

Exponential sums, Gauss sums and irreducible cyclic codes

MARKO MOISIO

Abstract. In this paper we shall develop a recursive method for computing exponential sums and Gauss sums in so called index 2 case. The method allows us to generalize previous results obtained by Baumert, Mykkeltveit and van der Vlugt.

1. Introduction

In this paper we shall study the distribution of the values of exponential sums with monomial arguments or equivalently the weight distribution of certain cyclic codes. Let \mathbb{F} be a finite prime field and $N \geq 3$ an odd integer, and assume that the multiplicative order of the characteristic of \mathbb{F} modulo N is $\phi(N)/2$, where ϕ is Euler's function. Let \mathbb{E} be the extension field of \mathbb{F} of degree $\phi(N)/2$ and consider the exponential sum over \mathbb{E} with αX^N as an argument, $\alpha \in \mathbb{E}$. The weight distribution of the codes related to these sums were studied in [1] when N is a prime, and in [8] when N is product of two primes.

In the present work we shall consider the case where $N = p^u q^v$, $u, v \geq 0$, $(u, v) \neq (0, 0)$, which can not be generalized since in the case in consideration N can have at most two prime divisors. We shall develop a recursive method for computing the distribution of the values of the exponential sums related to this case. Let us briefly describe the method. E.g. assume that $u, v \geq 1$. Suppose that we have computed the distribution of values of sums with $\alpha X^{N/p}$, $\alpha X^{N/q}$ and $\alpha X^{\frac{N}{pq}}$ as arguments. Then these values together with a Gauss sum contained in a quadratic extension of

\mathbb{Q} determine completely the distribution of the values of the sum with αX^N as an argument. The Gauss sum can be evaluated up to a possible ambiguity in the sign of the imaginary part from a diophantine equation, and from a congruence.

Although we consider the general case there remains classes of exponential sums to which the method does not seem to be applicable, namely: $N = p^u q^v$, $q \equiv 3 \pmod{4}$ and the multiplicative order of the characteristic of \mathbb{F} modulo q^v is $\phi(q^v)/2$.

In what follows we shall study only sums over fields of characteristic 2, but the technique is applicable for sums over fields of characteristic greater than 2, too.

The content of the paper is organized as follows. In the section 2 we shall discuss the relationship between the weight of trace codes, exponential sums and Gauss sums. In the section 3 we consider the well known case $-1 \in \langle 2 \rangle$ modulo N and evaluate, without using the Davenport-Hasse theorem, the exponential sums related to this case explicitly. In the section 4 we shall consider arithmetical lemmas which characterize the case $-1 \notin \langle 2 \rangle$ modulo N , and in the section 5 we prove our main theorems concerning the computing of exponential sums related to this case. In the section 6 we give numerical examples by determining the weight distribution of certain irreducible cyclic codes.

2. Irreducible cyclic codes and exponential sums

Let $N \geq 3$ be an odd integer. Let $l \in \mathbb{Z}_+$, and denote $k = \text{ord}_N(2)$, $r = 2^{lk}$ and $n = (r - 1)/N$. Suppose that γ is a fixed primitive element of \mathbb{F}_r . The linear space over \mathbb{F}_2 defined by

$$\mathcal{C}_n(N) = \{c(\alpha) = (\text{Tr}(\alpha), \text{Tr}(\alpha\gamma^N), \dots, \text{Tr}(\alpha\gamma^{(n-1)N}) : \alpha \in \mathbb{F}_r\},$$

where Tr is the trace map from \mathbb{F}_r to \mathbb{F}_2 , is called a binary irreducible cyclic code. It is cyclic in the sense that that it is closed under the cyclic shift of the coordinates of words $c(\alpha)$, and irreducible in the sense that it has no proper subspace which is cyclic.

The number of non-zero coordinates of a word $c(\alpha)$ is called the weight of the word, and we denote it by $w(c(\alpha))$. Let e denote the canonical additive character

of \mathbb{F}_r i.e. the map $x \mapsto (-1)^{Tr(x)}$. The weight of $c(\alpha)$ is now given by

$$\begin{aligned} w(c(\alpha)) &= \frac{1}{2} \sum_{i=0}^{n-1} (1 - e(\alpha \gamma^{Ni})) \\ &= \frac{1}{2} \left(n - \frac{1}{N} \sum_{x \in \mathbb{F}_r^*} e(\alpha x^N) \right) \\ &= \frac{1}{2N} \left(r - \sum_{x \in \mathbb{F}_r} e(\alpha x^N) \right). \end{aligned}$$

This formula is also valid for codes over \mathbb{F}_p , $p > 2$, if $N \mid (r-1)/(p-1)$ [7].

Let F be a homomorphism from \mathbb{F}_r to $\mathcal{C}_n(N)$ defined by $\alpha \mapsto c(\alpha)$. If F is a bijection then $\mathcal{C}_n(N)$ is called a non-degenerate irreducible cyclic code. A sufficient condition for the bijectivity of F is $N < \sqrt{r} + 1$, since for $\alpha \neq 0$, $|\sum_{x \in \mathbb{F}_r} e(\alpha x^N)| \leq (N-1)\sqrt{r}$. Furthermore, this condition holds if $l \geq 2$, since then $N \leq 2^{\frac{l}{2}} - 1$. In general, it can be shown (see [6]) that the cardinality of $\mathcal{C}_n(N)$ is $2^{k'}$, where $k' = \text{ord}_n(2)$.

Thus, to determine the weight distribution of the code $\mathcal{C}_n(N)$, we must investigate the distribution of the values of exponential sum $\sum_{x \in \mathbb{F}_r} e(\alpha x^N)$ for $\alpha \in \mathbb{F}_r$.

There is a close connection between this sum and Gauss sums. In fact, let χ be a multiplicative character on \mathbb{F}_r^* of order N , and let $G(\chi^t)$ denote the Gauss sum $\sum_{x \in \mathbb{F}_r^*} \chi^t(x) e(x)$. Now (see [5])

$$\sum_{x \in \mathbb{F}_r} e(\alpha x^N) = \sum_{t=1}^{N-1} G(\chi^t) \chi^{-t}(\alpha). \quad (1)$$

In general it is hard to determine the values of Gauss sums, but in some special cases this can be done. In the next section we consider such a class.

3. Case $-1 \in \langle 2 \rangle \pmod{N}$

Lemma 1. *If -1 is a power of 2 modulo N then*

$$G(\chi^t) = (-1)^{t-1} \sqrt{r}, \quad t = 1, \dots, N-1.$$

Proof. Since $G(\chi^{2t}) = G(\chi^t)$ and $-1 \in \langle 2 \rangle \pmod{N}$, it follows that $G(\chi^t) \in \mathbb{R}$. Thus $G(\chi^t) = \pm \sqrt{r}$.

Since $\text{ord}_N(2) = k$ and $-1 \in \langle 2 \rangle \subseteq \mathbb{Z}_N^*$, we must have $2 \mid k$ and $2^{k/2} \equiv -1 \pmod{N}$. Thus \sqrt{r} is congruent to 1 or -1 modulo N depending on whether l is even or odd, respectively. Denote

$$A = |\{1 \leq t \leq N-1 \mid G(\chi^t) = \sqrt{r}\}|,$$

$$B = |\{1 \leq t \leq N-1 \mid G(\chi^t) = -\sqrt{r}\}|.$$

By choosing $\alpha = 1$ in (1) we obtain

$$N \sum_{i=0}^{\frac{r-1}{N}-1} e(\gamma^{Ni}) = \sum_{x \in \mathbb{F}_r^*} e(x^N) = (A - B)\sqrt{r} - 1,$$

and this imply

$$(A - B)\sqrt{r} - 1 = (N - 1 - 2B)\sqrt{r} - 1 \equiv \begin{cases} -2(B + 1) \equiv 0 \pmod{N} & \text{if } 2 \mid l \\ 2B \equiv 0 \pmod{N} & \text{if } 2 \nmid l. \end{cases}$$

The claim follows from this. \square

Lemma 1 can also be proved by using a result of Stickelberger and the Davenport-Hasse theorem, see [5]. Our proof uses a technique which is a variant of that used in [8, prop. 2.4].

Theorem 1. *Assume that $\alpha \neq 0$. Then*

$$\sum_{x \in \mathbb{F}_r} e(\alpha x^N) = \begin{cases} (-1)^{l-1}(N-1)\sqrt{r} & \text{if } \alpha \in \langle \gamma^N \rangle \subseteq \mathbb{F}_r^*, \\ (-1)^l \sqrt{r} & \text{if } \alpha \notin \langle \gamma^N \rangle \subseteq \mathbb{F}_r^*. \end{cases}$$

Proof. The claim follows immediately from (1) and Lemma 1. \square

From now on we assume that $-1 \notin \langle 2 \rangle$ modulo N . Let ζ_N denote the complex primitive N th root of unity. As $\text{ord}_N(2) = k$ the fixed field of the subgroup of $\text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ isomorphic to $\langle 2 \rangle$ modulo N is an extension field of \mathbb{Q} of degree $\phi(N)/k$. We shall restrict our considerations to the case $k = \phi(N)/2$ and consequently $G(\chi^t)$ is contained in a quadratic subfield of $\mathbb{Q}(\zeta_N)$. If $k = \phi(N)/2$ and $-1 \notin \langle 2 \rangle$ modulo N we call this case as the *index 2 case* (since the index of $\langle 2 \rangle$ in \mathbb{Z}_N^* is 2).

In [1] the index 2 case was studied for primes $N \equiv 3 \pmod{4}$, and in [8] for $N = pq$ with primes p and q . The aim of the present work is to consider the general case $p^u q^v$ with p and q as above. (It is easy to see that in index 2 case N can have at most two prime divisor.)

4. Arithmetical lemmas

We now consider lemmas characterizing the index 2 property. Let us first consider the case $N = p^u$ with p an odd prime and $u \in \mathbb{Z}_+$.

Lemma 2. *If $\text{ord}_{p^u}(2) = \phi(p^u)$ or $\phi(p^u)/2$, then $\text{ord}_{p^i}(2) = \phi(p^i)$ or $\phi(p^i)/2$, respectively, for all $1 \leq i \leq u$.*

Proof. There exists a primitive root, say g , modulo p which is a primitive root modulo p^i for all $i \geq 1$. If $\text{ord}_{p^u}(2) = \phi(p^u)$, then $2 \equiv g^j \pmod{p^u}$ for some j satisfying $(\phi(p^u), j) = 1$. Clearly $2 \equiv g^j \pmod{p^i}$ and therefore

$$\text{ord}_{p^i}(2) = \frac{\phi(p^i)}{(\phi(p^i), j)} = \phi(p^i).$$

If $\text{ord}_{p^u}(2) = \phi(p^u)/2$, then $2 \equiv g^{2j} \pmod{p^u}$ for some j satisfying $(\phi(p^u)/2, j) = 1$. Clearly $2 \equiv g^{2j} \pmod{p^i}$ and therefore

$$\text{ord}_{p^i}(2) = \frac{\phi(p^i)}{(\phi(p^i), 2j)} = \frac{\phi(p^i)}{2(\phi(p^i)/2, j)} = \phi(p^i)/2. \quad \square$$

Lemma 3. *Assume that $N = p^u$ and $\text{ord}_N(2) = \phi(N)/2$. Then $-1 \notin \langle 2 \rangle$ modulo N if and only if $p \equiv 7 \pmod{8}$.*

Proof. From Lemma 2 we know that $\text{ord}_p(2) = (p-1)/2$, and therefore 2 generates the quadratic residues modulo p . Thus $p \equiv \pm 1 \pmod{8}$.

Assume that $-1 \notin \langle 2 \rangle$ modulo N . If $p \equiv 1 \pmod{8}$ then $2^{\phi(N)/4} \equiv -1 \pmod{N}$, which contradicts our assumption.

Suppose that $p \equiv 7 \pmod{8}$. If $-1 \in \langle 2 \rangle$ modulo N then clearly $-1 \in \langle 2 \rangle$ modulo p . Thus -1 is a quadratic residue modulo p and again we have a contradiction. \square

If $N = p^u$ and index 2 case holds, we call it case I.

Next we consider the case $N = p^u q^v$, where p and q are different primes, and $u, v > 0$.

Lemma 4. *If $N = p^u q^v$ and $\text{ord}_N(2) = \phi(N)/2$, then $(p-1, q-1) = 2$ and*

$$\begin{aligned} p \nmid (q-1) & \qquad \qquad \qquad \text{if } u > 1, v = 1 \\ q \nmid (p-1) & \qquad \qquad \qquad \text{if } u = 1, v > 1 \\ p \nmid (q-1) \text{ and } q \nmid (p-1) & \qquad \text{if } u, v > 1 \end{aligned}$$

Proof. The claim follows immediately from

$$\frac{\phi(p^u)\phi(q^v)}{2} = \text{ord}_N(2) = \text{l.c.m}(\text{ord}_{p^u}(2), \text{ord}_{q^v}(2)) = \frac{\text{ord}_{p^u}(2)\text{ord}_{q^v}(2)}{(\text{ord}_{p^u}(2), \text{ord}_{q^v}(2))} \quad \square$$

It follows from Lemma 4 that not both of p and q can be congruent to 1 modulo 4. From now on we assume that $q \equiv 3 \pmod{4}$.

Lemma 5. *Assume that $N = p^u q^v$ and $\text{ord}_N(2) = \phi(N)/2$. If $\text{ord}_{p^u}(2) = \phi(p^u)$, and $\text{ord}_{q^v}(2) = \phi(q^v)$ or $\text{ord}_{q^v}(2) = \phi(q^v)/2$, then $\text{ord}_{p^i q^j}(2) = \phi(p^i q^j)/2$ for all $1 \leq i \leq u, 1 \leq j \leq v$.*

Proof. By Lemma 2 we have

$$\text{ord}_{p^i q^j}(2) = \text{l.c.m}(\text{ord}_{p^i}(2), \text{ord}_{q^j}(2)) = \frac{\phi(p^i)\phi(q^j)}{(\phi(p^i), \phi(q^j))} \text{ or } \frac{\phi(p^i)\phi(q^j)/2}{(\phi(p^i), \phi(q^j)/2)}.$$

The claim follows now from Lemma 4. \square

Lemma 6. *Assume that $N = p^u q^v$ and $\text{ord}_N(2) = \phi(N)/2$. Then $-1 \notin \langle 2 \rangle$ modulo N if and only if case II or case III is valid:*

II. $p \equiv 1 \pmod{4}$, $\text{ord}_{p^u}(2) = \phi(p^u)$ and $q \equiv 3 \pmod{4}$, $\text{ord}_{q^v}(2) = \phi(q^v)$;

III. $p \equiv 1, 3 \pmod{4}$, $\text{ord}_{p^u}(2) = \phi(p^u)$ and $q \equiv 3 \pmod{4}$, $\text{ord}_{q^v}(2) = \phi(q^v)/2$.

Proof. Denote $o_p = \text{ord}_{p^u}(2)$ and $o_q = \text{ord}_{q^v}(2)$. By changing p and q if necessary our assumption $\text{ord}_N(2) = \phi(N)/2$ implies that one of the following cases is true:

$$\begin{aligned} o_p &= \phi(p^u), & o_q &= \phi(q^v)/2; \\ o_p &= \phi(p^u), & o_q &= \phi(q^v). \end{aligned}$$

Assume that $p \equiv 1 \pmod{4}$. Now, $-1 \in \langle 2 \rangle$ modulo N if and only if $2^m \equiv -1 \pmod{N}$ for some $m \in \mathbb{Z}_+$, or

$$2^m \equiv -1 \pmod{p^u}, \quad 2^m \equiv -1 \pmod{q^v}. \quad (2)$$

Suppose that (2) is solvable. From $2^{2m} \equiv 1 \pmod{q^v}$ we obtain $o_q \mid 2m$. Since $\phi(q^v)/2$ is odd, the equality $o_q = \phi(q^v)/2$ would imply $o_q \mid m$, which is impossible.

If $o_q = \phi(q^v)$, then $m \equiv \phi(q^v)/2 \pmod{\phi(q^v)}$ and $m \equiv \phi(p^u)/2 \pmod{\phi(p^u)}$. Thus $\phi(p^u)\phi(q^v)/4$ and also $\phi(q^v) = o_q$ is a factor of m . This is a contradiction. Thus our lemma is true in the case $p \equiv 1 \pmod{4}$.

Suppose that $p \equiv 3 \pmod{4}$. If $o_q = \phi(q^v)/2$ we have analogously to the above consideration a contradiction with (2). If $o_q = \phi(q^v)$ then $(2^{o_p/2})^{o_q/2} \equiv -1 \pmod{p^u}$ and $(2^{o_q/2})^{o_p/2} \equiv -1 \pmod{q^v}$. Thus the congruences (2) has a solution $k = \phi(N)/4$. \square

Remark. Since 2 is a quadratic residue modulo a prime p' if and only if $p' \equiv \pm 1 \pmod{8}$ we must have $p \equiv 5 \pmod{8}$, $q \equiv 3 \pmod{8}$ in case II, and $p \equiv 5, 3 \pmod{8}$, $q \equiv 7 \pmod{8}$ in case III, by Lemmas 2 and 6.

Our last arithmetical lemma considers the representatives of the cyclotomic cosets into which multiplication by 2 divides the integers modulo N . Let $i, j \in \mathbb{Z}_+$, and let C_i^j denote the cyclotomic coset modulo j defined by i .

Lemma 7. *In index 2 case the representatives of the cyclotomic cosets are*

$$\begin{aligned} 0, \pm p^i, \quad 0 \leq i \leq u-1, & \quad \text{in case I,} \\ 0, \pm p^i q^j, p^u q^j, p^i q^v, \quad 0 \leq i \leq u-1, 0 \leq j \leq v-1, & \quad \text{in case II,} \\ 0, \pm p^i q^j, \pm p^u q^j, p^i q^v, \quad 0 \leq i \leq u-1, 0 \leq j \leq v-1, & \quad \text{in case III.} \end{aligned}$$

Proof. It follows from Lemmas 3 and 6 that the given numbers define different cyclotomic cosets.

Let us consider the case II. It follows from Lemmas 2 and 5 that

$$\begin{aligned} \left| C_{\pm p^i q^j}^N \right| &= \text{ord}_{\frac{N}{p^i q^j}}(2) = \phi\left(\frac{N}{p^i q^j}\right)/2, \\ \left| C_{p^u q^j}^N \right| &= \text{ord}_{q^{v-j}}(2) = \phi(q^{v-j}), \\ \left| C_{p^i q^v}^N \right| &= \text{ord}_{p^{u-i}}(2) = \phi(p^{u-i}). \end{aligned}$$

When i and j run over the given values, $\frac{N}{p^i q^j}$, q^{v-j} and p^{u-i} run over all factors $\neq 1$ of N exactly once. Thus the total number of elements in these classes is

$$\sum_{\substack{d|N \\ d \neq 1}} \phi(d) = N - 1.$$

The proofs of cases I and III are analogous. \square

5. The distribution of the values of $\sum e(\alpha x^N)$

Let D be a divisor of N and $\alpha \in \mathbb{F}_r^*$. Denote $a = \text{ind}_\gamma \alpha$, and $S(a, D) = \sum_{x \in \mathbb{F}_r^*} e(\alpha x^D)$. To use the formula (1) for analyzing $S(a, D)$ we choose $\zeta = \exp(2\pi i/N)$ and normalize the character χ by defining $\chi(\gamma) = \zeta$. It follows from (1) that

$$S(a, D) = \sum_{t=0}^{D-1} G(\chi^{\frac{N}{D}t}) \chi^{-\frac{N}{D}t}(\alpha).$$

As the characters $\chi^{\frac{N}{D}t}$ run over the subgroup of order D of the multiplicative character group of \mathbb{F}_r , we have

$$S(a, D) = \sum_{d|D} \sum_{\substack{1 \leq j \leq d \\ (j,d)=1}} G(\chi^{\frac{N}{d}j}) \chi^{-\frac{N}{d}j}(\alpha) = \sum_{d|D} g(\alpha, d), \quad (3)$$

where $g(\alpha, d) = \sum_{\substack{1 \leq j \leq d \\ (j,d)=1}} G(\chi^{\frac{N}{d}j}) \chi^{-\frac{N}{d}j}(\alpha)$.

Since (3) holds for any divisor D of N , it follows from the Möbius's inversion formula that $g(\alpha, D) = \sum_{d|D} \mu(d) S(a, D/d)$ or

$$S(a, D) = \begin{cases} g(\alpha, D) + S(a, D/p) & \text{in case I,} \\ g(\alpha, D) + S(a, D/p) + S(a, D/q) - S\left(a, \frac{D}{pq}\right) & \text{otherwise.} \end{cases} \quad (4)$$

From now on we assume that $D > 1$. In the case II or III we write $D = p^s q^t$ and suppose that $s, t \geq 1$. By Lemmas 2,5 and 6 we have $\mathbb{Z}_D^* = \langle 2 \rangle \cup -1 \cdot \langle 2 \rangle$. Thus

$$g(\alpha, D) = 2\text{Re}(G(\chi^{\frac{N}{D}})) \sum_{j \in \langle 2 \rangle \subset \mathbb{Z}_D^*} \chi^{-\frac{N}{D}j}(\alpha). \quad (5)$$

Let us study the sum

$$s_D(\alpha) := \sum_{j \in \langle 2 \rangle \subset \mathbb{Z}_D^*} \chi^{-\frac{N}{D}j}(\alpha) = \sum_{j \in \langle 2 \rangle \subset \mathbb{Z}_D^*} \zeta_D^{-aj},$$

where $\zeta_D = \exp(2\pi i/D)$. First we notice that $2\operatorname{Re}(s_D(\alpha))$ is equal to the Ramanujan sum (see [2])

$$c_D(a) = \sum_{j \in \mathbb{Z}_D^*} \zeta_D^{aj} = \mu(D_0)\phi(D)/\phi(D_0), \quad D_0 = D/(D, a). \quad (6)$$

For evaluating the imaginary part of $s_D(\alpha)$ we consider a residueclass character modulo D , say χ_D , defined by

$$\chi_D(j) = \begin{cases} 1 & \text{if } j \in \langle 2 \rangle \subset \mathbb{Z}_D^*, \\ -1 & \text{if } j \notin \langle 2 \rangle \subset \mathbb{Z}_D^*. \end{cases}$$

Since $\chi_D(-1) = -1$ the quadratic Gauss sum $g(\zeta_D^a) := \sum_{j \in \mathbb{Z}_D^*} \chi_D(j)\zeta_D^{aj}$ is equal to $-i2\operatorname{Im}(s_D(\alpha))$.

Denote $a_0 = a/(D, a)$ and $D_0 = D/(D, a)$. By [3, p. 446, p.449 (IV), p.471 (XI)] we have

$$g(\zeta_D^a) = \begin{cases} 0 & \text{if } f \nmid D_0, \\ \frac{\phi(D)}{\phi(D_0)} \mu\left(\frac{D_0}{f}\right) \chi_D\left(\frac{D_0}{f}\right) \chi_D(a_0) \sqrt{-f} & \text{if } f \mid D_0, \end{cases} \quad (7)$$

where f is the conductor of χ_D .

Lemma 8. *In the cases I, II and III f is p , pq or q , respectively.*

Proof. We prove the claim in the cases II and III since the proof of the case I is similar. Let $\epsilon \in \{-1, 1\}$. By Lemmas 5 and 6 the condition $j \in \epsilon \langle 2 \rangle$ modulo pq imply $j \in \epsilon \langle 2 \rangle$ modulo D , and consequently $f \mid pq$.

It is now clear by Lemmas 5 and 6 that the claim holds in case II. In case III we apply similar reasoning to the above to obtain $f = q$. \square

Next we shall study the Gauss sum $G(\chi^{\frac{N}{D}})$ in (5). Since $s_D(\alpha)$ and $G(\chi^{\frac{N}{D}})$ are invariant under the automorphism of $\mathbb{Q}(\zeta)$ defined by $\zeta \mapsto \zeta^2$, they belong to the same subfield of $\mathbb{Q}(\zeta)$. Choosing a to be D/p , $\frac{D}{pq}$ or D/q depending whether the

case in consideration is I, II or III, respectively, it follows from (7) that $G(\chi^{\frac{N}{D}}) \in \mathbb{Q}(\sqrt{-f})$. We can now proceed along the same lines as it is done in [1] and [8] to evaluate Gauss sum $G(\chi^{\frac{N}{D}})$.

In fact, let $S_2(x)$ be the digit sum in the binary expansion of x and denote

$$\begin{aligned} h &= \min\{S_2(t(r-1)/D) \mid 1 \leq t \leq D, (t, D) = 1\} \\ &= \min\{S_2((r-1)/D), lk - S_2((r-1)/D)\}. \end{aligned}$$

According to Stickelberger's theorem [4, Ch. 14] the highest power of 2 dividing $G(\chi^{\frac{N}{D}})$ is 2^h .

Write $G(\chi^{\frac{N}{D}}) = 2^h(b + c\sqrt{-f})/2$, with $b, c \in \mathbb{Z}$, $b \equiv c \pmod{2}$. By the definition of h we have the next implications

$$\begin{aligned} G(\chi^{\frac{N}{D}}) \in \mathbb{R} &\implies (b, c) = (\pm 2, 0) \wedge h = \frac{lk}{2}, \\ G(\chi^{\frac{N}{D}}) \notin \mathbb{R} &\implies b \equiv c \equiv 1 \pmod{2} \wedge h < \frac{lk}{2}. \end{aligned}$$

Assume that $h < lk/2$. By the equation

$$G(\chi^{\frac{N}{D}})\overline{G(\chi^{\frac{N}{D}})} = 2^{2h} \frac{b^2 + fc^2}{4} = 2^{lk}$$

(b, c) is a solution of the Diophantine equation

$$x^2 + fy^2 = 2^{lk-2h+2}. \quad (8)$$

To show that the only solutions (x, y) with $x \equiv y \equiv 1 \pmod{2}$ are $(\pm c, \pm d)$, we use the fact that the ideal (2) is a product of two different prime ideals P_1 and P_2 in the ring of the integers of $\mathbb{Q}(\sqrt{-f})$ (see remark after Lemma 6).

Let (x, y) be a solution of (8). Now

$$\left(\frac{x + y\sqrt{-f}}{2}\right) \left(\frac{x - y\sqrt{-f}}{2}\right) = P_1^m P_2^m, \quad m = lk - 2h.$$

If x and y are odd then P_i , $i = 1, 2$, divides only one of the ideals. To see this we assume that P_1 divides both of them. Now $P_1 \mid (x)$ and therefore $2, x \in P_1$ which is impossible since P_1 is a prime ideal. Thus $((x + y\sqrt{-f})/2) = P_1^m$ and consequently

$$\frac{x + y\sqrt{-f}}{2} = \epsilon \frac{b \pm c\sqrt{-f}}{2},$$

where ϵ is a unit in the ring of the integers of $\mathbb{Q}(\sqrt{-f})$. Since $f > 3$ we have $\epsilon = \pm 1$, and therefore $(x, y) = (\pm c, \pm d)$.

Write $a = Di + j$, $0 \leq i \leq (r-1)/D - 1$, $0 \leq j \leq D - 1$. As $S(a, D) = S(j, D)$ we see that the value of $S(a, D)$ depends only on the residue class of a modulo D . Furthermore, it follows from a basic property of the trace map that $S(a, D) = S(2a, D)$ and therefore the value $S(a, D)$ is attained $(r-1)|C_a^D|/D$ times. From now on we assume that $0 \leq a \leq D - 1$ when are dealing with the sum $S(a, D)$.

We are now able to prove our main theorems concerning the computation of the distribution of the values of exponential sums in the index 2 case.

5.1. CASE I

In this subsection we assume that the case I is valid.

Lemma 9. *The sign of $Re(G(\chi^{\frac{N}{D}}))$ can be determined from the congruence*

$$\phi(D)Re(G(\chi^{\frac{N}{D}})) \equiv -S(0, D/p) \pmod{D}.$$

Proof. Denote $D = p^s$ and choose $a = 0$. It follows from (4) and (5) that

$$S(0, D') = \phi(D')Re(G(\chi^{\frac{N}{D'}})) + S(0, D'/p),$$

for any $D' = p^i$, $1 \leq i \leq s$. Since $D' \mid S(0, D')$ we have

$$\phi(D')Re(G(\chi^{\frac{N}{D'}})) \equiv -S(0, D'/p) \pmod{D'}.$$

Assume that $D' = p$. Now

$$(p-1)Re(G(\chi^{\frac{N}{p}})) \equiv 1 \pmod{p},$$

and this congruence determines the sign of $Re(G(\chi^{\frac{N}{p}}))$ by (8). Consequently we can compute $S(0, p)$.

If $D' = p^2$ then

$$\phi(p^2)Re(G(\chi^{\frac{N}{p^2}})) \equiv -S(0, p) \pmod{p^2},$$

and therefore the sign of $Re(G(\chi^{\frac{N}{p^2}}))$ is determined by (8). Furthermore, we can compute $S(0, p^2)$.

Continuing the process with respect to i , we finally obtain the result. \square

Theorem 2.

$$S(a, D) = \begin{cases} \phi(D) \operatorname{Re}(G(\chi^{\frac{N}{D}})) + S(0, D/p) & \text{if } a = 0, \\ -\frac{D}{p} \operatorname{Re}(G(\chi^{\frac{N}{D}})(1 - \epsilon\sqrt{-p})) + S(0, D/p) & \text{if } a \in C_{\epsilon D/p}^D, \\ S(a, D/p) & \text{if } a \notin C_{\epsilon D/p}^D \text{ and } a \neq 0, \end{cases}$$

where $\epsilon \in \{-1, 1\}$.

Proof. The equalities hold by (4), (6), (7), and by the equality $S(\pm D/p, D/p) = S(0, D/p)$ which is easy to verify. \square

Remark. Starting from $D = p$ we see by Theorem 2, by Lemma 9, and by the fact $|C_a^D| = |C_{-a}^D|$ that we can compute recursively the distribution of the values of $S(a, D)$ for all divisors $D > 1$ of N .

5.2 CASE II (AND CASE III)

In this subsection we assume that case II is valid. Let D' be a factor of N of the form $D' = p^i q^j$, where $i = 0$ or $j = 0$, $i \neq j$. Denote $k' = \operatorname{ord}_{D'}(2)$ and $l' = lk/k'$. Since $-1 \in \langle 2 \rangle$ modulo D' by Lemmas 2 and 6, we obtain from Theorem 1

$$S(a, D') = \begin{cases} (-1)^{l'-1} (D' - 1) \sqrt{r} - 1 & \text{if } D' \mid a, \\ (-1)^{l'} \sqrt{r} - 1 & \text{if } D' \nmid a. \end{cases} \quad (9)$$

Furthermore, it follows from Lemma 2 that l' is even if $i = 0$, and $l' \equiv l \pmod{2}$ if $j = 0$.

Recall that we denoted $D = p^s q^t$, $s, t \geq 1$. Denote $\Sigma(a, D) = S(a, D/p) + S(a, D/q) - S(a, \frac{D}{pq})$.

Lemma 10. *The sign of $\operatorname{Re}(G(\chi^{\frac{N}{D}}))$ can be determined from the congruence*

$$\phi(D) \operatorname{Re}(G(\chi^{\frac{N}{D}})) \equiv -\Sigma(0, D) \pmod{D}.$$

Proof. Choose $a = 0$. It follows from (4) and (5) that

$$S(0, D') = \phi(D') \operatorname{Re}(G(\chi^{\frac{N}{D'}})) + \Sigma(0, D'),$$

for any $D' = p^i q^j$, $1 \leq i \leq s$, $1 \leq j \leq t$, and consequently

$$\phi(D') \operatorname{Re}(G(\chi^{\frac{N}{D'}})) \equiv -\Sigma(0, D') \pmod{D'}.$$

Assume that $D' = pq$. Now

$$(p-1)(q-1) \operatorname{Re}(G(\chi^{\frac{N}{pq}})) \equiv -\Sigma(0, pq) \pmod{pq},$$

and $\Sigma(0, pq)$ can be computed by (9). We conclude by Lemma 4 and (8) that the congruence above determines the sign of $\operatorname{Re}(G(\chi^{\frac{N}{pq}}))$. Consequently we can compute $S(0, pq)$.

Next suppose that $D' = p^2 q$. Now

$$\phi(p^2 q) \operatorname{Re}(G(\chi^{\frac{N}{p^2 q}})) \equiv -\Sigma(0, p^2 q) \pmod{p^2 q}.$$

As we can compute $\Sigma(0, p^2 q)$ the congruence determines the sign of $\operatorname{Re}(G(\chi^{\frac{N}{p^2 q}}))$ by Lemma 4 and (8). We are also able to compute $S(0, p^2 q)$.

Continuing the reasoning above for all pairs (i, j) we finally obtain the result. \square

Lemma 11.

$$S(a, D) = \begin{cases} \phi(D) \operatorname{Re}(G(\chi^{\frac{N}{D}})) + \Sigma(0, D) & \text{if } a = 0, \\ -\frac{\phi(D)}{\phi(p)} \operatorname{Re}(G(\chi^{\frac{N}{D}})) + \Sigma(a, D) & \text{if } a \in C_{D/p}^D, \\ -\frac{\phi(D)}{\phi(q)} \operatorname{Re}(G(\chi^{\frac{N}{D}})) + \Sigma(a, D) & \text{if } a \in C_{D/q}^D, \\ \frac{\phi(D)}{\phi(pq)} \operatorname{Re}(G(\chi^{\frac{N}{D}})(1 + \epsilon \sqrt{-pq})) + \Sigma(a, D) & \text{if } a \in C_{\epsilon \frac{D}{pq}}^D, \\ \Sigma(a, D) & \text{otherwise,} \end{cases}$$

where $\epsilon \in \{-1, 1\}$.

Proof. The claim follows immediately from (4), (6), (7) and from the equalities $C_{D/p}^D = C_{-D/p}^D$ and $C_{D/q}^D = C_{-D/q}^D$, which follow from lemmas 2 and 6. \square

Lemma 12. Let $a = \pm p^i q^j$. If $D \nmid a$ then

$$C_a^D = \begin{cases} C_{p^s q^j}^D & \text{if } i \geq s, \\ C_{p^i q^t}^D & \text{if } j \geq t. \end{cases}$$

Proof. Assume that $i \geq s$. Now $j < t$. Let $a \equiv c2^m \pmod{D}$, where $m \in \mathbb{Z}_+$ and c is chosen to be a representative of the cyclotomic cosets modulo D as in Lemma 7. We see that $p^s q^j \mid c$. Since $j < t$ it follows that $q^j \mid c$ but $q^{j+1} \nmid c$. Thus $c = \pm p^s q^j$. Since $C_{p^s q^j}^D = C_{-p^s q^j}^D$ we obtain the result. The proof of the case $j \geq t$ is similar. \square

Lemma 13.

$$S(a, D) = \begin{cases} -\frac{1}{p-1} \sum_{i=0}^{t-1} \phi(D/q^i) \operatorname{Re}(G(\chi^{\frac{N}{D} q^i})) + S(0, D/p) + (-1)^t p^{s-1} \sqrt{r} & \text{if } a = D/p, \\ -\frac{1}{q-1} \sum_{i=0}^{s-1} \phi(D/p^i) \operatorname{Re}(G(\chi^{\frac{N}{D} p^i})) + S(0, D/q) + q^{t-1} \sqrt{r} & \text{if } a = D/q. \end{cases}$$

Proof. We prove only the case $a = D/p$ as the proof of the second case is quite similar.

As D/p and $\frac{D}{pq}$ divide a we have $S(a, D/p) = S(0, D/p)$ and $S(a, \frac{D}{pq}) = S(0, \frac{D}{pq})$.

It now follows from Lemma 11 that

$$S(a, D) = -\frac{\phi(D)}{p-1} \operatorname{Re}(G(\chi^{\frac{N}{D}})) + S(0, D/p) + S(a, D/q) - S\left(0, \frac{D}{pq}\right). \quad (\text{i})$$

By Lemma 12 we have $S(a, D/q) = S(\frac{D}{pq}, D/q)$. By applying Lemma 11 to $S(\frac{D}{pq}, D/q)$ we now obtain

$$S(a, D/q) = -\frac{\phi(D/q)}{p-1} \operatorname{Re}(G(\chi^{\frac{N}{D} q})) + S\left(0, \frac{D}{pq}\right) + S(a, D/q^2) - S\left(0, \frac{D}{pq^2}\right). \quad (\text{ii})$$

By substituting the expression for $S(a, D/q)$ in (ii) to (i) we obtain

$$S(a, D) = -\frac{\phi(D)}{p-1} \operatorname{Re}(G(\chi^{\frac{N}{D}})) - \frac{\phi(D/q)}{p-1} \operatorname{Re}(G(\chi^{\frac{N}{D} q})) + S(0, D/p) + S(a, D/q^2) - S\left(0, \frac{D}{pq^2}\right).$$

Next consider $S(a, D/q^2)$ and repeat the process to obtain finally

$$S(a, D) = -\frac{1}{p-1} \sum_{i=0}^{t-1} \phi(D/q^i) \operatorname{Re}(G(\chi^{\frac{N}{D} q^i})) + S(0, D/p) + S(a, p^s) - S(0, p^{s-1}).$$

The claim follows now from (9). \square

Theorem 3. $S(a, D)$

$$= \begin{cases} \phi(D) \operatorname{Re}(G(\chi^{\frac{N}{D}})) + S(0, D/p) + S(0, D/q) - S\left(0, \frac{D}{pq}\right) & \text{if } a = 0, \\ -\frac{\phi(D)}{p-1} \operatorname{Re}(G(\chi^{\frac{N}{D}})) + S(0, D/p) + S\left(\frac{D}{pq}, D/q\right) - S\left(0, \frac{D}{pq}\right) & \text{if } a \in C_{D/p}^D, \\ -\frac{\phi(D)}{q-1} \operatorname{Re}(G(\chi^{\frac{N}{D}})) + S\left(\frac{D}{pq}, D/p\right) + S(0, D/q) - S\left(0, \frac{D}{pq}\right) & \text{if } a \in C_{D/q}^D, \\ \frac{D}{pq} \operatorname{Re}(G(\chi^{\frac{N}{D}})(1 + \epsilon\sqrt{-pq})) + S\left(\frac{D}{pq}, D/p\right) + S\left(\frac{D}{pq}, D/q\right) - S\left(0, \frac{D}{pq}\right) & \text{if } a \in C_{\epsilon \frac{D}{pq}}^D, \\ S(a, D/p) & \text{if } a \in C_{\epsilon \frac{D}{p^i q^j}}^D, \\ S(a, D/q) & \text{if } a \in C_{\epsilon \frac{D}{p^j q^i}}^D, \\ S(a, D/p) = S(a, D/q) & \text{otherwise,} \end{cases}$$

where $\epsilon \in \{-1, 1\}$, $i \geq 2$ and $j \in \{0, 1\}$.

Proof. (1) $a = 0$. The equality holds by Lemma 11.

(2) $a = D/p$ or D/q . The equalities hold by Lemma 11, and by the the proof of Lemma 13.

(3) $a = \pm \frac{D}{pq}$. By Lemma 12 $S(-\frac{D}{pq}, D/p) = S(\frac{D}{pq}, D/p)$ and $S(-\frac{D}{pq}, D/q) = S(\frac{D}{pq}, D/q)$. Furthermore, $S(a, \frac{D}{pq}) = S(0, \frac{D}{pq})$, and the equality now holds by Lemma 11.

(4) $a = \pm \frac{D}{p^i q^j}$. Assume first that $D = p^2 q$. Now $a = q$ or ± 1 . It follows from (9) that $S(a, p^2) = S(a, p)$. Thus the claim is true in this case by Lemma 11.

Assume next that $s, t \geq 2$. The equality holds by Lemma 11 if we show that $S(a, D/q) = S(a, \frac{D}{pq})$. Since $S(a, D/q) = S(\frac{D}{p^i q}, D/q)$ and $S(a, \frac{D}{pq}) = S(\frac{D}{p^i q}, \frac{D}{pq})$, by Lemma 12, we may assume that $a = \frac{D}{p^i q}$.

Write

$$S\left(a, \frac{D}{pq}\right) = \frac{D}{pq} \sum_{i=0}^{\frac{r-1}{D/pq}-1} e(\gamma^a \gamma^{\frac{D}{pq} i}) = \frac{D}{pq} \sum_{x \in \langle \gamma^{\frac{D}{pq}} \rangle} e(\gamma^a x).$$

As $\langle \gamma^{\frac{D}{pq}} \rangle = \bigcup_{i=0}^{p-1} \gamma^{\frac{D}{pq} i} \langle \gamma^{D/q} \rangle$, we have

$$S\left(a, \frac{D}{pq}\right) = \frac{D}{pq} \sum_{i=0}^{p-1} \sum_{x \in \langle \gamma^{\frac{D}{q}} \rangle} e(\gamma^{\frac{D}{pq} i + a} x) = \frac{1}{p} \sum_{i=0}^{p-1} S\left(\frac{D}{pq} i + a, D/q\right).$$

Let $\frac{D}{pq}i + a \equiv c2^z \pmod{D/q}$, where $z \in \mathbb{Z}_+$ and c is chosen to be the representative of the cyclotomic cosets modulo D/q as in Lemma 7. Thus $a \equiv c2^z \pmod{\frac{D}{pq}}$, and consequently $a \mid c$. It follows from the preceding congruence that $c = \pm a$. By Lemma 12 we may choose $c = a$, and therefore

$$S\left(a, \frac{D}{pq}\right) = \frac{1}{p} \sum_{i=0}^{p-1} S(a, D/q) = S(a, D/q).$$

(5) $a = \pm \frac{D}{p^j q^i}$. The proof is quite similar as in (4).

(6) Other cases. Now $s, t \geq 2$. By writing $S(a, \frac{D}{pq}) = \frac{D}{pq} \sum_{x \in \langle \gamma \frac{D}{pq} \rangle} e(\gamma^a x)$, and proceeding as in (5) we obtain $a \equiv c2^z \pmod{\frac{D}{pq}}$, with $a = \pm p^m q^n$, $0 \leq m \leq s-2$, $0 \leq n \leq t-2$. Thus $a \mid c$. If $c \nmid a$, we have $p^{m+1} \mid c$ or $q^{n+1} \mid c$. But then, by the preceding congruence, $p^{m+1} \mid a$ or $q^{n+1} \mid a$, a contradiction. Thus $c = \pm a$. If $c = -a$ we have $-1 \equiv 2^z \pmod{p^{s-1-m} q^{t-1-n}}$ which contradicts Lemmas 5 and 6. Thus $S(a, \frac{D}{pq}) = S(a, D/q)$ and therefore $S(a, D) = S(a, D/p)$, by Lemma 11. The equality $S(a, D) = S(a, D/q)$ follows by similar reasoning. \square

Remark. Starting from $D = pq$ we see by Theorem 3, by lemmas 10 and 13, by (9), and by the fact $|C_a^D| = |C_{-a}^D|$ that we can compute recursively the distribution of the values of $S(a, D)$ for all divisors $D = p^s q^t$ of N .

At the end of this section we shall briefly discuss about case III. Let $a = N/p$. It now follows from (4), (6) and (7) that

$$S(a, N) = \frac{\phi(N)}{p-1} \operatorname{Re}(G(\chi)(-1 + (\frac{p}{q})\sqrt{-q})) + S(0, N/p) + S\left(0, \frac{N}{pq}\right),$$

where $(\frac{p}{q})$ is the Legendre symbol.

Thus the method used in the proof of Lemma 13 yields $S(a, N)$ to be equal to the sum of several Gauss sums, each with an ambiguous sign in the imaginary part. So it seems that the method applied to cases I and II is not applicable, at least for general N .

6. Numerical examples

In this section we shall compute the weight distribution of certain trace codes by method developed in previous sections.

Recall that the cardinality of the field we are dealing with was denoted by $r = 2^{kl}$. From now on we assume $l = 1$.

Example 1. Assume that $N = 7^2$. Now $k = \text{ord}_N(2) = 21$ and so the index 2 case holds by results of section 3.

Let $D = 7$. Now $h = 7$ and by (8) we have $G(\chi^{\frac{N}{D}}) = 2^6(b+c\sqrt{-7})$, $b^2+7c^2 = 2^9$. Thus $b = \pm 13, c = \pm 7$. It follows from Lemma 9 that $b = 13$. By Theorem 2 we have

$$S(0, 7) = 2^7 \cdot 39 - 1, \{S(\pm 1, 7)\} = \{2^8 \cdot 9 - 1, -2^7 \cdot 31 - 1\}.$$

Let $D = 49$. Now $h = 10$ and $G(\chi) = 2^9(b+c\sqrt{-7})$, $b^2+7c^2 = 2^3$. Thus $b = \pm 1, c = \pm 1$. It follows that $b = -1$, and so

$$S(0, 49) = -2^7 \cdot 129 - 1, \{S(\pm 7, 49)\} = \{2^7 \cdot 263 - 1, -2^7 \cdot 129 - 1\}, S(\pm 1, 49) = S(\pm 1, 7).$$

Thus we have the following weight distributions for the trace codes $\mathcal{C}_n(7)$, $n = (r-1)/7 = 299593$, and $\mathcal{C}_n(49)$, $n = (r-1)/49 = 42799$, respectively:

W	F	W	F
0	1	0	1
$2^6 \cdot 2335$	1	$2^6 \cdot 337$	4
$2^7 \cdot 1169$	3	$2^6 \cdot 329$	3
$2^6 \cdot 2345$	3	$2^7 \cdot 167$	21
		$2^6 \cdot 335$	21

Where W is the weight of a codeword and F the number of codewords of weight W divided by n .

Example 2. Assume that $N = 5^23^2$. Now $k = \text{ord}_N(2) = 60$ and we have index 2 case.

Let $D = 15$. Now $h = 15$ and $G(\chi^{\frac{N}{D}}) = 2^{14}(b + c\sqrt{-15})$, $b^2 + 15c^2 = 2^{32}$. Thus $b = \pm 39589, c = \pm 13485$. It follows from (9) and lemma 10 that $b = 39589$. By Theorem 3 we have

$$S(0, 15) = 2^{17} \cdot 55973 - 1, \quad S(3, 15) = -2^{15} \cdot 137893 - 1, \quad S(5, 15) = 2^{16} \cdot 42331 - 1, \\ \{S(\pm 1, 15)\} = \{-2^{15} \cdot 81343 - 1, 2^{17} \cdot 30233 - 1\}.$$

Let $N = 45$. Now $h = 25$ and $G(\chi^{\frac{N}{D}}) = 2^{24}(b + c\sqrt{-15})$, $b^2 + 15c^2 = 2^{12}$. Thus $b = \pm 61, c = \pm 5$. It follows that $b = 61$, and so

$$S(0, 45) = 2^{17} \cdot 194213 - 1, \quad S(9, 45) = -2^{15} \cdot 521893 - 1, \\ S(15, 45) = -2^{17} \cdot 13147 - 1, \quad \{S(\pm 3, 45)\} = \{2^{15} \cdot 169307 - 1, -2^{15} \cdot 61093\}, \\ S(5, 45) = S(5, 15), \quad S(\pm 1, 45) = S(\pm 1, 15).$$

Let $N = 75$. Now $h = 27$ and $G(\chi^{\frac{N}{D}}) = 2^{26}(b + c\sqrt{-15})$, $b^2 + 15c^2 = 2^8$. Thus $b = \pm 11, c = \pm 3$. It follows that $b = -11$, and so

$$S(0, 75) = -2^{17} \cdot 5467 - 1, \quad S(15, 75) = 2^{17} \cdot 71333 - 1, \quad S(25, 75) = 2^{16} \cdot 595291 - 1, \\ \{S(\pm 5, 75)\} = \{2^{16} \cdot 134491 - 1, -2^{16} \cdot 326309\}, \quad S(3, 75) = S(3, 15), \\ S(\pm 1, 75) = S(\pm 1, 15).$$

Let $N = 225$. Now $h = 29$ and $G(\chi) = 2^{28}(b + c\sqrt{-15})$, $b^2 + 15c^2 = 2^4$. Thus $b = \pm 1, c = \pm 1$. It follows that $b = 1$, and so

$$S(0, 225) = 2^{17} \cdot 378533 - 1, \quad S(45, 225) = 2^{17} \cdot 148133 - 1, \\ S(75, 225) = -2^{17} \cdot 197467 - 1, \quad \{S(\pm 15, 225)\} = \{2^{17} \cdot 493733 - 1, -2^{17} \cdot 427867 - 1\}, \\ S(9, 225) = S(9, 45), \quad S(25, 225) = S(25, 75), \quad S(\pm 1, 225) = S(\pm 1, 15), \\ S(\pm 3, 225) = S(\pm 3, 45), \quad S(\pm 5, 225) = S(\pm 5, 75).$$

Thus the weight distributions of $\mathcal{C}_n(15)$, $n = (r - 1)/15$, $\mathcal{C}_n(45)$, $n = (r - 1)/45$, $\mathcal{C}_n(75)$, $n = (r - 1)/75$, and $\mathcal{C}_n(225)$, $n = (r - 1)/225$, are respectively

W	F	W	F	W	F	W	F
0	1	0	1	0	1	0	1
$2^{16} \cdot \frac{2^{43}-55973}{15}$	1	$2^{16} \cdot \frac{2^{43}-194213}{45}$	1	$2^{16} \cdot \frac{2^{43}+5467}{75}$	1	$2^{16} \cdot \frac{2^{43}-378533}{225}$	1
$2^{14} \cdot \frac{2^{45}+137893}{15}$	4	$2^{14} \cdot \frac{2^{45}+521893}{45}$	4	$2^{16} \cdot \frac{2^{43}-71333}{75}$	4	$2^{16} \cdot \frac{2^{43}-148133}{225}$	4
$2^{15} \cdot \frac{2^{44}-42331}{15}$	2	$2^{16} \cdot \frac{2^{43}+13147}{45}$	2	$2^{15} \cdot \frac{2^{44}-595291}{75}$	2	$2^{16} \cdot \frac{2^{43}+197467}{225}$	2
$2^{14} \cdot \frac{2^{45}+81343}{15}$	4	$2^{14} \cdot \frac{2^{45}-169307}{45}$	4	$2^{15} \cdot \frac{2^{44}-134491}{75}$	4	$2^{16} \cdot \frac{2^{43}-493733}{225}$	4
$2^{16} \cdot \frac{2^{43}-30233}{15}$	4	$2^{14} \cdot \frac{2^{45}+61093}{45}$	4	$2^{15} \cdot \frac{2^{44}+326309}{75}$	4	$2^{16} \cdot \frac{2^{43}+427867}{225}$	4
		$2^{15} \cdot \frac{2^{44}-42331}{45}$	6	$2^{14} \cdot \frac{2^{45}+137893}{75}$	20	$2^{14} \cdot \frac{2^{45}+521893}{225}$	20
		$2^{14} \cdot \frac{2^{45}+81343}{45}$	12	$2^{14} \cdot \frac{2^{45}+81343}{75}$	20	$2^{15} \cdot \frac{2^{44}-595291}{225}$	6
		$2^{16} \cdot \frac{2^{43}-30233}{45}$	12	$2^{16} \cdot \frac{2^{43}-30233}{75}$	20	$2^{14} \cdot \frac{2^{45}+81343}{225}$	60
						$2^{16} \cdot \frac{2^{43}-30233}{225}$	60
						$2^{14} \cdot \frac{2^{45}-169307}{225}$	20
						$2^{14} \cdot \frac{2^{45}+61093}{225}$	20
						$2^{15} \cdot \frac{2^{44}-134491}{225}$	12
						$2^{15} \cdot \frac{2^{44}+326309}{225}$	12

REFERENCES

1. Baumert L.D. & Mykkeltveit J. (1973) Weight distributions of some irreducible cyclic codes. JPL Tech. Report 32-1526: 128-131.
2. Hardy G. H. & Wright E. M.(1995) An Introduction to the Theory of Numbers. Oxford Science Publications, Oxford.
3. Hasse H. (1964) Vorlesungen über Zahlentheorie. Grudl. der Math. Wiss. Vol. 59. Springer-Verlag, Berlin.
4. Ireland K. & Rosen M. (1982) A Classical Introduction to Modern Number Theory. Grad. Texts in Math. Vol. 84. Springer-Verlag, New York.
5. Lidl R. & Niederreiter H. (1984) Finite Fields. Cambridge Univ. Press, Cambridge.
6. van Lint J. H. (1982) Introduction to Coding Theory. Springer-Verlag, New York.
7. McEliece R.J. (1974) Irreducible cyclic codes and Gauss sums. In: Hall M. Jr. & van Lint J.H. (ed) Combinatorics (Part 1): 179-196. Mathematical Centre Tracts 55, Mathematical Centre, Amsterdam.
8. van der Vlugt M. (1995) Hasse-Davenport curves, Gauss sums, and weight distributions of irreducible cyclic codes. J. Number Theory 55: 145-159.