Solution counts and sums of roots of unity

Jincheng Zhuang[1,2], Qi Cheng[3], and Jiejing Wen[1,2]

[1] Key Laboratory of Cryptologic Technology and Information Security of Ministry of
Education, Shandong University, Qingdao, Shandong, 266237, China
[2] School of Cyber Science and Technology, Shandong University,
Qingdao, Shandong, 266237, China
{jzhuang,jjwen}@sdu.edu.cn
[3] School of Computer Science, University of Oklahoma, Norman, OK, 73019, USA
qcheng@ou.edu

Abstract. In this work, we count the number of ways to represent an element in a prime finite field as a sum of elements from different multiples of a small subset. More generally, we study the problem of solution counting of certain linear equations over subsets of finite fields. We establish the basic properties about the number of solutions, and connect the number with lower bounds of complex norms of sums of roots of unity.

Keywords: linear equations, solution counts, sums of roots of unity

1 Introduction

1.1 Sums of roots of unity

Finding good upper bounds for various exponential sums is one of the most important problems of analytic number theory. Estimating lower bounds for exponential sums is less studied but is also an interesting problem in the theory of Diophantine Approximation. In this paper, we relate the problem of lower bounds on sums of roots of unity to a certain counting problem in finite fields. A similar but different connection was made in the work of Myerson [11, 12].

Let $k < T$ be positive integers. Consider α a sum of k roots of unity of orders dividing T. Let $L(\alpha)$ be the product of conjugates of α with complex norm less than 1. Define $f(k, T)$ to be the least absolute value of the non-zero α's:

$$f(k,T) = \min\left\{ \left| \sum_{i=1}^{k} {\zeta_T}^{a_i} \right| \mid (a_1, a_2, \ldots, a_k) \in (\mathbb{Z}/T\mathbb{Z})^k, \sum_{i=1}^{k} {\zeta_T}^{a_i} \neq 0 \right\}.$$

One can also consider a variant $f'(k, T)$ of $f(k, T)$ such that the roots of unity are required to be different. Namely,

$$f'(k,T) = \min\left\{ \left| \sum_{a \in S} {\zeta_T}^{a} \right| \mid S \subset (\mathbb{Z}/T\mathbb{Z}), |S| = k \right\}.$$

The problem of determining the optimal lower bound of $f(k,T)$ or $f'(k,T)$ has appeared in different settings. For example, for the sake of studying certain non-interference problem from the theory of Riemann zeta function, Littlewood [10] considered bounds of sums of cosines. Given a circulant matrix with the first row $(c_0, c_1, \dots, c_{T-1})$, the eigenvalues of the matrix are of the form $\sum_{i=0}^{T-1} c_i \zeta_T^{ik}$ for $0 \le k \le T-1$ [14]. Graham and Sloane [4] asked about the lower bound of $f(k,T)$ in the context of considering certain values attached with binary matrices. This problem also has connection to the growth rate of periodic points of actions of $\mathbb{Z}^k$ by automorphisms of compact abelian groups [15, Chapter 19].

Konyagin and Lev [8] considered the distribution of the exponential sums $S_A(z) = \sum_{a\in A} \zeta_p^{az}$, where $A \subset \mathbb{F}_p$,$|A| = k$,$z \in \mathbb{F}_p$. They gave a lower bound on the complex value $|S_A(z)|$ that decreases exponentially in the prime modulus p. Some estimates on the norms of Gaussian periods were obtained by Myerson [12], Habegger [6] and Dimitrov [1, 2].

In [13], Myerson proposed the problem of finding tight bounds on the complex norms of $f(k,T)$ and $L(\alpha)$. He showed that $f(k,T) \ge c_k T^{-1}$ for $k = 2,3$, and $f(4,T) \ge c_4 T^{-2}$, where c_k is a positive constant depending on k. In general, since the norm of a non-vanishing algebraic integer is a non-zero rational integer, it follows trivially that $f(k,T) \ge k^{-T}$. It remains an open problem to improve this sub-exponentially in $-T$, in the asymptotic that k is fixed and T grows.

Many researchers have expected that the tight lower bound of $|\alpha|$ decreases polynomially in T. Myerson [13] has asked the following question.

Problem 1. Let $k \ge 1$ be a given integer. Do there exist positive constants $c_k, \lambda_k > 0$ depending on k such that $f(k,T) \ge c_k T^{-\lambda_k}$ for all $T \ge 1$?

Some discussions about the history of Myerson's problem can be found in [17].

In [16], Shkredov surveyed applications of harmonic analysis to combinatorial number theory. In particular, he reformulated Myerson's problem as bounding the Fourier coefficients of a characteristic function, and gave an estimate by a result of Lev [9]. Dubickas [3] studied the upper bound of $L(\alpha)$, solved the case $k = 2$, and gave partial results for the case $k = 3$.

Habegger [5] presented evidence supporting an affirmative answer to Problem 1 when the moduli are prime. He proved that the set of prime orders p such that the assertion in Problem 1 does not hold is sparse.

Theorem 1 ([5]). *For given $\varepsilon > 0, k \ge 1$, and $a_0, \dots, a_k \in \mathbb{C} \setminus \{0\}$, there exist constants $c \ge 1, \lambda \ge 1$ both depending on $a_0, \dots, a_n, \varepsilon$ such that*

$$\#\{\text{prime } p \le B \mid \exists\ e_1, \dots, e_k \in \mathbb{F}_p, \\ 0 < |a_0 + a_1\zeta_p^{e_1} + \cdots + a_k\zeta_p^{e_k}| \le c^{-1}p^{-\lambda}\} \le cB^{\varepsilon}$$

for all $B \ge 1$.

In this work, we connect lower bounds of sums of unity with the number of solutions of certain linear equations over subsets of a finite field.

Definition 1. *Let p be an odd prime, $S \subset \mathbb{Z}/p\mathbb{Z}, |S| = k$. Define two functions $F : \mathbb{F}_p^{p-1} \to \mathbb{F}_p$ and $f_a : \mathbb{F}_p^{p-3} \to \mathbb{F}_p$ by*

$$F = x_1 + 2x_2 + \cdots + (p-2)x_{p-2} + (p-1)x_{p-1},$$
$$f_a = F - ax_a - (p-a)x_{p-a},$$

where $1 \leq a \leq \frac{p-1}{2}$. Denote

$$N_S(i) = \#\{X_F \in S^{p-1} | F(X_F) = i\}, 1 \leq i \leq p-1,$$
$$N_S(a,b) = \#\{X_f \in S^{p-3} | f_a(X_f) = b\}, 1 \leq b \leq p-1,$$

We will omit the subscript S if it is clear from the context.

Equivalently, given an element $a \in \mathbb{F}_p$, we consider the problem of counting the number of ways of representing a as a sum of elements $a_i \in c_i S$, with $c_i \in \mathbb{F}_p^*$ distinct.

We show that there is a precise relation between $f'(k,p), N(1,0)$ and $N(0)$.

Theorem 2. *Let $k < p$. We have*

$$\frac{1}{f'(k,p)^2} \leq \max_{S \subset (\mathbb{Z}/p\mathbb{Z}), |S|=k} (p-1) \frac{N_S(1,0) - k^{p-3}/p}{N_S(0) - k^{p-1}/p} \leq \frac{p-1}{f'(k,p)^2}.$$

Equivalently,

$$f'(k,p)^2 \geq \min_{S \subset (\mathbb{Z}/p\mathbb{Z}), |S|=k} \frac{1}{p-1} \frac{N_S(0) - k^{p-1}/p}{N_S(1,0) - k^{p-3}/p} \geq \frac{1}{p-1} f'(k,p)^2.$$

1.2 Upper bounds of $\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(|\alpha|^{-2})$

Let p be an odd prime. Motivated by the study of $f'(k,p)$, we take the approach of transforming the problem from considering lower bounds to upper bounds. Let $\sigma_t \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ be such that $\sigma_t(\zeta_p) = \zeta_p^t$ for $1 \leq t \leq p-1$, and $\alpha = \sum_{i \in S} \zeta_p^i$. Since $|\alpha|$ is small precisely when $\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(|\alpha|^{-2})$ is large, it is of interest to compute the latter trace. We deduce

$$\begin{aligned}\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(|\alpha|^{-2}) &= \sum_{t=1}^{p-1} \frac{1}{(\sum_{i \in S} \sigma_t(\zeta_p^i))\overline{(\sum_{i \in S} \sigma_t(\zeta_p^i))}} \\ &= \frac{\sum_{1 \leq k \leq p-1} \prod_{j \neq k, j \neq p-k} (\sum_{i \in S} (\zeta_p^j)^i)}{\mathrm{Norm}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\sum_{i \in S} \zeta_p^i)}.\end{aligned}$$

We connect the number of solutions $N(i), N(a,b)$ to the complex norm of sums of roots of unity.

Theorem 3. *Let $\zeta_p = e^{\frac{2\pi i}{p}}$,$\sigma_t(\zeta_p) = \zeta_p^t$,$S \subset \mathbb{Z}/p\mathbb{Z}, |S| = k$. Then*

$$\sum_{t=1}^{p-1} \frac{1}{(\sum_{i \in S} \sigma_t(\zeta_p^i))\overline{(\sum_{i \in S} \sigma_t(\zeta_p^i))}} = (p-1) \frac{N(1,0) - k^{p-3}/p}{N(0) - k^{p-1}/p}.$$

1.3 Solution counts

We first establish the properties of number of solutions $N(i)$ in Definition 1.

Theorem 4. *Let p be an odd prime. Fix a subset $S \subset \mathbb{Z}/p\mathbb{Z}, |S| = k$. Then*

(1) $N(i) = N(j),\ 1 \leq i < j \leq p-1$.
(2) Denote $N = N(i), 1 \leq i \leq p-1$. Then

$$N(0) - N = Norm_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(\sum_{i\in S}\zeta_p^i\right).$$

(3)

$$\begin{cases} N(0) = \dfrac{k^{p-1} + (p-1)Norm_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(\sum_{i\in S}\zeta_p^i\right)}{p}, \\ N = \dfrac{k^{p-1} - Norm_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(\sum_{i\in S}\zeta_p^i\right)}{p}. \end{cases}$$

For a fixed k, we also discuss the problem of the number of all possible $(N(0), N)$ pairs for all $S \subset \mathbb{F}_p, |S| = k$.

We then consider the number of solutions $N(a, b)$.

Theorem 5. *Let p be an odd prime. Fix $S \subset \mathbb{Z}/p\mathbb{Z}, |S| = k$. Then*

(1) $N(a, b) = N(a, p-b)$ for $1 \leq a, b \leq \frac{p-1}{2}$.
(2) Let $1 \leq a_1, a_2 \leq \frac{p-1}{2}$, $0 \leq b_1, b_2 \leq p-1$. If $b_2 = a_1^{-1}a_2b_1$, then $N(a_1, b_1) = N(a_2, b_2)$.
(3) Let $m_{i,j} = N(i, -j^{-1})$, then the matrix $M = (m_{i,j})_{\frac{p-1}{2}\times\frac{p-1}{2}}$ is symmetric.
(4) Suppose the eigenvalues of M is ordered as

$$\mu_0 \geq \mu_1 \geq \cdots \geq \mu_{\frac{p-1}{2}-1}.$$

Then
(a) $\mu_0 = \sum_{1\leq b\leq\frac{p-1}{2}} N(a, b)$ for every $1 \leq a \leq \frac{p-1}{2}$.
(b) For any $a, b \in \mathbb{F}_p$, the number $N(a, b)$ of solutions $X \in \mathbb{F}_p^{p-3}$ to the equation $f_a(X) = b$ satisfies

$$\left|N(a, b) - \frac{\mu_0}{(p-1)/2}\right| \leq \max\{|\mu_1|, |\mu_{\frac{p-3}{2}}|\}.$$

The rest of the paper is organized as follows. In Section 2, we demonstrate the proof of Theorem 4 and Theorem 5. Besides, we present some corollaries and further discussions. In Section 3, we give the proof of Theorem 2 and Theorem 3.

2 Number of solutions of the linear equations

In this section, we demonstrate basic properties of the linear forms defined in Definition 1.

2.1 Properties of $N(i)$

We first establish the properties of the function $N(i)$.
Proof of Theorem 4: (1) We want to show that

$$N(i) = N(j),\ 1 \leq i < j \leq p-1.$$

For each solution of $F(t_1, \ldots, t_{p-1}) = i \neq 0$, we multiply $i^{-1}j$ on both sides and obtain equality $F(i^{-1}jt_1, \ldots, i^{-1}jt_{p-1}) = j$. Furthermore, different solutions of $F = i$ correspond to different solutions of $F = j$. Hence $N(i) \leq N(j)$. By symmetry, we have $N(i) \geq N(j)$. Thus $N(i) = N(j)$.

(2) In the sequel, we will denote $N = N(i), 1 \leq i \leq p-1$. For $t \in \mathbb{F}_p$, consider the field automorphism $\sigma_t \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ defined by $\sigma_t(\zeta_p) = \zeta_p^t$. Then

$$\begin{aligned}
\mathrm{Norm}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(\sum_{i\in S} \zeta_p^i\right) &= \prod_{i=1}^{p-1} \sigma_i \left(\sum_{x\in S} \zeta_p^x\right) \\
&= \prod_{i=1}^{p-1} \left(\sum_{x\in S} \zeta_p^{ix}\right) \\
&= \sum_{i=0}^{p-1} n_i \zeta_p^i,
\end{aligned}$$

where $n_i = |\{(x_1, \ldots, x_{p-1}) \in S^{p-1} | \sum_{j=1}^{p-1} jx_j = i\}| = N(i) = N$ for $1 \leq i \leq p-1$. Since $N(i) = N$ for $i \in \mathbb{F}_p^*$, $\sum_{i=0}^{p-1} \zeta_p^i = 0$ for $1 \leq i \leq p-1$, we have

$$\begin{aligned}
\mathrm{Norm}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(\sum_{i\in S} \zeta_p^i\right) &= N(0) + N\sum_{i=1}^{p-1} \zeta_p^i \\
&= N(0) - N.
\end{aligned}$$

(4) We deduce the following linear equations

$$\begin{cases} N(0) + (p-1)N = k^{p-1} \\ N(0) - N \qquad\quad = \mathrm{Norm}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\sum_{i\in S} \zeta_p^i). \end{cases}$$

Thus the simultaneous solution of the linear equations yields

$$\begin{cases} N(0) = \dfrac{k^{p-1} + (p-1)\mathrm{Norm}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\sum_{i\in S} \zeta_p^i)}{p} \\ \quad N = \dfrac{k^{p-1} - \mathrm{Norm}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\sum_{i\in S} \zeta_p^i)}{p}. \end{cases}$$

□

Remark 1. By Theorem 4, it is equivalent to evaluate $\mathrm{Norm}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(\sum_{i\in S} \zeta_p^i\right)$ and to evaluate $N(0)$ and N.

Corollary 1. *Let $a \in \mathbb{F}_p, d \in \mathbb{F}_p^*, S = \{a, a+d, \dots, a+(k-1)d\}$ be an arithmetic progression. Then*

$$\begin{cases} N(0) = \dfrac{k^{p-1}+p-1}{p}, \\ \quad N = \dfrac{k^{p-1}-1}{p}. \end{cases}$$

Proof. We first evaluate $\mathrm{Norm}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(\sum_{i=0}^{d-1} \zeta_p^{a+d\cdot i}\right)$. We have

$$\begin{aligned} &\mathrm{Norm}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(\sum_{i=0}^{d-1} \zeta_p^{a+d\cdot i}\right) \\ =&\mathrm{Norm}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(\zeta_p^a\right) \cdot \mathrm{Norm}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(\sum_{i=0}^{d-1} \zeta_p^{d\cdot i}\right) \\ =&\mathrm{Norm}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\frac{1-\zeta_p^{kd}}{1-\zeta_p^d} \\ =&\frac{\mathrm{Norm}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(1-\zeta_p^{kd}\right)}{\mathrm{Norm}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(1-\zeta_p^{d}\right)} \\ =&1, \end{aligned}$$

where the last equation follows as $1-\zeta_p^{kd}$ and $1-\zeta_p^d$ are conjugate to each other. Thus the results follows from Theorem 4. □

Number of different pairs of $(N(0), N)$: Fix a positive number $k < p$. In general, there are $\binom{p}{k}$ possibilities for S. But the pairs $(N(0), N)$ may be the same for different subsets. In the following, we use Burnside's lemma to compute the number of pairs $(N(0), N)$ on the example $p = 7$, $k = 3$.

Lemma 1 (Burnside's lemma). *Let G be a finite group that acts on a set X with orbit number $|X/G|$. For any $g \in G$, denote X^g the set of elements fixed by g. Then*

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|X^g|.$$

Proposition 1. *Let $k < p, S_1 = \{a_1, a_2, \dots, a_k\} \subset \mathbb{F}_p, S_2 = \{b_1, b_2, \dots, b_k\} \subset \mathbb{F}_p$. If there is a linear map*

$$\begin{aligned} T: S_1 &\longrightarrow S_2 \\ x_i &\longmapsto cx_i + d \end{aligned}$$

where $c \in \mathbb{F}_p^*, d \in \mathbb{F}_p$, then $N_{S_1}(i) = N_{S_2}(i)$ for $i \in \mathbb{F}_p$.

Proof. Suppose

$$F(x_1, \dots, x_{p-1}) = i, x_j \in S_1, 1 \le j \le p-1.$$

Then $F(cx_1 + d, \dots, cx_{p-1} + d) = c \cdot i$. Thus each solution in S_1 corresponds to a solution in S_2 by T. Furthermore, different solutions in S_1 correspond to different solutions in S_2 by T. Hence $N_{S_1}(i) \leq N_{S_2}(c \cdot i) = N_{S_2}(i)$. By symmetry, $N_{S_1}(i) \geq N_{S_2}(i)$. Consequently, we have $N_{S_1}(i) = N_{S_2}(i)$. □

Example 1. Let $p = 7, k = 3$, we determine the number of different pairs $N(0), N$ over all subsets of 3 elements.

Let $A = \{S \subset \mathbb{F}_7 \mid |S| = 3\}$, $G = \{T_{c,d} : S_1 \to S_2 \mid T_{c,d}(s) = cs + d, c, d \in \mathbb{F}_7, c \neq 0\}$. Then G acts on A, we first determines the number of orbits. Let A^T be the set of invariant elements under the action of T. By computation, we have

$$\begin{aligned} A^{T_{1,0}} &= 35, \\ A^{T_{2,i}} &= 2, 0 \leq i \leq 6, \\ A^{T_{4,i}} &= 2, 0 \leq i \leq 6, \\ A^{T_{6,i}} &= 3, 0 \leq i \leq 6, \end{aligned}$$

and the numbers not listed above are all 0. By Burnside's lemma, we have the number of orbits

$$\begin{aligned} |A/G| &= \frac{1}{|G|} \sum_{g \in G} |A^g| \\ &= \frac{1}{42}(1 \times 35 + 2 \times 14 + 3 \times 7) \\ &= 2. \end{aligned}$$

In fact, there are only two possibilities of pairs $(N(0), N)$ as follows.

$$\begin{aligned} N(0) = 105, N &= 104, \\ N(0) = 111, N &= 103. \end{aligned}$$

For example, the first pair arise when $S = \{1, 2, 3\}$, and the second pair arise when $S = \{1, 2, 4\}$.

2.2 Properties of $N(a, b)$

In this section, we consider properties of the number $N(a, b)$ of solutions of $f_a = b$.

We recall the expander mixing lemma first which we will use later. For a more detailed explanation, we refer the reader to [7, Lemma 2.5].

Lemma 2 (Expander Mixing Lemma). *Let $G = (V, E), |V| = n$ be a $d = \mu_0$-regular graph with adjacency matrix M. Let the eigenvalues of M be $\mu_0 \geq \mu_1 \geq \cdots \geq \mu_{n-1}$. Let $\lambda = \max(|\mu_1|, |\mu_{n-1}|)$. For all $S, T \subset V$, let $E(S, T) = \{(u, v) \in E \mid u \in S, v \in T\}$. Then*

$$\left| |E(S, T)| - \frac{d|S||T|}{n} \right| \leq \lambda \sqrt{|S||T|}.$$

Proof of Theorem 5: (1) By definition,

$$f_a = F - ax_a - (p-a)x_{p-a}. \tag{1}$$

If the vector $X_f \in S^{p-3}$ is a solution for $f_a = b$, then we conclude that X_f corresponds a solution for $f_a = p - b$ by multiplying -1 to both sides of Equation 1. Thus $N(a,b) \leq N(a, p-b)$. By symmetry, we have $N(a,b) \geq N(a,p-b)$, which implies $N(a,b) = N(a,p-b)$.

(2) Suppose $X \in S^{p-3}$ is a solution of the equation

$$F - a_1 x_{a_1} - (p - a_1)x_{p-a_1} = b_1.$$

Multiplying both sides by $a_1^{-1}a_2$, we get

$$F - a_2 x_{a_2} - (p-a_2)x_{p-a_2} = a_1^{-1}a_2 b_1.$$

Thus $N(a_1,b_1) \leq N(a_2,b_2)$ where $b_2 = a_1^{-1}a_2b_1$. By symmetry $N(a_1,b_1) \geq N(a_2,b_2)$. Hence $N(a_1,b_1) = N(a_2,b_2)$.

(3) By definition $m_{i,j} = N(i, -j^{-1})$, in order to show the matrix $M = (m_{i,j})_{\frac{p-1}{2}\times\frac{p-1}{2}}$ is symmetric, it suffices to verify that

$$N(i, -j^{-1}) = N(j, -i^{-1}).$$

This is a special case of (2).

(4) By (3), the sum $\sum_{1\leq b \leq (p-1)/2} N(a,b)$ is independent of a. Consequently, this common value equals μ_0, and the non-oriented graph $G(M)$ defined by the adjacency matrix M is μ_0-regular. The result now follows by the expander mixing lemma. □

Example 2. Let $p = 13, k = 5,\ S = \{2,5,7,9,12\}$. We have

$$M = \begin{bmatrix} 751203 & 751199 & 751205 & 751200 & 751204 & 751198 \\ 751199 & 751200 & 751198 & 751204 & 751205 & 751203 \\ 751205 & 751198 & 751200 & 751203 & 751199 & 751204 \\ 751200 & 751204 & 751203 & 751205 & 751198 & 751199 \\ 751204 & 751205 & 751199 & 751198 & 751203 & 751200 \\ 751198 & 751203 & 751204 & 751199 & 751200 & 751205 \end{bmatrix},$$

where the element at the i-th row and j-th column is $m_{i,j} = N(i, -j^{-1})$.

3 Relation with sums of roots of unity

In this section, we connect the number of solutions of equations over subsets of finite fields and the complex norm of sums of roots of unity.

Proof of Theorem 3: First, we make the following transform.

$$\sum_{t=1}^{p-1} \frac{1}{(\sum_{i\in S}\sigma_t(\zeta_p^i))\overline{(\sum_{i\in S}\sigma_t(\zeta_p^i))}} = \frac{\sum_{1\leq k\leq p-1}\prod_{j\neq k, j\neq p-k}(\sum_{i\in S}(\zeta_p^j)^i)}{\mathrm{Norm}(\sum_{i\in S}\zeta_p^i)}.$$

Next, we calculate the denominator and numerator respectively. From Theorem 4, we have

$$\mathrm{Norm}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(\sum_{i\in S}\zeta_p^i\right) = N(0) - N.$$

For the numerator, we compute

$$\begin{aligned}\sum_{1\leq k\leq p-1}\prod_{j\neq k, j\neq p-k}\left(\sum_{i\in S}(\zeta_p^j)^i\right) &= \sum_{1\leq k\leq p-1}\left(N(k,0)+\sum_{1\leq i\leq p-1}N(k,i)\zeta_p^i\right)\\ &= (p-1)N(1,0)+\sum_{1\leq i\leq p-1}\left(\sum_{1\leq k\leq p-1}N(k,i)\right)\zeta_p^i\\ &= (p-1)N(1,0)+\sum_{1\leq i\leq p-1}A\zeta_p^i\\ &= (p-1)N(1,0)-A,\end{aligned}$$

where $A = k^{p-3} - N(1,0)$. Consequently,

$$\begin{aligned}\sum_{t=1}^{p-1}\frac{1}{(\sum_{i\in S}\sigma_t(\zeta_p^i))\overline{(\sum_{i\in S}\sigma_t(\zeta_p^i))}} &= \frac{(p-1)N(1,0)-A}{N(0)-N}\\ &= \frac{pN(1,0)-k^{p-3}}{N(0)-(k^{p-1}-N(0))/(p-1)}\\ &= (p-1)\frac{N(1,0)-k^{p-3}/p}{N(0)-k^{p-1}/p}.\end{aligned}$$

□

Remark 2. Note that $\frac{k^{p-3}}{p}$ is the average number of solutions for $f_a = b$, thus $N(1,0) - \frac{k^{p-3}}{p}$ measures the difference of $N(1,0)$ and the average number. Similarly, $\frac{k^{p-1}}{p}$ is the average number of solutions for $F = i$, thus $N(0) - \frac{k^{p-1}}{p}$ measures the difference of $N(0)$ and the average number.

Proof of Theorem 2: This follows directly from Theorem 3. □

Corollary 2. *For given $\varepsilon > 0, k \geq 1$, there exists constants c depending on ε such that*

$$\#\{p \leq B \textit{ is a prime} \mid \exists S \subset (\mathbb{Z}/p\mathbb{Z}), |S| = k, \frac{N_S(1,0)-k^{p-3}/p}{N_S(0)-k^{p-1}/p} \geq p^c\} \leq cB^\varepsilon$$

for all $B \geq 1$.

Proof. Recall that $f(k,T)$ denotes the least complex value of k T-th roots of unity. We have

$$\sum_{t=1}^{p-1}\frac{1}{(\sum_{i\in S}\sigma_t(\zeta_p^i))\overline{(\sum_{i\in S}\sigma_t(\zeta_p^i))}} \leq \frac{p-1}{f'(k,p)^2} \leq pf(k,p)^{-2}.$$

The result follows from a combination of Theorem 1 and Theorem 3. □

Acknowledgements

This work was partially supported by the National Key Research and Development Program of China (No. 2021YFB3100200, 2018YFA0704702), the Major Basic Research Project of Natural Science Foundation of Shandong Province, China (No. ZR202010220025) for J. Zhuang, by US NSF (No. CCF-1900820) for Q. Cheng, and by Fundamental Research Funds of Shandong University for J. Wen. Part of the content is based on the master thesis of the first author. We thank the anonymous referees for a number of very helpful comments.

References

1. V. Dimitrov. Convergence to the Mahler measure and the distribution of periodic points for algebraic noetherian $\mathbf{Z}^d$-actions. arXiv:1611.04664v2, 2017.
2. V. Dimitrov. *Diophantine approximations by special points and applications to Dynamics and Geometry*. PhD thesis, Yale University, 2017.
3. A. Dubickas. On sums of two and three roots of unity. *Journal of Number Theory*, 192:65–79, 2018.
4. R. L. Graham and N. J. A. Sloane. Anti-hadamard matrices. *Linear Algebra and Its Applications*, 62:113–137, 1984.
5. P. Habegger. Diophantine approximations on definable sets. *Selecta Mathematica*, 24(2):1633–1675, 2018.
6. P. Habegger. The norm of gaussian periods. *Q. J. Math.*, 69(1):153–182, 2018.
7. S. Hoory, N. Linial, and A. Wigderson. Expander graphs and their applications. *Bulletin of the American Mathematical Society*, 43(4):439–561, 2006.
8. S.V. Konyagin and V.F. Lev. On the distribution of exponential sums. *INTEGERS*, A01, 2000.
9. V. F. Lev. Linear equations over F_p and moments of exponential sums. *Duke Mathematical Journal*, 107:239–263, 2001.
10. J. E. Littlewood. Mathematical notes (12): An inequality for a sum of cosines. *Journal of the London Mathematical Society*, s1-12:217–221, 1937.
11. G. Myerson. A combinatorial problem in finite fields, I. *Pacific Journal of Mathematics*, 82(1):179–187, 1979.
12. G. Myerson. A combinatorial problem in finite fields, II. *The Quarterly Journal of Mathematics*, 31(2):219–231, 1980.
13. G. Myerson. How small can a sum of roots of unity be? *The American Mathematical Monthly*, 93(6):457–459, 1986.
14. P.J.Davis. *Circulant matrices.* Wiley, New York, 1979.
15. K. Schmidt. *Dynamical Systems of Algebraic Origin.* Springer Basel, 1995.
16. Il'ya D Shkredov. Fourier analysis in combinatorial number theory. *Russian Math Surveys*, 65(3):513–567, 2010.
17. T. Tao. How small can a sum of a few roots of unity be? MathOverflow. http://mathoverflow.net/q/46068.