AIMS Mathematics, 8(7): 15317–15331.
DOI: 10.3934/math.2023783
Received: 03 April 2023
Revised: 19 April 2023
Accepted: 22 April 2023
Published: 26 April 2023

http://www.aimspress.com/journal/Math

Research article

Two classes of two-weight linear codes over finite fields

Jianying Rong[1], **Fengwei Li**[2,*] **and Ting Li**[2]

[1] Jiangsu Vocational College of Electronics and Information, Huai'an 223003, China
[2] School of Mathematics and Statistics, Zaozhuang University, Zaozhuang 277160, China

* **Correspondence:** Email: lfwzzu@126.com.

Abstract: Let $p \equiv 1 \pmod 4$ be a prime, m a positive integer, $\frac{\phi(p^m)}{2}$ the multiplicative order of 2 modulo p^m, and let $q = 2^{\frac{\phi(p^m)}{2}}$, where $\phi(\cdot)$ is the Euler's function. In this paper, we construct two classes of linear codes over $\mathbb{F}_q$ and investigate their weight distributions. By calculating two classes of special exponential sums, the desired results are obtained.

Keywords: exponential sum; cyclotomy; linear code; two-weight code
Mathematics Subject Classification: 11T71, 11T24

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a power of a prime 2. Let $\mathrm{Tr}_{q/2}$ be the trace function from $\mathbb{F}_q$ onto $\mathbb{F}_2$. An $[n, k, d]$ binary linear code C is a k-dimensional subspace of $\mathbb{F}_2^n$ with minimum Hamming distance d. Let $D = \{x_1, x_2, \ldots, x_n\} \subseteq \mathbb{F}_q$. A binary linear code of length n over $\mathbb{F}_2$ is defined by

$$C_D = \{C = (\mathrm{Tr}_{q/2}(bx_i))_{i=1}^n : b \in \mathbb{F}_q\}.$$

If the set D is well chosen, the code C_D may have good parameters. Let A_i be the number of codewords in C_D with Hamming weight i. The weight enumerator of C_D is defined by

$$1 + A_1 z + A_2 z^2 + \cdots + A_l z^l.$$

The sequence $(1, A_1, A_2, \ldots, A_l)$ is called the weight distribution of C_D. It is said to be a t-weight code if the number of nonzero A_i in the sequence $(1, A_1, \ldots, A_l)$ is equal to t.

In coding theory, it is often desirable to know the weight distributions of the codes because they can be used to estimate the error correcting capability and the error probability of error detection and correction with respect to some algorithms. Hence weight distributions of codes are an interesting topic and were investigated in [4, 5, 7–13, 18, 19, 21, 22] etc. Moreover, those codes with few nonzero

weights are of special interest in association schemes, secret sharing schemes, and frequency hopping sequences [2].

In this paper, let p be an odd prime with $p \equiv 1 \pmod 4$, $N = p^m$ a positive integer, $\mathrm{ord}_N(2) = f$, and $q = 2^f$, where $f = \frac{\phi(N)}{2}$ and $\phi(\cdot)$ is the Euler's function. Let α be a primitive element of $\mathbb{F}_q$ and $\beta = \alpha^{\frac{q-1}{N}}$ an N-th primitive root of unity in $\mathbb{F}_q$. We choose

$$D_a = \{x \in \mathbb{F}_q^* : \mathrm{Tr}_{q/2}(ax^{\frac{q-1}{N}}) = 0\}$$

as a defining set of C_{D_a}, and

$$C_{D_a} = \{C = (\mathrm{Tr}_{q/2}(bx))_{x\in D_a} : b \in \mathbb{F}_q\}. \tag{1.1}$$

It is obvious that the dimension of C_{D_a} is $\frac{\phi(N)}{2}$.

For $C \in C_{D_a}$, the Hamming weights of the codeword C with respect to $b \in \mathbb{F}_q$ is denoted by $W_H(C)$.

Denote

$$S(a,b) = \sum_{x\in\mathbb{F}_q^*} (-1)^{\mathrm{Tr}_{q/2}(ax^{\frac{q-1}{N}}+bx)}.$$

The length of C_{D_a} is

$$\begin{aligned} n &= |D_a| = \frac{1}{2}\sum_{x\in\mathbb{F}_q^*}(\sum_{y\in\mathbb{F}_2}(-1)^{\mathrm{Tr}_{q/2}(yax^{\frac{q-1}{N}})}) = \frac{q-1}{2} + \frac{1}{2}\sum_{x\in\mathbb{F}_q^*}(-1)^{\mathrm{Tr}_{q/2}(ax^{\frac{q-1}{N}})} \\ &= \frac{1}{2}(q-1+S(a,0)). \end{aligned} \tag{1.2}$$

If $b = 0$, then $W_H(C) = 0$.

If $b \neq 0$, then $W_H(C) = n - Z(b)$ and

$$\begin{aligned} Z(b) &= |\{x \in \mathbb{F}_q^* : \mathrm{Tr}_{q/2}(ax^{\frac{q-1}{N}}) = 0, \mathrm{Tr}_{q/2}(bx) = 0\}| \\ &= \frac{1}{4}\sum_{x\in\mathbb{F}_q^*}(\sum_{y\in\mathbb{F}_2}(-1)^{\mathrm{Tr}_{q/2}(yax^{\frac{q-1}{N}})}\sum_{z\in\mathbb{F}_2}(-1)^{\mathrm{Tr}_{q/2}(zbx)}) \\ &= \frac{q-1}{4} + \frac{1}{4}\sum_{x\in\mathbb{F}_q^*}(-1)^{\mathrm{Tr}_{q/2}(ax^{\frac{q-1}{N}})} + \frac{1}{4}\sum_{x\in\mathbb{F}_q^*}(-1)^{\mathrm{Tr}_{q/2}(bx)} \\ &\quad + \frac{1}{4}\sum_{x\in\mathbb{F}_q^*}(-1)^{\mathrm{Tr}_{q/2}(ax^{\frac{q-1}{N}}+bx)}. \end{aligned}$$

It is simple to see that $\sum_{x\in\mathbb{F}_q^*}(-1)^{\mathrm{Tr}_{q/2}(bx)} = -1$. Then

$$Z(b) = \frac{1}{4}(q-2+S(a,0)+S(a,b)). \tag{1.3}$$

In order to obtain the length of C_{D_a} and the weight of $C \in C_{D_a}$, we only need to calculate $S(a,0)$ and $S(a,b)$. In general, the exact values of $S(a,0)$ and $S(a,b)$ are hard to calculate, in Section 3, we shall consider two special cases.

This paper is organized as follows. In Section 2, we recall some concepts and several results about Gaussian sums in semi-primitive case. In Sections 3, we focus on the computation of the weight distribution of C_{D_a} defined as (1.1). In Section 4, we make a conclusion.

2. Preliminaries

Let $\mathbb{F}_q$ be a finite field with q elements and α a fixed primitive element of $\mathbb{F}_q$, i.e., $\mathbb{F}_q^* = \langle\alpha\rangle$. For two positive integers $n > 1$ and $N > 1$ with $q - 1 = nN$, define cyclotomic cosets of order N in $\mathbb{F}_q$: $C_i^{(N,q)} = \alpha^i\langle\alpha^N\rangle, i = 0, 1, \ldots, N-1$. The cyclotomic numbers of order N in $\mathbb{F}_q$ are defined as follows:

$$(i, j)_N = |(1 + C_i^{(N,q)}) \cap C_j^{(N,q)}|, 0 \le i \le N-1, 0 \le j \le N-1.$$

When $q = p$ is an odd prime, Lemmas 2.1–2.3 give cyclotomic numbers of order 2, 6 and order 8, respectively.

Lemma 2.1. *[17] If* $p \equiv 1 \pmod 4$*, then* $(0,0)_2 = \frac{p-5}{4}, (0,1)_2 = (1,0)_2 = (1,1)_2 = \frac{p-1}{4}$*. If* $p \equiv 3 \pmod 4$*, then* $(0,1)_2 = \frac{p+1}{4}, (0,0)_2 = (1,0)_2 = (1,1)_2 = \frac{p-3}{4}$.

Lemma 2.2. *[3] Suppose that* $p \equiv 1 \pmod{24}$ *is a prime. Then* $4p = u^2 + 27v^2$*,* $u, v \in \mathbb{Z}$ *and* $u \equiv 1 \pmod 3$*. The possible values for the cyclotomic numbers of order 6 as follows (Table 1):*

Table 1. The cyclotomic numbers of order 6.

$(i, j)_6$	0	1	2	3	4	5
0	(0, 0)	(0, 1)	(0, 2)	(0, 3)	(0, 4)	(0, 5)
1	(0, 1)	(0, 5)	(1, 2)	(1, 3)	(1, 4)	(1, 2)
2	(0, 2)	(1, 2)	(0, 4)	(1, 4)	(2, 4)	(1, 3)
3	(0, 3)	(1, 3)	(1, 4)	(0, 3)	(1, 3)	(1, 4)
4	(0, 4)	(1, 4)	(2, 4)	(1, 3)	(0, 2)	(1, 2)
5	(0, 5)	(1, 2)	(1, 3)	(1, 4)	(1, 2)	(0, 1)

These 10 *fundamental constants* $(0,0), \ldots, (2,4)$ *are given by the relations contained in the following table (Table 2).*

Table 2. The values of cyclotomic numbers of order 6.

	If 2 is a cubic residue of p	If 2 is not a cubic residue of p
$36(0,0)$	$p - 17 + 10u$	$p - 17 - \frac{7u+27v}{2}$
$36(0,1)$	$p - 5 - 2u + 27v$	$p - 5 + \frac{5u+9v}{2}$
$36(0,2)$	$p - 5 - 2u + 9v$	$p - 5 - 2u - 18v$
$36(0,3)$	$p - 5 - 2u$	$p - 5 + \frac{5u+9v}{2}$
$36(0,4)$	$p - 5 - 2u - 9v$	$p - 5 + \frac{5u+9v}{2}$
$36(0,5)$	$p - 5 - 2u - 27v$	$p - 5 - 2u + 18v$
$36(1,2)$	$p + 1 + u$	$p + 1 + u - 9v$
$36(1,3)$	$p + 1 + u$	$p + 1 - \frac{7u-9v}{2}$
$36(1,4)$	$p + 1 + u$	$p + 1 + u - 9v$
$36(2,4)$	$p + 1 + u$	$p + 1 + u + 27v$

Lemma 2.3. *[1, 3] Suppose that* $p \equiv 1 \pmod{16}$ *is a prime. Then* $p = E^2 + 4F^2 = A^2 + 2B^2$, $E, F, A, B \in \mathbb{Z}$ *and* $E \equiv A \equiv 1 \pmod{4}$. *The possible values for the cyclotomic numbers of order 8 as follows (Table 3):*

Table 3. The cyclotomic numbers of order 8.

$(i, j)_8$	0	1	2	3	4	5	6	7
0	(0, 0)	(0, 1)	(0, 2)	(0, 3)	(0, 4)	(0, 5)	(0, 6)	(0, 7)
1	(0, 1)	(0, 7)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	(1, 6)	(1, 2)
2	(0, 2)	(1, 2)	(0, 6)	(1, 6)	(2, 4)	(2, 5)	(2, 4)	(1, 3)
3	(0, 3)	(1, 3)	(1, 6)	(0, 5)	(1, 5)	(2, 5)	(2, 5)	(1, 4)
4	(0, 4)	(1, 4)	(2, 4)	(1, 5)	(0, 4)	(1, 4)	(2, 4)	(1, 5)
5	(0, 5)	(1, 5)	(2, 5)	(2, 5)	(1, 4)	(0, 3)	(1, 3)	(1, 6)
6	(0, 6)	(1, 6)	(2, 4)	(2, 5)	(2, 4)	(1, 3)	(0, 2)	(1, 2)
7	(0, 7)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	(1, 6)	(1, 2)	(0, 1)

These 15 fundamental constants $(0, 0), \ldots, (2, 5)$ *are given by the relations contained in the following table (Table 4).*

Table 4. The values of cyclotomic numbers of order 8.

	If 2 is a quartic residue of p	If 2 is not a quartic residue of p
$64(0, 0)$	$p - 23 - 18E - 24A$	$p - 23 + 6E$
$64(0, 1)$	$p - 7 + 2E + 4A + 16F + 16B$	$p - 7 + 2E + 4A$
$64(0, 2)$	$p - 7 + 6E + 16F$	$p - 7 - 2E - 8A - 16F$
$64(0, 3)$	$p - 7 + 2E + 4A - 16F + 16B$	$p - 7 + 2E + 4A$
$64(0, 4)$	$p - 7 - 2E + 8A$	$p - 7 - 10E$
$64(0, 5)$	$p - 7 + 2E + 4A + 16F - 16B$	$p - 7 + 2E + 4A$
$64(0, 6)$	$p - 7 + 6E - 16F$	$p - 7 - 2E - 8A + 16F$
$64(0, 7)$	$p - 7 + 2E + 4A - 16F - 16B$	$p - 7 + 2E + 4A$
$64(1, 2)$	$p + 1 + 2E - 4A$	$p + 1 - 6E + 4A$
$64(1, 3)$	$p + 1 - 6E + 4A$	$p + 1 + 2E - 4A - 16B$
$64(1, 4)$	$p + 1 + 2E - 4A$	$p + 1 + 2E - 4A + 16F$
$64(1, 5)$	$p + 1 + 2E - 4A$	$p + 1 + 2E - 4A - 16F$
$64(1, 6)$	$p + 1 - 6E + 4A$	$p + 1 + 2E - 4A + 16B$
$64(2, 4)$	$p + 1 - 4E$	$p + 1 + 6E + 8A$
$64(2, 5)$	$p + 1 + 2E - 4A$	$p + 1 - 6E + 4A$

Let q be odd, define the quadratic multiplicative character of $\mathbb{F}_q$ denoted by η as follows: $\eta(c) = 1$ if c is the square element of $\mathbb{F}_q^*$ and $\eta(c) = -1$ otherwise. If q is an odd prime, then for $c \in \mathbb{F}_q^*$, we have $\eta(c) = (\frac{c}{q})$, where $(\frac{\cdot}{q})$ is the Legendre symbol.

Let $\mathrm{Tr}_{q/2}$ be the trace function from $\mathbb{F}_q$ to $\mathbb{F}_2$ defined by $\mathrm{Tr}_{q/2}(x) = x + x^2 + \cdots + x^{q/2}$, $x \in \mathbb{F}_q$, and χ is the canonical additive character of $\mathbb{F}_q$: For $c \in \mathbb{F}_q$, $\chi(c) = (-1)^{\mathrm{Tr}_{q/2}(c)}$. It is a well-known fact that $\sum_{c\in\mathbb{F}_q} \chi(c) = 0$. In the following, we list a useful result, which is called the semi-primitive case.

Lemma 2.4. *[15, Theorem 1] Let $q = 2^{2sd}$ and $N \mid (2^d + 1)$, where s and d are positive integers. Let α be a primitive element of $\mathbb{F}_q$. Then for $a = \alpha^b \in \mathbb{F}_q^*$ and $\mathrm{Ind}_\alpha(a) = b$,*

$$\sum_{x\in\mathbb{F}_q^*}(-1)^{\mathrm{Tr}_{q/2}(ax^N)} = \begin{cases} (-1)^{s-1}(N-1)\sqrt{q}-1, & \text{if } \mathrm{Ind}_\alpha a \equiv 0 \pmod N, \\ (-1)^s\sqrt{q}-1, & \text{if } \mathrm{Ind}_\alpha a \not\equiv 0 \pmod N. \end{cases}$$

Lemma 2.5. *[3] Suppose that p is a prime and $p \equiv 1 \pmod{24}$. Then $p = A^2+3B^2$ and $4p = u^2+27v^2$, where $A, B \in \mathbb{Z}$ and $A \equiv 1 \pmod 3$, $u, v \in \mathbb{Z}, u \equiv 1 \pmod 3$ and $v = \frac{A-B}{3}$.*

3. Main results

In this section, let p be an odd prime with $p \equiv 1 \pmod 4$, $N = p^m$ a positive integer, $\mathrm{ord}_N(2) = f$, and $q = 2^f$, where $f = \frac{\phi(N)}{2}$ and $\phi(\cdot)$ is the Euler's function. We always suppose that α is a primitive element of $\mathbb{F}_q$, $\beta = \alpha^{\frac{q-1}{N}}$ and $\gamma = \beta^{p^{m-1}}$ is a primitive N-th and p-th root of unity in $\mathbb{F}_q$.

Recall that the length of C_{D_a} is equal to

$$n = \frac{1}{2}(q - 1 + S(a, 0))$$

and for $b \in \mathbb{F}_q^*$, the weight $W_H(C), C \in C_{D_a}$ is

$$\begin{aligned} W_H(C) &= n - \frac{1}{4}(q - 2 + S(a, 0) + S(a, b)) \\ &= \frac{1}{4}(q + S(a, 0) - S(a, b)). \end{aligned}$$

The length of C_{D_a} and the weight $W_H(C), C \in C_{D_a}$ is relate to the value $S(a, 0)$ and $S(a, b)$, respectively.

Let $S(a) = \sum_{i=0}^{N-1}(-1)^{\mathrm{Tr}_{q/2}(a\beta^i)}$. Then

$$S(a, 0) = \sum_{x\in\mathbb{F}_q^*}(-1)^{\mathrm{Tr}_{q/2}(ax^{\frac{q-1}{N}})} = \frac{q-1}{N}S(a).$$

Recall that for $b \in \mathbb{F}_q^*$,

$$S(a, b) = \sum_{x\in\mathbb{F}_q^*}(-1)^{\mathrm{Tr}_{q/2}(ax^{\frac{q-1}{N}}+bx)}.$$

Let $H = \langle\alpha^N\rangle$, $\mathbb{F}_q^* = \cup_{i=0}^{N-1}\alpha^i H$. Then

$$\begin{aligned} S(a, b) &= \sum_{x\in\mathbb{F}_q^*}(-1)^{\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}}x^{\frac{q-1}{N}}+x)} \\ &= \sum_{i=0}^{N-1}(-1)^{\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}}\beta^i)}\sum_{h\in H}(-1)^{\mathrm{Tr}_{q/2}(\alpha^i h)} \\ &= \frac{1}{N}\sum_{i=0}^{N-1}(-1)^{\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}}\beta^i)}\sum_{x\in\mathbb{F}_q^*}(-1)^{\mathrm{Tr}_{q/2}(\alpha^i x^N)}. \end{aligned}$$

By $p \equiv 1 \pmod 4$ and Lemma 2.4,

$$\begin{aligned} S(a,b) &= \frac{1}{N}((-1)^{\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}})}((N-1)\sqrt{q}-1)+\sum_{i=1}^{N-1}(-1)^{\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}}\beta^i)}(-\sqrt{q}-1)) \\ &= \sqrt{q}(-1)^{\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}})}-\frac{\sqrt{q}+1}{N}S(ab^{-\frac{q-1}{N}}) \\ &= \sqrt{q}(-1)^{\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}})}-\frac{\sqrt{q}+1}{N}S(a). \end{aligned}$$

In the following, for two cases about $a \in \mathbb{F}_q$, we calculate the values $S(a,0)$ and $S(a,b), b \in \mathbb{F}_q^*$. Let $\mathbb{F}_p^* = \langle\theta\rangle = H_0 \cup H_1$, $H_0 = \langle\theta^2\rangle$ is a subgroup consisting of all square elements of index 2 in $\mathbb{F}_p^*$, and $H_1 = \theta H_0$ consists of all non-square elements in $\mathbb{F}_p^*$. First, we give an lemma.

Lemma 3.1. *[14] Suppose that H_1 is the set consisting of all non-square elements in $\mathbb{F}_p^*$, then for $0 \le i \le N-1$,*

$$\mathrm{Tr}_{q/2}(\beta^i) = \begin{cases} 1, & \text{if } p^{m-1} \| i \text{ and } \frac{i}{p^{m-1}} \in H_1, \\ 0, & \text{otherwise.} \end{cases}$$

Suppose that $r|(p-1)$ and $a = \sum_{j=0}^{r-1}\gamma^{w\zeta_r^j} \in \mathbb{F}_q$, where $\gamma = \beta^{p^{m-1}}$, $w \in \mathbb{F}_p^*$, and ζ_r is a primitive r-th root of unity in $\mathbb{F}_p$.

For $0 \le i \le N-1$, let $i = kp^{m-1}+l$, $0 \le k \le p-1$, $0 \le l \le p^{m-1}-1$. By Lemma 3.1 and note that if $l \ne 0$, then $\mathrm{Tr}_{q/2}(\beta^{(k+w\zeta_r^j)p^{m-1}+l}) = 0$. Then

$$\begin{aligned} S(a) &= \sum_{i=0}^{N-1}(-1)^{\mathrm{Tr}_{q/2}(a\beta^i)} = \sum_{i=0}^{N-1}(-1)^{\mathrm{Tr}_{q/2}(\sum_{j=0}^{r-1}\gamma^{w\zeta_r^j}\beta^i)} \\ &= \sum_{l=0}^{p^{m-1}-1}\sum_{k=0}^{p-1}(-1)^{\mathrm{Tr}_{q/2}(\sum_{j=0}^{r-1}\beta^{(k+w\zeta_r^j)p^{m-1}+l})} \\ &= (p^{m-1}-1)p+\sum_{k=0}^{p-1}(-1)^{\mathrm{Tr}_{q/2}(\sum_{j=0}^{r-1}\gamma^{k+w\zeta_r^j})} = p^m-p+\Omega, \end{aligned} \tag{3.1}$$

where

$$\Omega = \sum_{k=0}^{p-1}(-1)^{\mathrm{Tr}_{q/2}(\sum_{j=0}^{r-1}\gamma^{k+w\zeta_r^j})} = \sum_{x\in\mathbb{F}_p}(-1)^{\sum_{j=0}^{r-1}\mathrm{Tr}_{q/2}(\gamma^{x+w\zeta_r^j})}.$$

Let $W = \{-w, -w\zeta_r, \ldots, -w\zeta_r^{r-1}\}$. By Lemma 3.1 and by the fact that the product of any two square elements or any two non-square elements is a square element and the product of a square element with a non-square element is a non-square element, we can easily check that if $x \in \mathbb{F}_p \setminus W$, then $\sum_{j=0}^{r-1}\mathrm{Tr}_{q/2}(\gamma^{x+w\zeta_r^j})$ and $\mathrm{Tr}_{q/2}(\gamma^{\prod_{j=0}^{r-1}(x+w\zeta_r^j)})$ have the same parity. Then

$$\Omega = \sum_{x\in\mathbb{F}_p\setminus W}(-1)^{\mathrm{Tr}_{q/2}(\gamma^{\prod_{j=0}^{r-1}(x+w\zeta_r^j)})}+\sum_{x\in W}(-1)^{\sum_{j=0}^{r-1}\mathrm{Tr}_{q/2}(\gamma^{x+w\zeta_r^j})}. \tag{3.2}$$

Theorem 3.2. *The notations are as above. Let* $p \equiv 1 \pmod{24}$ *be a prime. Then* $4p = u^2 + 27v^2$, $u, v \in \mathbb{Z}$ *and* $u \equiv 1 \pmod 3$. *Suppose that* $a = \sum_{j=0}^{5} \gamma^{w\zeta_6^j} \in \mathbb{F}_q$.

(1) If $(\frac{2}{p})_3 = 1$, *then*

$$S(a) = p^m - p - 1 + 2u + 6(\frac{w}{p}).$$

(1) If $(\frac{2}{p})_3 \neq 1$, *then*

$$S(a) = p^m - p - 1 - u - 9v + 6(\frac{w}{p}).$$

Proof. By (3.1), we only need to calculate Ω denoted by (3.2). Let

$$\Delta = |\{x \in \mathbb{F}_p \backslash W : \Pi_{j=0}^{5}(x + w\zeta_6^j) = y^2, y \in \mathbb{F}_p\}|,$$

where $W = \{-w, -w\zeta_6, -w\zeta_6^2, -w\zeta_6^3, -w\zeta_6^4, -w\zeta_6^5\}$.

Let $\mathbb{F}_p^* = \langle\theta\rangle$, $C_i^{(2,p)} = \theta^i\langle\theta^2\rangle$, $i = 0, 1$, and $C_i^{(6,p)} = \theta^j\langle\theta^6\rangle$, $j = 0, 1, 2, 3, 4, 5$. It is clear that $C_0^{(2,p)} = C_0^{(6,p)} \cup C_2^{(6,p)} \cup C_4^{(6,p)}$ and $C_1^{(2,p)} = C_1^{(6,p)} \cup C_3^{(6,p)} \cup C_5^{(6,p)}$. For $w \in \mathbb{F}_p^*$, $\Pi_{j=0}^{5}(x + w\zeta_6^j) = x^6 - w^6$. Now we count the number :

$$\begin{aligned}\Delta &= |\{x \in \mathbb{F}_p \backslash W : x^6 - w^6 = y^2, y \in \mathbb{F}_p\}| \\ &= |\{x \in \mathbb{F}_p \backslash W : x^6 - w^6 = y^6 \text{ or } x^6 - w^6 = \gamma^2 y^6, \\ &\quad \text{or } x^6 - w^6 = \gamma^4 y^6, y \in \mathbb{F}_p\}|.\end{aligned}$$

If $x = 0$, then $x^6 - w^6 = y^2$ has a solution $y \in \mathbb{F}_p$, i.e., when $x = 0$, there exists a $y \in \mathbb{F}_p$, but not unique, such that $x^6 - w^6 = y^2$.

If $x \neq 0$, $x^6 - w^6 = y^6$ is equivalent to $1 + (-(\frac{w}{x})^6) = (\frac{y}{x})^6$, then the number of $\frac{w}{x}$ such that $1 + (-(\frac{w}{x})^6) = (\frac{y}{x})^6$ is equal to $|(1 + C_0^{(6,q)}) \cap C_0^{(6,q)}| = (0, 0)_6$ and the number of x such that $x^6 - w^6 = y^6$ is equal to $6(0, 0)_6$. Similarly, the number of x such that $x^6 - w^6 = \gamma^2 y^6$ is equal to $6(0, 2)_6$ and the number of x such that $x^6 - w^6 = \gamma^4 y^6$ is equal to $6(0, 4)_6$.

Suppose that 2 is a cubic residue modulo p, i.e, $(\frac{2}{p})_3 = 1$. By Lemma 2.2,

$$\Delta = 6((0, 0)_6 + (0, 2)_6 + (0, 4)_6) + 1 = \frac{p - 7 + 2u}{2}.$$

Suppose that 2 is not a cubic residue modulo p, i.e., $(\frac{2}{p})_3 \neq 1$. By Lemma 2.2,

$$\Delta = 6((0, 0)_6 + (0, 2)_6 + (0, 4)_6) + 1 = \frac{p - 7 - u - 9v}{2}.$$

Moreover, by $p \equiv 1 \pmod{24}$,

$$\begin{aligned}&(-1)^{\mathrm{Tr}_{q/2}(\gamma^{-w+w\zeta_6}) + \mathrm{Tr}_{q/2}(\gamma^{-w+w\zeta_6^2}) + \mathrm{Tr}_{q/2}(\gamma^{-w+w\zeta_6^3}) + \mathrm{Tr}_{q/2}(\gamma^{-w+w\zeta_6^4}) + \mathrm{Tr}_{q/2}(\gamma^{-w+w\zeta_6^5})} \\ =\ &\eta((-w + w\zeta_6)(-w + w\zeta_6^2)(-w + w\zeta_6^3)(-w + w\zeta_6^4)(-w + w\zeta_6^5)) \\ =\ &\eta(w) = (\frac{w}{p}).\end{aligned}$$

Similarly,

$$(-1)^{\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6+w})+\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6+w\zeta_6^2})+\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6+w\zeta_6^3})+\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6+w\zeta_6^4})+\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6+w\zeta_6^5})} = (\frac{w}{p}),$$

$$(-1)^{\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6^2+w})+\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6^2+w\zeta_6})+\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6^2+w\zeta_6^3})+\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6^2+w\zeta_6^4})+\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6^2+w\zeta_6^5})} = (\frac{w}{p}),$$

$$(-1)^{\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6^3+w})+\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6^3+w\zeta_6})+\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6^3+w\zeta_6^2})+\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6^3+w\zeta_6^4})+\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6^3+w\zeta_6^5})} = (\frac{w}{p}),$$

$$(-1)^{\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6^4+w})+\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6^4+w\zeta_6})+\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6^4+w\zeta_6^2})+\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6^4+w\zeta_6^3})+\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6^4+w\zeta_6^5})} = (\frac{w}{p}),$$

$$(-1)^{\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6^5+w})+\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6^5+w\zeta_6})+\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6^5+w\zeta_6^2})+\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6^5+w\zeta_6^3})+\mathrm{Tr}_{q/2}(\gamma^{-w\zeta_6^5+w\zeta_6^4})} = (\frac{w}{p}).$$

Thus

$$\sum_{x\in W}(-1)^{\sum_{j=0}^{5}\mathrm{Tr}_{q/2}(\gamma^{x+w\zeta_6^j})} = 6(\frac{w}{p}).$$

Note that

$$\begin{aligned}\Omega &= \Delta-(p-6-\Delta)+\sum_{x\in W}(-1)^{\sum_{j=0}^{5}\mathrm{Tr}_{q/2}(\gamma^{x+w\zeta_6^j})}\\ &= 2\Delta-p+6+6(\frac{w}{p}).\end{aligned}$$

Hence

$$S(a) = \begin{cases} p^m-p-1+2u+6(\frac{w}{p}), & \text{if } (\frac{2}{p})_3=1,\\ p^m-p-1-u-9v+6(\frac{w}{p}), & \text{if } (\frac{2}{p})_3\neq 1.\end{cases}$$

□

Theorem 3.3. *The notations are as above. Let* $p\equiv 1 \pmod{16}$ *be a prime. Then* $p=E^2+4F^2=A^2+2B^2$, $E,F,A,B\in\mathbb{Z}$ *and* $E\equiv A\equiv 1 \pmod 4$. *Suppose that* $a=\sum_{j=0}^{7}\gamma^{w\zeta_8^j}\in\mathbb{F}_q$, *then*

$$S(a) = p^m-p-2E-4A-1+8(\frac{w}{p}).$$

Proof. By (3.1), we only need to calculate Ω denoted by (3.2). Let

$$\Delta = |\{x\in\mathbb{F}_p\backslash W : \Pi_{j=0}^{7}(x+w\zeta_8^j)=y^2, y\in\mathbb{F}_p\}|,$$

where $W=\{-w,-w\zeta_8,-w\zeta_8^2,-w\zeta_8^3,-w\zeta_8^4,-w\zeta_8^5,-w\zeta_8^6,-w\zeta_8^7\}$.

Let $\mathbb{F}_p^* = \langle\theta\rangle$, $C_i^{(2,p)} = \theta^i\langle\theta^2\rangle$, $i = 0, 1$, and $C_i^{(8,p)} = \theta^j\langle\theta^8\rangle$, $j = 0, 1, 2, 3, 4, 5, 6, 7$. It is clear that $C_0^{(2,p)} = C_0^{(8,p)} \cup C_2^{(8,p)} \cup C_4^{(8,p)} \cup C_6^{(8,p)}$. For $w \in \mathbb{F}_p^*$, $\Pi_{j=0}^7(x + w\zeta_8^j) = x^8 - w^8$. Now we count the number :

$$\begin{aligned}\Delta &= |\{x \in \mathbb{F}_p \backslash W : x^8 - w^8 = y^2, y \in \mathbb{F}_p\}| \\ &= |\{x \in \mathbb{F}_p \backslash W : x^8 - w^8 = y^8 \text{ or } x^8 - w^8 = \gamma^2 y^8, \\ &\quad \text{or } x^8 - w^8 = \gamma^4 y^8, \text{ or } x^8 - w^8 = \gamma^6 y^8, y \in \mathbb{F}_p\}|.\end{aligned}$$

If $x = 0$, then $x^8 - w^8 = y^2$ has a solution $y \in \mathbb{F}_p$, i.e., when $x = 0$, there exists a $y \in \mathbb{F}_p$, but not unique, such that $x^6 - w^6 = y^2$.

If $x \neq 0$, similar to the discussion of Theorem 3.2, the number of x such that $x^8 - w^8 = y^8$, $x^8 - w^8 = \gamma^2 y^8$, $x^8 - w^8 = \gamma^4 y^8$, and $x^8 - w^8 = \gamma^6 y^8$ is equal to $8(0, 0)_8$, $8(0, 2)_8$, $8(0, 4)_8$, and $8(0, 6)_8$, respectively.

Suppose that $(\frac{2}{p})_4 = 1$ or suppose that $(\frac{2}{p})_4 \neq 1$. By Lemma 2.3,

$$\Delta = 8((0, 0)_8 + (0, 2)_8 + (0, 4)_8 + (0, 6)_8) + 1 = \frac{p - 9 - 2E - 4A}{2}.$$

Moreover, by $p \equiv 1 \pmod{16}$, it is easy to check that if $x \in W$, then

$$(-1)^{\sum_{j=0}^7 \mathrm{Tr}_{q/2}(\gamma^{x+w\zeta_8^j})} = (\frac{w}{p}).$$

Thus

$$\sum_{x\in W}(-1)^{\sum_{j=0}^7 \mathrm{Tr}_{q/2}(\gamma^{x+w\zeta_8^j})} = 8(\frac{w}{p}).$$

Hence

$$\begin{aligned}\Omega &= \Delta - (p - 8 - \Delta) + \sum_{x\in W}(-1)^{\sum_{j=0}^7 \mathrm{Tr}_{q/2}(\gamma^{x+w\zeta_8^j})} \\ &= -2E - 4A - 1 + 8(\frac{w}{p}),\end{aligned}$$

and

$$S(a) = p^m - p - 2E - 4A - 1 + 8(\frac{w}{p}).$$

□

Recall that the length of C_{D_a} defined as (1.1) is equal to $n = \frac{1}{2}(q - 1 + S(a, 0))$ and $S(a, 0) = \frac{q-1}{N}S(a)$. Then the following results are obtained.

Theorem 3.4. *The notations are as Theorem 3.2.*

(1) If $(\frac{2}{p})_3 \neq 1$, then the length of C_{D_a} defined as (1.1) is equal to

$$n = \frac{(q - 1)(2p^m - p + 5 - u - 9v)}{2p^m}.$$

(2) If $(\frac{2}{p})_3 = 1$, then the length of C_{D_a} defined as (1.1) is equal to

$$n = \frac{(q - 1)(2p^m - p + 5 + 2u)}{2p^m}.$$

Theorem 3.5. *The notations are as Theorem 3.3. The length of C_{D_a} defined as (1.1) is equal to*

$$n = \frac{(q-1)(2p^m - p - 2E - 4A - 9)}{2p^m}.$$

Now we return to investigate the weight $W_H(C)$ of $C \in C_{D_a}$.

Theorem 3.6. *Let $p \equiv 1 \pmod{24}$ be a prime. Then $4p = u^2 + 27v^2$, $u, v \in \mathbb{Z}$ and $u \equiv 1 \pmod 3$. Suppose that $a = \sum_{j=0}^{5} \gamma^{w\zeta_6^j} \in \mathbb{F}_q$, where $w \in H_0$.*

(1) If $(\frac{2}{p})_3 \neq 1$, then C_{D_a} defined as (1.1) is a two weight binary linear code with length $\frac{(q-1)(2p^m-p+5-u-9v)}{2p^m}$ and its weight distributions are given by Table 5.

Table 5. Weight distributions of C_{D_a} if $a = \sum_{j=0}^{5} \gamma^{w\zeta_6^j} \in \mathbb{F}_q, w \in H_0$.

weights	frequencies
0	1
$\frac{q}{2} - \frac{\sqrt{q}+q}{4p^m}(p + u + 9v - 5)$	$\frac{(q-1)(2p^m-p+5-u-9v)}{2p^m}$
$\frac{\sqrt{q}+q}{4p^m}(2p^m - p - u - 9v + 5)$	$\frac{(q-1)(p-5+u+9v)}{2p^m}$

(2) If $(\frac{2}{p})_3 = 1$, then C_{D_a} defined as (1.1) is a two weight binary linear code with length $\frac{(q-1)(2p^m-p+5+2u)}{2p^m}$ and its weight distributions are given by Table 6.

Table 6. Weight distributions of C_{D_a} if $a = \sum_{j=0}^{5} \gamma^{w\zeta_6^j} \in \mathbb{F}_q, w \in H_0$.

weights	frequencies
0	1
$\frac{q}{2} - \frac{\sqrt{q}+q}{4p^m}(p - 2u - 5)$	$\frac{(q-1)(2p^m-p+5+2u)}{2p^m}$
$\frac{\sqrt{q}+q}{4p^m}(2p^m - p - 2u - 5)$	$\frac{(q-1)(p-5-2u)}{2p^m}$

Proof. Suppose that $a = \sum_{j=0}^{5} \gamma^{w\zeta_6^j} \in \mathbb{F}_q$, $w \in H_0$. By Theorem 3.2,

$$S(a) = p^m - p - u - 9v + 5.$$

If $b \in \mathbb{F}_q^*$, then

$$\begin{aligned} W_H(C) &= \frac{1}{4}(q + S(a,0) - S(a,b)) \\ &= \frac{1}{4}(q + \frac{q+\sqrt{q}}{N}S(a) - \sqrt{q}(-1)^{\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}})}) \\ &= \begin{cases} \frac{q}{2} - \frac{\sqrt{q}+q}{4p^m}(p + u + 9v - 5), & \text{if } \mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}}) = 0, \\ \frac{\sqrt{q}+q}{4p^m}(2p^m - p - u - 9v + 5), & \text{if } \mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}}) = 1. \end{cases} \end{aligned}$$

We only need to count the number of $b \in \mathbb{F}_q^*$ such that $\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}}) = 0$ or 1. It is clear that $\mathrm{ord}(b^{-\frac{q-1}{N}}) = p^t, 0 \le t \le m$.

If $t \ge 2$, then $\mathrm{ord}(\gamma^{w\zeta_6^j} b^{-\frac{q-1}{N}}) = p^t > p$, where $j = 0, \ldots, 5$. So by Lemma 3.1, $\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}}) = 0$. Moreover, $b = \alpha^{p^{m-t}\mu}$, where $0 < \mu \le \frac{q-1}{p^{m-t}} - 1$ and $\gcd(\mu, p) = 1$. Hence there are $\sum_{t=2}^{m}(\frac{q-1}{p^{m-t}} - \frac{q-1}{p^{m-t+1}}) = q - 1 - \frac{q-1}{p^{m-1}}$ such elements $b \in \mathbb{F}_q^*$ such that $\mathrm{ord}(b^{-\frac{q-1}{N}}) > p$.

If $0 \le t \le 1$, i.e, $b^{-\frac{q-1}{N}} = \gamma^x$, $0 \le x \le p-1$, it is obvious that there are $\frac{q-1}{p^m}$ elements b.

Moreover,

$$(-1)^{\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}})} = (-1)^{\sum_{j=0}^{5}\mathrm{Tr}_{q/2}(\gamma^{x+w\zeta_6^j})}.$$

Suppose that $x \in W = \{-w, -w\zeta_6, -w\zeta_6^2, -w\zeta_6^3, -w\zeta_6^4, -w\zeta_6^5\}$. Then

$$(-1)^{\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}})} = (-1)^{\sum_{j=1}^{5}\mathrm{Tr}_{q/2}(\gamma^{-w+w\zeta_6^j})} = \eta(\Pi_{j=1}^{5}(-w + w\zeta_6^j)) = 1.$$

Hence there are $\frac{6(q-1)}{p^m}$ such elements $b \in \mathbb{F}_q^*$ such that $b^{-\frac{q-1}{N}} = \gamma^x$.

Suppose that $x \in \mathbb{F}_p \setminus W$. Then

$$(-1)^{\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}})} = (-1)^{\sum_{j=0}^{5}\mathrm{Tr}_{q/2}(\gamma^{x+w\zeta_6^j})} = \eta(\Pi_{j=0}^{5}(x + w\zeta_6^j)).$$

By the proof of Theorem 3.2, there are $\Delta = \frac{p-7-u-9v}{2}$ such elements $x \in \mathbb{F}_p \setminus W$ such that $\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}}) = 0$; there are $p - 6 - \Delta = \frac{p-5+u+9v}{2}$ such elements $x \in \mathbb{F}_p \setminus W$ such that $\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}}) = 1$, where $4p = u^2 + 27v^2$, $u, v \in \mathbb{Z}$ and $u \equiv 1 \pmod 3$.

Therefore there are

$$q - 1 - \frac{q-1}{p^{m-1}} + \frac{p+5-u-9v}{2} \cdot \frac{q-1}{p^m} = \frac{(q-1)(2p^m - p + 5 - u - 9v)}{2p^m}$$

elements $b \in \mathbb{F}_q^*$ such that $\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}}) = 0$; there are $\frac{p-5+u+9v}{2} \cdot \frac{q-1}{p^m}$ such elements $b \in \mathbb{F}_q^*$ such that $\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}}) = 1$. Then the Table 5 is given.

Suppose that $(\frac{2}{p})_3 = 1$, we obtain the Table 6 similarly. □

Theorem 3.7. *Let $p \equiv 1 \pmod{16}$ be a prime. Then $p = E^2 + 4F^2 = A^2 + 2B^2$, $E, F, A, B \in \mathbb{Z}$ and $E \equiv A \equiv 1 \pmod 4$. Suppose that $a = \sum_{j=0}^{7}\gamma^{w\zeta_8^j} \in \mathbb{F}_q$, where $w \in H_1$. Then C_{D_a} defined in (1.1) is a two weight binary linear code with length $\frac{(q-1)(2p^m-p-2E-4A-9)}{2p^m}$ and its weight distributions are given by Table 7.*

Table 7. Weight distribution of C_{D_a} if $a = \sum_{j=0}^{7}\gamma^{w\zeta_8^j} \in \mathbb{F}_q, w \in H_1$.

weights	frequencies
0	1
$\frac{q}{2} - \frac{\sqrt{q}+q}{4p^m}(p + 2E + 4A + 9)$	$\frac{(q-1)(2p^m-p-9-2E-4A)}{2p^m}$
$\frac{\sqrt{q}+q}{4p^m}(2p^m - p - 2E - 4A - 9)$	$\frac{(q-1)(p+9+2E+4A)}{2p^m}$

Proof. Suppose that $a = \sum_{j=0}^{7} \gamma^{w\zeta_8^j} \in \mathbb{F}_q$, $w \in H_1$. By Theorem 3.3,

$$S(a) = p^m - p - 2E - 4A - 9.$$

If $b \in \mathbb{F}_q^*$, then

$$\begin{aligned} W_H(C) &= \frac{1}{4}(q + S(a,0) - S(a,b)) \\ &= \frac{1}{4}(q + \frac{q+\sqrt{q}}{N}S(a) - \sqrt{q}(-1)^{\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}})}) \\ &= \begin{cases} \frac{q}{2} - \frac{\sqrt{q}+q}{4p^m}(p + 2E + 4A + 9), & \text{if } \mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}}) = 0, \\ \frac{\sqrt{q}+q}{4p^m}(2p^m - p - 2E - 4A - 9), & \text{if } \mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}}) = 1. \end{cases} \end{aligned}$$

We only need to count the number of $b \in \mathbb{F}_q^*$ such that $\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}}) = 0$ or 1. It is clear that $\mathrm{ord}(b^{-\frac{q-1}{N}}) = p^t, 0 \le t \le m$.

If $t \ge 2$, then $\mathrm{ord}(\gamma^{w\zeta_8^j} b^{-\frac{q-1}{N}}) = p^t > p$, where $j = 0, \ldots, 7$. So by Lemma 3.1, $\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}}) = 0$. Moreover, $b = \alpha^{p^{m-t}\mu}$, where $0 < \mu \le \frac{q-1}{p^{m-t}} - 1$ and $\gcd(\mu, p) = 1$. Hence there are $\sum_{t=2}^{m}(\frac{q-1}{p^{m-t}} - \frac{q-1}{p^{m-t+1}}) = q - 1 - \frac{q-1}{p^{m-1}}$ such elements $b \in \mathbb{F}_q^*$ such that $\mathrm{ord}(b^{-\frac{q-1}{N}}) > p$.

If $0 \le t \le 1$, i.e, $b^{-\frac{q-1}{N}} = \gamma^x$, $0 \le x \le p-1$. it is obvious that there are $\frac{q-1}{p^m}$ elements b.

Moreover,

$$(-1)^{\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}})} = (-1)^{\sum_{j=0}^{7}\mathrm{Tr}_{q/2}(\gamma^{x+w\zeta_8^j})}.$$

Suppose that $x \in W = \{-w, -w\zeta_8, -w\zeta_8^2, -w\zeta_8^3, -w\zeta_8^4, -w\zeta_8^5, -w\zeta_8^6, -w\zeta_8^7\}$. Then

$$(-1)^{\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}})} = (-1)^{\sum_{j=1}^{7}\mathrm{Tr}_{q/2}(\gamma^{-w+w\zeta_8^j})} = \eta(\Pi_{j=1}^{7}(-w + w\zeta_8^j)) = -1.$$

Hence there are $\frac{8(q-1)}{p^m}$ such elements $b \in \mathbb{F}_q^*$ such that $b^{-\frac{q-1}{N}} = \gamma^x$.

Suppose that $x \in \mathbb{F}_p \setminus W$. Then

$$(-1)^{\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}})} = (-1)^{\sum_{j=0}^{7}\mathrm{Tr}_{q/2}(\gamma^{x+w\zeta_8^j})} = \eta(\Pi_{j=0}^{7}(x + w\zeta_8^j)).$$

By the proof of Theorem 3.3, there are $\Delta = \frac{p-9-2E-4A}{2}$ such elements $x \in \mathbb{F}_p \setminus W$ such that $\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}}) = 0$; there are $p - 8 - \Delta = \frac{p-7+2E+4A}{2}$ such elements $x \in \mathbb{F}_p \setminus W$ such that $\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}}) = 1$, where $p = E^2 + 4F^2 = A^2 + 2B^2$, $E, F, A, B \in \mathbb{Z}$ and $E \equiv A \equiv 1 \pmod 4$.

Therefore there are

$$q - 1 - \frac{q-1}{p^{m-1}} + \frac{p-9-2E-4A}{2} \cdot \frac{q-1}{p^m} = \frac{(q-1)(2p^m - p - 9 - 2E - 4A)}{2p^m}$$

such elements $b \in \mathbb{F}_q^*$ such that $\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}}) = 0$; there are $\frac{p+9+2E+4A}{2} \cdot \frac{q-1}{p^m}$ such elements $b \in \mathbb{F}_q^*$ such that $\mathrm{Tr}_{q/2}(ab^{-\frac{q-1}{N}}) = 1$.

The desired result follows. □

In the following, we give some examples.

Example 3.8. *Let* $p = 17$. *Then* C_{D_a} *is an* $[135, 8, 64]$ *two-weight binary linear code with weight enumerator* $1 + 135z^{64} + 120z^{72}$. *The dual is an* $[135, 127, 3]$ *binary linear code and is optimal, due to [6]. The code is also obtained from Theorem 3.2 in [20].*

Example 3.9. *Let* $p = 97$. *Then* $97 \equiv 1 \pmod{24}$ *and* $97 \equiv 1 \pmod{16}$. *By Theorem 3.6 (1),* $4p = 19^2 + 27v^2$, *by Lemma 2.5,* $v = 1$. *By Theorem 3.7,* $p = 9^2 + 4F^2 = 5^2 + 2B^2$, $F^2 = 4$ *and* $B^2 = 36$. *The weight distributions of* C_{D_a} *are given by Table* 8.

Table 8. Weight distributions of C_{D_a} in Theorems 3.6 (1) and 3.7.

Theorem 3.6 (1) $n = \frac{37(2^{48}-1)}{97}$		Theorem 3.7 $n = \frac{25(2^{48}-1)}{97}$	
weights	frequencies	weights	frequencies
0	1	0	1
$2^{47} - \frac{30(2^{24}+2^{48})}{97}$	$\frac{37(2^{48}-1)}{97}$	$2^{47} - \frac{36(2^{24}+2^{48})}{97}$	$\frac{25(2^{48}-1)}{97}$
$\frac{37(2^{24}+2^{48})}{194}$	$\frac{60(2^{48}-1)}{97}$	$\frac{25(2^{24}+2^{48})}{194}$	$\frac{72(2^{48}-1)}{97}$

From the above Table 8, *we can see that the minimum Hamming distance of the line code in Theorems 3.6 (1) is larger than that of in Theorem 3.7.*

Example 3.10. *Let* $p = 193$. *Then* $193 \equiv 1 \pmod{24}$ *and* $193 \equiv 1 \pmod{16}$. *By Theorem 3.6 (1),* $4p = (-23)^2 + 27v^2$, *by Lemma 2.5,* $v = 3$. *By Theorem 3.7,* $p = (-7)^2 + 4F^2 = (-11)^2 + 2B^2$, $F^2 = 36$ *and* $B^2 = 36$. *The weight distributions of* C_{D_a} *are given by Table* 9.

Table 9. Weight distributions of C_{D_a} in Theorems 3.6 (1) and 3.7.

Theorem 3.6 (1) $n = \frac{97(2^{96}-1)}{193}$		Theorem 3.7 $n = \frac{121(2^{96}-1)}{193}$	
weights	frequencies	weights	frequencies
0	1	0	1
$2^{95} - \frac{48(2^{96}+2^{48})}{193}$	$\frac{97(2^{96}-1)}{193}$	$2^{95} - \frac{36(2^{96}+2^{48})}{193}$	$\frac{121(2^{96}-1)}{193}$
$\frac{97(2^{96}+2^{48})}{386}$	$\frac{96(2^{96}-1)}{193}$	$\frac{121(2^{96}+2^{48})}{386}$	$\frac{72(2^{96}-1)}{193}$

From the above Table 9, we can see that the minimum Hamming distance of the line code in Theorems 3.7 is larger than that of in Theorem 3.6.

4. Conclusions

Suppose that $p \equiv 1 \pmod 4$ is a prime and $\frac{\phi(p^m)}{2}$ is the multiplicative order of 2 modulo p^m. Let $q = 2^{\frac{\phi(p^m)}{2}}$, in this paper, we constructed two classes of two-weight linear codes over $\mathbb{F}_q$ and obtained their weight distributions. The main work was the calculations of two classes of exponential sums,

which were special forms of exponential sums defined by Moisio in [16]. The technique that we adopted was to count the number of the square elements by cyclotomic numbers over $\mathbb{F}_p$. By this method, other problems such as cross correlations of sequences and Walsh spectrums of functions can also be investigated.

Acknowledgments

We are very grateful to the reviewers and the editor for their valuable comments and suggestions that much improved the quality of this paper. The work was supported by National Natural Science Foundation of China under Grant 12171420 and Natural Science Foundation of Shandong Province under Grant ZR2021MA046.

Conflict of interest

The authors declare no conflicts of interest.

References

1. K. T. Arasu, C. Ding, T. Helleseth, P. V. Kumar, H. M. Martinsen, Almost difference sets and their sequences with optimal autocorrelation, *IEEE Trans. Inf. Theory*, **47** (2001), 2934–2943. http://dx.doi.org/10.1109/18.959271
2. C. Carlet, C. Ding, J. Yuan, Linear codes from perfect nonlinear mappings and their secret sharing schemes, *IEEE Trans. Inf. Theory*, **51** (2005), 2089–2102. http://dx.doi.org/10.1109/TIT.2005.847722
3. L. E. Dickson, Cyclotomy, higher congruences, and Waring's problem, *Amer. J. Math.*, **57** (1935), 391–424. https://doi.org/10.2307/2371217
4. K. Ding, C. Ding, Binary linear codes with three weights, *IEEE Commun. Lett.*, **18** (2014), 1879–1882. http://dx.doi.org/10.1109/LCOMM.2014.2361516
5. K. Ding, C. Ding, A class of two-weight and three-weight codes and their applications in secret sharing, *IEEE Trans. Inf. Theory,* **61** (2015), 5835–5842. http://dx.doi.org/10.1109/TIT.2015.2473861
6. M. Grassl, *Bounds on the minumum distance of linear codes*, 2022. Avaiable from: `http://www.codetables.de`.
7. Z. Heng, C. Ding, Z. Zhou, Minimal linear codes over finite fields, *Finite Fields Appl.*, **54** (2018), 176–196. https://doi.org/10.1016/j.ffa.2018.08.010
8. Z. Heng, W. Wang, Y. Wang, Projective binary linear codes from special Boolean functions, *AAECC*, **32** (2021), 521–552. https://doi.org/10.1007/s00200-019-00412-z
9. Z. Heng, Q. Yue, A class of binary linear codes with at most three weights, *IEEE Commun. Lett.*, **19** (2015), 1488–1491. http://dx.doi.org/10.1109/LCOMM.2015.2455032
10. Z. Heng, Q. Yue, Two classes of two-weight linear codes, *Finite Fields Appl.*, **38** (2016), 72–92. https://doi.org/10.1016/j.ffa.2015.12.002

11. Z. Heng, Q. Yue, Evaluation of the Hamming weights of a class of linear codes based on Gauss sums, *Des. Codes Cryptogr.*, **83** (2017), 307–326. http://dx.doi.org/10.1007/s10623-016-0222-7
12. Z. Heng, Q. Yue, C. Li, Three classes of linear codes with two or three weights, *Discrete Math.*, **339** (2016), 2832–2847. https://doi.org/10.1016/j.disc.2016.05.033
13. C. Li, Q. Yue, F. Li, Weight distributions of cyclic codes with respect to pairwise coprime order elements, *Finite Fields Appl.*, **28** (2014), 94–114. http://dx.doi.org/10.1016/j.ffa.2014.01.009
14. F. Li, Several classes of exponential sums and three-valued Walsh spectrums over finite fields, *Finite Fields Appl.*, **87** (2023), 102142. https://doi.org/10.1016/j.ffa.2022.102142
15. M. Moisio, A note on evaluations of some exponential sums, *Acta Arith.*, **93** (2000), 117–119. https://doi.org/10.4064/aa-93-2-117-119
16. M. Moisio, Explicit evaluation of some exponential sums, *Finite Fields Appl.*, **15** (2009), 644–651. https://doi.org/10.1016/j.ffa.2009.05.005
17. T. Storer, *Cyclotomic and difference sets*, Markham, Chicago, 1967.
18. Q. Wang, K. Ding, D. D. Lin, R. Xue, A kind of three-weight linear codes, *Cryptogr. Commun.*, **9** (2017), 315–322. http://dx.doi.org/10.1007/s12095-015-0180-3
19. Q. Wang, K. Ding, R. Xue, Binary linear codes with two weights, *IEEE Commun. Lett.*, **19** (2015), 1097–1100. https://doi.org/10.1109/LCOMM.2015.2431253
20. Y. Wu, Q. Yue, X. Shi, At most three-weight binary linear codes from generalized Moisio's exponential sums, *Des. Codes Cryptogr.*, **87** (2019), 1927–1943. https://doi.org/10.1007/s10623-018-00595-5
21. Z. Zhou, C. Ding, J. Luo, A. Zhang, A family of five-weight cyclic codes and their weight enumerators, *IEEE Trans. Inf. Theory*, **59** (2013), 6674–6682. http://dx.doi.org/10.1109/TIT.2013.2267722
22. Z. Zhou, A. Zhang, C. Ding, M. Xiong, The weight enumerator of three families of cyclic codes, *IEEE Trans. Inf. Theory*, **59** (2013), 6002–6009. http://dx.doi.org/10.1109/TIT.2013.2262095

AIMS Press