THE SIEGEL NORM, THE LENGTH FUNCTION AND CHARACTER VALUES OF FINITE GROUPS

AMITA MALIK, FLORIN STAN, AND ALEXANDRU ZAHARESCU

Abstract. In this paper we present some new results on the connection between the Siegel norm, the length function and irreducible character values of finite groups. In addition, we provide algorithms to compute the length of a cyclotomic integer and the set of cyclotomic integers with Siegel norm bounded by a given positive real number.

1. Introduction

Let $\mathbb{Q}$ be the field of rational numbers, let $\mathbb{C}$ be the field of complex numbers and for any number field K, let O_K denote its ring of integers. For any positive integer n we let ζ_n denote a primitive n^{th} root of unity. Cassels [2] introduced the following map, and used it in certain problems related to roots of unity. For any algebraic number α, let

$$A(\alpha) = \frac{1}{[K:\mathbb{Q}]} \sum_{\sigma} |\sigma(\alpha)|^2 ,$$

where σ runs over all the embeddings of K into $\mathbb{C}$. Note that $A(\alpha)$ depends only on α and not on the field K containing α. This function has many useful properties. For example, its square root is a vector space norm on the field of algebraic numbers (called the Siegel norm in [9] due to its connection, in the particular case of a cyclotomic field, to Siegel's trace problem [7]).

For any cyclotomic integer α, its length $l(\alpha)$ is defined to be the smallest number l such that α can be written as a sum of l roots of unity. This function is well defined, since any cyclotomic integer is a sum of roots of unity. Also if χ is an irreducible character of a finite group G, and $g \in G$, then $\chi(g)$ is a sum of $|G|^{\text{th}}$ roots of unity. Hence $l(\chi(g))$ is well defined. Burnside [1] showed that a nonlinear irreducible character of a finite group takes the value zero on at least one element of the group. An unpublished theorem of Thompson [3, Exercise 3.15, page 46] states that any irreducible character of a finite group attains the value zero or a root of unity at more than one third of the group elements. Cassels [2] proved that an algebraic integer α in an abelian field with $A(\alpha) < 2$ is a sum of at most two roots of unity. Two of the authors [8] showed that any irreducible character of a finite group is a sum of at most three roots of unity at more than three fifths of the elements of the group and is a sum of at most four roots of unity at more than two thirds of the elements of the group.

In the present paper, we complement the work from [8] with some further results concerning the connection between the Siegel norm, the length function and irreducible

2010 *Mathematics Subject Classification.* Primary 11R18; Secondary 11R04.

Key words and phrases. Sums of roots of unity, characters of finite groups.

character values of finite groups. A natural question that arises is whether one can obtain nontrivial results for character values that can be written as sums of at most m roots of unity for values of m that are larger than four. In other words, if χ is a nonlinear character of an irreducible representation of a finite group G, and m is a positive integer, we are interested in obtaining lower bounds for the number of elements in the set

$$\mathcal{B}_{\chi,m} := \{g \in G : l(\chi(g)) \leq m\}. \tag{1.1}$$

In connection with this, we prove the following result.

Theorem 1.1. *Let G be a finite group and q be the smallest prime dividing the order of G. Let m be a nonnegative integer and χ be a nonlinear irreducible character of G. Then*

$$|\mathcal{B}_{\chi,m}| \geq \frac{M-1}{M}|G| + \frac{(\chi(1))^2}{M} - 1, \tag{1.2}$$

where $\mathcal{B}_{\chi,m}$ is given by (1.1) *and* $M = \frac{1}{2}\left(\frac{q}{q-1}\frac{\phi(|G|)}{|G|}\frac{m+1}{2^{\omega(|G|)-1}} + 1\right)$.

Here ϕ is the Euler function and ω is the number of distinct prime factors function.

We also consider a dual problem to the one above, where instead of fixing a character χ and counting those $g \in G$ for which $l(\chi(g)) \leq m$, we now fix an element $g \in G$, and count those irreducible characters χ of G for which $l(\chi(g)) \leq m$.

For any element g in a finite group G and any nonnegative integer m, let $\mathcal{B}_{g,m}$ denote the set

$$\mathcal{B}_{g,m} := \{\chi : \chi \text{ is an irreducible character of } G \text{ and } l(\chi(g)) \leq m\}. \tag{1.3}$$

We prove the following result.

Theorem 1.2. *Let G be a finite group and let q be the smallest prime factor of $|G|$. Let $g \in G$ and let m be any nonnegative integer. Then*

$$|\mathcal{B}_{g,m}| \geq k(G) - \frac{|G|}{M|\mathcal{C}_g|}, \tag{1.4}$$

where $M = \frac{1}{2}\left(\frac{q}{q-1}\frac{\phi(|G|)}{|G|}\frac{m+1}{2^{\omega(|G|)-1}} + 1\right)$, *$\mathcal{B}_{g,m}$ is given by* (1.3), *$\mathcal{C}_g$ denotes the conjugacy class of g and $k(G)$ is the number of conjugacy classes in G.*

As an example, in the case of p-groups, $M = \frac{m+2}{2}$ in Theorems 1.1 and 1.2. Therefore by (1.2),

$$|\mathcal{B}_{\chi,m}| \geq \frac{m}{m+2}|G| + \frac{8}{m+2} - 1,$$

uniformly for all nonnegative integers m, all primes p, all p-groups G and all nonlinear irreducible characters χ of G.

A natural question that arises would be to assess how accurate the bounds from Theorems 1.1 and 1.2 are for various groups G. In other words, one may ask how large or how small the ratios between the bounds for $|\mathcal{B}_{\chi,m}|$ provided by Theorem 1.1 and the actual values of $|\mathcal{B}_{\chi,m}|$ are, and similarly for Theorem 1.2. The table below shows, for some values of m and some groups G, the actual values of $|\mathcal{B}_{\chi,m}|$ and respectively $|\mathcal{B}_{g,m}|$, and the corresponding bounds provided by Theorems 1.1 and 1.2.

Group	D_8, Q_8	D_8, Q_8	D_{10}	D_{10}	A_4
Value of m	0	1	0	1	3
Bound for $|\mathcal{B}_{\chi,m}|$ from (1.2)	3	5	1	3	9
Actual value of $|\mathcal{B}_{\chi,m}|$	6	6	5	5	10
Accuracy	50%	83%	20%	60%	90%
Bound for $|\mathcal{B}_{g,m}|$ from (1.4)	1	3	2	2	2
Actual value of $|\mathcal{B}_{g,m}|$	1	5	2	4	4
Accuracy	100%	60%	100%	50%	50%

The reader may wonder whether a result dual to that of Burnside would hold in the following form: for any non-identity element in a finite (non-abelian) group, there is a nonlinear character which takes the value zero on this element (hence on all the elements in its conjugacy class). It turns out that this is not true in general (see for instance the character tables of the symmetric group S_3 and the quaternion group Q_8). However, this is the case for elements with nontrivial conjugacy class in a certain infinite family of groups, as follows from Theorem 1.2. To see this, let us take G to be an arbitrary group of order p^l, $l \geq 3$, with the property that $|Z(G)| = |[G,G]| = p$. Then by [6, Proposition 7.1],

$$k(G) = p^{l-1} + p - 1.$$

Since $|\mathcal{C}_g|$ divides the order of the group, $|\mathcal{C}_g|$ is a power of p. Also, for a p-group, $M = \frac{m+2}{2}$ and therefore $M = 1$ for $m = 0$. For any $g \in G \setminus Z(G)$ one has $|\mathcal{C}_g| > 1$, and from (1.4) it follows that

$$|\mathcal{B}_{g,0}| \geq p^{l-1} + p - 1 - \frac{p^l}{|\mathcal{C}_g|} = p^{l-1}\big(1 - \frac{p}{|\mathcal{C}_g|}\big) + p - 1 > 0.$$

Note that for a non-abelian group of order p^3, $|Z(G)| = |[G,G]| = p$, so the above result is true for all such groups. Also, the bound in Theorem 1.2 is attained in some cases. For instance, for the dihedral group D_{10}, one may choose an element $g \in D_{10}$ with $|\mathcal{C}_g| = 5$. Then by (1.4), $|\mathcal{B}_{g,0}| \geq 2$ and the actual value of $|\mathcal{B}_{g,0}|$ is 2.

In Section 3, we provide an algorithm to compute the set of all cyclotomic integers in a fixed cyclotomic field which have bounded Siegel norm. In other words, given a cyclotomic field and a positive real number m, the algorithm computes the set consisting of algebraic integers α with $A(\alpha) < m$. In Section 4, an algorithm to compute the length of a cyclotomic integer is given. And finally in Section 5, we provide an example of an algebraic integer α such that $A(\alpha) < \frac{k+2}{2}$, but $l(\alpha) > k, k \in \mathbb{N}$ with smallest such k possible.

2. Proof of Theorem 1.1 and Theorem 1.2

We start by recalling some results from [2] and [8].

Lemma 2.1 ([2], Equations (3.1) and (3.4))**.** *Let N be a positive integer and $N = pN_0$ and $p \nmid N_0$. For $\alpha \in \mathbb{Q}(\zeta_N)$,*

$$\alpha = \sum_{j=0}^{p-1} \alpha_j \zeta^j,$$

where $\alpha_j \in \mathbb{Q}(\zeta_{N_0})$ and ζ is a primitive p-th root of unity. If α is an algebraic integer, then α_j can be chosen to be algebraic integers. Moreover,

$$(p-1)A(\alpha) = \sum_{0 \le j < k \le p-1} A(\alpha_j - \alpha_k).$$

Lemma 2.2 ([2], Equations (3.14) and (3.16))**.** *Let N be a positive integer and p be a prime such that $p^r || N$ (i.e. $p^r \mid N$ and $p^{r+1} \nmid N$), for some positive integer $r \ge 2$. Let $N_0 = N/p$ and ζ be a primitive p^r-th primitive root of unity. Then any $\alpha \in \mathbb{Q}(\zeta_N)$ can be written uniquely as*

$$\alpha = \sum_{j=0}^{p-1} \alpha_j \zeta^j,$$

where $\alpha_j \in \mathbb{Q}(\zeta_{N_0})$. And if α is an algebraic integer, then α_j are also algebraic integers. Moreover,

$$A(\alpha) = \sum_{j=0}^{p-1} A(\alpha_j).$$

Lemma 2.3 ([8], Theorem 1)**.** *Let p be a prime, $a \in \mathbb{N}$ and let $\alpha \in O_{\mathbb{Q}(\zeta_{p^a})}$ be a nonzero algebraic integer, where ζ_{p^a} is a primitive root of unity of order p^a. Then*

$$A(\alpha) \ge \frac{l(\alpha)+1}{2}.$$

The next result offers a generalization of Lemma 2.3 above.

Lemma 2.4. *Let $n \ge 1$ be an integer and let q be the smallest prime factor of n. Let $\alpha \in O_{\mathbb{Q}(\zeta_n)}$ be a nonzero algebraic integer. Then*

$$A(\alpha) \ge \frac{1}{2}\left(\frac{q}{q-1}\frac{\phi(n)}{n}\frac{l(\alpha)}{2^{\omega(n)-1}} + 1\right).$$

Proof. To prove this, we use induction on $\omega(n)$, the number of distinct prime factors of n. For $\omega(n) = 1$, the desired inequality holds by Lemma 2.3. Let us assume the result for $\omega(n) = k \ge 1$ and show that the same is true for N with $\omega(N) = k+1$. Let p be the second smallest prime factor of N and let r be its exponent in N. Also let q be the smallest prime dividing N. Consider $n = N/p^r$, thus $\omega(N) = \omega(n) + 1$, and $p \ne q$.

First we consider the case when $N = pn$, in other words when $r = 1$. Let $\alpha \in \mathbb{Q}(\zeta_N)$ be a nonzero algebraic integer. Using Lemma 2.1, we have

$$\alpha = \sum_{j=0}^{p-1} \alpha_j \zeta^j,$$

where $\alpha_j \in \mathbb{Q}(\zeta_n)$ and ζ is a primitive p-th root of unity. Also

$$(p-1)A(\alpha) = \sum_{0 \leq j < k \leq p-1} A(\alpha_j - \alpha_k).$$

For fixed $k, 0 \leq k \leq p-1$, since $\sum_{j=0}^{p-1} \alpha_k \zeta^j = 0$, we can write

$$\alpha = \sum_{j=0}^{p-1} \alpha_j \zeta^j = \sum_{j=0}^{p-1} (\alpha_j - \alpha_k)\zeta^j.$$

Now for any $\beta, \gamma \in O_{\mathbb{Q}^{ab}}$ and ρ a root of unity, we know that $l(\beta+\gamma) \leq l(\beta) + l(\gamma)$ and $l(\rho\beta) = l(\beta)$. Using this, we obtain

$$l(\alpha) \leq \sum_{j=0}^{p-1} l(\alpha_j - \alpha_k). \tag{2.1}$$

Also by the induction hypothesis, for the algebraic integers $\alpha_j \neq \alpha_k \in \mathbb{Q}(\zeta_n)$, we have the inequality

$$A(\alpha_j - \alpha_k) \geq \frac{1}{2}\left(\frac{1}{2^{\omega(n)-1}} \frac{\phi(n)}{n} \frac{q}{q-1} l(\alpha_j - \alpha_k) + 1\right),$$

which yields

$$l(\alpha_j - \alpha_k) \leq \frac{n 2^{\omega(n)-1}}{\phi(n)} \frac{q-1}{q} \left(2A(\alpha_j - \alpha_k) - 1\right) \text{ for } \alpha_j \neq \alpha_k.$$

Using this in (2.1),

$$l(\alpha) \leq \frac{n 2^{\omega(n)-1}}{\phi(n)} \frac{q-1}{q} \sum_{\substack{0 \leq j \leq p-1 \\ \alpha_j \neq \alpha_k}} (2A(\alpha_j - \alpha_k) - 1).$$

Now sum over $k : 0 \leq k \leq p-1$ to obtain

$$\begin{aligned} pl(\alpha) &\leq \frac{q-1}{q} \frac{n 2^{\omega(n)-1}}{\phi(n)} \sum_{k=0}^{p-1} \sum_{\substack{0 \leq j \leq p-1 \\ \alpha_j \neq \alpha_k}} (2A(\alpha_j - \alpha_k) - 1) \\ &= \frac{q-1}{q} \frac{n 2^{\omega(n)-1}}{\phi(n)} \left(\sum_{j,k=0}^{p-1} \Big(2A(\alpha_j - \alpha_k) - \# \{ j \in \{0, 1, \ldots, p-1\} : \alpha_j \neq \alpha_k \} \Big) \right) \\ &= \frac{q-1}{q} \frac{n 2^{\omega(n)-1}}{\phi(n)} \left(4(p-1)A(\alpha) - \sum_{j,k=0}^{p-1} \# \{ j \in \{0, 1, \ldots, p-1\} : \alpha_j \neq \alpha_k \} \right) \\ &\leq \frac{q-1}{q} \frac{n 2^{\omega(n)-1}}{\phi(n)} \big(4(p-1)A(\alpha) - 2p + 2 \big) \\ &= \frac{q-1}{q} \frac{(p-1) n 2^{\omega(n)}}{\phi(n)} \left(2A(\alpha) - 1 \right). \end{aligned}$$

Here we used Lemma 2.1 and the fact that since α is nonzero, at least two of the coefficients α_j are distinct. Hence

$$l(\alpha) \leq \frac{q-1}{q}\frac{p-1}{p}\frac{n2^{\omega(n)}}{\phi(n)}(2A(\alpha)-1),$$

which implies

$$\begin{aligned} A(\alpha) &\geq \frac{1}{2}\left(\frac{q}{q-1}\frac{p}{p-1}\frac{\phi(n)}{n2^{\omega(n)}}l(\alpha)+1\right) \geq \frac{1}{2}\left(\frac{q}{q-1}\frac{\phi(p)}{p}\frac{\phi(n)}{n2^{\omega(n)}}l(\alpha)+1\right) \\ &= \frac{1}{2}\left(\frac{q}{q-1}\frac{\phi(N)}{N}\frac{l(\alpha)}{2^{\omega(N)-1}}+1\right). \end{aligned}$$

Thus if $r = 1$, then we are done. Now let $r = 2$ and let $\alpha \in \mathbb{Q}(\zeta_N)$ be a nonzero algebraic integer. Then by Lemma 2.2,

$$\alpha = \sum_{j=0}^{p-1} \alpha_j \zeta^j \quad \text{and} \quad A(\alpha) = \sum_{j=0}^{p-1} A(\alpha_j),$$

where ζ is a root of unity of order p^r and α_j is an algebraic integer in $\mathbb{Q}(\zeta_{N/p})$. By the case considered above, we know for each j for which $\alpha_j \neq 0$,

$$A(\alpha_j) \geq \frac{1}{2}\left(\frac{q}{q-1}\frac{\phi(\frac{N}{p})}{\frac{N}{p}}\frac{l(\alpha_j)}{2^{\omega(\frac{N}{p})-1}}+1\right) = \frac{1}{2}\left(\frac{q}{q-1}\frac{\phi(N)}{N}\frac{l(\alpha_j)}{2^{\omega(N)-1}}+1\right).$$

Therefore

$$\begin{aligned} A(\alpha) &\geq \sum_{\substack{j=0 \\ \alpha_j \neq 0}}^{p-1} \frac{1}{2}\left(\frac{q}{q-1}\frac{\phi(N)}{N}\frac{l(\alpha_j)}{2^{\omega(N)-1}}+1\right) \\ &\geq \frac{1}{2}\Big(\frac{q}{q-1}\frac{\phi(N)}{N}\frac{1}{2^{\omega(N)-1}}\sum_{\substack{j=0 \\ \alpha_j \neq 0}}^{p-1} l(\alpha_j)+1\Big) \\ &\geq \frac{1}{2}\left(\frac{q}{q-1}\frac{\phi(N)}{N}\frac{l(\alpha)}{2^{\omega(N)-1}}+1\right), \end{aligned}$$

since $l(\beta) + l(\gamma) \geq l(\beta + \gamma)$ and $\alpha_j \neq 0$ for at least one j. This gives us the desired inequality for $r = 2$. Continuing this way, we conclude the same is true for any positive integer r. This completes the proof of Lemma 2.4. □

We now provide the proofs of Theorem 1.1 and Theorem 1.2.

Proof. of Theorem 1.1.
Let G be a finite group and q be the smallest prime dividing the order of G. Let m be a positive integer and χ be a non-linear irreducible character of G. We know by the orthogonality of characters that

$$\sum_{g \in G} |\chi(g)|^2 = |G|. \tag{2.2}$$

Let ζ be a root of unity of order $|G|$ and let $\mathcal{G}$ be the Galois group of the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. By averaging both sides of (2.2) over the Galois conjugates, we have

$$\frac{1}{|\mathcal{G}|}\sum_{\sigma\in\mathcal{G}}\left(\sum_{g\in G}|\chi(g)|^2\right)=|G|.$$

Interchanging the order of summation, we obtain

$$\sum_{g\in G}A(\chi(g))=|G|.$$

Since $A(.)\geq 0$ and $A(\chi(1))=(\chi(1))^2$, we have the inequality

$$(\chi(1))^2+\sum_{1\neq g\in G\setminus\mathcal{B}_{\chi,m}}A(\chi(g))\leq|G|. \tag{2.3}$$

If we let M denote the quantity

$$M=\frac{1}{2}\left(\frac{q}{q-1}\frac{\phi(|G|)}{|G|}\frac{m+1}{2^{\omega(|G|)-1}}+1\right),$$

then by Lemma 2.4, $A(\chi(g))\geq M$ for all $g\notin\mathcal{B}_{\chi,m}$. Combining this with (2.3), we obtain

$$M\left(|G|-|\mathcal{B}_{\chi,m}|-1\right)+(\chi(1))^2\leq|G|,$$

and that yields the desired inequality

$$|\mathcal{B}_{\chi,m}|\geq\frac{M-1}{M}|G|+\frac{(\chi(1))^2}{M}-1.$$

□

We now move on to prove Theorem 1.2.

Proof. of Theorem 1.2.
Let G be a finite group and denote by $k(G)$ the number of conjugacy classes of G, and by $\mathrm{Irr}(G)$ the set of irreducible characters of G. For $\sigma\in G$, we denote by $C(\sigma)=C_G(\sigma)$ the centralizer of σ in G. Let q be the smallest prime dividing the order of G and let m be a positive integer. Using the orthogonality of columns of the character table of G, we have, for $g\in G$,

$$\sum_{\chi}|\chi(g)|^2=|G|/|\mathcal{C}_g|,$$

where the sum is taken over all irreducible characters χ of G and $\mathcal{C}_g$ denotes the conjugacy class of g. Averaging both sides by the Galois conjugates and rewriting, as in the proof of Theorem 1.1, we obtain

$$\sum_{\chi}A(\chi(g))=|G|/|\mathcal{C}_g|.$$

Now using the positivity of $A(.)$, we have

$$\sum_{\chi\notin\mathcal{B}_{g,m}}A(\chi(g))\leq|G|/|\mathcal{C}_g|. \tag{2.4}$$

Let $M = \frac{1}{2}\left(\frac{q}{q-1}\frac{\phi(|G|)}{|G|}\frac{m+1}{2^{\omega(|G|)-1}}+1\right)$. Then by Lemma 2.4,

$$A(\chi(g)) \geq M \text{ for } \chi \notin \mathcal{B}_{g,m}.$$

This along with (2.4) gives

$$\frac{|G|}{|\mathcal{C}_g|} \geq M\left(|\operatorname{Irr}(G)| - |\mathcal{B}_{g,m}|\right).$$

i.e.

$$\mathcal{B}_{g,m} \geq |\operatorname{Irr}(G)| - \frac{|G|}{M|\mathcal{C}_g|}.$$

Since the number of irreducible characters equals the number of conjugacy classes for a finite group G, for a given $m \in \mathbb{N}$ and $g \in G$, there are at least

$$k(G) - \frac{|G|}{M|\mathcal{C}_g|} = \frac{1}{|G|}\sum_{\sigma\in G}|C(\sigma)| - \frac{|C(g)|}{M}$$

irreducible characters χ for which $\chi(g)$ can be written as a sum of at most m roots of unity. □

3. An algorithm for finding the cyclotomic integers with bounded Siegel norm

In this section we describe an algorithm which determines all cyclotomic integers α in a fixed cyclotomic field which have $A(\alpha) \leq m$, for a given $m > 0$.

We will need the following consequence of Lemma 2.1.

Corollary 1 ([2], relation (3.9))**.** *Let X be the number of nonzero coefficients in the representation of α in Lemma 2.1. Write*

$$\alpha = \sum_{j=1}^{X}\gamma_j\zeta^{r_j},$$

where $\gamma_j \in \mathbb{Q}(\zeta_{\frac{N}{p}})$, and $0 \leq r_j < p$ are distinct. Then

$$(p-1)A(\alpha) = (p-X)\sum_{j=1}^{X}A(\gamma_j) + \sum_{1\leq i<j\leq X}A(\gamma_i-\gamma_j).$$

Let $N \geq 1$ be an integer, let m be a positive real number, and let $\alpha \in \mathbb{Q}(\zeta_N)$ be a cyclotomic integer with $A(\alpha) \leq m$. Let p be the largest prime divisor of N. We distinguish two cases:

Case 1. $p||N$. In this case using Lemma 2.1, we can write

$$\alpha = \sum_{j=0}^{p-1}\alpha_j\zeta^j, \text{ where } \alpha_j \in \mathbb{Q}(\zeta_{\frac{N}{p}}) \text{ and } \zeta = \zeta_p. \tag{3.1}$$

Denote by X the number of nonzero coefficients in the representation (3.1) of α. Write

$$\alpha = \sum_{j=1}^{X} \gamma_j \zeta^{r_j} \text{ where } \gamma_j \in \mathbb{Q}(\zeta_{\frac{N}{p}}), \text{ and } 0 \leq r_j < p.$$

Now Corollary 1 implies that

$$(p-1)m \geq (p-1)A(\alpha) = (p-X)\sum_{j=1}^{X} A(\gamma_j) + \sum_{1 \leq i < j \leq X} A(\gamma_i - \gamma_j).$$

Using the positivity of A, we derive

$$(p-1)m \geq (p-X)\sum_{j=1}^{X} A(\gamma_j). \tag{3.2}$$

Note that we can always assume that $X \leq p-1$ (if all coefficients α_j in the representation (3.1) of α are nonzero, subtracting $0 = \alpha_0(1+\zeta+\zeta^2+\ldots+\zeta^{p-1})$ from both sides, we obtain a representation of α in which $\alpha_0 = 0$, so $X \leq p-1$). Thus, for any $j \in \{1, 2, \ldots, X\}$,

$$A(\gamma_j) \leq \sum_{i=1}^{X} A(\gamma_j) \leq \frac{(p-1)m}{p-X} \leq (p-1)m. \tag{3.3}$$

Case 2. $p^2 \mid N$. In this case using Lemma 2.2 we can write

$$\alpha = \sum_{j=0}^{p-1} \alpha_j \zeta^j \quad \text{with } \alpha_j \in \mathbb{Q}(\zeta_{\frac{N}{p}}) \text{ and } \zeta = \zeta_{p^r}, \text{ where } p^r || N. \tag{3.4}$$

Since $m \geq A(\alpha) = \sum_{j=0}^{p-1} A(\alpha_j)$, we obtain

$$A(\alpha_j) \leq m, \quad \text{for } 0 \leq j \leq p-1. \tag{3.5}$$

Now that we have bounds for $A(\alpha_j)$, (α_j are the coefficients in the representations (3.1) or (3.4) of α), we can repeat the above for these coefficients, i.e. we consider the largest prime divisor q of N/p and we write the representations (3.1) or (3.4) for the α_j.

Since α is an algebraic integer and at each step we can take α_j to be algebraic integers, at the end of this process (we will be in Case 1) the coefficients appearing in the representation (3.1) are in the ground field $\mathbb{Q}$, so they are rational integers. But $A(n) = n^2$, for $n \in \mathbb{Z}$, so from (3.3) we can find the possible values of these coefficients, and then, working backwards, we can find all the possible values of the coefficients of α in the initial representation (3.1) or (3.4).

4. Computing the length of a cyclotomic integer

In this section we present an algorithm which determines the length of a cyclotomic integer.

We will use the following results. The first one of them is a more general version of Lemma 2.2.

Lemma 4.1 ([5], Lemma 2)**.** *Suppose $N = p^n N_2$, where p is a prime, $p \nmid N_2$ and $n > 1$. Let L be a positive integer with $L < n$ and put $N = p^L N_1$. Let ζ be a primitive p^n-th root of unity. Then every $\beta \in \mathbb{Q}(\zeta_N)$ is uniquely of the shape*

$$\beta = \sum_{j=0}^{p^L-1} \alpha_j \zeta^j,$$

with the α_j in $\mathbb{Q}(\zeta_{N_1})$. The α_j are integers if β is.

Lemma 4.2 ([4], Lemma 9)**.** *Let $p_1, p_2, \ldots, p_n$ be distinct primes. Then $A(\alpha) \geq \frac{l(\alpha)}{2^n}$, for any algebraic integer $\alpha \in \mathbb{Q}(\zeta_{p_1p_2\ldots p_n})$.*

Lemma 4.3 ([5], Theorem 1 (i))**.** *Let β be a cyclotomic integer and suppose $\beta = \sum_{j=1}^{n} \rho_j$ is a representation of β as a sum of n roots of unity. Let $\mathbb{Q}(\zeta_N)$ be the smallest cyclotomic field containing β and let $\mathbb{Q}(\zeta_{N^*})$ be the smallest cyclotomic field containing $\rho_1, \rho_2, \ldots, \rho_n$. If $n = l(\beta)$, then $N = N^*$.*

We are now set to describe the algorithm to compute $l(\alpha)$.

Let $N \geq 1$ be an integer and let $\alpha \in \mathbb{Q}(\zeta_N)$ be a cyclotomic integer. Let

$$N = p_1 p_2 \ldots p_n {q_1}^{r_1} {q_2}^{r_2} \ldots {q_m}^{r_m},$$

with $p_i \neq q_j$ for any i, j, and $r_j \geq 2$, for any $1 \leq j \leq m$ be the prime factorization of N.

Step 1. Obtaining upper bounds for $l(\alpha)$.

Applying successively Lemmas 2.2 and 5.1, we obtain

$$\alpha = \sum_{j_1=0}^{{q_1}^{r_1-1}-1} \alpha_{j_1} \zeta_{{q_1}^{r_1}}^{j_1}, \quad \text{with } \alpha_{j_1} \in \mathbb{Q}(\zeta_{p_1p_2\ldots p_n q_1 {q_2}^{r_2} \ldots {q_m}^{r_m}}) \text{ and } l(\alpha) = \sum_{j_1} l(\alpha_{j_1}).$$

$$\alpha_{j_1} = \sum_{j_2=0}^{{q_2}^{r_2-1}-1} \alpha_{j_1,j_2} \zeta_{{q_2}^{r_2}}^{j_2}, \quad \text{with } \alpha_{j_1,j_2} \in \mathbb{Q}(\zeta_{p_1p_2\ldots p_n q_1 q_2 {q_3}^{r_3} \ldots {q_m}^{r_m}}),\ l(\alpha_{j_1}) = \sum_{j_2} l(\alpha_{j_1,j_2}).$$

Continuing in this fashion, one obtains

$$\alpha_{j_1,j_2,\ldots,j_{m-1}} = \sum_{j_m=0}^{{q_m}^{r_m-1}-1} \alpha_{j_1,j_2,\ldots,j_m} \zeta_{{q_m}^{r_m}}^{j_m}, \quad \text{with } \alpha_{j_1,j_2,\ldots,j_m} \in \mathbb{Q}(\zeta_{p_1p_2\ldots p_n q_1 q_2 \ldots q_m}) \text{ and}$$

$$l(\alpha_{j_1,j_2,\ldots,j_{m-1}}) = \sum_{j_m} l(\alpha_{j_1,j_2,\ldots,j_m}).$$

Therefore

$$l(\alpha) = \sum_{j_1,j_2,\ldots,j_m} l(\alpha_{j_1,j_2,\ldots,j_m}).$$

To simplify notation, let $p_{n+1} := q_1$, $p_{n+2} := q_2$,...,$p_{n+m} := q_m$, and let $s := n+m$. Using Lemma 4.2 we derive

$$l(\alpha) = \sum_{j_1,j_2,\ldots,j_m} l(\alpha_{j_1,j_2,\ldots,j_m}) \leq 2^s \sum_{j_1,j_2,\ldots,j_m} A(\alpha_{j_1,j_2,\ldots,j_m}).$$

Let $M := \lfloor 2^s \sum_{j_1,j_2,\ldots,j_m} A(\alpha_{j_1,j_2,\ldots,j_m}) \rfloor$. Hence $l(\alpha) \leq M$.

Step 2. Expressing α as a sum of l roots of unity.

Denote $\zeta = \zeta_N$ and write $\alpha \in \mathbb{Z}[\zeta]$ as $\alpha = a_0 + a_1\zeta + \ldots + a_{N-1}\zeta^{N-1}$, where $a_j \in \mathbb{Z}$.

From [5] Theorem 1(i), we know that if α can be written as $\alpha = \eta_1 + \eta_2 + \ldots + \eta_l$, where $l = l(\alpha)$, and η_j are roots of unity, then α can be written as

$$\alpha = c_1\zeta^{d_1} + c_2\zeta^{d_2} + \ldots + c_k\zeta^{d_k}, \tag{4.1}$$

with $c_j \in \mathbb{Z}$, $0 \leq d_j \leq N-1$ and $\sum_{i=1}^{k} |c_i| = l$.

For $b = (b_0, b_1, \ldots, b_{N-1}) \in \mathbb{Z}^N$, let $L(b) = \sum_{j=0}^{N-1} |b_j|$ and for any $n \geq 0$, denote

$$A_n := \{b_0 + b_1\zeta + \ldots + b_{N-1}\zeta^{N-1} \in \mathbb{Z}[\zeta] : L(b) = n\}.$$

From (4.1) we obtain that $\alpha \in A_l$. Hence $\alpha \in \bigcup_{n=0}^{M} A_n$.

For $0 \leq n \leq M$ we check whether $\alpha \in A_n$ (by writing both α and the general element of A_n in the integral basis $1, \zeta, \zeta^2, \ldots, \zeta^{\phi(N)-1}$. The algorithm stops as soon as we find coefficients $b_0, b_1, \ldots, b_{N-1} \in \mathbb{Z}$ such that $\alpha = b_0 + b_1\zeta + \ldots + b_{N-1}\zeta^{N-1} \in A_l$.

5. A counterexample

As mentioned in [8] (page 222), the implication

$$A(\alpha) < \frac{k+2}{2} \Rightarrow l(\alpha) \leq k \tag{5.1}$$

does not hold in general. Also from Theorem 2, [8], combined with the results of Siegel and Cassels [2], one knows that a counterexample would require $k \geq 5$. And, from Theorem 1 of [8], we know that we should look for a counterexample in $\mathbb{Q}(\zeta_n)$, where n is divisible by at least two primes. In this section we will show that counterexamples to

(5.1) can be found as soon as n is divisible by at least two odd primes. More precisely, we'll exhibit an infinite set T of cyclotomic integers such that any $\beta \in T$ satisfies

$$A(\beta) < \frac{1 + l(\beta)}{2} \tag{5.2}$$

Then take $k := l(\beta) - 1$, and $\alpha := \beta$ to obtain the desired counterexample. Moreover, one of the elements of T violates (5.1) for $k = 5$ (as mentioned above, this is the least value of k for which a counterexample to (5.1) can exist).

We will use the following result.

Lemma 5.1 ([5], Theorem 2)**.** *Let $N \geq 1$ be an integer, let $\beta \in \mathbb{Q}(\zeta_N)$ be a cyclotomic integer, and let p be a prime divisor of N. Let*

$$\beta = \sum_j \alpha_j \zeta^j$$

be a representation for β as in Lemma 2.1 if $p||N$, or as in Lemma 2.2 if $p^2|N$. In the former case, suppose in addition that at most $\frac{1}{2}(p-1)$ of the α_j are non-zero. Then

$$l(\beta) = \sum_j l(\alpha_j).$$

For any prime $p > 2$, denote $C_p := \sum_{i=1}^{\frac{p-1}{2}} \zeta_p^i$, and for any prime $q > p$, let

$$\beta_{p,q} = C_p C_q = \sum_{i=1}^{\frac{q-1}{2}} C_p \zeta_q^i.$$

Using Corollary 1 (with $X = \frac{q-1}{2}$), we obtain

$$(q-1)A(\beta_{p,q}) = (q - \frac{q-1}{2}) \sum_{j=1}^{\frac{q-1}{2}} A(C_p) = \frac{q+1}{2} \cdot \frac{q-1}{2} A(C_p).$$

Hence

$$A(\beta_{p,q}) = \frac{q+1}{4} A(C_p). \tag{5.3}$$

Similarly we obtain

$$A(C_p) = \frac{p+1}{4} A(1) = \frac{p+1}{4}. \tag{5.4}$$

Combining relations (5.3) and (5.4) we derive

$$A(\beta_{p,q}) = \frac{(p+1)(q+1)}{16}. \tag{5.5}$$

Applying Lemma 5.1 twice, we obtain

$$l(\beta_{p,q}) = l(C_p C_q) = \frac{q-1}{2} l(C_p) = \frac{q-1}{2} \cdot \frac{p-1}{2} = \frac{(p-1)(q-1)}{4}. \tag{5.6}$$

From (5.5) and (5.6) we see that the inequality (5.2) is equivalent to $(p-3)(q-3) > 0$.

Taking $q > p > 4$ we obtain that $\beta_{p,q}$ is the desired counterexample. Let $T = \{\beta_{p,q} : q > p \text{ primes}\}$. Finally note that $l(\beta_{5,7}) = 6$. Hence $\beta_{5,7}$ is a counterexample for (5.1) when $k = 5$.

References

[1] W. Burnside, *Theory of groups of finite order*, 2nd edition, Dover Publications, New York 1955.

[2] J. W. Cassels, *On a conjecture of R. M. Robinson about sums of roots of unity*, J. Reine Angew. Math **238** (1969), 112 - 131.

[3] I. M. Isaacs, *Character theory of finite groups*, Corrected reprint of the 1976 original [Academic Press, New York; MR0460423]. AMS Chelsea Publishing, Providence, RI, 2006.

[4] J. H. Loxton, *On the maximum modulus of cyclotomic integers*, Acta Arith. **22** (1972), 69 - 85.

[5] J. H. Loxton, *On two problems of R. M. Robinson about sums of roots of unity*, Acta Arith. **26** (1974/75), 159 - 174.

[6] C. A. Pantea, *On the number of conjugacy classes of finite p-groups*, Mathematica **46** (69), no. 2, (2004), 193 - 203.

[7] C. L. Siegel, *The trace of totally positive and real algebraic integers*, Ann. of Math. (2) **46** (1945), 302-312.

[8] F. Stan and A. Zaharescu, *Siegel's trace problem and character values of finite groups*, J. Reine Angew. Math **637** (2009), 217 - 234.

[9] F. Stan and A. Zaharescu, *The Siegel norm of algebraic numbers*, Bull. Math. Soc. Sci. Math. Roumanie, Tome **55** (103), no. 1, (2012), 69 - 77.

Amita Malik
Department of Mathematics, University of Illinois at Urbana-Champaign
Altgeld Hall, 1409 W. Green Street, Urbana, IL, 61801, USA
e-mail: amalik10@illinois.edu

Florin Stan
Simion Stoilow Institute of Mathematics of the Romanian Academy, Research unit 5, P. O. Box 1-764, RO-014700 Bucharest, Romania
e-mail: sfloringabriel@yahoo.com

Alexandru Zaharescu
Simion Stoilow Institute of Mathematics of the Romanian Academy, Research unit 5, P. O. Box 1-764, RO-014700 Bucharest, Romania
and
Department of Mathematics, University of Illinois at Urbana-Champaign
Altgeld Hall, 1409 W. Green Street, Urbana, IL, 61801, USA
e-mail: zaharesc@math.uiuc.edu