Des. Codes Cryptogr. (2018) 86:1007–1022
https://doi.org/10.1007/s10623-017-0374-0

# Four classes of linear codes from cyclotomic cosets

**Dabin Zheng**[1] · **Jingjun Bao**[2]

Received: 8 October 2016 / Revised: 12 March 2017 / Accepted: 8 June 2017 /
Published online: 20 June 2017

**Abstract** This paper presents four classes of linear codes from coset representatives of subgroups and cyclotomic coset families of certain finite field, and determines their weight enumerators. These linear codes may have applications in consumer electronics, communications and secret sharing schemes.

**Keywords** Linear code · Cyclic code · Weight distribution · Gauss sum

**Mathematics Subject Classification** 11T71 · 94B15

## 1 Introduction

Let $q$ be a power of a prime $p$ and $\mathbb{F}_q$ be a finite field of size $q$. An $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_q$ is a $k$-dimensional subspace of $\mathbb{F}_q^n$ with minimum distance $d$. Let $A_i$ denote the number of codewords with Hamming weight $i$ in $\mathcal{C}$. The weight enumerator of $\mathcal{C}$ is defined by $1 + A_1x + A_2x^2 + \cdots + A_nx^n$. The weight distribution of a code not only gives the error correcting ability of the code, but also allows the computation of the probability of error detection and correction [12]. So the study of the weight distributions of linear codes is important in both theory and applications.

Communicated by Q. Xiang.

✉ Jingjun Bao
baojingjun@hotmail.com

Dabin Zheng
dzheng@hubu.edu.cn

[1] Hubei Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University, Wuhan 430062, China

[2] Department of Mathematics, Ningbo University, Ningbo 315211, China

Let $\mathbb{F}_{q^m}$ be a finite field with $q^m$ elements. Note that $\mathbb{F}_{q^m}$ is the unique degree $m$ extension of $\mathbb{F}_q$. Let $\mathrm{Tr}_q^{q^m}$ be the trace function from $\mathbb{F}_{q^m}$ onto $\mathbb{F}_q$. From a subset $D = \{d_1, d_2, \ldots, d_n\} \subset \mathbb{F}_{q^m}$, we define a class of generic linear code of length $n = |D|$ over $\mathbb{F}_q$ as follows:

$$\mathcal{C}_D = \left\{\mathbf{c}_y = \left(\mathrm{Tr}_q^{q^m}(yd_1), \mathrm{Tr}_q^{q^m}(yd_2), \ldots, \mathrm{Tr}_q^{q^m}(yd_n)\right) : y \in \mathbb{F}_{q^m}\right\}. \tag{1}$$

The dimension of $\mathcal{C}_D$ equals the dimension of the vector space $V_D$ generated by $d_1, d_2, \ldots, d_n \in \mathbb{F}_{q^m}$ over $\mathbb{F}_q$ [5]. If $e = dim_{\mathbb{F}_q} V_D < m$, then $\mathcal{C}_D$ has repeated codewords and each codeword repeats $q^{m-e}$ times. If $e = m$ then each codeword occurs once. One may get different codes $\mathcal{C}_D$ from different orderings of the elements of $D$, but these codes are permutation equivalent and have the same lengths, dimensions and weight distributions. Hence, the orderings of the elements of $D$ will not affect the results in this correspondence.

Let $\zeta_p$ be a primitive $p$-th root of an unity, and let

$$\chi_m(y) = \zeta_p^{\mathrm{Tr}_p^{q^m}(y)} \quad \text{and} \quad \chi(y) = \zeta_p^{\mathrm{Tr}_p^{q}(y)}$$

be canonical additive characters over $\mathbb{F}_{q^m}$ and $\mathbb{F}_q$, respectively. For a codeword $\mathbf{c}_y$ in $\mathcal{C}_D$, its Hamming weight is equal to

$$\begin{aligned} wt(\mathbf{c}_y) &= n - |\{1 \le i \le n : \mathrm{Tr}_q^{q^m}(yd_i) = 0\}| \\ &= n - \frac{1}{q}\sum_{d\in D}\sum_{z\in\mathbb{F}_q}\chi\left(z\mathrm{Tr}_q^{q^m}(dy)\right) \\ &= \frac{(q-1)n}{q} - \frac{1}{q}\sum_{d\in D}\sum_{z\in\mathbb{F}_q^*}\chi_m(zdy). \end{aligned} \tag{2}$$

From (2) the weight distribution of $\mathcal{C}_D$ is directly derived from the value distribution of the exponential sum over the subsets $\mathbb{F}_q^* Dy$ of $\mathbb{F}_{q^m}^*$ for $y \in \mathbb{F}_{q^m}$. If the set $D$ is well chosen, $\mathcal{C}_D$ may have good parameters. This construction technique was employed in [5,7] for obtaining linear codes with only a few weights. Following this generic construction, in the past three years, many authors present works [2–4,9–11,14,15,20,21,24] on constructions of linear codes with few weights. Along this line we will give four classes of linear codes with a defining set from representatives of coset decomposition of subgroups or cyclotomic cosets families of some finite fields. By using some combinatorial techniques and Gauss sums with index 2 case, we determine the weight distributions of these linear codes.

The rest of the paper is organized as follows. Section 2 recalls the theory of Gauss sums over finite fields. Section 3 presents a class of linear codes from coset representatives of some subgroup of $\mathbb{F}_q^*$, and determines their weight distributions. In Sect. 4 we give three classes of cyclic codes from cyclotomic cosets and determine their weight distributions. Section 5 concludes this paper.

## 2 Gauss sums

Let $\mathbb{F}_{q^m}$ be a finite field with $q^m$ elements, where $q$ is a power of a prime $p$. The canonical additive character $\chi_m$ over $\mathbb{F}_{q^m}$ is defined by

$$\chi_m(y) = \zeta_p^{\mathrm{Tr}_p^{q^m}(y)},$$

where $\zeta_p$ is a primitive $p$-th root of an unity and $\mathrm{Tr}_p^{q^m}(\cdot)$ is the trace function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_p$. As $m = 1$ the $\chi_1$ is the canonical additive character over $\mathbb{F}_q$, and we denote it by $\chi$ for short. The additive characters have the following orthogonal property,

$$\sum_{y \in \mathbb{F}_q} \chi(ay) = \begin{cases} q, & \text{if } a = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Let $\psi$ be a multiplicative character of $\mathbb{F}_q^*$. The Gauss sum over $\mathbb{F}_q$ is defined by

$$g(\psi) = \sum_{y \in \mathbb{F}_q^*} \psi(y)\chi(y).$$

Gauss sums can be viewed as the Fourier coefficients in the Fourier expansion of $\psi|_{\mathbb{F}_q^*}$ in terms of the multiplicative characters of $\mathbb{F}_q^*$.

**Lemma 1** (see [16]) *Let $q$ be a prime power, $\chi$ the canonical additive character of $\mathbb{F}_q$ is defined by $\chi(y) = \zeta_p^{\mathrm{Tr}_p^q(y)}$, where $y \in \mathbb{F}_q$. And let $\psi$ be a multiplicative character of $\mathbb{F}_q$. Then, for every $y \in \mathbb{F}_q^*$,*

$$\chi(y) = \frac{1}{q-1} \sum_{\psi \in \widehat{\mathbb{F}}_q^*} g(\bar{\psi})\psi(y),$$

*where $\bar{\psi} = \psi^{-1}$ and $\widehat{\mathbb{F}}_q^*$ denotes the character group of $\mathbb{F}_q^*$.*

In general, the explicit evaluation of Gauss sums is very difficult. There are only a few cases where the Gauss sums have been evaluated [13,17,18]. We state here some results in the index 2 case which will be used in our constructions. Below we use $\phi(N)$ to denote the number of integers $k$ with $0 < k \leq N$ such that $\gcd(k, N) = 1$ and $ord_N(p)$ to denote the order of $p$ modulo $N$, which is the smallest positive integer $f$ such that $p^f \equiv 1 \pmod N$.

**Lemma 2** ([22], Theorem 4.12) *Let $N = 2p_1^m$, where $m$ is a positive integer, and $p_1 > 3$ is a prime such that $p_1 \equiv 3 \pmod 4$. Assume that $p$ is a prime such that $[\mathbb{Z}_N^* : \langle p \rangle] = 2$. Let $f = \phi(N)/2$, $q = p^f$, and let $\psi$ be a multiplicative character of order $N$ of $\mathbb{F}_q$. Then for $0 \leq t < m$ we have*

$$g(\psi^{p_1^t}) = \begin{cases} (-1)^{\frac{p-1}{2}(m-1)} p^{\frac{f-1}{2} - hp_1^t} \sqrt{p^*} \left(\frac{b+c\sqrt{-p_1}}{2}\right)^{2p_1^t}, & \text{if } p_1 \equiv 3 \pmod 8, \\ (-1)^{\frac{p-1}{2}m} p^{\frac{f-1}{2}} \sqrt{p^*}, & \text{if } p_1 \equiv 7 \pmod 8. \end{cases}$$

$$g(\psi^{2p_1^t}) = p^{\frac{f-p_1^t h}{2}} \left(\frac{b+c\sqrt{-p_1}}{2}\right)^{p_1^t};$$

$$g(\psi^{p_1^m}) = (-1)^{\frac{p-1}{2}\frac{f-1}{2}} p^{\frac{f-1}{2}} \sqrt{p^*},$$

*where $p^* = (-1)^{\frac{p-1}{2}} p$, and $h$ is the class number of $\mathbb{Q}(\sqrt{-p_1})$, and $b$, $c$ are integers determined by $4p^h = b^2 + p_1 c^2$ and $bp^{\frac{f-h}{2}} \equiv -2 \pmod{p_1}$.*

**Lemma 3** ([22], Theorem 4.10) *Let $N = p_1^{m_1} p_2^{m_2}$, where $m_1, m_2$ are positive integers, $p_1, p_2$ are primes such that $p_1 \equiv 3 \pmod 4$ and $p_2 \equiv 1 \pmod 4$. Assume that $p$ is a prime such that $[\mathbb{Z}_N^* : \langle p \rangle] = 2$, $ord_{p_1^{m_1}}(p) = \phi(p_1^{m_1})$ and $ord_{p_2^{m_2}}(p) = \phi(p_2^{m_2})$. Let*

*$f = \phi(N)/2, q = p^f$, and $\psi$ be a multiplicative character of order $N$ of $\mathbb{F}_q$. Then for $0 \le s < m_1$ and $0 \le t < m_2$, we have*

$$g(\psi^{p_1^s p_2^t}) = p^{\frac{1}{2}(f-h_{12}p_1^s p_2^t)} \left(\frac{b+c\sqrt{-p_1p_2}}{2}\right)^{p_1^s p_2^t},$$
$$g(\psi^{p_1^{m_1} p_2^t}) = p^{\frac{f}{2}};$$
$$g(\psi^{p_1^s p_2^{m_2}}) = -p^{\frac{f}{2}},$$

*where $h_{12}$ is the class number of $\mathbb{Q}(\sqrt{-p_1p_2})$, and $b$, $c$ are integers determined by $b, c \not\equiv 0 \pmod{p}$, $4p^{h_{12}} = b^2 + p_1p_2c^2$ and $b \equiv 2p^{\frac{1}{2}h_{12}} \pmod{p_1}$.*

**Lemma 4** ([22], Theorem 4.14) *Let $N = 4p_1^m$, where $m$ is a positive integer, and $p_1$ is a prime such that $p_1 \equiv 1 \pmod{4}$. Assume that $p$ is a prime such that $p \equiv 3 \pmod{4}$, $[\mathbb{Z}_N^* : \langle p\rangle] = 2$ and $\mathrm{ord}_{p_1^m}(p) = \phi(p_1^m)$. Let $f = \phi(N)/2, q = p^f$, and let $\psi$ be a multiplicative character of order $N$ of $\mathbb{F}_q$. Then for $0 \le s < m$ we have*

$$g(\psi^{p_1^s}) = p^{\frac{f}{4}}(b + c\sqrt{p_1})^{p_1^s},$$
$$g(\psi^{p_1^m}) = g(\psi^{2p_1^s}) = g(\psi^{2p_1^m}) = -p^{\frac{f}{2}};$$
$$g(\psi^{4p_1^s}) = p^{\frac{f}{2}},$$

*where $b$, $c$ are integers determined by $p^{\frac{f}{2}} = b^2 + p_1c^2$ and $b \equiv -p^{\frac{f}{4}} \pmod{p_1}$.*

## 3 A class of linear codes from coset representatives of some subgroup of $\mathbb{F}_q^*$

Let $G$ be a subgroup of $\mathbb{F}_q^*$ with order $\lambda$. Then $\lambda|(q-1)$ and $\lambda|(q^m-1)$. Let $\alpha$ be a primitive element of $\mathbb{F}_{q^m}$, then $\beta = \alpha^{\frac{q^m-1}{q-1}}$ is a primitive element of $\mathbb{F}_q$. It is clear that $\mathbb{F}_{q^m}^*$ has the following coset decomposition,

$$\mathbb{F}_{q^m}^* = \bigcup_{i=0}^{\frac{q^m-q}{q-1}} \alpha^i \mathbb{F}_q^* = \bigcup_{i=0}^{\frac{q^m-q}{q-1}} \bigcup_{j=0}^{\frac{q-\lambda-1}{\lambda}} \alpha^i \beta^j G. \qquad (3)$$

In this section we will study a class of linear codes over $\mathbb{F}_q$ as follows,

$$\mathcal{C}_D = \left\{ c_y = (\mathrm{Tr}_q^{q^m}(yd_1), \mathrm{Tr}_q^{q^m}(yd_2), \ldots, \mathrm{Tr}_q^{q^m}(yd_n)) : y \in \mathbb{F}_{q^m} \right\}, \qquad (4)$$

where $D = \{d_1, d_2, \ldots, d_n\} \subset \mathbb{F}_{q^m}$ is a defining set. By choosing proper coset representatives in (3) as the defining set $D$, we can obtain linear codes $\mathcal{C}_D$ with only few weights. To this end, we introduce some preliminary lemmas.

**Lemma 5** *Let $k$ be a positive integer with $k \le m$, and let $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$. Denote by*

$$V_i = \{y \in \mathbb{F}_{q^m} \mid \mathrm{Tr}_q^{q^m}(\alpha_i y) = 0\},\ i = 1, 2, \ldots, k.$$

*Let $I$ and $J$ be subsets of $\{1, 2, \ldots, k\}$ such that $I \cap J = \emptyset$ and $I \cup J = \{1, 2, \ldots, k\}$. Let $S_I = \bigcap_{i \in I} V_i$ and $S_\emptyset = \mathbb{F}_{q^m}$. Then*

$$\mid S_I \backslash (\bigcup_{j \in J} V_j) \mid = q^{m-k}(q-1)^{k-|I|}.$$

*Proof* It is clear that $|I|+|J|=k$, and $|S_I|=q^{m-|I|}$. Let $A_j=S_I\cap V_j$ for $j\in J$.

$$\begin{aligned}
&\mid S_I\backslash(\underset{j\in J}{\cup}V_j)\mid = \mid S_I\mid - \mid \underset{j\in J}{\cup}A_j\mid\\
&=q^{m-|I|}-\left(\sum_{j\in J}|A_j|-\sum_{j_1<j_2}|A_{j_1}\cap A_{j_2}|+\cdots+(-1)^{|J|-1}|\underset{j\in J}{\cap}A_j|\right)\\
&=q^{m-|I|}-\binom{|J|}{1}q^{m-|I|-1}+\binom{|J|}{2}q^{m-|I|-2}+\cdots+(-1)^{|J|}\binom{|J|}{|J|}q^{m-|I|-|J|}\\
&=q^{m-k}(q-1)^{|J|}=q^{m-k}(q-1)^{k-|I|}.
\end{aligned}$$

□

**Lemma 6** *Let $D_k$ be a set with $k$ elements in $\mathbb{F}_{q^m}$ which are linearly independent over $\mathbb{F}_q$. Let $\chi_m$ be the canonical additive character over $\mathbb{F}_{q^m}$. For $y$ running through $\mathbb{F}_{q^m}$, the value distribution of the exponential sum*

$$S_{D_k}(y)=\sum_{d\in D_k}\sum_{z\in\mathbb{F}_q^*}\chi_m(zdy)$$

*is as follows,*

| Values | Frequency |
|---|---|
| $iq-k$ | $q^{m-k}\binom{k}{i}(q-1)^{k-i},\quad i=0,1,\ldots,k$ |

*Proof* It is clear that

$$\begin{aligned}
S_{D_k}(y)&=\sum_{d\in D_k}\sum_{z\in\mathbb{F}_q^*}\chi_m(dzy)\\
&=\sum_{d\in D_k}\sum_{z\in\mathbb{F}_q^*}\chi\left(\mathrm{Tr}_q^{q^m}(dy)z\right),
\end{aligned}$$

where $\chi$ is the canonical additive character on $\mathbb{F}_q$. With notations introduced in Lemma 5 we set $\Delta_{IJ}=S_I\backslash(\cup_{j\in J}V_j)$. If $y\in\Delta_{IJ}$ with $|I|=i$, then

$$S_{D_k}(y)=i(q-1)-(k-i)=iq-k.$$

Moreover, the number of such $y$ is $\binom{k}{i}|\Delta_{IJ}|$ for $|I|=i$, and by Lemma 5 it equals $\binom{k}{i}q^{m-k}(q-1)^{k-i}$. □

Let $\alpha$ and $\beta$ be as in (3), and $T=\{\beta^j,\beta^j\alpha,\ldots,\beta^j\alpha^{\frac{q^m-q}{q-1}}\}$ for some $j$ with $0\le j\le\frac{q-1}{\lambda}-1$. Let $D_n$ with $1\le n\le m$ be a $n$-subset of $T$, and elements in $D_n$ are linearly independent over $\mathbb{F}_q$.

**Theorem 1** *With notations as above, we have*

(1) *If $D=T$, then $\mathcal{C}_D$ is a one-weight code with parameters $[\frac{q^m-1}{q-1},m,q^{m-1}]$.*
(2) *If $D=D_n$, then $\mathcal{C}_D$ is an [n, n, 1] code with the weight enumerator as follows,*

$$\sum_{i=0}^{n}\binom{n}{i}(q-1)^{n-i}x^{n-i}.$$

(3) *If* $D = T\backslash D_n$ *and* $q^m > 4$, *then* $\mathcal{C}_D$ *is a* $[\frac{q^m-1}{q-1} - n, m, q^{m-1} - n]$ *code with the weight enumerator as follows,*

$$1 + \sum_{i=0}^{n-1} q^{m-n} \binom{n}{i} (q-1)^{n-i} x^{q^{m-1}+i-n} + (q^{m-n} - 1)x^{q^{m-1}}.$$

*Proof* (1) When $D = \{\beta^j, \beta^j\alpha, \ldots, \beta^j\alpha^{\frac{q^m-q}{q-1}}\}$, we have $\mathbb{F}_{q^m}^* = D\mathbb{F}_q^*$. For $y \in \mathbb{F}_{q^m}^*$,

$$S_D(y) = \sum_{d \in D} \sum_{z \in \mathbb{F}_{q^*}} \chi(dzy) = \sum_{z' \in \mathbb{F}_{q^m}^*} \chi(z'y) = -1.$$

It is clear that the dimension of $\mathcal{C}_D$ is $m$ and it has a constant weight $q^{m-1}$ from equation (2).

(2) When $D = D_n$, from equation (2) and Lemma 6 we can easily get the weight enumerator. Since $n$ elements in $D$ are linearly independent over $\mathbb{F}_q$ we know that the dimension of $\mathcal{C}_D$ is $n$.

(3) When $D = T\backslash D_n$, for $y \in \mathbb{F}_{q^m}^*$ we have

$$\begin{aligned} S_D(y) &= \sum_{d \in D} \sum_{z \in \mathbb{F}_{q^*}} \chi_m(dzy) \\ &= \sum_{z' \in \mathbb{F}_{q^m}^*} \chi_m(z'y) - \sum_{d \in D_n} \sum_{z \in \mathbb{F}_{q^*}} \chi\left(\mathrm{Tr}_q^{q^m}(dzy)\right) \\ &= -1 - S_{D_n}(y). \end{aligned}$$

By (2) and Lemma 6 we get the weight enumerator of $\mathcal{C}_D$.

*Remark 1* Let $E$ be a subset of $\mathbb{F}_q^*$, and $ED = \{ed \mid e \in E, d \in D\}$ where $D$ is introduced in Theorem 1. For each case in Theorem 1, if choose $ED$ as a new defining set we get new linear codes with longer codewords. This result also can be derived from Theorem 1 in [21].

*Remark 2* When $|D_n|$ is small, and $D = T\backslash D_n$, from (3) of Theorem 1 we get linear codes $\mathcal{C}_D$ with only few weights. Moreover, the code constructed in (3) of Theorem 1 has minimum nonzero weight $w_{min} = q^{m-1} - n$ and maximum weight $w_{max} = q^{m-1}$, and so it satisfies that $w_{min}/w_{max} > \frac{q-1}{q}$ whenever $n < q^{m-2}$. Thus the code can be employed to obtain secret sharing schemes with interesting access structures using the framework in [23].

*Example 1* Using the primitive polynomial $f(x) = x^3 + x^2 - x + 1 \in \mathbb{F}_3[x]$, we construct the $\mathbb{F}_{3^3}$ as $\mathbb{F}_3[\alpha]$ where $f(\alpha) = 0$. Let $D = \{1, \alpha\}$ be a defining set. Then each codeword in $\mathcal{C}_D$ repeats once and its weight enumerator of the irreducible cyclic code $\mathcal{C}_D$ defined by (4) is

$$1 + 4x^1 + 4x^2.$$

This is confirmed by Magma.

## 4 Three classes of linear codes from cyclotomic cosets

In this section, we investigate the weight distribution of linear codes with a defining set from some cyclotomic cosets, and their Hamming weights of the codewords can be expressed by Gauss sums with index 2 case.

Let $N$ be a divisor of $q-1$ and $\beta$ a fixed primitive element of $\mathbb{F}_q$. Define $C_i^{(N,q)} = \beta^i \langle \beta^N \rangle$ for $i = 0, 1, \ldots, N-1$, where $\langle \beta^N \rangle$ is a subgroup of $\mathbb{F}_q^*$ generated by $\beta^N$. Let $\mathcal{C}_D$ be a linear code as follows,

$$\mathcal{C}_D = \left\{ \mathbf{c}_x = (\mathrm{Tr}_p^q(xd_1), \mathrm{Tr}_p^q(xd_2), \ldots, \mathrm{Tr}_p^q(xd_n)),\ x \in \mathbb{F}_q \right\} \tag{5}$$

with a defining set

$$D = \{d_1, d_2, \ldots, d_n\} = C_0^{(N,q)} = \{\beta^{Nj} : 0 \leq j < n\}, \tag{6}$$

where $n = \frac{q-1}{N}$. It is known that $\mathcal{C}_D$ is an irreducible cyclic code. When $\gcd(\frac{q-1}{p-1}, N)$ is small or $N$ is small, Ding and Yang in [6] studied the weight distribution of $\mathcal{C}_D$ by some known Gauss sums and Gauss periods. In this paper, we will use Gauss sum of index 2 case to determine Hamming weight of the codeword in $\mathcal{C}_D$. To this end, we firstly introduce some preliminary lemmas.

**Lemma 7** *Let $q$ be a prime power and let $s$ be an integer such that $s \mid (q-1)$. Let $\tau$ be a multiplicative character of $\mathbb{F}_q^*$ with order $s$ and $x \in \mathbb{F}_q$, then*

$$\sum_{0<i<s} \tau^i(x) = \begin{cases} s-1, & \text{if } x \in C_0^{(s,q)}, \\ -1, & \text{if } x \notin C_0^{(s,q)} \cup \{0\}. \end{cases}$$

**Lemma 8** *Let $q$ be a prime power and let $p'$ be an odd prime such that $p' | (q-1)$. Let $\tau$ be a multiplicative character of $\mathbb{F}_q^*$ defined by $\tau(\beta) = \zeta_{p'}$, where $\beta$ is a primitive element of $\mathbb{F}_q$ and $\zeta_{p'}$ is a primitive $p'$-th root of an unity. Then*

$$\sum_{0<s<p'} \left(\frac{s}{p'}\right) \tau^s(x) = \begin{cases} 0, & \text{if } x \in C_0^{(p',q)}, \\ \left(\frac{i}{p'}\right) \sqrt{(-1)^{\frac{p'-1}{2}} p'}, & \text{if } x \in C_i^{(p',q)} \text{ and } i \neq 0, \end{cases}$$

*where $\left(\frac{\cdot}{p'}\right)$ is the Legendre symbol.*

*Proof* If $\tau(x) = 1$, we have $\sum_{0<s<p'} \left(\frac{s}{p'}\right) \tau^s(x) = \sum_{0<s<p'} \left(\frac{s}{p'}\right) = 0$. Since $\tau(\beta) = \zeta_{p'}$, $x \in C_i^{(p',q)}$ and $i \neq 0$, we have $\tau(x) = \tau^i(\beta) = \zeta_{p'}^i$. It follows that

$$\begin{aligned} \sum_{0<s<p'} \left(\frac{s}{p'}\right) \tau^s(x) &= \sum_{0<s<p'} \left(\frac{s}{p'}\right) \tau^{is}(\beta) \\ &= \left(\frac{i}{p'}\right) \sum_{0<s<p'} \left(\frac{s}{p'}\right) \zeta_{p'}^s = \left(\frac{i}{p'}\right) \sqrt{(-1)^{\frac{p'-1}{2}} p'}. \end{aligned}$$

This completes the proof. □

In order to determine Hamming weight of the codeword $\mathbf{c}_x$ in (5) we need to calculate the following number.

$$S_D(x) = \left| \left\{ d \in D \mid \mathrm{Tr}_p^q(xd) = 0 \right\} \right| = \frac{n}{p} + \frac{1}{p} \sum_{z \in \mathbb{F}_p^*} \sum_{d \in D} \chi(zxd). \tag{7}$$

Let $\varphi$ be a multiplicative character of $\mathbb{F}_q^*$ of order $q-1$ and $\widehat{\mathbb{F}}_q^* = \{\varphi^j : 0 \le j < q-1\}$. By Fourier expansion formula, Lemma 1 and Lemma 7,

$$\begin{aligned}
S_D(x) &= \frac{n}{p} + \frac{1}{p(q-1)} \sum_{z\in\mathbb{F}_p^*} \sum_{d\in D} \sum_{\psi\in\widehat{\mathbb{F}}_q^*} g(\bar{\psi})\psi(zxd)\\
&= \frac{n}{p} + \frac{1}{p(q-1)} \sum_{0\le j<q-1} g(\bar{\varphi}^j)\varphi^j(x) \sum_{z\in\mathbb{F}_p^*} \varphi^j(z) \sum_{d\in D} \varphi^j(d)\\
&= \frac{n}{p} + \frac{1}{pN} \sum_{0\le j<N} g(\bar{\varphi}^{nj})\varphi^{nj}(x) \sum_{z\in\mathbb{F}_p^*} \varphi^{nj}(z)\\
&= \frac{n}{p} + \frac{p-1}{pN} \sum_{\substack{0\le j<N,\\ (p-1)|nj}} g(\bar{\varphi}^{nj})\varphi^{nj}(x)\\
&= \frac{n}{p} + \frac{p-1}{pN} \sum_{\substack{0\le j<N,\\ l|j}} g(\bar{\varphi}^{nj})\varphi^{nj}(x)\\
&= \frac{n}{p} + \frac{p-1}{pN} \sum_{0\le j<\frac{N}{l}} g(\bar{\varphi}^{nlj})\varphi^{nlj}(x), \qquad (8)
\end{aligned}$$

where $l = \frac{p-1}{\gcd(n,p-1)}$. From $q-1 = n\cdot N$ we know that $l \mid N$.

Next we will construct three classes of irreducible cyclic codes as in (5) and (6) by choosing a proper defining set $D$, and determine their weight distributions.

**Theorem 2** *Let $N = 2p_1$, where $p_1 > 3$ is a prime such that $p_1 \equiv 3 \pmod 4$. Assume that $p$ is a prime such that $[\mathbb{Z}_N^* : \langle p\rangle] = 2$. Let $f = \phi(N)/2$ and $q = p^f$. Let $h$ be the class number of $\mathbb{Q}(\sqrt{-p_1})$, and $b, c$ be integers determined by $4p^h = b^2 + p_1c^2$ and $bp^{\frac{f-h}{2}} \equiv -2 \pmod{p_1}$. Let $\mathcal{C}_D$ be a linear code defined in (5) and (6), then the weight enumerator of $\mathcal{C}_D$ is as follows:*

$$\begin{aligned}
1 &+ \frac{q-1}{p_1} x^{\frac{p-1}{pN}\left(q-\frac{b(p_1-1)}{2}p^{\frac{f-h}{2}}\right)} + \frac{(q-1)(p_1-1)}{2p_1} x^{\frac{p-1}{pN}\left(q+\frac{b+cp_1}{2}p^{\frac{f-h}{2}}\right)}\\
&+ \frac{(q-1)(p_1-1)}{2p_1} x^{\frac{p-1}{pN}\left(q+\frac{b-cp_1}{2}p^{\frac{f-h}{2}}\right)}. \qquad (9)
\end{aligned}$$

*Proof* Since $p_1$ is a prime with $p_1 \equiv 3 \pmod 4$, we have that $f = \frac{p_1-1}{2}$ is odd, and $\frac{q-1}{p-1} = p^{f-1} + \cdots + 1 \equiv 1 \pmod 2$. Since $p_1 > 3$ and $[\mathbb{Z}_N^* : \langle p\rangle] = 2$, we know that $p \not\equiv 1 \pmod{p_1}$. Since $N = 2p_1 \mid (q-1)$, we have $l = \frac{p-1}{\gcd(n,p-1)} = \frac{(p-1)2p_1}{\gcd(q-1,(p-1)2p_1)} = \frac{2p_1}{\gcd(\frac{q-1}{p-1},2p_1)} = 2$.

Let $\psi$ be a multiplicative character of $\mathbb{F}_q^*$ defined by $\psi(\beta) = \zeta_{2p_1}$. By Lemma 2, we have

$$g(\bar{\psi}^2) = p^{\frac{f-h}{2}} \frac{b + c\sqrt{-p_1}}{2},$$

where $h$ is the class number of $\mathbb{Q}(\sqrt{-p_1})$, and $b, c$ are integers determined by $4p^h = b^2 + p_1c^2$ and $bp^{\frac{f-h}{2}} \equiv -2 \pmod{p_1}$. By the same argument as in Theorem 5.1 of [8] we have

$$g(\bar{\psi}^{2s}) = \frac{1}{2} p^{\frac{f-h}{2}} \left( b + \left( \frac{s}{p_1} \right) c\sqrt{-p_1} \right), \tag{10}$$

where $0 < s < p_1$ and $(\frac{\cdot}{p_1})$ is the Legendre symbol.

Let $\tau = \varphi^{2n}$ in (8). Since $l = 2$ and $N = 2p_1$, by (8) the Hamming weight of codeword $\mathbf{c}_x$ equals

$$\begin{aligned} wt(\mathbf{c}_x) = n - S_D(x) &= \frac{(p-1)n}{p} - \frac{p-1}{pN} \sum_{0 \le j < \frac{N}{l}} g(\bar{\tau}^j)\tau^j(x) \\ &= \frac{(p-1)q}{pN} - \frac{p-1}{pN} \sum_{0 < j < \frac{N}{l}} g(\bar{\tau}^j)\tau^j(x) \\ &= \frac{(p-1)q}{pN} - \frac{p-1}{pN} \sum_{0 < j < p_1} g(\bar{\tau}^j)\tau^j(x). \end{aligned} \tag{11}$$

By (10) it is followed that

$$\begin{aligned} \sum_{0<j<p_1} g(\bar{\tau}^j)\tau^j(x) &= \sum_{0<s<p_1} \frac{1}{2} p^{\frac{f-h}{2}} \left( b + \left( \frac{s}{p_1} \right) c\sqrt{-p_1} \right) \tau^s(x) \\ &= \frac{b}{2} p^{\frac{f-h}{2}} \sum_{0<s<p_1} \tau^s(x) + \frac{c}{2}\sqrt{-p_1}\, p^{\frac{f-h}{2}} \sum_{0<s<p_1} \left( \frac{s}{p_1} \right) \tau^s(x). \end{aligned} \tag{12}$$

By Lemma 7 and Lemma 8, we have

$$\sum_{0<j<p_1} g(\bar{\tau}^j)\tau^j(x) = \begin{cases} \frac{b(p_1-1)}{2} p^{\frac{f-h}{2}}, & x \in C_0^{(p_1,q)}, \\ -\left( \frac{b}{2} + \frac{cp_1}{2} \left( \frac{i}{p_1} \right) \right) p^{\frac{f-h}{2}}, & x \in C_i^{(p_1,q)} \text{ and } i \neq 0. \end{cases} \tag{13}$$

Hence, we obtain

$$wt(\mathbf{c}_x) = \begin{cases} \frac{p-1}{pN} \left( q - \frac{b(p_1-1)}{2} p^{\frac{f-h}{2}} \right), & \text{if } x \in C_0^{(p_1,q)}, \\ \frac{p-1}{pN} \left( q + \frac{b}{2} p^{\frac{f-h}{2}} + \frac{cp_1}{2} \left( \frac{i}{p_1} \right) p^{\frac{f-h}{2}} \right), & \text{if } x \in C_i^{(p_1,q)} \text{ and } i \neq 0. \end{cases} \tag{14}$$

Frequency of each Hamming weight is derived from (14) directly. So we get the weight enumerator of $\mathcal{C}_D$ as in (9). □

*Remark 3* When $b, c \in \{-1, 1\}$, the obtained codes are two-weighted.

*Example 2* Let $p = 11$, $p_1 = 7$ and $N = 14$. Then $f = 3$ and $q = 11^3$. The class number $h$ of $\mathbb{Q}(\sqrt{-7})$ is equal to 1 (see [19]). Since $4p^h = b^2 + p_1c^2$ and $bp^{\frac{f-h}{2}} \equiv -2 \pmod{p_1}$, we have $c^2 = 4$ and $b = -4$. By Theorem 2, the weight enumerator of the irreducible cyclic code $\mathcal{C}_D$ defined by (5) is

$$1 + 190x^{95} + 570x^{90} + 570x^{80}.$$

This is confirmed by Magma.

*Example 3* Let $p = 3$, $p_1 = 11$ and $N = 22$. Then $f = 5$ and $q = 3^5$. The class number $h$ of $\mathbb{Q}(\sqrt{-11})$ is equal to 1 (see [19]). Since $4p^h = b^2 + p_1c^2$ and $bp^{\frac{f-h}{2}} \equiv -2 \pmod{p_1}$, we have $c^2 = 1$ and $b = 1$. By Theorem 2, the weight enumerator of the irreducible cyclic code $\mathcal{C}_D$ defined by (5) is

$$1 + 132x^6 + 110x^9.$$

This is confirmed by Magma.

**Theorem 3** *Let $N = p_1p_2$, where $p_1, p_2$ are primes such that $p_1 \equiv 3 \pmod 4$ and $p_2 \equiv 1 \pmod 4$. Assume that $p$ is a prime such that $[\mathbb{Z}_N^* : \langle p\rangle] = 2$, $ord_{p_1}(p) = \phi(p_1)$ and $ord_{p_2}(p) = \phi(p_2)$. Let $f = \phi(N)/2$, $q = p^f$. Let $h_{12}$ be the class number of $\mathbb{Q}(\sqrt{-p_1p_2})$, and let $b$, $c$ be integers determined by $b, c \not\equiv 0 \pmod p$, $4p^{h_{12}} = b^2 + p_1p_2c^2$ and $b \equiv 2p^{\frac{1}{2}h_{12}} \pmod{p_1}$. Let $h = \frac{1}{2}(f - h_{12})$ and $\mathcal{C}_D$ be a linear code defined in (5) and (6), then the weight enumerator of the linear code $\mathcal{C}_D$ is as follows:*

$$\begin{aligned}
&1 + \frac{q-1}{p_1p_2}x^{\frac{p-1}{pN}(q-\frac{b}{2}p^h(p_1-1)(p_2-1)-p^{\frac{f}{2}}(p_2-p_1))}\\
&\quad+\frac{(q-1)(p_2-1)}{p_1p_2}x^{\frac{p-1}{pN}(q+\frac{b}{2}p^h(p_1-1)+p^{\frac{f}{2}}p_1)} + \frac{(q-1)(p_1-1)}{p_1p_2}x^{\frac{p-1}{pN}(q+\frac{b}{2}p^h(p_2-1)-p^{\frac{f}{2}}p_2)}\\
&\quad+\frac{(q-1)(p_1-1)(p_2-1)}{2p_1p_2}\left(x^{\frac{p-1}{pN}(q-\frac{b}{2}p^h+\frac{cp_1p_2}{2}p^h)} + x^{\frac{p-1}{pN}(q-\frac{b}{2}p^h-\frac{cp_1p_2}{2}p^h)}\right).
\end{aligned} \tag{15}$$

*Proof* Since $p_1, p_2$ are primes, $\text{ord}_{p_1}(p) = \phi(p_1)$ and $\text{ord}_{p_2}(p) = \phi(p_2)$, we have $p \not\equiv 1 \pmod{p_1}$ and $p \not\equiv 1 \pmod{p_2}$. Since $N = p_1p_2 \,|\, (q-1)$, we have $p_1p_2 | \frac{q-1}{p-1}$ and $l = \frac{p-1}{\gcd(n,p-1)} = \frac{(p-1)p_1p_2}{\gcd(q-1,(p-1)p_1p_2)} = \frac{p_1p_2}{\gcd(\frac{q-1}{p-1},p_1p_2)} = 1$.

Let $\tau_1$ be a multiplicative character of $\mathbb{F}_q^*$ defined by $\tau_1(\beta) = \zeta_{p_1}$ and let $\tau_2$ be a multiplicative character of $\mathbb{F}_q^*$ defined by $\tau_2(\beta) = \zeta_{p_2}$. By Lemma 3, we have

$$g(\bar{\tau}_1\bar{\tau}_2) = p^h\frac{b + c\sqrt{-p_1p_2}}{2},\ \ g(\bar{\tau}_2) = p^{\frac{f}{2}},\ \ g(\bar{\tau}_1) = -p^{\frac{f}{2}},$$

where $h_{12}$ is the class number of $\mathbb{Q}(\sqrt{-p_1p_2})$, $h = \frac{1}{2}(f - h_{12})$ and $b$, $c$ are integers determined by $b, c \not\equiv 0 \pmod p$, $4p^{h_{12}} = b^2 + p_1p_2c^2$ and $b \equiv 2p^{\frac{1}{2}h_{12}} \pmod{p_1}$. Every multiplicative character of $\mathbb{F}_q^*$ with order $p_1p_2$ is of the form $\tau_1^s\tau_2^t$, where $s \in \mathbb{Z}_{p_1}^*$ and $t \in \mathbb{Z}_{p_2}^*$. By the same argument as in Theorem 5.1 in [8], we have

$$g(\bar{\tau}_1^s\bar{\tau}_2^t) = \frac{p^h}{2}\left(b + c\left(\frac{s}{p_1}\right)\left(\frac{t}{p_2}\right)\sqrt{-p_1p_2}\right),\ \ g(\bar{\tau}_2^t) = p^{\frac{f}{2}},\ \ g(\bar{\tau}_1^s) = -p^{\frac{f}{2}}, \tag{16}$$

where $(\frac{\cdot}{p_1})$ is the Legendre symbol.

Let $\tau = \varphi^n$ in (8). Since $l = 1$ and $N = p_1p_2$, from (8) we have

$$\begin{aligned}
wt(\mathbf{c}_x) = n - S_D(x) &= \frac{(p-1)n}{p} - \frac{p-1}{pN}\sum_{0\le j<\frac{N}{l}} g(\bar{\tau}^j)\tau^j(x)\\
&= \frac{(p-1)q}{pN} - \frac{p-1}{pN}\sum_{0<j<\frac{N}{l}} g(\bar{\tau}^j)\tau^j(x)\\
&= \frac{(p-1)q}{pN} - \frac{p-1}{pN}\sum_{0<j<N} g(\bar{\tau}^j)\tau^j(x).
\end{aligned} \tag{17}$$

Since $\tau$ is a character with order $N$, we get

$$\sum_{0<j<N} g(\bar{\tau}^j)\tau^j(x) = \sum_{\substack{0<j<N,\\ \gcd(j,N)=1}} g(\bar{\tau}^j)\tau^j(x) + \sum_{\substack{0<j<N,\\ \gcd(j,N)=p_2}} g(\bar{\tau}^j)\tau^j(x) + \sum_{\substack{0<j<N,\\ \gcd(j,N)=p_1}} g(\bar{\tau}^j)\tau^j(x). \tag{18}$$

Below we will compute each sum individually. By (16) and Lemma 7 and Lemma 8,

$$\begin{aligned}
\sum_{\substack{0<j<N,\\ \gcd(j,N)=1}} g(\bar{\tau}^j)\tau^j(x) &= \sum_{\substack{0<s<p_1,\\ 0<t<p_2}} g(\bar{\tau}_1^s\bar{\tau}_2^t)\tau_1^s\tau_2^t(x)\\
&= \sum_{\substack{0<s<p_1,\\ 0<t<p_2}} \frac{p^h}{2}\left(b + c\left(\frac{s}{p_1}\right)\left(\frac{t}{p_2}\right)\sqrt{-p_1p_2}\right)\tau_1^s\tau_2^t(x)\\
&= \frac{bp^h}{2}\sum_{\substack{0<s<p_1,\\ 0<t<p_2}} \tau_1^s\tau_2^t(x) + \frac{cp^h\sqrt{-p_1p_2}}{2}\sum_{0<s<p_1}\left(\frac{s}{p_1}\right)\tau_1^s(x)\sum_{0<t<p_2}\left(\frac{t}{p_2}\right)\tau_2^t(x)\\
&= \begin{cases}
\frac{b}{2}p^h(p_1-1)(p_2-1), & \text{if } x \in C_0^{(p_1p_2,q)},\\
-\frac{b}{2}p^h(p_1-1), & \text{if } x \in C_0^{(p_1,q)} \text{ and } x \notin C_0^{(p_2,q)},\\
-\frac{b}{2}p^h(p_2-1), & \text{if } x \notin C_0^{(p_1,q)} \text{ and } x \in C_0^{(p_2,q)},\\
\frac{b}{2}p^h - \frac{cp_1p_2p^h}{2}\left(\frac{i}{p_1}\right)\left(\frac{j}{p_2}\right), & \text{if } x \in C_i^{(p_1,q)},\ x \in C_j^{(p_2,q)} \text{ and } ij \neq 0.
\end{cases}
\end{aligned} \tag{19}$$

From (16) and Lemma 7 we have

$$\begin{aligned}
\sum_{\substack{0<j<N,\\ \gcd(j,N)=p_2}} g(\bar{\tau}^j)\tau^j(x) &= \sum_{0<i<p_1} g(\bar{\tau}_1^i)\tau_1^i(x) = -p^{\frac{f}{2}}\sum_{0<i<p_1}\tau_1^i(x)\\
&= \begin{cases}
-p^{\frac{f}{2}}(p_1-1), & \text{if } x \in C_0^{(p_1,q)},\\
p^{\frac{f}{2}}, & \text{if } x \notin C_0^{(p_1,q)} \cup \{0\},
\end{cases}
\end{aligned} \tag{20}$$

and

$$\begin{aligned}
\sum_{\substack{0<j<N,\\ \gcd(j,N)=p_1}} g(\bar{\tau}^j)\tau^j(x) &= \sum_{0<i<p_2} g(\bar{\tau}_2^i)\tau_2^i(x) = p^{\frac{f}{2}}\sum_{0<i<p_2}\tau_2^i(x)\\
&= \begin{cases}
p^{\frac{f}{2}}(p_2-1), & \text{if } x \in C_0^{(p_2,q)},\\
-p^{\frac{f}{2}}, & \text{if } x \notin C_0^{(p_2,q)} \cup \{0\}.
\end{cases}
\end{aligned} \tag{21}$$

Combing (17), (18), (19), (20) and (21) we obtain

$$wt(\mathbf{c}_x)=\begin{cases}\frac{p-1}{pN}\left(q-\frac{b}{2}p^h(p_1-1)(p_2-1)-p^{\frac{f}{2}}(p_2-p_1)\right), & \text{if } x\in C_0^{(p_1p_2,q)},\\ \frac{p-1}{pN}\left(q+\frac{b}{2}p^h(p_1-1)+p^{\frac{f}{2}}p_1\right), & \text{if } x\in C_0^{(p_1,q)} \text{ and } x\notin C_0^{(p_2,q)},\\ \frac{p-1}{pN}\left(q+\frac{b}{2}p^h(p_2-1)-p^{\frac{f}{2}}p_2\right), & \text{if } x\notin C_0^{(p_1,q)} \text{ and } x\in C_0^{(p_2,q)},\\ \frac{p-1}{pN}\left(q-\frac{b}{2}p^h+\frac{cp_1p_2}{2}p^h\left(\frac{i}{p_1}\right)\left(\frac{j}{p_2}\right)\right), & \text{if } x\in C_i^{p_1},\ x\in C_j^{p_2} \text{ and } ij\neq 0.\end{cases} \tag{22}$$

Frequency of each Hamming weight is derived from equation (22) directly. So we get the weight enumerator of $\mathcal{C}_D$ as in (15). □

*Remark 4* When $c^2=1, b=\frac{p_2-p_1}{2}$ and $p^{\frac{h_{12}}{2}}=\frac{p_1+p_2}{4}$, the obtained codes are three-weighted.

*Example 4* Let $p=2$, $p_1=3$, $p_2=13$ and $N=39$. Then $f=12$ and $q=2^{12}$. The class number $h_{12}$ of $\mathbb{Q}(\sqrt{-39})$ is equal to 4 (see [1]). Since $b^2+p_1p_2c^2=4p^{h_{12}}$ and $b\equiv 2p^{\frac{h_{12}}{2}} \pmod{p_1}$, we have $c^2=1$ and $b=5$. By Theorem 3, the weight enumerator of the irreducible cyclic code $\mathcal{C}_D$ defined by (5) is

$$1+\frac{2^{12}-1}{39}x^{32}+\frac{8(2^{12}-1)}{13}x^{56}+\frac{14(2^{12}-1)}{39}x^{48}.$$

This weight enumerator coincides with that computed by Magma.

*Example 5* Let $p=2$, $p_1=11$, $p_2=5$ and $N=55$. Then $f=20$ and $q=2^{20}$. The class number $h_{12}$ of $\mathbb{Q}(\sqrt{-55})$ is equal to 4 ([1]). Since $b^2+p_1p_2c^2=4p^h$ and $b\equiv 2p^{\frac{h_{12}}{2}}$ $\pmod{p_1}$, we have $c^2=1$ and $b=-3$. By Theorem 3, the complete weight enumerator of the irreducible cyclic code $\mathcal{C}_D$ defined by (5) is

$$1+\frac{2^{20}-1}{55}x^{9728}+\frac{24(2^{20}-1)}{55}x^{9600}+\frac{30(2^{20}-1)}{55}x^{9472},$$

This weight enumerator coincides with that computed by Magma.

**Theorem 4** *Let $N=4p_1$, where $p_1$ is prime such that $p_1\equiv 1 \pmod 4$. Assume that $p$ is a prime such that $p\equiv 3 \pmod 4$, $[\mathbb{Z}_N^*:\langle p\rangle]=2$ and $ord_{p_1}(p)=\phi(p_1)$. Let $f=\phi(N)/2$, $q=p^f$, and $b, c$ be integers determined by $p^{\frac{f}{2}}=b^2+p_1c^2$ and $b\equiv -p^{\frac{f}{4}}$ $\pmod{p_1}$. Let $\mathcal{C}_D$ be a linear code defined in (5) and (6), then the weight enumerator of $\mathcal{C}_D$ is as follows:*

$$\begin{aligned}1&+\frac{q-1}{4p_1}x^{\frac{(p-1)}{pN}\left(q+3p^{\frac{f}{2}}-2b(p_1-1)p^{\frac{f}{4}}\right)}+\frac{q-1}{2p_1}x^{\frac{(p-1)}{pN}\left(q-(2p_1-1)p^{\frac{f}{2}}\right)}\\&+\frac{q-1}{4p_1}x^{\frac{(p-1)}{pN}\left(q+2b(p_1-1)p^{\frac{f}{4}}-p^{\frac{f}{2}}\right)}+\frac{(q-1)(p_1-1)}{4p_1}x^{\frac{(p-1)}{pN}\left(q+3p^{\frac{f}{2}}+2bp^{\frac{f}{4}}\right)}\\&+\frac{(q-1)(p_1-1)}{4p_1}x^{\frac{(p-1)}{pN}\left(q+p^{\frac{f}{2}}+2cp_1p^{\frac{f}{4}}\right)}+\frac{(q-1)(p_1-1)}{4p_1}x^{\frac{(p-1)}{pN}\left(q-p^{\frac{f}{2}}-2bp^{\frac{f}{4}}\right)}\\&+\frac{(q-1)(p_1-1)}{4p_1}x^{\frac{(p-1)}{pN}\left(q+p^{\frac{f}{2}}-2cp_1p^{\frac{f}{4}}\right)}.\end{aligned} \tag{23}$$

*Proof* Since $p_1$ is a prime, and $\mathrm{ord}_{p_1}(p) = \phi(p_1)$, we have $p \not\equiv 1 \pmod{p_1}$. Since $4 \mid f = p_1 - 1$ and $p \equiv 3 \pmod 4$, it follows that $\frac{q-1}{p-1} = p^{f-1} + p^{f-2} + \cdots + 1 \equiv 0 \pmod 4$. Since $N = 4p_1 \mid (q-1)$, we imply that $4p_1 | \frac{q-1}{p-1}$ and $l = \frac{p-1}{\gcd(n, p-1)} = \frac{(p-1)4p_1}{\gcd(q-1,(p-1)4p_1)} = \frac{4p_1}{\gcd(\frac{q-1}{p-1}, 4p_1)} = 1$.

Let $\tau_1$ be the multiplicative character of $\mathbb{F}_q^*$ defined by $\tau_1(\beta) = \zeta_{p_1}$ and let $\tau_2$ be the character of $\mathbb{F}_q^*$ defined by $\tau_2(\beta) = \zeta_4$. By Lemma 4, we know that

$$g(\bar{\tau}_1\bar{\tau}_2) = p^{\frac{f}{4}}(b + c\sqrt{-p_1}),\ g(\bar{\tau}_1) = p^{\frac{f}{2}},\ g(\bar{\tau}_2) = g(\bar{\tau}_2^2) = g(\bar{\tau}_1\bar{\tau}_2^2) = -p^{\frac{f}{2}},$$

where $b$, $c$ are integers determined by $p^{\frac{f}{2}} = b^2 + p_1c^2$ and $b \equiv -p^{\frac{f}{4}} \pmod{p_1}$. Every multiplicative character of $\mathbb{F}_q^*$ with order $4p_1$ is of the form $\tau_1^s\tau_2^t$, where $s \in \mathbb{Z}_{p_1}^*$ and $t \in \mathbb{Z}_4^*$. It follows that for any $s \in \mathbb{Z}_{p_1}^*$ and $t \in \mathbb{Z}_4^*$,

$$\begin{aligned}&g(\bar{\tau}_1^s\bar{\tau}_2) = p^{\frac{f}{4}}\left(b + c\left(\frac{s}{p_1}\right)\sqrt{-p_1}\right),\ g(\bar{\tau}_1^s\bar{\tau}_2^3) = p^{\frac{f}{4}}\left(b - c\left(\frac{s}{p_1}\right)\sqrt{-p_1}\right),\\ &g(\bar{\tau}_2^t) = g(\bar{\tau}_2^{2t}) = g(\bar{\tau}_1^s\bar{\tau}_2^{2t}) = -p^{\frac{f}{2}},\ g(\bar{\tau}_1^s) = p^{\frac{f}{2}},\end{aligned} \tag{24}$$

where $\left(\frac{\cdot}{p_1}\right)$ is the Legendre symbol.

Let $\tau = \varphi^n$ in (8). Since $l = 1$ and $N = 4p_1$, by (8) the Hamming weight of codeword $\mathbf{c}_x$ equals

$$\begin{aligned}wt(\mathbf{c}_x) = n - S_D(x) &= \frac{(p-1)n}{p} - \frac{p-1}{pN}\sum_{0\le j<\frac{N}{l}} g(\bar{\tau}^j)\tau^j(x)\\ &= \frac{(p-1)q}{pN} - \frac{p-1}{pN}\sum_{0<j<\frac{N}{l}} g(\bar{\tau}^j)\tau^j(x)\\ &= \frac{(p-1)q}{pN} - \frac{p-1}{pN}\sum_{0<j<N} g(\bar{\tau}^j)\tau^j(x).\end{aligned} \tag{25}$$

Since $\tau$ is a character with order $N$, it follows that every multiplicative character of $\mathbb{F}_q^*$ with order $4p_1$ is of the form $\tau_1^s\tau_2^t$, where $s \in \mathbb{Z}_{p_1}^*$ and $t \in \mathbb{Z}_4^*$. By (24) we have

$$\begin{aligned}&\sum_{0<j<N} g(\bar{\tau}^j)\tau^j(x) = \sum_{\tau, o(\tau)=2} g(\bar{\tau})\tau(x) + \sum_{\tau, o(\tau)=4} g(\bar{\tau})\tau(x) + \sum_{\tau, o(\tau)=p_1} g(\bar{\tau})\tau(x)\\ &\quad + \sum_{\tau, o(\tau)=2p_1} g(\bar{\tau})\tau(x) + \sum_{\tau, o(\tau)=4p_1} g(\bar{\tau})\tau(x)\\ &\quad = g({\bar{\tau}_2}^2)\tau_2^2(x) + \left(g(\bar{\tau}_2)\tau_2(x) + g({\bar{\tau}_2}^3)\tau_2^3(x)\right) + \sum_{0<s<p_1} g({\bar{\tau}_1}^s)\tau_1^s(x)\\ &\quad\quad + \sum_{0<s<p_1} g({\bar{\tau}_1}^s{\bar{\tau}_2}^2)\tau_1^s\tau_2^2(x) + \sum_{0<s<p_1}\left(g({\bar{\tau}_1}^s\bar{\tau}_2)\tau_1^s\tau_2(x) + g({\bar{\tau}_1}^s{\bar{\tau}_2}^3)\tau_1^s\tau_2^3(x)\right)\\ &\quad = -p^{\frac{f}{2}}\left(\tau_2(x) + \tau_2^2(x) + \tau_2^3(x)\right) + p^{\frac{f}{2}}\sum_{0<s<p_1}\tau_1^s(x) - p^{\frac{f}{2}}\tau_2^2(x)\sum_{0<s<p_1}\tau_1^s(x)\\ &\quad\quad + \sum_{0<s<p_1} p^{\frac{f}{4}}\left(b + c\left(\frac{s}{p_1}\right)\sqrt{-p_1}\right)\tau_1^s\tau_2(x) + \sum_{0<s<p_1} p^{\frac{f}{4}}\left(b - c\left(\frac{s}{p_1}\right)\sqrt{-p_1}\right)\tau_1^s\tau_2^3(x)\end{aligned}$$

$$= -p^{\frac{f}{2}}\left(\tau_2(x)+\tau_2^2(x)+\tau_2^3(x)\right)+\left(p^{\frac{f}{2}}(1-\tau_2^2(x))+bp^{\frac{f}{4}}(\tau_2(x)+\tau_2^3(x))\right)\sum_{0<s<p_1}\tau_1^s(x)$$
$$+cp^{\frac{f}{4}}(\tau_2(x)-\tau_2^3(x))\sqrt{-p_1}\sum_{0<s<p_1}\left(\frac{s}{p_1}\right)\tau_1^s(x), \tag{26}$$

where $o(\tau)$ denotes the order of the character $\tau$. Next we evaluate above sum according to $x$.

If $x \in C_0^{(p_1,q)}$ and $x \in C_0^{(4,q)}$ from (26) we have

$$\sum_{0<j<N} g(\bar{\tau}^j)\tau^j(x) = -3p^{\frac{f}{2}} + 2b(p_1-1)p^{\frac{f}{4}}.$$

If $x \in C_0^{(p_1,q)}$ and $x \in C_1^{(4,q)}$ from (26) we get

$$\sum_{0<j<N} g(\bar{\tau}^j)\tau^j(x) = (2p_1-1)p^{\frac{f}{2}}.$$

If $x \in C_0^{(p_1,q)}$ and $x \in C_2^{(4,q)}$ from (26) we obtain

$$\sum_{0<j<N} g(\bar{\tau}^j)\tau^j(x) = p^{\frac{f}{2}} - 2b(p_1-1)p^{\frac{f}{4}}.$$

If $x \in C_0^{(p_1,q)}$ and $x \in C_3^{(4,q)}$ from (26) we imply

$$\sum_{0<j<N} g(\bar{\tau}^j)\tau^j(x) = (2p_1-1)p^{\frac{f}{2}}.$$

If $x \in C_i^{(p_1,q)}, i \neq 0$ and $x \in C_0^{(4,q)}$ from (26) we have

$$\sum_{0<j<N} g(\bar{\tau}^j)\tau^j(x) = -3p^{\frac{f}{2}} - 2bp^{\frac{f}{4}}.$$

If $x \in C_i^{(p_1,q)}, i \neq 0$ and $x \in C_1^{(4,q)}$ from (26) we get

$$\sum_{0<j<N} g(\bar{\tau}^j)\tau^j(x) = -p^{\frac{f}{2}} + 2cp_1p^{\frac{f}{4}}\left(\frac{i}{p_1}\right).$$

If $x \in C_i^{(p_1,q)}, i \neq 0$ and $x \in C_2^{(4,q)}$ from (26) we obtain

$$\sum_{0<j<N} g(\bar{\tau}^j)\tau^j(x) = p^{\frac{f}{2}} + 2bp^{\frac{f}{4}}.$$

If $x \in C_i^{(p_1,q)}, i \neq 0$ and $x \in C_3^{(4,q)}$ from (26) we imply

$$\sum_{0<j<N} g(\bar{\tau}^j)\tau^j(x) = -p^{\frac{f}{2}} - 2cp_1p^{\frac{f}{4}}\left(\frac{i}{p_1}\right).$$

Combing (25), (26) and above discussions, we obtain

$$wt(\mathbf{c}_x)=\begin{cases}\frac{(p-1)}{pN}(q+3p^{\frac{f}{2}}-2b(p_1-1)p^{\frac{f}{4}}), & \text{if } x\in C_0^{(p_1,q)}\cap C_0^{(4,q)},\\ \frac{(p-1)}{pN}(q-(2p_1-1)p^{\frac{f}{2}}), & \text{if } x\in C_0^{(p_1,q)}\cap (C_1^{(4,q)}\cup C_3^{(4,q)}),\\ \frac{(p-1)}{pN}(q+2b(p_1-1)p^{\frac{f}{4}}-p^{\frac{f}{2}}), & \text{if } x\in C_0^{(p_1,q)}\cap C_2^{(4,q)},\\ \frac{(p-1)}{pN}(q+3p^{\frac{f}{2}}+2bp^{\frac{f}{4}}), & \text{if } x\in C_i^{(p_1,q)}\cap C_0^{(4,q)}, i\neq 0,\\ \frac{(p-1)}{pN}\left(q+p^{\frac{f}{2}}-2cp_1p^{\frac{f}{4}}\left(\frac{i}{p_1}\right)\right), & \text{if } x\in C_i^{(p_1,q)}\cap C_1^{(4,q)}, i\neq 0,\\ \frac{(p-1)}{pN}(q-p^{\frac{f}{2}}-2bp^{\frac{f}{4}}), & \text{if } x\in C_i^{(p_1,q)}\cap C_2^{(4,q)}, i\neq 0,\\ \frac{(p-1)}{pN}\left(q+p^{\frac{f}{2}}+2cp_1p^{\frac{f}{4}}\left(\frac{i}{p_1}\right)\right), & \text{if } x\in C_i^{(p_1,q)}\cap C_3^{(4,q)}, i\neq 0.\end{cases} \tag{27}$$

Frequency of each Hamming weight is derived from (27) directly. So we get the weight enumerator of $\mathcal{C}_D$ as in (23).

*Example 6* Let $p=3$, $p_1=5$ and $N=20$. Then $f=4$ and $q=3^4$. Since $b^2+p_1c^2=p^{\frac{f}{2}}$ and $b\equiv -p^{\frac{f}{4}} \pmod{p_1}$, we have $c^2=1$ and $b=2$. By Theorem 4, the weight enumerator of $\mathcal{C}_D$ defined by (5) is

$$1+4x^2+4x^4.$$

This result is confirmed by Magma, and shows that $\mathcal{C}_D$ has dimension 2. In fact, the dimension of the vector space generated by $\{1,\alpha^{20},\alpha^{40},\alpha^{60}\}$ is 2 for some primitive element $\alpha\in\mathbb{F}_{3^4}$, which is equal to the dimension of the code $\mathcal{C}_D$ by Theorem 6 in [5].

*Example 7* Let $p=3$, $p_1=17$ and $N=68$. Then $f=16$ and $q=3^{16}$. Since $b^2+p_1c^2=p^{\frac{f}{2}}$ and $b\equiv -p^{\frac{f}{4}} \pmod{p_1}$, we have $c^2=81$ and $b=72$. By Theorem 4, the weight enumerator of the irreducible cyclic code $\mathcal{C}_D$ defined by (5) is

$$1+\frac{3^{16}-1}{34}x^{419904}+\frac{3^{16}-1}{68}x^{420390}+\frac{8(3^{16}-1)}{17}x^{421848}+\\ \frac{8(3^{16}-1)}{17}x^{422334}+\frac{3^{16}-1}{68}x^{423792}.$$

This weight enumerator coincides with that computed by Magma.

## 5 Concluding remark

In this paper we present four classes of linear codes from coset decomposition of subgroups and cyclotomic coset families of certain finite field, and determine their weight distributions by Gauss sums with index 2 cases. Many other similar linear codes maybe constructed and their corresponding weight distributions maybe determined by Gauss sums with other index 2 cases.

**Acknowledgements** The authors wish to thank prof. Qing Xiang for his helpful comments. The work was partially supported by National Natural Science Foundation of China (NSFC) under Grant 11101131.

## References

1. Arno S.: The imaginary quadratic fields of class number 4. Acta Arith. **60**, 321–334 (1992).
2. Ding C.: Linear codes from some 2-designs. IEEE Trans. Inf. Theory **61**(6), 3265–3275 (2015).
3. Ding C.: A construction of binary linear codes from Boolean functions. Discret. Math. **339**(9), 2288–2303 (2016).
4. Ding K., Ding C.: Binary linear codes with three weights. IEEE Commun. Lett. **18**, 1879–1882 (2014).
5. Ding C., Niederreiter H.: Cyclotomic linear codes of order 3. IEEE Trans. Inf. Theory **53**(6), 2274–2277 (2007).
6. Ding C., Yang J.: Hamming weights in Irreducible cyclic codes. Discret. Math. **313**, 434–446 (2013).
7. Ding C., Luo J., Niederreiter H.: Two weight codes punctured from irreducible cyclic codes. In: Li Y., Ling S., Niederreiter H., Wang H., Xing C., Zhang S (Eds.) Proceedings of the First International Workshop on Coding Theory and Cryptography, pp. 119–124. World Scientific, Singapore (2008)
8. Feng T., Xiang Q.: Strongly regular graphs from unions of cyclotomic classes. J. Comb. Theory (B) **102**, 982–995 (2012).
9. Heng Z., Yue Q.: A class of binary linear codes with at most three weights. IEEE Commun. Lett. **19**, 1488–1491 (2015).
10. Heng Z., Yue Q.: Evaluation of the Hamming weights of a classes of linear codes based on Gauss sums. Des. Codes Cryptogr. (2016). doi:10.1007/s10623-016-0222-7.
11. Heng Z., Yue Q.: Optimal linear codes, constant-weight codes and constant-composition codes over $\mathbb{F}_q$. arXiv:1605.04063v1.
12. Kløve T.: Codes for Error Detection. World Scientific, Hackensack (2007).
13. Langevin P.: Calcus de certaines sommes de Gauss. J. Number Theory **63**, 59–64 (1997).
14. Li C., Bae S., Ahn J., et al.: Complete weight enumerartors of some linear codes and their applications. Des. Codes Cryptogr. **81**(1), 153–168 (2016).
15. Li F., Wang Q., Lin D.: A class of three-weight and five-wiehgt linear codes. arXiv:1509.06242.
16. Lidl R., Niederreiter H.: Finite Fields. Cambridge University Press, Cambridge (1997).
17. Mbodj O.D.: Quadratic Gauss Sums. Finite Fields Appl. **4**, 347–361 (1998).
18. Meijer P., van der Vlugt M.: The evaluation of Gauss sums for characters of 2-power order. J. Number Theory **100**, 381–395 (2003).
19. Neukirch J.: Algebraic Number Theory. Springer, Berlin (1999).
20. Wang Q., Ding K., Xue R.: Binary linear codes with two weight. IEEE Commun. Lett. **19**, 1097–1100 (2015).
21. Xiang C.: Linear codes from a generic construction. Cryptogr. Commun. **8**, 525–539 (2016).
22. Yang J., Xia L.: Complete solving of explicit evaluation of Gauss sums in the index 2 case. Sci. China Ser. A **53**, 2525–2542 (2010).
23. Yuan J., Ding C.: Secret sharing schemes from three classes of linear codes. IEEE Trans. Inf. Theory **52**(1), 206–212 (2006).
24. Zhou Z., Li N., Fan C., Helleseth T.: Linear codes with two or three weight from quafratic bent functions. Des. Codes Cryptogr. **81**(2), 283–295 (2016).