{v}_2^T, \cdots, \mathbf{v}_k^T)$ by V. Then $|det(V)| = \prod_{i=1}^{k} |\mathbf{v}_i^*|$. Consider the lattice $\mathbf{v}_1\mathbf{Z} + \mathbf{v}_2\mathbf{Z} + \cdots + \mathbf{v}_k\mathbf{Z}$. The smallest norm of nonzero vectors in the lattice, denoted by $\lambda(V)$, is no shorter than the shortest vector in the Gram-Schmidt orthogonalization, i.e.

$$\lambda \geq \min_i |\mathbf{v}_i^*| \geq \frac{|det(V)|}{|\max_i \mathbf{v}_i|^{k-1}}.$$

Lemma 6 *If the norm of a vector $\mathbf{v} = (v_1, v_2, \cdots, v_k) \in \mathbf{C}^k$ is greater than λ, then there exists $1 \leq i \leq k$ such that $|v_i| \geq \lambda/\sqrt{k}$.*

We are interested in designing a deterministic algorithm to find a conjugate with large absolute value.

Theorem 2 *Let k be a positive integer. Let n be a positive integer whose prime factors are all greater than k. Let $e_1, e_2, \cdots, e_k$ be distinct nonnegative integers less than n. Let $c_1, c_2, \cdots, c_k$ be nonzero integers. Then there exists $1 \leq i \leq k$, such that*

$$|\sigma^{(i)}(c_k\omega_n^{e_k} + c_{k-1}\omega_n^{e_{k-1}} + \cdots + c_1\omega_n^{e_1})| > \frac{1}{2^{(k^2 \log n + k \log k)}}.$$

Proof: It is obvious that $\sigma^{(i)}$ is a field automorphism in $Gal(\mathbf{Q}(\omega_n)/\mathbf{Q})$ for $1 \leq i \leq k$ and the matrix $V = (\sigma^{(i)}(\omega_n^{e_j}))_{1 \leq i,j \leq k}$ is Vandermonde, hence

$$\begin{aligned} det(V) &= det((\sigma^{(i)}(\omega_n^{e_j}))_{1 \leq i,j \leq k}) \\ &= \prod_{i=1}^{k} \omega_n^{e_i} \prod_{1 \leq i < j \leq k} (\omega_n^{e_j} - \omega_n^{e_i}). \end{aligned}$$

If $e_j \not\equiv e_i \pmod{n}$, then $|\omega_n^{e_j} - \omega_n^{e_i}| \geq 1/n$. Hence we can bound the absolute value of $det(V)$ from below:

$$|det(V)| = \prod_{1 \leq i < j \leq k} |(\omega_n^{e_j} - \omega_n^{e_i})| \geq (1/n)^{k^2}.$$

Consider the lattice formed by the column vectors of V:

$$\begin{pmatrix} \sigma^{(1)}(\omega^{e_1}) \\ \sigma^{(2)}(\omega^{e_1}) \\ \vdots \\ \sigma^{(k)}(\omega^{e_1}) \end{pmatrix} \mathbf{Z} + \begin{pmatrix} \sigma^{(1)}(\omega^{e_2}) \\ \sigma^{(2)}(\omega^{e_2}) \\ \vdots \\ \sigma^{(k)}(\omega^{e_2}) \end{pmatrix} \mathbf{Z} + \cdots + \begin{pmatrix} \sigma^{(1)}(\omega^{e_k}) \\ \sigma^{(2)}(\omega^{e_k}) \\ \vdots \\ \sigma^{(k)}(\omega^{e_k}) \end{pmatrix} \mathbf{Z}.$$

The shortest vector has a norm greater than $det(V)/(\sqrt{k})^{k-1} \geq 1/(n^{k^2}k^{(k-1)/2})$. By Lemma 6, we have that there must exist $1 \leq i \leq k$ such that

$$|\sigma^{(i)}(\sum_{i=1}^{k} c_i\omega_n^{e_i})| \geq \frac{1}{2^{(k^2 \log n + k \log k)}}$$

□

A nice feature of the theorem is that the lower bound is independent of the height of the polynomial $\sum_{i=1}^{k} c_i x^{e_i}$.

5 Conclusion and Future Research Direction

In this paper, we study the zero testing problem of sparse cyclotomic integers and some related problems. We present the first deterministic polynomial time algorithm for the zero testing problem of sparse cyclotomic integers. We also show that a large conjugate of a cyclotomic integer $f(\omega_n)$ in $\mathbf{Q}(\omega_n)$ can be found in polynomial time if n is free of prime factor less than $sps(f(x)) + 1$. We believe that our method uses the sparseness in an essential way, and hope that it may help to solve the sign determination problem of real sparse cyclotomic integers.

References

[1] Eric Allender, Peter Buergisser, Johan Kjeldgaard-Pedersen, and Peter Bro Miltersen. On the complexity of numerical analysis. In *IEEE Conference on Computational Complexity*, 2006.

[2] E. Bach, J. Driscoll, and J. Shallit. Factor refinement. *Journal of Algorithms*, 15:199–222, 1993.

[3] Johannes Blomer. A probabilistic zero-test for expressions involving roots of rational numbers. In *Proc. ESA*, volume 1461 of *LNCS*, pages 151–162, 1998.

[4] Zhi-Zhong Chen and Ming-Yang Kao. Reducing randomness via irrational numbers. *SIAM J. Comput.*, 29(4):1247–1256, 2000.

[5] Erik D. Demaine, Joseph S. B. Mitchell, and Joseph O'Rourke. The open problems project: Problem 33. http://maven.smith.edu/˜orourke/TOPP/.

[6] Michael Filaseta and Andrzej Schinzel. On testing the divisibility of lacunary polynomials by cyclotomic polynomials. *Math. Comp.*, 73(246):957–965, 2004.

[7] M. Garey, R.L. Graham, and D.S. Johnson. Some NP-complete geometric problems. In *Proc. ACM Symp. Theory Comp.*, pages 10–21, 1976.

[8] David A. Plaisted. New NP-hard and NP-complete polynomial and integer divisibility problems. *Theoretical Computer Science*, 31:125–138, 1984.

[9] Terence Tao. An uncertainty principle for cyclic groups of prime order. *Math. Res. Lett.*, 12(1):121–127, 2005.