Available online at www.sciencedirect.com
ScienceDirect
Finite Fields and Their Applications 14 (2008) 390–409
FINITE FIELDS AND THEIR APPLICATIONS
http://www.elsevier.com/locate/ffa

Weight distribution of some reducible cyclic codes

Keqin Feng [1], Jinquan Luo *

Department of Mathematics, Tsinghua University, Beijing 100084, China

Received 10 September 2006; revised 13 March 2007

Available online 30 March 2007

Communicated by Jacques Wolfmann

Abstract

Let $q = p^m$ where p is an odd prime, $m \geqslant 3$, $k \geqslant 1$ and $\gcd(k, m) = 1$. Let Tr be the trace mapping from $\mathbb{F}_q$ to $\mathbb{F}_p$ and $\zeta_p = e^{\frac{2\pi i}{p}}$. In this paper we determine the value distribution of following two kinds of exponential sums

$$\sum_{x \in \mathbb{F}_q} \chi\left(\alpha x^{p^k+1} + \beta x^2\right) \quad (\alpha, \beta \in \mathbb{F}_q)$$

and

$$\sum_{x \in \mathbb{F}_q} \chi\left(\alpha x^{p^k+1} + \beta x^2 + \gamma x\right) \quad (\alpha, \beta, \gamma \in \mathbb{F}_q),$$

where $\chi(x) = \zeta_p^{\mathrm{Tr}(x)}$ is the canonical additive character of $\mathbb{F}_q$. As an application, we determine the weight distribution of the cyclic codes $\mathcal{C}_1$ and $\mathcal{C}_2$ over $\mathbb{F}_p$ with parity-check polynomial $h_2(x)h_3(x)$ and $h_1(x)h_2(x)h_3(x)$, respectively, where $h_1(x)$, $h_2(x)$ and $h_3(x)$ are the minimal polynomials of π^{-1}, π^{-2} and $\pi^{-(p^k+1)}$ over $\mathbb{F}_p$, respectively, for a primitive element π of $\mathbb{F}_q$.

Keywords: Exponential sum; Cyclic code; Galois group; Quadratic form; Weight distribution

* Corresponding author.
E-mail addresses: kfeng@math.tsinghua.edu.cn (K. Feng), luojq01@mails.tsinghua.edu.cn (J. Luo).

[1] Supported by the National Fundamental Research Project of China, No. 2004CB3180004, and the NSFC Grant No. 60433050.

1071-5797/$ – see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2007.03.003

1. Introduction

For a cyclic code $\mathcal{C}$ with length n over a finite field $\mathbb{F}_p$ where p is an odd prime, let A_i be the number of codewords in $\mathcal{C}$ with Hamming weight i. The weight distribution $\{A_0, A_1, \dots, A_n\}$ is an important research object in coding theory. If $\mathcal{C}$ is irreducible which means that the parity-check polynomial of $\mathcal{C}$ is irreducible in $\mathbb{F}_p[x]$, the weight of each codeword can be expressed by Gaussian sums so that the weight distribution of $\mathcal{C}$ can be determined if the corresponding Gaussian sums (or their certain combinations) can be calculated explicitly (see [3,8] and the references therein).

For a reducible cyclic code, the Hamming weight of each codeword can be expressed by more general exponential sums. More exactly speaking, let $q = p^m$, $\mathcal{C}$ be the cyclic code over $\mathbb{F}_p$ with length $n = q - 1$ and parity-check polynomial

$$h(x) = h_1(x) \cdots h_l(x) \quad (l \geqslant 2),$$

where $h_i(x)$ $(1 \leqslant i \leqslant l)$ are distinct irreducible polynomials in $\mathbb{F}_p[x]$ with the same degree d $(1 \leqslant i \leqslant l)$, then $k = \dim_{\mathbb{F}_p} \mathcal{C} = ld$. Let π be a primitive element of $\mathbb{F}_q$ and π^{-s_i} be a zero of $h_i(x)$, $1 \leqslant s_i \leqslant q-2$ $(1 \leqslant i \leqslant l)$. Then the codewords in $\mathcal{C}$ can be expressed by

$$c(\alpha_1, \dots, \alpha_l) = (c_0, c_1, \dots, c_{n-1}) \quad (\alpha_1, \dots, \alpha_l \in \mathbb{F}_q),$$

where $c_i = \sum_{\lambda=1}^{l} \mathrm{Tr}(\alpha_\lambda \pi^{i s_\lambda})$ $(0 \leqslant i \leqslant n-1)$ and $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the trace mapping from $\mathbb{F}_q$ to $\mathbb{F}_p$. Therefore the Hamming weight of the codeword $c = c(\alpha_1, \dots, \alpha_l)$ is:

$$\begin{aligned}
w_H(c) &= \#\{i \mid 0 \leqslant i \leqslant n-1,\ c_i \neq 0\} \\
&= n - \#\{i \mid 0 \leqslant i \leqslant n-1,\ c_i = 0\} \\
&= n - \frac{1}{p} \sum_{i=0}^{n-1} \sum_{a=0}^{p-1} \zeta_p^{a \cdot \mathrm{Tr}(\sum_{\lambda=1}^{l} \alpha_\lambda \pi^{i s_\lambda})} \\
&= n - \frac{n}{p} - \frac{1}{p} \sum_{a=1}^{p-1} \sum_{x \in \mathbb{F}_q^*} \zeta_p^{\mathrm{Tr}(a f(x))} \\
&= n - \frac{n}{p} + \frac{p-1}{p} - \frac{1}{p} \sum_{a=1}^{p-1} S(a\alpha_1, \dots, a\alpha_l) \\
&= p^{m-1}(p-1) - \frac{1}{p} \sum_{a=1}^{p-1} S(a\alpha_1, \dots, a\alpha_l),
\end{aligned} \tag{1}$$

where $f(x) = \alpha_1 x^{s_1} + \alpha_2 x^{s_2} + \cdots + \alpha_l x^{s_l} \in \mathbb{F}_p[x]$, $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$, $n = q - 1$ and

$$S(\alpha_1, \dots, \alpha_l) = \sum_{x \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}(\alpha_1 x^{s_1} + \cdots + \alpha_l x^{s_l})}.$$

In this way, the weight distribution of cyclic code $\mathcal{C}$ can be derived from the value distribution of the exponential sum

$$S(\alpha_1,\dots,\alpha_l) \quad (\alpha_1,\dots,\alpha_l \in \mathbb{F}_q).$$

Recently, the weight distribution of linear codes constructed from perfect nonlinear function over $\mathbb{F}_q$ have been determined. A function $\varphi(x)$ on $\mathbb{F}_q$ is called perfect nonlinear if for each $a \in \mathbb{F}_q^*$, the function $\Delta_a\varphi : \mathbb{F}_q \to \mathbb{F}_q$ defined by $(\Delta_a\varphi)(x) = \varphi(x+a) - \varphi(x)$ is a permutation on $\mathbb{F}_q$. For all known power perfect nonlinear function $\varphi(x) = x^s$ over $\mathbb{F}_q$, the exponential sums

$$\sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}(\alpha\varphi(x)+\beta x)} \quad (\alpha,\beta \in \mathbb{F}_q)$$

has been calculated with variety of techniques in [1,2,6,9] and then the weight distribution of cyclic code over $\mathbb{F}_p$ with parity-check polynomial $h_1(x)h_2(x)$ is determined where $h_1(x)$ and $h_2(x)$ are minimal polynomials of π^{-1} and π^{-s} over $\mathbb{F}_p$, respectively.

Let $m \geqslant 3$, $k \geqslant 1$ and $\gcd(k,m) = 1$. Let $h_1(x)$, $h_2(x)$ and $h_3(x)$ be the minimal polynomials of π^{-1}, π^{-2} and $\pi^{-(p^k+1)}$ over $\mathbb{F}_p$, respectively. Then $\deg h_i(x) = m$ for $i = 1,2,3$. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be the cyclic codes over $\mathbb{F}_p$ with length $n = q-1$ and parity-check polynomial $h_2(x)h_3(x)$ and $h_1(x)h_2(x)h_3(x)$, respectively. Then the dimensions of $\mathcal{C}_1$ and $\mathcal{C}_2$ over $\mathbb{F}_p$ are $2m$ and $3m$, respectively. (If $m = 2$, then $\deg h_3(x) = 1$; the dimensions of $\mathcal{C}_1$ and $\mathcal{C}_2$ are 3 and 5, respectively.) In this paper we determine the weight distribution of $\mathcal{C}_1$ and $\mathcal{C}_2$. For doing this we should determine the value distribution of the multi-sets

$$\left\{T(\alpha,\beta) = \sum_{x\in\mathbb{F}_q} \chi\left(\alpha x^{p^k+1} + \beta x^2\right):\ \alpha,\beta \in \mathbb{F}_q\right\} \tag{2}$$

and

$$\left\{S(\alpha,\beta,\gamma) = \sum_{x\in\mathbb{F}_q} \chi\left(\alpha x^{p^k+1} + \beta x^2 + \gamma x\right):\ \alpha,\beta,\gamma \in \mathbb{F}_q\right\}, \tag{3}$$

where $\chi(x) = \zeta_p^{\mathrm{Tr}(x)}$.

Here we present a uniform treatment to determine the values $T(\alpha,\beta)$ and $S(\alpha,\beta,\gamma)$ by using quadratic form theory, and their multiplicities by giving some moment identities on $T(\alpha,\beta)$ and $S(\alpha,\beta,\gamma)$. We introduce some preliminaries and give auxiliary results in Section 2 and prove our main results in Sections 3 and 4.

2. Preliminaries

The first machinery to determine the values of exponential sums $T(\alpha,\beta)$ $(\alpha,\beta \in \mathbb{F}_q)$ defined in (2) is quadratic form theory over $\mathbb{F}_p$.

Let H be an $m \times m$ symmetric matrix over $\mathbb{F}_p$ and $r = \operatorname{rank} H$. Then there exists $M \in \mathrm{GL}_m(\mathbb{F}_p)$ such that $H' = MHM^T$ is a diagonal matrix and $H' = \mathrm{diag}(a_1,\dots,a_r,0,\dots,0)$ where $a_i \in \mathbb{F}_p^*$ $(1 \leqslant i \leqslant r)$. Let $\Delta = a_1 \cdots a_r$ (we assume $\Delta = 1$ when $r = 0$). Then the Legendre symbol $(\frac{\Delta}{p})$ is an invariant of H under the action of $M \in \mathrm{GL}_m(\mathbb{F}_p)$. For $\zeta_p = e^{\frac{2\pi i}{p}}$ and the quadratic form

$$F : \mathbb{F}_p^m \to \mathbb{F}_p, \quad F(x) = XHX^T \quad \big(X = (x_1, \ldots, x_m) \in \mathbb{F}_p^m\big), \tag{4}$$

we have the following result (see [5, Exercises 6.27 and 6.28] for the case $r = m$).

Lemma 1.

(i) *For the quadratic form $F = XHX^T$ defined in* (4)*,*

$$\sum_{X \in \mathbb{F}_p^m} \zeta_p^{F(X)} = \begin{cases} (\frac{\Delta}{p}) p^{m-r/2} & \text{if } p \equiv 1 \pmod 4, \\ i^r (\frac{\Delta}{p}) p^{m-r/2} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

(ii) *For $A = (a_1, \ldots, a_m) \in \mathbb{F}_p^m$, if $2YH + A = 0$ has solution $Y = B \in \mathbb{F}_p^m$, then $\sum_{X \in \mathbb{F}_p^m} \zeta_p^{F(X)+AX^T} = \zeta_p^c \sum_{X \in \mathbb{F}_p^m} \zeta_p^{F(X)}$ where $c = \frac{1}{2}AB^T \in \mathbb{F}_p$.*
Otherwise $\sum_{X \in \mathbb{F}_p^m} \zeta_p^{F(X)+AX^T} = 0$.

Proof. (i) From the formula of quadratic Gaussian sum over $\mathbb{F}_p$ we know that for $a \in \mathbb{F}_p^*$, $\sum_{x \in \mathbb{F}_p} \zeta_p^{ax^2} = (\frac{a}{p})\sqrt{p^*}$ where $p^* = (-1)^{\frac{p-1}{2}} p$ (see [5, Theorem 5.15]). Therefore

$$\sum_{X \in \mathbb{F}_p^m} \zeta_p^{F(X)} = \sum_{x_1, \ldots, x_m \in \mathbb{F}_p} \zeta_p^{a_1 x_1^2 + \cdots + a_r x_r^2} = \left(\frac{\Delta}{p}\right) p^{m-r} \left(p^*\right)^{\frac{r}{2}}$$
$$= \begin{cases} (\frac{\Delta}{p}) p^{m-r/2} & \text{if } p \equiv 1 \pmod 4, \\ i^r (\frac{\Delta}{p}) p^{m-r/2} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

(ii) If there is no $Y \in \mathbb{F}_p^m$ such that $2YH + A = 0$, then

$$\begin{aligned} &\sum_{X \in \mathbb{F}_p^m} \zeta_p^{-F(X)} \sum_{X' \in \mathbb{F}_p^m} \zeta_p^{F(X')+AX'^T} \\ &= \sum_{X, Y \in \mathbb{F}_p^m} \zeta_p^{F(X+Y)+A(X+Y)^T - F(X)} \\ &= \sum_{Y \in \mathbb{F}_p^m} \zeta_p^{YHY^T + AY^T} \sum_{X \in \mathbb{F}_p^m} \zeta_p^{2YHX^T + AX^T} \\ &= 0. \end{aligned}$$

Therefore $\sum_{X \in \mathbb{F}_p^m} \zeta_p^{F(X)+AX^T} = 0$. If $2BH + A = 0$ for some $B \in \mathbb{F}_p^m$, then

$$\sum_{X \in \mathbb{F}_p^m} \zeta_p^{F(X)+AX^T} = \sum_{X \in \mathbb{F}_p^m} \zeta_p^{F(X+B)+A(X+B)^T} = \sum_{X \in \mathbb{F}_p^m} \zeta_p^{F(X)+c},$$

where $c = BHB^T + AB^T = \frac{1}{2}AB^T \in \mathbb{F}_p$. □

The field $\mathbb{F}_q$ is a vector space over $\mathbb{F}_p$ with dimension m. We fix a basis $v_1, \ldots, v_m$ of $\mathbb{F}_q$ over $\mathbb{F}_p$. Then each $x \in \mathbb{F}_q$ can be uniquely expressed as

$$x = x_1 v_1 + \cdots + x_m v_m \quad (x_i \in \mathbb{F}_p).$$

Thus we have the following $\mathbb{F}_p$-linear isomorphism:

$$\mathbb{F}_q \xrightarrow{\sim} \mathbb{F}_p^m, \quad x = x_1 v_1 + \cdots + x_m v_m \mapsto X = (x_1, \ldots, x_m).$$

With this isomorphism, a function $f : \mathbb{F}_q \to \mathbb{F}_p$ induces a function $F : \mathbb{F}_p^m \to \mathbb{F}_p$ where for $X = (x_1, \ldots, x_m) \in \mathbb{F}_p^m$, $F(X) = f(x)$ where $x = x_1 v_1 + \cdots + x_m v_m$. In this way, function $f(x) = \mathrm{Tr}(\gamma x)$ for $\gamma \in \mathbb{F}_q$ induces a linear form $F(X) = \sum_{i=1}^m \mathrm{Tr}(\gamma v_i) x_i = A_\gamma X^T$ where $A_\gamma = (\mathrm{Tr}(\gamma v_1), \ldots, \mathrm{Tr}(\gamma v_m))$, and function $f_{\alpha,\beta}(x) = \mathrm{Tr}(\alpha x^{p^k+1} + \beta x^2)$ induces a quadratic form

$$\begin{aligned}
F_{\alpha,\beta}(X) &= \mathrm{Tr}\left(\alpha\left(\sum_{i=1}^m x_i v_i\right)^{p^k+1} + \beta\left(\sum_{i=1}^m x_i v_i\right)^2\right) \\
&= \mathrm{Tr}\left(\alpha\left(\sum_{i=1}^m x_i v_i^{p^k}\right)\left(\sum_{i=1}^m x_i v_i\right) + \beta\left(\sum_{i=1}^m x_i v_i\right)^2\right) \\
&= \sum_{i,j=1}^m \mathrm{Tr}\big(\alpha v_i^{p^k} v_j + \beta v_i v_j\big) x_i x_j = X H_{\alpha,\beta} X^T,
\end{aligned}$$

where

$$H_{\alpha,\beta} = (h_{ij}) \quad \text{and} \quad h_{ij} = \frac{1}{2}\mathrm{Tr}\big(\alpha v_i^{p^k} v_j + \alpha v_i v_j^{p^k}\big) + \mathrm{Tr}(\beta v_i v_j) \quad \text{for } 1 \leqslant i, j \leqslant m.$$

Let m and k be co-prime positive integers. In order to determine the values of

$$T(\alpha, \beta) = \sum_{x \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}(\alpha x^{p^k+1} + \beta x^2)} = \sum_{X \in \mathbb{F}_p^m} \zeta_p^{X H_{\alpha,\beta} X^T}$$

and

$$S(\alpha, \beta, \gamma) = \sum_{x \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}(\alpha x^{p^k+1} + \beta x^2 + \gamma x)} = \sum_{X \in \mathbb{F}_p^m} \zeta_p^{X H_{\alpha,\beta} X^T + A_\gamma X^T} \quad (\alpha, \beta, \gamma \in \mathbb{F}_q),$$

we need to determine the rank of $H_{\alpha,\beta}$ over $\mathbb{F}_p$ and the solvability of $\mathbb{F}_p$-linear equation $2X H_{\alpha,\beta} + A_\gamma = 0$.

Lemma 2.

(i) *For* $(\alpha, \beta) \in \mathbb{F}_q^2 \setminus \{(0,0)\}$, $r_{\alpha,\beta} = \mathrm{rank}\, H_{\alpha,\beta}$ *is* m, $m-1$ *or* $m-2$.

(ii) *Let* n_i *be the number of* $H_{\alpha,\beta}$ *with* $r_{\alpha,\beta} = m - i$ *for* $(\alpha, \beta) \in \mathbb{F}_q^2 \setminus \{(0,0)\}$ *and* $0 \leqslant i \leqslant 2$. *Then*

$$n_2 = \frac{(p^m - 1)(p^{m-1} - 1)}{p^2 - 1}, \qquad n_1 = \big(p^m - 1\big)p^{m-1}, \qquad n_0 = p^{2m} - 1 - n_1 - n_2.$$

Proof. (i) For $Y=(y_1,\dots,y_m)\in\mathbb{F}_p^m$, $y=y_1v_1+\cdots+y_mv_m\in\mathbb{F}_q$, we have

$$F_{\alpha,\beta}(X+Y)-F_{\alpha,\beta}(X)-F_{\alpha,\beta}(Y)=2YH_{\alpha,\beta}X^T$$

and

$$f_{\alpha,\beta}(x+y)-f_{\alpha,\beta}(x)-f_{\alpha,\beta}(y)=\mathrm{Tr}\big(y^{p^k}\big(\alpha^{p^k}x^{p^{2k}}+2\beta^{p^k}x^{p^k}+\alpha x\big)\big).$$

Let $\phi_{\alpha,\beta}(x)=\alpha^{p^k}x^{p^{2k}}+2\beta^{p^k}x^{p^k}+\alpha x$. Therefore,

$$\begin{aligned} r_{\alpha,\beta}=r \quad &\Leftrightarrow\quad \text{the number of common solutions of } YH_{\alpha,\beta}X^T=0 \quad \text{for all } Y\in\mathbb{F}_p^m \text{ is } p^{m-r},\\ &\Leftrightarrow\quad \text{the number of common solutions of } \mathrm{Tr}\big(y^{p^k}\phi_{\alpha,\beta}(x)\big)=0\\ &\qquad\ \ \text{for all } y\in\mathbb{F}_q \text{ is } p^{m-r},\\ &\Leftrightarrow\quad \phi_{\alpha,\beta}(x)=0 \text{ has } p^{m-r} \text{ solutions in } \mathbb{F}_q. \end{aligned}$$

Fix an algebraic closure $\mathbb{F}_{p^\infty}$ of $\mathbb{F}_p$, then the zeroes of $\phi_{\alpha,\beta}(x)$ in $\mathbb{F}_{p^\infty}$, say V, form an $\mathbb{F}_{p^k}$-vector space of dimension 2. Note that $\gcd(m,k)=1$. Then $V\cap\mathbb{F}_{p^m}$ is a vector space on $\mathbb{F}_{p^{\gcd(m,k)}}=\mathbb{F}_p$ with dimension at most 2 since any elements in $\mathbb{F}_q$ which are linear independent over $\mathbb{F}_p$ are also linear independent over $\mathbb{F}_{p^k}$(see [7, Lemma 4]). Therefore $r_{\alpha,\beta}$ is not less than $m-2$ for $(\alpha,\beta)\in\mathbb{F}_q^2\setminus\{(0,0)\}$.

(ii) Let $N_i=\#\{(\alpha,\beta)\in\mathbb{F}_q^2\setminus\{(0,0)\}\colon r_{\alpha,\beta}=m-i\}$ for $i=0,1,2$. Then

$$n_0+n_1+n_2=q^2-1=p^{2m}-1. \tag{5}$$

Suppose that $(\alpha,\beta)\in\mathbb{F}_q^2\setminus\{(0,0)\}$ and rank $H_{\alpha,\beta}=m-2$ which means that the set V' of zeros of $\phi_{\alpha,\beta}(x)=\alpha^{p^k}x^{p^{2k}}+2\beta^{p^k}x^{p^k}+\alpha x$ is a 2-dimensional subspace of $\mathbb{F}_q$ over $\mathbb{F}_p$. Let $\{v_1,v_2\}$ be a fixed basis of V' over $\mathbb{F}_p$, then $v_1,v_2\in\mathbb{F}_q^*$ and $v_1v_2^{-1}\notin\mathbb{F}_p$. From $\phi_{\alpha,\beta}(v_1)=\phi_{\alpha,\beta}(v_2)=0$ we get

$$\alpha^{p^k}\big(v_1^{p^{2k}}v_2^{p^k}-v_1^{p^k}v_2^{p^{2k}}\big)=\alpha\big(v_1^{p^k}v_2-v_1v_2^{p^k}\big). \tag{6}$$

Let $w=\alpha(v_1^{p^k}v_2-v_1v_2^{p^k})$. Then $w^{p^k}=w$ so that $w\in\mathbb{F}_{p^k}\cap\mathbb{F}_q=\mathbb{F}_p$. We claim that $w\neq 0$. In fact, if $w=0$, then either $\alpha=0$ so that $\beta\neq 0$ and $\phi_{0,\beta}(x)=2\beta^{p^k}x^{p^k}$ has unique solution $x=0$, or $v_1^{p^k}v_2-v_1v_2^{p^k}=0$ so that $(v_1v_2^{-1})^{p^k-1}=1$ and $v_1v_2^{-1}\in\mathbb{F}_{p^k}\cap\mathbb{F}_q=\mathbb{F}_p$. Therefore $w\in\mathbb{F}_p^*$ which means that $\alpha=w(v_1^{p^k}v_2-v_1v_2^{p^k})^{-1}$ is determined by V' up to a factor in $\mathbb{F}_p^*$. Then β is determined by

$$\beta=-\frac{1}{2}v_1^{-1}\big(\alpha v_1^{p^k}+\alpha^{p^{m-k}}v_1^{p^{m-k}}\big). \tag{7}$$

Conversely, if $\omega=\alpha(v_1^{p^k}v_2-v_1v_2^{p^k})\in\mathbb{F}_p^*$ and $\beta=-\frac{1}{2}v_1^{-1}(\alpha v_1^{p^k}+\alpha^{p^{m-k}}v_1^{p^{m-k}})$, then $v_1v_2^{-1}\notin\mathbb{F}_p^*$ and we get from (6) and (7) that $\phi_{\alpha,\beta}(v_1)=\phi_{\alpha,\beta}(v_2)=0$. Therefore the set of zeros of

$\phi_{\alpha,\beta}(x) = 0$ is the $\mathbb{F}_p$-linear space spanned by v_1 and v_2. The number of 2-dimensional subspaces of $\mathbb{F}_q$ over $\mathbb{F}_p$ is

$$\begin{bmatrix} m \\ 2 \end{bmatrix}_p = \frac{(q-1)(q-p)}{(p^2-1)(p^2-p)}.$$

Therefore

$$n_2 = (p-1)\begin{bmatrix} m \\ 2 \end{bmatrix}_p = \frac{(p^m-1)(p^{m-1}-1)}{(p^2-1)}. \tag{8}$$

Now consider the following map:

$$\psi : \mathbb{F}_q^* \times \mathbb{F}_q^* \to \mathbb{F}_q, \quad (\alpha, s) \mapsto \psi(\alpha, s) = -\frac{1}{2}s^{-1}\big(\alpha s^{p^k} + \alpha^{p^{m-k}} s^{p^{m-k}}\big).$$

Then for $\alpha, s \in \mathbb{F}_q^*$ and $\beta \in \mathbb{F}_q$,

$$\alpha^{p^k} s^{p^{2k}} + 2\beta^{p^k} s^{p^k} + \alpha s = 0 \quad \Leftrightarrow \quad \psi(\alpha, s) = \beta.$$

For $\alpha \in \mathbb{F}_q^*$, let

$$N_{\alpha 1} = \big\{\beta \in \mathbb{F}_q \bigm| \text{the number of } s \in \mathbb{F}_q^* \text{ satisfying } \psi(\alpha, s) = \beta \text{ is } p-1\big\},$$
$$N_{\alpha 2} = \big\{\beta \in \mathbb{F}_q \bigm| \text{the number of } s \in \mathbb{F}_q^* \text{ satisfying } \psi(\alpha, s) = \beta \text{ is } p^2-1\big\}.$$

Then

$$(p-1)|N_{\alpha 1}| + \big(p^2-1\big)|N_{\alpha 2}| = \sum_{s \in \mathbb{F}_q^*} 1 = q-1$$

so that

$$\begin{aligned}\big(p^m-1\big)^2 &= \sum_{\alpha \in \mathbb{F}_q^*} (q-1) = (p-1)\sum_{\alpha \in \mathbb{F}_q^*} |N_{\alpha 1}| + \big(p^2-1\big)\sum_{\alpha \in \mathbb{F}_q^*} |N_{\alpha 2}| \\ &= (p-1)n_1 + \big(p^2-1\big)n_2. \end{aligned} \tag{9}$$

The conclusion of Lemma 2(ii) is derived from (5), (8) and (9). □

In order to determine the multiplicity of each value of $T(\alpha, \beta)$ and $S(\alpha, \beta, \gamma)$ for $\alpha, \beta, \gamma \in \mathbb{F}_q$, we need the following result on moments of $T(\alpha, \beta)$ and $S(\alpha, \beta, \gamma)$.

Lemma 3. *For the exponential sum $T(\alpha, \beta)$ and $S(\alpha, \beta, \gamma)$,*

(i)
$$\sum_{\alpha, \beta \in \mathbb{F}_q} T(\alpha, \beta) = p^{2m};$$

(ii)
$$\sum_{\alpha, \beta \in \mathbb{F}_q} T(\alpha, \beta)^2 = \begin{cases} (2p^m-1) \cdot p^{2m} & \text{if } p \equiv 1 \pmod 4, \\ p^{2m} & \text{if } p \equiv 3 \pmod 4; \end{cases}$$

(iii) *if m is even* (*so that k is odd*), *then*

$$\sum_{\alpha,\beta\in\mathbb{F}_q} T(\alpha,\beta)^3 = \left(p^m + p^{m-1} - 1\right)\cdot p^{2m+1};$$

(iv) *let N be a subset of $\mathbb{F}_q^2$, then*

$$\sum_{\substack{(\alpha,\beta)\in N\\ \gamma\in\mathbb{F}_q}} S(\alpha,\beta,\gamma) = q\cdot|N|.$$

Proof. (i) We can calculate:

$$\begin{aligned}\sum_{\alpha,\beta\in\mathbb{F}_q} T(\alpha,\beta) &= \sum_{\alpha,\beta\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_q}\chi\left(\alpha x^{p^k+1}+\beta x^2\right)\\ &= \sum_{x\in\mathbb{F}_q}\sum_{\alpha\in\mathbb{F}_q}\chi\left(\alpha x^{p^k+1}\right)\sum_{\beta\in\mathbb{F}_q}\chi\left(\beta x^2\right) = q\cdot\sum_{\substack{\alpha\in\mathbb{F}_q\\ x=0}}\chi\left(\alpha x^{p^k+1}\right) = q^2.\end{aligned}$$

(ii) We observe that

$$\begin{aligned}\sum_{\alpha,\beta\in\mathbb{F}_q} T(\alpha,\beta)^2 &= \sum_{\alpha,x,y\in\mathbb{F}_q}\chi\left(\alpha\left(x^{p^k+1}+y^{p^k+1}\right)\right)\sum_{\beta\in\mathbb{F}_q}\chi\left(\beta\left(x^2+y^2\right)\right)\\ &= T\cdot p^{2m},\end{aligned}$$

where

$$\begin{aligned}T &= \#\left\{(x,y)\in\mathbb{F}_q^2 \mid x^2+y^2=0,\ x^{p^k+1}+y^{p^k+1}=0\right\}\\ &= \#\left\{(x,y)\in\mathbb{F}_q^2 \mid x^2+y^2=0, \left(1+(-1)^{\frac{p^k+1}{2}}\right)x^{p^k+1}=0\right\}.\end{aligned}$$

If $p\equiv 1 \pmod 4$, there exists $t\in\mathbb{F}_q^*$ such that $t^2=-1$. Since $\frac{p^k+1}{2}$ is odd, we have

$$\begin{aligned}T &= \#\left\{(x,y)\in\mathbb{F}_q^2 \mid x^2+y^2=0\right\} = \#\left\{(x,y)\in\mathbb{F}_q^2 \mid y=\pm tx\right\}\\ &= 1+2(q-1) = 2q-1.\end{aligned}\tag{10}$$

Suppose that $p\equiv 3 \pmod 4$. If k is even so that m is odd and $q=p^m\equiv 3 \pmod 4$. There is no $t\in\mathbb{F}_q$ such that $t^2=-1$. Therefore

$$T = \#\left\{(x,y)\in\mathbb{F}_q^2 \mid y^2=-x^2\right\} = \#\left\{(x,y)\in\mathbb{F}_q^2 \mid y^2=-x^2,\ x=0\right\} = 1.\tag{11}$$

If k is odd, then $\frac{p^k+1}{2}$ is even and $1+(-1)^{\frac{p^k+1}{2}}=2$ so that we also have

$$T = \#\left\{(x,y)\in\mathbb{F}_q^2 \mid y^2=-x^2,\ x=0\right\} = 1.\tag{12}$$

(iii) We have

$$\sum_{\alpha,\beta\in\mathbb{F}_q} T(\alpha,\beta)^3 = M\cdot q^2, \quad \text{where}$$

$$\begin{aligned} M &= \#\{(x,y,z)\in\mathbb{F}_q^3 \mid x^2+y^2+z^2=0,\ x^{p^k+1}+y^{p^k+1}+z^{p^k+1}=0\} \\ &= T + T'\cdot(q-1) \end{aligned} \tag{13}$$

and

$$\begin{aligned} T' &= \#\{(x,y)\in\mathbb{F}_q^2 \mid x^2+y^2+1=0,\ x^{p^k+1}+y^{p^k+1}+1=0\} \\ &= \#\{(x,y)\in\mathbb{F}_q^2 \mid x^{p^k+1}+(-1)^{\frac{p^k+1}{2}}(x^2+1)^{\frac{p^k+1}{2}}+1=0,\ y^2=-(1+x^2)\}. \end{aligned}$$

For each $x\in\mathbb{F}_q$, let $\theta = 2x^2+1+2x\sqrt{x^2+1}\in\mathbb{F}_{q^2}^*$. Then $4x^2+2=\theta+\theta^{-1}$.

If $p\equiv 1 \pmod 4$, then

$$\begin{aligned} x^{p^k+1}+(-1)^{\frac{p^k+1}{2}}(x^2+1)^{\frac{p^k+1}{2}}+1 &= \left(\frac{1}{4}(\theta+\theta^{-1}-2)\right)^{\frac{p^k+1}{2}} - \left(\frac{1}{4}(\theta+\theta^{-1}+2)\right)^{\frac{p^k+1}{2}}+1 \\ &= \frac{1}{4}\cdot\theta^{-\frac{p^k+1}{2}}\cdot\left[(\theta-1)^{p^k+1}-(\theta+1)^{p^k+1}+4\theta^{\frac{p^k+1}{2}}\right] \\ &= \frac{1}{4}\cdot\theta^{-\frac{p^k+1}{2}}\cdot\left(-2\theta^{p^k}-2\theta+4\theta^{\frac{p^k+1}{2}}\right) \\ &= -\frac{1}{2}\cdot\theta^{\frac{-p^k+1}{2}}\cdot\left(\theta^{\frac{p^k-1}{2}}-1\right)^2. \end{aligned}$$

Note that $\gcd(\frac{p^k-1}{2}, p^{2m}-1) = \frac{p-1}{2}$ since k is odd and $\gcd(k,m)=1$. Therefore

$$x^{p^k+1}+(-1)^{\frac{p^k+1}{2}}(x^2+1)^{\frac{p^k+1}{2}}+1=0 \quad\Leftrightarrow\quad \theta^{\frac{p^k-1}{2}}=1 \quad\Leftrightarrow\quad \theta\in(\mathbb{F}_{p^k}^*)^2\cap\mathbb{F}_{q^2}^* = (\mathbb{F}_p^*)^2.$$

Let $\theta\in(\mathbb{F}_p^*)^2$ so that $\theta=\tau^2$ where $\tau\in\mathbb{F}_p^*$, then $1+x^2=\frac{1}{4}(\theta+\theta^{-1}+2)=\frac{1}{4}(\tau+\tau^{-1})^2$. Therefore $T'=|S|$ where

$$S=\{(x,y)\in\mathbb{F}_q^2 \mid \text{there exists } \tau\in\mathbb{F}_p^* \text{ such that } 4x^2=(\tau-\tau^{-1})^2,\ 4y^2=-(\tau+\tau^{-1})^2\}.$$

Since $p\equiv 1 \pmod 4$, we have $t\in\mathbb{F}_p^*$ such that $t^2=-1$. Then $\tau=\pm 1$ gives $x=0$ and $y=\pm t$ in S, $\tau=\pm t$ gives $y=0$ and $x=\pm t$ in S. For remaining $p-5$ elements in $\mathbb{F}_p^*$, $\tau=\pm a$ and $\pm a^{-1}$ gives four (x,y) in S: $x=\pm\frac{1}{2}(a-a^{-1})$, $y=\pm\frac{1}{2}t(a+a^{-1})$. Therefore $T'=2+2+4\cdot\frac{p-5}{4}=p-1$ and by (10) and (13), $\sum_{\alpha,\beta\in\mathbb{F}_q} T(\alpha,\beta)^3 = q^2(T+T'(q-1)) = q^2(2q-1+(p-1)(q-1)) = (p^m+p^{m-1}-1)p^{2m+1}$.

If $p\equiv 3 \pmod 4$, then $p^k+1\equiv 0 \pmod 4$ so that

$$\begin{aligned} x^{p^k+1}+(-1)^{\frac{p^k+1}{2}}\big(x^2+1\big)^{\frac{p^k+1}{2}}+1 &= \left(\frac{1}{4}\big(\theta+\theta^{-1}-2\big)\right)^{\frac{p^k+1}{2}}+\left(\frac{1}{4}\big(\theta+\theta^{-1}+2\big)\right)^{\frac{p^k+1}{2}}+1\\ &= \frac{1}{4}\cdot\theta^{-\frac{p^k+1}{2}}\cdot\big[(\theta-1)^{p^k+1}+(\theta+1)^{p^k+1}+4\theta^{\frac{p^k+1}{2}}\big]\\ &= \frac{1}{4}\cdot\theta^{-\frac{p^k+1}{2}}\cdot\big(2\theta^{p^k+1}+2+4\theta^{\frac{p^k+1}{2}}\big)\\ &= \frac{1}{2}\cdot\theta^{-\frac{p^k+1}{2}}\cdot\big(\theta^{\frac{p^k+1}{2}}+1\big)^2. \end{aligned}$$

Therefore

$$\begin{aligned} &x^{p^k+1}+(-1)^{\frac{p^k+1}{2}}\big(x^2+1\big)^{\frac{p^k+1}{2}}+1=0\\ &\quad\Leftrightarrow\quad \theta^{\frac{p^k+1}{2}}=-1\\ &\quad\Leftrightarrow\quad \theta^{\frac{p+1}{2}}=-1\quad\left(\text{since } \theta^{q^2-1}=1, k \text{ is odd and } \gcd\left(\frac{p^k+1}{2},q^2-1\right)=\frac{p+1}{2}\right)\\ &\quad\Leftrightarrow\quad \theta=g^{(2j+1)(p-1)}\quad\left(0\leqslant j\leqslant\frac{p-1}{2} \text{ and } g \text{ is a primitive element of } \mathbb{F}_{p^2}\right). \end{aligned}$$

For $\theta=g^{(2j+1)(p-1)}$, $\tau=\sqrt{\theta}=\pm g^{(2j+1)\frac{p-1}{2}}\in\mathbb{F}_{p^2}^*$. Since m is even, then $-1=t^2$ for some $t\in\mathbb{F}_{p^2}^*\subset\mathbb{F}_q^*$. Hence we have $T'=|R|$ where

$$R=\left\{(x,y)\in\mathbb{F}_q^2\ \middle|\ x=\pm\frac{1}{2}\big(\tau-\tau^{-1}\big),\ y=\pm\frac{1}{2}t\big(\tau+\tau^{-1}\big)\ \text{for } \tau=\pm g^{(2j+1)\frac{p-1}{2}}, 0\leqslant j\leqslant\frac{p-1}{2}\right\}.$$

Define

$$L=\left\{\tau=\pm g^{(2j+1)\frac{p-1}{2}}\ \middle|\ 0\leqslant j\leqslant\frac{p-1}{2}\right\}.$$

If $\tau\in L$ and $\tau=\pm g^{(2j+1)\frac{p-1}{2}}$ for some j, $0\leqslant j\leqslant\frac{p-1}{2}$, then $-\tau=\mp g^{(2j+1)\frac{p-1}{2}}$, $\tau^{-1}=\mp g^{(p-2j)\frac{p-1}{2}}$ and $-\tau^{-1}=\pm g^{(p-2j)\frac{p-1}{2}}$ are all in L. Note that $\frac{1}{2}(-\tau-(-\tau)^{-1})=\frac{1}{2}(\tau^{-1}-\tau)=-\frac{1}{2}(\tau-\tau^{-1})$ and $\frac{1}{2}(-\tau+(-\tau)^{-1})=-\frac{1}{2}(\tau^{-1}+\tau)$. Then four different elements $\pm\tau,\pm\tau^{-1}$ with $\tau=\pm g^{(2j+1)\frac{p-1}{2}}$ for some j, $0\leqslant j\leqslant\frac{p-1}{2}$, give four different pairs (x,y) with $x=\pm\frac{1}{2}(\tau-\tau^{-1})$, $y=\pm\frac{1}{2}t(\tau+\tau^{-1})$ in R. We have $T'=2\cdot\frac{p+1}{2}=p+1$. By (12) and (13) we obtain

$$\sum_{\alpha,\beta\in\mathbb{F}_q}T(\alpha,\beta)^3=q^2\big(1+(p+1)(q-1)\big)=\big(p^m+p^{m-1}-1\big)p^{2m+1}.$$

(iv) We can calculate

$$\sum_{\substack{(\alpha,\beta)\in N\\ \gamma\in\mathbb{F}_q}} S(\alpha,\beta,\gamma)=\sum_{(\alpha,\beta)\in N}\sum_{x\in\mathbb{F}_q}\chi\left(\alpha x^{p^k+1}+\beta x^2\right)\sum_{\gamma\in\mathbb{F}_q}\chi(\gamma x)$$

$$=q\cdot\sum_{\substack{(\alpha,\beta)\in N\\ x=0}}\chi\left(\alpha x^{p^k+1}+\beta x^2\right)=q\cdot|N|. \qquad \square$$

Remark. For case m is odd, $\sum_{\alpha,\beta\in\mathbb{F}_q} T(\alpha,\beta)^3$ can also be determined, but it is not necessary in this paper.

At the end of this section, we state a well-known fact on Galois group of the cyclotomic field $\mathbb{Q}(\zeta_p)$ since $T(\alpha,\beta)$ and $S(\alpha,\beta,\gamma)$ are elements in $\mathbb{Q}(\zeta_p)$ (see [4], for example).

Lemma 4. *The Galois group of $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$ is $\{\sigma_a \mid 1\leqslant a\leqslant p-1\}$ where the automorphism σ_a of $\mathbb{Q}(\zeta_p)$ is determined by $\sigma_a(\zeta_p)=\zeta_p^a$. The unique quadratic subfield of $\mathbb{Q}(\zeta_p)$ is $\mathbb{Q}(\sqrt{p^*})$ where $p^*=(\frac{-1}{p})p$ and $\sigma_a(\sqrt{p^*})=(\frac{a}{p})\sqrt{p^*}$ $(1\leqslant a\leqslant p-1)$.*

3. Results on exponential sums $T(\alpha,\beta)$ and cyclic code $\mathcal{C}_1$

In this section we prove the following results.

Theorem 1. *For $m\geqslant 3$ and $\gcd(m,k)=1$, the value distribution of the multi-set $\{T(\alpha,\beta)\mid \alpha,\beta\in\mathbb{F}_q\}$ is shown as following.*

(i) *For case m is odd, Table 1 holds.*
(ii) *For case m is even, Table 2 holds.*

Proof. According to the possible values of $T(\alpha,\beta)$ given by Lemma 1, we define that for $\varepsilon=\pm 1$ and $i\in\{0,1,2\}$

$$N_{\varepsilon,i}=\begin{cases}\{(\alpha,\beta)\in\mathbb{F}_q^2\setminus\{(0,0)\}\mid T(\alpha,\beta)=\varepsilon p^{\frac{m+i}{2}}\} & \text{if } m-i \text{ is even},\\ \{(\alpha,\beta)\in\mathbb{F}_q^2\setminus\{(0,0)\}\mid T(\alpha,\beta)=\varepsilon\sqrt{p^*}p^{\frac{m+i-1}{2}}\} & \text{if } m-i \text{ is odd},\end{cases}$$

and $n_{\varepsilon,i}=|N_{\varepsilon,i}|$.

Table 1

Values	Multiplicity
$\sqrt{p^*}p^{\frac{m-1}{2}}, -\sqrt{p^*}p^{\frac{m-1}{2}}$	$\frac{1}{2}p^2(p^m-p^{m-1}-p^{m-2}+1)(p^m-1)/(p^2-1)$
$p^{\frac{m+1}{2}}$	$\frac{1}{2}p^{\frac{m-1}{2}}(p^{\frac{m-1}{2}}+1)(p^m-1)$
$-p^{\frac{m+1}{2}}$	$\frac{1}{2}p^{\frac{m-1}{2}}(p^{\frac{m-1}{2}}-1)(p^m-1)$
$\sqrt{p^*}p^{\frac{m+1}{2}}, -\sqrt{p^*}p^{\frac{m+1}{2}}$	$\frac{1}{2}(p^m-1)(p^{m-1}-1)/(p^2-1)$
p^m	1

Table 2

Values	Multiplicity
$p^{\frac{m}{2}}$	$\frac{1}{2}p^2(p^m - p^{m-1} - p^{m-2} + p^{\frac{m}{2}} - p^{\frac{m}{2}-1} + 1)(p^m - 1)/(p^2 - 1)$
$-p^{\frac{m}{2}}$	$\frac{1}{2}p^2(p^m - p^{m-1} - p^{m-2} - p^{\frac{m}{2}} + p^{\frac{m}{2}-1} + 1)(p^m - 1)/(p^2 - 1)$
$\sqrt{p^*}p^{\frac{m}{2}}, -\sqrt{p^*}p^{\frac{m}{2}}$	$\frac{1}{2}p^{m-1}(p^m - 1)$
$p^{\frac{m}{2}+1}$	$\frac{1}{2}(p^{\frac{m}{2}} - 1)(p^{\frac{m}{2}-1} + 1)(p^m - 1)/(p^2 - 1)$
$-p^{\frac{m}{2}+1}$	$\frac{1}{2}(p^{\frac{m}{2}} + 1)(p^{\frac{m}{2}-1} - 1)(p^m - 1)/(p^2 - 1)$
p^m	1

Then from Lemma 2 we have

$$n_{1,i} + n_{-1,i} = \begin{cases} (p^m - 1)(p^{m-1} - 1)/(p^2 - 1) & \text{for } i = 2, \\ (p^m - 1)p^{m-1} & \text{for } i = 1, \\ p^{2m} - 1 - n_1 - n_2 & \text{for } i = 0. \end{cases} \tag{14}$$

If $m - i$ is odd, and $T(\alpha, \beta) = \varepsilon(p^*)^{\frac{m-i}{2}} p^i$, by Lemma 4 we know that for $1 \leqslant a \leqslant p - 1$,

$$T(a\alpha, a\beta) = \sigma_a\big(T(\alpha, \beta)\big) = \varepsilon\big(\sigma_a\big(\sqrt{p^*}\big)\big)^{m-i} p^i = \varepsilon\left(\frac{a}{p}\right)\big(\sqrt{p^*}\big)^{m-i} p^i = \left(\frac{a}{p}\right)T(\alpha, \beta).$$

Therefore

$$n_{1,i} = n_{-1,i} = \frac{1}{2}n_i \quad \text{for } m - i \text{ odd.} \tag{15}$$

(i) For case m is odd, by (14) and (15) we know that

$$n_{1,0} = n_{-1,0} = \frac{1}{2}n_0 = \frac{1}{2}p^2\big(p^m - p^{m-1} - p^{m-2} + 1\big)\frac{p^m - 1}{p^2 - 1}, \tag{16}$$

$$n_{1,2} = n_{-1,2} = \frac{1}{2}n_2 = \frac{1}{2}\big(p^m - 1\big)\frac{p^{m-1} - 1}{p^2 - 1}, \tag{17}$$

$$n_{1,1} + n_{-1,1} = n_1 = \big(p^m - 1\big)p^{m-1}. \tag{18}$$

Moreover, from Lemma 3 we have

$$p^{2m} = \sum_{\alpha, \beta \in \mathbb{F}_q} T(\alpha, \beta) = p^m + (n_{1,1} - n_{-1,1})p^{\frac{m+1}{2}}.$$

Thus

$$n_{1,1} - n_{-1,1} = p^{\frac{m-1}{2}}\big(p^m - 1\big). \tag{19}$$

From (18) and (19) we get

$$n_{\pm 1,1} = \frac{1}{2}p^{\frac{m-1}{2}}\big(p^{\frac{m-1}{2}} \pm 1\big)\big(p^m - 1\big). \tag{20}$$

The value distribution of $T(\alpha, \beta)$ for m odd is obtained from (16), (17) and (20).

(ii) For case m is even, by (14) and (15) we know that

$$n_{1,0}+n_{-1,0}=n_0=p^2\big(p^m-p^{m-1}-p^{m-2}+1\big)\frac{p^m-1}{p^2-1}, \tag{21}$$

$$n_{1,2}+n_{-1,2}=n_2=\big(p^{m-1}-1\big)\frac{p^m-1}{p^2-1}, \tag{22}$$

$$n_{1,1}=n_{-1,1}=\frac{1}{2}n_1=\frac{1}{2}\big(p^m-1\big)p^{m-1}. \tag{23}$$

Moreover, from Lemma 3(i) and (iii) we have

$$p^{2m}=\sum_{\alpha,\beta\in\mathbb{F}_q}T(\alpha,\beta)=p^m+(n_{1,0}-n_{-1,0})p^{\frac{m}{2}}+(n_{1,2}-n_{-1,2})p^{\frac{m}{2}+1}, \tag{24}$$

$$\big(p^m+p^{m-1}-1\big)p^{2m+1}=\sum_{\alpha,\beta\in\mathbb{F}_q}T(\alpha,\beta)^3=p^{3m}+(n_{1,0}-n_{-1,0})p^{\frac{3m}{2}}+(n_{1,2}-n_{-1,2})p^{\frac{3m}{2}+3}. \tag{25}$$

From (24) and (25) we get

$$n_{1,0}-n_{-1,0}=p^{\frac{m}{2}+1}\cdot\frac{p^m-1}{p+1}, \tag{26}$$

$$n_{1,2}-n_{-1,2}=p^{\frac{m}{2}-1}\cdot\frac{p^m-1}{p+1}. \tag{27}$$

Then from (21), (22), (26) and (27) we have

$$n_{\pm1,0}=\frac{1}{2}p^2\big(p^m-p^{m-1}-p^{m-2}+1\pm\big(p^{\frac{m}{2}}-p^{\frac{m}{2}-1}\big)\big)\frac{p^m-1}{p^2-1}, \tag{28}$$

$$n_{\pm1,2}=\frac{1}{2}\big(p^{\frac{m}{2}}\mp1\big)\big(p^{\frac{m}{2}-1}\pm1\big)\frac{p^m-1}{p^2-1}. \tag{29}$$

The value distribution of $T(\alpha,\beta)$ for m even is obtained by (23), (28) and (29). This completes the proof of Theorem 1. □

Theorem 2. *For $m\geqslant 3$ and $\gcd(m,k)=1$, the weight distribution $\{A_0,A_1,\dots,A_n\}$ of the cyclic code $\mathcal{C}_1$ over $\mathbb{F}_p$ $(p\geqslant 3)$ with length $n=q-1$ and $\dim_{\mathbb{F}_p}\mathcal{C}_1=2m$ is shown as following.*

(i) *For case m is odd, $A_i=0$ except for values indicated in Table 3.*
(ii) *For case m is even, $A_i=0$ except for values indicated in Table 4.*

Table 3

i	A_i
$(p-1)(p^{m-1}-p^{\frac{m-1}{2}})$	$\frac{1}{2}p^{\frac{m-1}{2}}(p^{\frac{m-1}{2}}+1)(p^m-1)$
$(p-1)p^{m-1}$	$(p^m-1)(p^m-p^{m-1}+1)$
$(p-1)(p^{m-1}+p^{\frac{m-1}{2}})$	$\frac{1}{2}p^{\frac{m-1}{2}}(p^{\frac{m-1}{2}}-1)(p^m-1)$
0	1

Table 4

i	A_i
$(p-1)(p^{m-1}-p^{\frac{m}{2}})$	$\frac{1}{2}(p^{\frac{m}{2}}-1)(p^{\frac{m}{2}-1}+1)(p^m-1)/(p^2-1)$
$(p-1)(p^{m-1}-p^{\frac{m}{2}-1})$	$\frac{1}{2}p^2(p^m-p^{m-1}-p^{m-2}+p^{\frac{m}{2}}-p^{\frac{m}{2}-1}+1)(p^m-1)/p^2-1$
$(p-1)p^{m-1}$	$p^{m-1}(p^m-1)$
$(p-1)(p^{m-1}+p^{\frac{m}{2}-1})$	$\frac{1}{2}p^2(p^m-p^{m-1}-p^{m-2}-p^{\frac{m}{2}}+p^{\frac{m}{2}-1}+1)(p^m-1)/(p^2-1)$
$(p-1)(p^{m-1}+p^{\frac{m}{2}})$	$\frac{1}{2}(p^{\frac{m}{2}}+1)(p^{\frac{m}{2}-1}-1)(p^m-1)/(p^2-1)$
0	1

Proof. From (1) we know that for each non-zero codeword $c(\alpha,\beta)=(c_0,\dots,c_{n-1})$ ($n=p^m-1$, $c_i=\mathrm{Tr}(\alpha\pi^{(p^k+1)i}+\beta\pi^{2i})$, $0\leqslant i\leqslant n-1$, and $(\alpha,\beta)\in\mathbb{F}_q^2\setminus\{(0,0)\}$), the Hamming weight of $c(\alpha,\beta)$ is

$$w_H\big(c(\alpha,\beta)\big)=p^{m-1}(p-1)-\frac{1}{p}\cdot R(\alpha,\beta),\tag{30}$$

where

$$R(\alpha,\beta)=\sum_{a=1}^{p-1}T(a\alpha,a\beta)=\sum_{a=1}^{p-1}\sigma_a\big(T(\alpha,\beta)\big).$$

If $T(\alpha,\beta)=\varepsilon p^l$ ($\varepsilon=\pm1, l\in\mathbb{Z}$), then $R(\alpha,\beta)=(p-1)\varepsilon p^l$. If $T(\alpha,\beta)=\varepsilon\sqrt{p^*}p^l$, then $R(\alpha,\beta)=T(\alpha,\beta)\cdot\sum_{a=1}^{p-1}(\frac{a}{p})=0$. Thus the weight distribution of $\mathcal{C}_1$ can be derived from Theorem 1 and (30) directly. □

Remark. Since $2=\gcd(p^m-1,2)\mid\gcd(p^m-1,p^k+1)$, the first $n'=\frac{n}{2}=\frac{p^m-1}{2}$ coordinates of each codeword of $\mathcal{C}_1$ form a cyclic code $\mathcal{C}_1'$ over $\mathbb{F}_p$ with length $n'=\frac{p^m-1}{2}$ and dimension $2m$. Let $(A_0',\dots,A_{n'}')$ be the weight distribution of $\mathcal{C}_1'$, then $A_i'=A_{2i}$ $(0\leqslant i\leqslant n')$.

4. Results on exponential sums $S(\alpha,\beta,\gamma)$ and cyclic code $\mathcal{C}_2$

In this section we prove the following results.

Theorem 3. *For $m\geqslant3$ and $\gcd(m,k)=1$, the value distribution of the multi-set $\{S(\alpha,\beta,\gamma)\mid\alpha,\beta,\gamma\in\mathbb{F}_q\}$ is shown as following.*

(i) *For case m is odd, Table 5 holds.*

Table 5

Value	Multiplicity
$\sqrt{p^*}p^{\frac{m-1}{2}}, -\sqrt{p^*}p^{\frac{m-1}{2}}$	$\frac{1}{2}p^{m+1}(p^m - p^{m-1} - p^{m-2} + 1)(p^m - 1)/(p^2 - 1)$
$\zeta_p^j\sqrt{p^*}p^{\frac{m-1}{2}}$, for $1 \leqslant j \leqslant p-1$	$\frac{1}{2}p^{\frac{m+3}{2}}(p^{\frac{m-1}{2}} + (\frac{-j}{p}))(p^m - p^{m-1} - p^{m-2} + 1)\frac{p^m-1}{p^2-1}$
$-\zeta_p^j\sqrt{p^*}p^{\frac{m-1}{2}}$, for $1 \leqslant j \leqslant p-1$	$\frac{1}{2}p^{\frac{m+3}{2}}(p^{\frac{m-1}{2}} - (\frac{-j}{p}))(p^m - p^{m-1} - p^{m-2} + 1)\frac{p^m-1}{p^2-1}$
$p^{\frac{m+1}{2}}$	$\frac{1}{2}p^{m-2}(p^{\frac{m-1}{2}} + 1)(p^{\frac{m-1}{2}} + p - 1)(p^m - 1)$
$-p^{\frac{m+1}{2}}$	$\frac{1}{2}p^{m-2}(p^{\frac{m-1}{2}} - 1)(p^{\frac{m-1}{2}} - p + 1)(p^m - 1)$
$\zeta_p^j p^{\frac{m+1}{2}}$, for $1 \leqslant j \leqslant p-1$	$\frac{1}{2}p^{m-2}(p^{m-1} - 1)(p^m - 1)$
$-\zeta_p^j p^{\frac{m+1}{2}}$, for $1 \leqslant j \leqslant p-1$	$\frac{1}{2}p^{m-2}(p^{m-1} - 1)(p^m - 1)$
$\sqrt{p^*}p^{\frac{m+1}{2}}, -\sqrt{p^*}p^{\frac{m+1}{2}}$	$\frac{1}{2}p^{m-3}(p^{m-1} - 1)(p^m - 1)/(p^2 - 1)$
$\zeta_p^j\sqrt{p^*}p^{\frac{m+1}{2}}$, for $1 \leqslant j \leqslant p-1$	$\frac{1}{2}p^{\frac{m-3}{2}}(p^{\frac{m-3}{2}} + (\frac{-j}{p}))(p^{m-1} - 1)\frac{p^m-1}{p^2-1}$
$-\zeta_p^j\sqrt{p^*}p^{\frac{m+1}{2}}$, for $1 \leqslant j \leqslant p-1$	$\frac{1}{2}p^{\frac{m-3}{2}}(p^{\frac{m-3}{2}} - (\frac{-j}{p}))(p^{m-1} - 1)\frac{p^m-1}{p^2-1}$
0	$(p^m - 1)(p^{2m-1} - p^{2m-2} + p^{2m-3} - p^{m-2} + 1)$
p^m	1

Table 6

Value	Multiplicity
$p^{\frac{m}{2}}$	$\frac{1}{2}p^{\frac{m}{2}+1}(p^{\frac{m}{2}} + p - 1)(p^m - p^{m-1} - p^{m-2} + p^{\frac{m}{2}} - p^{\frac{m}{2}-1} + 1)\frac{p^m-1}{p^2-1}$
$-p^{\frac{m}{2}}$	$\frac{1}{2}p^{\frac{m}{2}+1}(p^{\frac{m}{2}} - p + 1)(p^m - p^{m-1} - p^{m-2} - p^{\frac{m}{2}} + p^{\frac{m}{2}-1} + 1)\frac{p^m-1}{p^2-1}$
$\zeta_p^j p^{\frac{m}{2}}$, for $1 \leqslant j \leqslant p-1$	$\frac{1}{2}p^{\frac{m}{2}+1}(p^{\frac{m}{2}} - 1)(p^m - p^{m-1} - p^{m-2} + p^{\frac{m}{2}} - p^{\frac{m}{2}-1} + 1)\frac{p^m-1}{p^2-1}$
$-\zeta_p^j p^{\frac{m}{2}}$, for $1 \leqslant j \leqslant p-1$	$\frac{1}{2}p^{\frac{m}{2}+1}(p^{\frac{m}{2}} + 1)(p^m - p^{m-1} - p^{m-2} - p^{\frac{m}{2}} + p^{\frac{m}{2}-1} + 1)\frac{p^m-1}{p^2-1}$
$\sqrt{p^*}p^{\frac{m}{2}}, -\sqrt{p^*}p^{\frac{m}{2}}$	$\frac{1}{2}p^{2m-3}(p^m - 1)$
$\zeta_p^j\sqrt{p^*}p^{\frac{m}{2}}$, for $1 \leqslant j \leqslant p-1$	$\frac{1}{2}p^{\frac{3}{2}m-2}(p^{\frac{m}{2}-1} + (\frac{-j}{p}))(p^m - 1)$
$-\zeta_p^j\sqrt{p^*}p^{\frac{m}{2}}$, for $1 \leqslant j \leqslant p-1$	$\frac{1}{2}p^{\frac{3}{2}m-2}(p^{\frac{m}{2}-1} - (\frac{-j}{p}))(p^m - 1)$
$p^{\frac{m}{2}+1}$	$\frac{1}{2}p^{\frac{m}{2}-2}(p^{\frac{m}{2}-1} + 1)(p^{\frac{m}{2}} - 1)(p^{\frac{m}{2}-1} + p - 1)(p^m - 1)/(p^2 - 1)$
$-p^{\frac{m}{2}+1}$	$\frac{1}{2}p^{\frac{m}{2}-2}(p^{\frac{m}{2}-1} - 1)(p^{\frac{m}{2}} + 1)(p^{\frac{m}{2}-1} - p + 1)(p^m - 1)/(p^2 - 1)$
$\zeta_p^j p^{\frac{m}{2}+1}$, for $1 \leqslant j \leqslant p-1$	$\frac{1}{2}p^{\frac{m}{2}-2}(p^{\frac{m}{2}} - 1)(p^{m-2} - 1)(p^m - 1)/(p^2 - 1)$
$-\zeta_p^j p^{\frac{m}{2}+1}$, for $1 \leqslant j \leqslant p-1$	$\frac{1}{2}p^{\frac{m}{2}-2}(p^{\frac{m}{2}} + 1)(p^{m-2} - 1)(p^m - 1)/(p^2 - 1)$
0	$(p^m - 1)(p^{2m-1} - p^{2m-2} + p^{2m-3} - p^{m-2} + 1)$
p^m	1

(ii) *For case m is even, Table* 6 *holds.*

Proof. According to the possible values of $S(\alpha, \beta, \gamma)$ given by Lemma 1, we define for $\varepsilon = \pm 1$, $0 \leqslant i \leqslant 2$ and $j \in \mathbb{F}_p^*$ that

$$n_{\varepsilon,i,j} = \begin{cases} \#\{(\alpha, \beta, \gamma) \in \mathbb{F}_q^3 \mid S(\alpha, \beta, \gamma) = \varepsilon\zeta_p^j p^{\frac{m+i}{2}}\} & \text{if } m - i \text{ is even,} \\ \#\{(\alpha, \beta, \gamma) \in \mathbb{F}_q^3 \mid S(\alpha, \beta, \gamma) = \varepsilon\zeta_p^j \sqrt{p^*} p^{\frac{m+i-1}{2}}\} & \text{if } m - i \text{ is odd,} \end{cases}$$

and

$$\omega = \#\big\{(\alpha, \beta, \gamma) \in \mathbb{F}_q^3 \;\big|\; S(\alpha, \beta, \gamma) = 0\big\}.$$

Recall $n_i, H_{\alpha,\beta}, r_{\alpha,\beta}, A_\gamma$ in Section 2 and $N_{\varepsilon,i}, n_{\varepsilon,i}$ in Section 3 for $i \in \{0, 1, 2\}$. From Lemma 2(i) we know that if $(\alpha, \beta) \neq (0, 0)$, then $r_{\alpha,\beta} = m - i$ for some $i \in \{0, 1, 2\}$. Therefore there are exactly p^{m-i} many $\gamma \in \mathbb{F}_q$ such that $2XH_{\alpha,\beta} + A_\gamma = 0$ is solvable. From Lemma 1 we have

$$\sum_{j=0}^{p-1} n_{\varepsilon,i,j} = p^{m-i} n_{\varepsilon,i}. \tag{31}$$

Since $2XH_{0,0} + A_\gamma = 0$ is solvable if and only if $\gamma = 0$, then we have

$$\begin{aligned}\omega &= p^m - 1 + \big(p^m - p^{m-1}\big)n_1 + \big(p^m - p^{m-2}\big)n_2 \\ &= \big(p^m - 1\big)\big(p^{2m-1} - p^{2m-2} + p^{2m-3} - p^{m-2} + 1\big).\end{aligned} \tag{32}$$

If $m - i$ is odd and $S(\alpha, \beta, \gamma) = \varepsilon\zeta_p^j \sqrt{p^*}\, p^{\frac{m+i-1}{2}}$ for $i \in \{0, 1, 2\}$ and $j \in \mathbb{F}_p^*$, from Lemma 4 we know that for $a \in \mathbb{F}_p^*$,

$$S(a\alpha, a\beta, a\gamma) = \sigma_a\big(S(\alpha, \beta, \gamma)\big) = \varepsilon\zeta^{aj}\left(\frac{a}{p}\right)\sqrt{p^*}\, p^{\frac{m+i-1}{2}}.$$

Therefore

$$n_{\varepsilon,i,aj} = \begin{cases} n_{\varepsilon,i,j} & \text{if } (\frac{a}{p}) = 1, \\ n_{-\varepsilon,i,j} & \text{if } (\frac{a}{p}) = -1. \end{cases} \tag{33}$$

By (31) and (33) we know that for $\varepsilon \in \{\pm 1\}$ and $i \in \{0, 1, 2\}$,

$$n_{\varepsilon,i,0} + \frac{p-1}{2}(n_{\varepsilon,i,1} + n_{-\varepsilon,i,1}) = p^{m-i} n_{\varepsilon,i}. \tag{34}$$

Substituting $N_{\varepsilon,i}$ for N in Lemma 3(iv), by Lemma 1(ii) we have

$$q n_{\varepsilon,i} = \varepsilon\sqrt{p^*}\, p^{\frac{m+i-1}{2}} \sum_{j=0}^{p-1} n_{\varepsilon,i,j}\zeta_p^j. \tag{35}$$

By (33) and (35) we have

$$\begin{aligned}\varepsilon\left(\frac{-1}{p}\right)\sqrt{p^*}\, p^{\frac{m-i-1}{2}} n_{\varepsilon,i} &= n_{\varepsilon,i,0} + n_{\varepsilon,i,1} \cdot \sum_{j=1,\ (\frac{j}{p})=1}^{p-1} \zeta_p^j + n_{-\varepsilon,i,1} \cdot \sum_{j=1,\ (\frac{j}{p})=-1}^{p-1} \zeta_p^j \\ &= n_{\varepsilon,i,0} + \frac{1}{2}\big(\sqrt{p^*} - 1\big)n_{\varepsilon,i,1} + \frac{1}{2}\big(-\sqrt{p^*} - 1\big)n_{-\varepsilon,i,1}\end{aligned}$$

$$= \left[n_{\varepsilon,i,0} - \frac{1}{2}(n_{\varepsilon,i,1} + n_{-\varepsilon,i,1})\right] + \frac{1}{2}\sqrt{p^*}(n_{\varepsilon,i,1} - n_{-\varepsilon,i,1}).$$

Then we get

$$n_{\varepsilon,i,0} = \frac{1}{2}(n_{\varepsilon,i,1} + n_{-\varepsilon,i,1}), \tag{36}$$

$$n_{\varepsilon,i,1} - n_{-\varepsilon,i,1} = 2\varepsilon\left(\frac{-1}{p}\right)p^{\frac{m-i-1}{2}}n_{\varepsilon,i}. \tag{37}$$

By (33), (34), (36) and (37) we have that for $\varepsilon \in \{\pm 1\}$, $i \in \{0, 1, 2\}$ and $j \in \mathbb{F}_p^*$,

$$n_{\varepsilon,i,0} = p^{m-i-1}n_{\varepsilon,i}, \tag{38}$$

$$n_{\varepsilon,i,j} = \left(p^{m-i-1} + \varepsilon\left(\frac{-j}{p}\right)p^{\frac{m-i-1}{2}}\right)n_{\varepsilon,i}. \tag{39}$$

If $m - i$ is even and $S(\alpha, \beta, \gamma) = \varepsilon\zeta_p^j p^{\frac{m+i}{2}}$ for $j \in \mathbb{F}_p^*$, by Lemma 4 we know that for $a \in \mathbb{F}_p^*$,

$$S(a\alpha, a\beta, a\gamma) = \sigma_a\big(S(\alpha, \beta, \gamma)\big) = \varepsilon\zeta^{aj}p^{\frac{m+i}{2}}.$$

Therefore for $\varepsilon \in \{\pm 1\}$ and $i \in \{0, 1, 2\}$, we get

$$n_{\varepsilon,i,1} = n_{\varepsilon,i,2} = \cdots = n_{\varepsilon,i,p-1}. \tag{40}$$

Let $n_{\varepsilon,(i)} = n_{\varepsilon,i,j}$ for $j \in \mathbb{F}_p^*$. Then by (31) and (40) we have

$$n_{\varepsilon,i,0} + (p-1)n_{\varepsilon,(i)} = p^{m-i}n_{\varepsilon,i}. \tag{41}$$

Substituting $N_{\varepsilon,i}$ for N in Lemma 3(iv), by Lemma 1(ii) we have

$$p^m n_{\varepsilon,i} = \varepsilon p^{\frac{m+i}{2}}\sum_{j=0}^{p-1} n_{\varepsilon,i,j}\zeta_p^j. \tag{42}$$

Since $\sum_{j=1}^{p-1}\zeta_p^j = -1$, by (40) and (42) we get

$$n_{\varepsilon,i,0} - n_{\varepsilon,(i)} = \varepsilon p^{\frac{m-i}{2}}n_{\varepsilon,i}. \tag{43}$$

By (41) and (43) we obtain

$$n_{\varepsilon,i,0} = \big(p^{m-i-1} + \varepsilon(p-1)p^{\frac{m-i-2}{2}}\big)n_{\varepsilon,i}, \tag{44}$$

$$n_{\varepsilon,(i)} = \big(p^{m-i-1} - \varepsilon p^{\frac{m-i-2}{2}}\big)n_{\varepsilon,i}. \tag{45}$$

From Theorem 1, combining (38), (39), (44) and (45) we get the results of (i) and (ii). □

Recall $n_{\varepsilon,i,j}$ and ω in the proof of Theorem 3, we have the following result.

Table 7

i	A_i
$(p-1)p^{m-1}-(p-1)p^{\frac{m}{2}}$	$n_{1,2,0}$
$(p-1)p^{m-1}-p^{\frac{m}{2}}$	$(p-1)n_{(\frac{-1}{p}),1,1}+(p-1)n_{-1,2,1}$
$(p-1)p^{m-1}-(p-1)p^{\frac{m}{2}-1}$	$n_{1,0,0}$
$(p-1)p^{m-1}-p^{\frac{m}{2}-1}$	$(p-1)n_{-1,0,1}$
$(p-1)p^{m-1}$	$\omega+2n_{1,1,0}$
$(p-1)p^{m-1}+p^{\frac{m}{2}-1}$	$(p-1)n_{1,0,1}$
$(p-1)p^{m-1}+(p-1)p^{\frac{m}{2}-1}$	$n_{-1,0,0}$
$(p-1)p^{m-1}+p^{\frac{m}{2}}$	$(p-1)n_{-(\frac{-1}{p}),1,1}+(p-1)n_{1,2,1}$
$(p-1)p^{m-1}+(p-1)p^{\frac{m}{2}}$	$n_{-1,2,0}$
0	1

Table 8

i	A_i
$(p-1)p^{m-1}-p^{\frac{m+1}{2}}$	$(p-1)n_{(\frac{-1}{p}),2,1}$
$(p-1)p^{m-1}-(p-1)p^{\frac{m-1}{2}}$	$n_{1,1,0}$
$(p-1)p^{m-1}-p^{\frac{m-1}{2}}$	$(p-1)n_{(\frac{-1}{p}),0,1}+(p-1)n_{-1,1,1}$
$(p-1)p^{m-1}$	$\omega+2n_{1,0,0}+2n_{1,2,0}$
$(p-1)p^{m-1}+p^{\frac{m-1}{2}}$	$(p-1)n_{-(\frac{-1}{p}),0,1}+(p-1)n_{1,1,1}$
$(p-1)p^{m-1}+(p-1)p^{\frac{m-1}{2}}$	$n_{-1,1,0}$
$(p-1)p^{m-1}+p^{\frac{m+1}{2}}$	$(p-1)n_{-(\frac{-1}{p}),2,1}$
0	1

Theorem 4. *For $m \geqslant 3$ and $\gcd(m,k)=1$, the weight distribution $\{A_0, A_1, \ldots, A_n\}$ of the cyclic code $\mathcal{C}_2$ over $\mathbb{F}_p$ $(p \geqslant 3)$ with length $n=q-1$ and $\dim_{\mathbb{F}_p}\mathcal{C}_1 = 3m$ is shown as following.*

(i) *In the case m is even, Table 7 holds.*
(ii) *In the case m is odd, Table 8 holds.*

Proof. From (1) we know that for each non-zero codeword $c(\alpha,\beta,\gamma)=(c_0,\ldots,c_{n-1})$ $(n = p^m-1, c_i = \mathrm{Tr}(\alpha\pi^{(p^k+1)i}+\beta\pi^{2i}+\gamma\pi^i), 0 \leqslant i \leqslant n-1$, and $(\alpha,\beta,\gamma) \in \mathbb{F}_q^3 \setminus \{(0,0,0)\})$, the Hamming weight of $c(\alpha,\beta,\gamma)$ is

$$w_H\big(c(\alpha,\beta,\gamma)\big) = p^{m-1}(p-1) - \frac{1}{p}\cdot R(\alpha,\beta,\gamma), \tag{46}$$

where

$$R(\alpha,\beta,\gamma) = \sum_{a=1}^{p-1} S(a\alpha, a\beta, a\gamma) = \sum_{a=1}^{p-1} \sigma_a\big(S(\alpha,\beta,\gamma)\big).$$

For $\varepsilon \in \{\pm 1\}$, $0 \leqslant i \leqslant 2$ and $j \in \mathbb{F}_p^*$,

- if $m-i$ is even and $S(\alpha,\beta,\gamma)=\varepsilon p^{\frac{m+i}{2}}$, then

$$R(\alpha,\beta,\gamma)=\varepsilon(p-1)p^{\frac{m+i}{2}};$$

- if $m-i$ is even and $S(\alpha,\beta,\gamma)=\varepsilon\zeta_p^j p^{\frac{m+i}{2}}$, then

$$R(\alpha,\beta,\gamma)=\varepsilon p^{\frac{m+i}{2}}\sum_{a=1}^{p-1}\zeta_p^{aj}=-\varepsilon p^{\frac{m+i}{2}};$$

- if $m-i$ is odd and $S(\alpha,\beta,\gamma)=\varepsilon\sqrt{p^*}p^{\frac{m+i-1}{2}}$, then

$$R(\alpha,\beta,\gamma)=\varepsilon\sqrt{p^*}p^{\frac{m+i-1}{2}}\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)=0;$$

- if $m-i$ is odd and $S(\alpha,\beta,\gamma)=\varepsilon\zeta_p^j\sqrt{p^*}p^{\frac{m+i-1}{2}}$, then

$$R(\alpha,\beta,\gamma)=\varepsilon\sqrt{p^*}p^{\frac{m+i-1}{2}}\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\zeta_p^{aj}=\varepsilon\left(\frac{-j}{p}\right)p^{\frac{m+i+1}{2}}.$$

Thus the weight distribution of $\mathcal{C}_2$ can be derived from Theorem 3 and (46) directly. □

5. Further study

If $\gcd(k,m)$ is odd, these machineries we have developed can also work with some modifications if necessary.

If $\gcd(k,m)$ is even, then $T(\alpha,\beta)$ for $(\alpha,\beta)\in\mathbb{F}_q^2$ are integers. Therefore Galois theory tells us nothing on $n_{\varepsilon,i}$ for $\varepsilon=\pm1, 0\leqslant i\leqslant 2$, and the moment identities in Lemma 3 is not enough to determine $n_{\varepsilon,i}$.

Denote by $d=\gcd(k,m)$. For general d, we need to develop more machineries to determine the weight distributions of $\mathcal{C}_1$ and $\mathcal{C}_2$. Furthermore, we can generalize the cyclic codes to the field $\mathbb{F}_{p^s}$ with $s\mid d$ and determine their weight distributions. These methods and results will be presented in a following paper.

Acknowledgements

The authors thank the anonymous referees for their helpful comments.

References

[1] R.S. Coulter, Further evaluation of some Weil sums, Acta Arith. 86 (1998) 217–226.
[2] K. Feng, J. Luo, Value distribution of exponential sums from perfect nonlinear functions and their applications, preprint, 2006.

[3] R.W. Fitzgerald, J.L. Yucas, Sums of Gauss sums and weights of irreducible codes, Finite Fields Appl. 11 (2005) 89–110.

[4] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, second ed., Grad. Texts in Math., vol. 84, Springer-Verlag, 1990.

[5] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia Math. Appl., vol. 20, Addison–Wesley, 1983.

[6] G. Ness, T. Helleseth, A. Kholosha, On the correlation distribution of the Coulter–Matthews decimation, IEEE Trans. Inform. Theory 52 (2006) 2241–2247.

[7] H.M. Tranchtenberg, On the cross-correlation function of maximal linear sequences, PhD dissertation, University of Southern California, Los Angeles, 1970.

[8] M. Van Der Vlugt, Hasse–Davenport curve, Gauss sums and weight distribution of irreducible cyclic codes, J. Number Theory 55 (1995) 145–159.

[9] J. Yuan, C. Carlet, C. Ding, The weight distribution of a class of linear codes from perfect nonlinear functions, IEEE Trans. Inform. Theory 52 (2006) 712–717.