

A Class of Five-weight Cyclic Codes and Their Weight Distribution*

Yan Liu[†], Haode Yan[‡]

Abstract

In this paper, a family of five-weight reducible cyclic codes is presented. Furthermore, the weight distribution of these cyclic codes is determined, which follows from the determination of value distributions of certain exponential sums.

Key words and phrases: cyclic code, quadratic form, weight distribution.

MSC: 94B15, 11T71.

1 INTRODUCTION

Recall that an $[n, l, d]$ linear code \mathcal{C} over \mathbb{F}_q is a linear subspace of \mathbb{F}_q^n with dimension l and minimum Hamming distance d , where q is a prime power. Let A_i denote the number of codewords in \mathcal{C} with Hamming weight i . The sequence $(A_0, A_1, A_2, \dots, A_n)$ is called the weight distribution of the code \mathcal{C} . And \mathcal{C} is called cyclic if for any $(c_0, c_1, \dots, c_{n-1}) \in \mathcal{C}$, also $(c_{n-1}, c_0, \dots, c_{n-2}) \in \mathcal{C}$. A linear code \mathcal{C} in \mathbb{F}_q^n is cyclic if and only if \mathcal{C} is an ideal of the polynomial residue class ring $\mathbb{F}_q[x]/(x^n - 1)$. Since $\mathbb{F}_q[x]/(x^n - 1)$ is a principal ideal ring, every cyclic code corresponds to a principal ideal $(g(x))$ of the multiples of a polynomial $g(x)$ which is the monic polynomial of lowest degree in the ideal. This polynomial $g(x)$ is called the generator polynomial, and $h(x) = (x^n - 1)/g(x)$ is called the parity-check polynomial of the code \mathcal{C} . We also recall that a cyclic code over \mathbb{F}_q is called irreducible if its parity-check polynomial is irreducible over \mathbb{F}_q and reducible, otherwise. Determining the weight distribution of a cyclic code is an important research object in coding theory. Information on the weight distribution of binary cyclic codes can be found in [8–10, 17]. For information on the weight distribution of non-binary cyclic codes, the reader is referred to [1–7, 12–16, 18–20]. In this paper, we will determine the weight distribution of a class of five-weight reducible non-binary cyclic codes.

Throughout this paper, let m and k be any two positive integers such that $s = m/d \geq 5$ is odd, where $d = \gcd(m, k)$. Let p be an odd prime, $q = p^m$ and $q_0 = p^d$. Then we have $q = q_0^s$. Let t be a divisor of d such that d/t is odd, and $m_0 = m/t$.

*This work is supported by the NSFC under Grants 11071160 and 11001170.

[†]Corresponding author, Dept. of Math., SJTU, Shanghai, 200240, liuyan0916@sjtu.edu.cn.

[‡]Dept. of Math., Shanghai Jiaotong Univ., Shanghai, 200240, hdyan@sjtu.edu.cn.

Let π be a primitive element of the finite field \mathbb{F}_q . Let $h_0(x)$, $h_1(x)$ and $h_2(x)$ be the minimal polynomials of π^{-2} , $\pi^{-(p^k+1)}$ and $\pi^{-(p^{2k}+1)}$ over \mathbb{F}_{p^t} , respectively. The cyclic codes over \mathbb{F}_{p^t} with parity-check polynomial $h_0(x)h_1(x)$ has been extensively studied by [13]. Let \mathcal{C} be the cyclic code with parity-check polynomial $h_0(x)h_1(x)h_2(x)$. In the case of $t = 1$, the weight distribution of \mathcal{C} can be obtained by the results of [19, 20]. The objective of this paper is to consider the problem for any positive t such that d/t is odd. For $t \geq 2$ and even k , the case of $2 \nmid \frac{m}{(m,k)}$ but $2 \mid \frac{m}{(m,k/2)}$ exists, which was not considered neither in [19] nor in [20]. Moreover, the weight distribution of this class of cyclic codes in this special case can not be obtained with the same arguments as in [19] and [20] in a straightforward generalization. In this paper, we always assume d/t is odd and will show that \mathcal{C} has five nonzero weights and determine the weight distribution of this class of cyclic codes.

The rest of this paper is organized as follows. Some preliminaries will be introduced in Section 2. A family of cyclic codes and their weight distributions will be given in Section 3.

2 PRELIMINARIES

We follow the notation in Section 1. In this section, we first give a brief introduction to the theory of quadratic forms over finite fields.

For any quadratic form F over \mathbb{F}_{q_0} , there exists a symmetric matrix A of order s such that $F(X) = XAX^T$, where $X = (x_1, x_2, \dots, x_s) \in \mathbb{F}_{q_0}^s$ and X^T denotes the transpose of X . Then there exists a non-singular matrix M of order s over \mathbb{F}_{q_0} such that MAM^T is a diagonal matrix (see [11]). Under the non-singular linear substitution $X = ZM$ with $Z = (z_1, z_2, \dots, z_s) \in \mathbb{F}_{q_0}^s$, then $F(X) = ZMAM^TZ^T = \sum_{i=1}^r d_i z_i^2$, where r is the rank of $F(X)$ and $d_i \in \mathbb{F}_{q_0}^*$. Let $\Delta = d_1 d_2 \cdots d_r$ (we assume $\Delta = 0$ when $r = 0$). Let η_0 be the quadratic multiplicative character of \mathbb{F}_{q_0} . Then $\eta_0(\Delta)$ is an invariant of A under the action of $M \in GL_s(\mathbb{F}_{q_0})$.

Lemma 2.1 ([19]) *Let $F(X)$ be a quadratic form in s variables of rank r over \mathbb{F}_{q_0} , then*

$$\sum_{X \in \mathbb{F}_{q_0}^s} \zeta_p^{Tr_p^{q_0}(F(X))} = \begin{cases} \eta_0(\Delta)(-1)^{(d-1)r} q_0^{s-\frac{r}{2}}, & p \equiv 1 \pmod{4}, \\ \eta_0(\Delta)(\sqrt{-1})^{dr} (-1)^{(d-1)r} q_0^{s-\frac{r}{2}}, & p \equiv 3 \pmod{4}. \end{cases}$$

where ζ_p is a primitive p -th root of unity.

For any fixed $(a, b, c) \in \mathbb{F}_q^3$, let $Q_{a,b,c}(x) = Tr_{q_0}^q(ax^2 + bx^{p^k+1} + cx^{p^{2k}+1})$, we have the following result.

Lemma 2.2 *For any $(a, b, c) \in \mathbb{F}_q^3 \setminus \{(0, 0, 0)\}$, $Q_{a,b,c}(x)$ is a quadratic form over \mathbb{F}_{q_0} with rank at least $s - 4$.*

Proof. The proof is similar to the proof of Lemma 2 in [13], so we omit the details. ■

3 A CLASS OF FIVE-WEIGHT CYCLIC CODES AND THEIR WEIGHT DISTRIBUTION

We follow the notation and conditions fixed in Section 1 and 2. It is easy to check that $h_0(x)$, $h_1(x)$ and $h_2(x)$ are polynomials of degree m_0 and are pairwise distinct when $s \geq 5$. Let \mathcal{C} be the cyclic code with parity-check polynomial $h_0(x)h_1(x)h_2(x)$. Then \mathcal{C} has length $q - 1$ and dimension $3m_0$. Moreover, it can be expressed as

$$\mathcal{C} = \{\mathbf{c}_{(a,b,c)} : a, b, c \in \mathbb{F}_q\},$$

where $\mathbf{c}_{(a,b,c)} = (Tr_{p^t}^q(a\pi^{2i} + b\pi^{(p^k+1)i} + c\pi^{(p^{2k+1})i}))_{i=0}^{q-2}$. The weight of the codeword $\mathbf{c}_{(a,b,c)} = (c_0, c_1, \dots, c_{q-2})$ can be expressed by exponential sums in the following way.

$$\begin{aligned} W(\mathbf{c}_{(a,b,c)}) &= \#\{0 \leq i \leq p^m - 2 : c_i \neq 0\} \\ &= q - 1 - \frac{1}{p^t} \sum_{i=0}^{q-2} \sum_{y \in \mathbb{F}_{p^t}} \zeta_p^{Tr_p^{p^t}(yc_i)} \\ &= q - 1 - \frac{1}{p^t} \sum_{i=0}^{q-2} \sum_{y \in \mathbb{F}_{p^t}} \zeta_p^{Tr_p^{p^t}(y \cdot Tr_{p^t}^q(a\pi^{2i} + b\pi^{(p^k+1)i} + c\pi^{(p^{2k+1})i}))} \\ &= q - 1 - \frac{1}{p^t} \sum_{x \in \mathbb{F}_q^*} \sum_{y \in \mathbb{F}_{p^t}} \zeta_p^{Tr_p^{p^t}(y \cdot Tr_{p^t}^q(ax^2 + bx^{p^k+1} + cx^{p^{2k+1}}))} \\ &= p^{m-t}(p^t - 1) - \frac{1}{p^t} \sum_{y \in \mathbb{F}_{p^t}^*} \sum_{x \in \mathbb{F}_q} \zeta_p^{Tr_p^{p^t}(y \cdot Tr_{p^t}^q(ax^2 + bx^{p^k+1} + cx^{p^{2k+1}}))} \\ &= p^{m-t}(p^t - 1) - \frac{1}{p^t} \left(\sum_{y \in SQ} \sum_{x \in \mathbb{F}_q} \zeta_p^{Tr_p^{p^t}(a(xy^{\frac{1}{2}})^2 + b(xy^{\frac{1}{2}})^{p^k+1} + c(xy^{\frac{1}{2}})^{p^{2k+1}})} \right. \\ &\quad \left. + \sum_{y \in \overline{SQ}} \sum_{x \in \mathbb{F}_q} \zeta_p^{Tr_p^{p^t}(y \cdot Tr_{q_0}^q(ax^2 + bx^{p^k+1} + cx^{p^{2k+1}}))} \right) \\ &= p^{m-t}(p^t - 1) - \frac{1}{p^t} \left(\sum_{y \in SQ} \sum_{x \in \mathbb{F}_q} \zeta_p^{Tr_p^{p^t}(a(xy^{\frac{1}{2}})^2 + b(xy^{\frac{1}{2}})^{p^k+1} + c(xy^{\frac{1}{2}})^{p^{2k+1}})} \right. \\ &\quad \left. + \sum_{y \in SQ} \sum_{x \in \mathbb{F}_q} \zeta_p^{Tr_p^{p^t}(\lambda \cdot Tr_{q_0}^q(a(xy^{\frac{1}{2}})^2 + b(xy^{\frac{1}{2}})^{p^k+1} + c(xy^{\frac{1}{2}})^{p^{2k+1}}))} \right) \\ &= p^{m-t}(p^t - 1) - \frac{p^t - 1}{2p^t} \left(\sum_{x \in \mathbb{F}_q} \zeta_p^{Tr_p^{q_0}(Q_{a,b,c}(x))} + \sum_{x \in \mathbb{F}_q} \zeta_p^{Tr_p^{q_0}(\lambda Q_{a,b,c}(x))} \right), \end{aligned} \tag{1}$$

where $SQ(\overline{SQ})$, resp.) denotes the set of nonzero square elements (non-square elements, resp.) of \mathbb{F}_{p^t} and λ is a non-square in \mathbb{F}_{p^t} . If we define

$$T(a, b, c) = \sum_{x \in \mathbb{F}_q} \zeta_p^{Tr_p^{q_0}(Q_{a,b,c}(x))} + \sum_{x \in \mathbb{F}_q} \zeta_p^{Tr_p^{q_0}(\lambda Q_{a,b,c}(x))}, \tag{2}$$

then the weight distribution of the code \mathcal{C} is completely determined by the value distribution of $T(a, b, c)$. Firstly, we have the following lemma.

Lemma 3.1 For any fixed $(a, b, c) \in \mathbb{F}_q^3 \setminus \{(0, 0, 0)\}$, let $T(a, b, c)$ be defined by (2) and r be the rank of $Q_{a,b,c}(x)$.

- If r is even, then $T(a, b, c) = \pm 2q_0^{s-\frac{r}{2}}$.
- If r is odd, then $T(a, b, c) = 0$.

Proof. According to Lemma 2.1, we have

$$\sum_{x \in \mathbb{F}_q} \zeta_p^{Tr_p^{q_0}(\lambda Q_{a,b,c}(x))} = \sum_{x \in \mathbb{F}_q} \zeta_p^{Tr_p^{q_0}(Q_{a,b,c}(x))} \eta_0(\lambda^r).$$

Then $T(a, b, c) = (1 + \eta_0(\lambda^r)) \sum_{x \in \mathbb{F}_q} \zeta_p^{Tr_p^{q_0}(Q_{a,b,c}(x))}$. Since d/t is odd, λ is also a non-square in \mathbb{F}_{q_0} . Thus, if r is even, $T(a, b, c) = \pm 2q_0^{s-\frac{r}{2}}$ and 0, otherwise. This completes the proof. ■

Theorem 3.2 Let $T(a, b, c)$ be defined by (2). Then as (a, b, c) runs through \mathbb{F}_q^3 , the value distribution of $T(a, b, c)$ is given by Table 1.

Table 1: Value Distribution of $T(a, b, c)$

Value	Frequency
$2p^m$	1
0	$(p^m - 1)(p^{2m} - p^{2m-d} + p^{2m-4d} + p^m - p^{m-d} - p^{m-3d} + 1)$
$2p^{\frac{m+d}{2}}$	$\frac{(p^{m+d} + p^{(m+3d)/2})(p^{2m} - p^{2m-2d} - p^{2m-3d} + p^{m-2d} + p^{m-3d} - 1)}{2(p^{2d} - 1)}$
$-2p^{\frac{m+d}{2}}$	$\frac{(p^{m+d} - p^{(m+3d)/2})(p^{2m} - p^{2m-2d} - p^{2m-3d} + p^{m-2d} + p^{m-3d} - 1)}{2(p^{2d} - 1)}$
$2p^{\frac{m+3d}{2}}$	$\frac{(p^{m-3d} + p^{(m-3d)/2})(p^m - 1)(p^{m-d} - 1)}{2(p^{2d} - 1)}$
$-2p^{\frac{m+3d}{2}}$	$\frac{(p^{m-3d} - p^{(m-3d)/2})(p^m - 1)(p^{m-d} - 1)}{2(p^{2d} - 1)}$

We prove this theorem only for the case that $q_0 \equiv 3 \pmod{4}$. The proof for the case that $q_0 \equiv 1 \pmod{4}$ is similar and omitted. Hence we assume that $q_0 \equiv 3 \pmod{4}$ from now on. In order to determine the value distribution of $T(a, b, c)$, we need a series of lemmas. Before introducing them, for any positive integer k , we define $d_1 = p^k + 1$ and $d_2 = p^{2k} + 1$. Since -1 is a non-square in \mathbb{F}_{p^t} when $q_0 \equiv 3 \pmod{4}$, so in the following, we set $\lambda = -1$.

Lemma 3.3 Let $q_0 \equiv 3 \pmod{4}$ and let N_2 denote the number of solutions $(x_1, x_2) \in \mathbb{F}_{p^m}^2$ of the following system of equations

$$\begin{cases} x_1^2 + x_2^2 = 0 \\ x_1^{d_1} + x_2^{d_1} = 0 \\ x_1^{d_2} + x_2^{d_2} = 0. \end{cases}$$

Then $N_2 = 1$.

Proof. This system of equations have only one solution $(0, 0)$, since -1 is a non-square in \mathbb{F}_{p^m} when $q_0 \equiv 3 \pmod{4}$. ■

Lemma 3.4 *Let $q_0 \equiv 3 \pmod{4}$ and let $\overline{N_2}$ denote the number of solutions $(x_1, x_2) \in \mathbb{F}_{p^m}^2$ of the following system of equations*

$$\begin{cases} x_1^2 - x_2^2 = 0 \\ x_1^{d_1} - x_2^{d_1} = 0 \\ x_1^{d_2} - x_2^{d_2} = 0. \end{cases} \quad (3)$$

Then $\overline{N_2} = 2p^m - 1$.

Proof. We observe that (x_1, x_2) is a solution of (3) if and only if (x_1, x_2) is a solution of the first equation of it. So the conclusion follows from the Lemma 6.24 in [11]. ■

Lemma 3.5 *Let $q_0 \equiv 3 \pmod{4}$ and let N_3 denote the number of solutions $(x_1, x_2, x_3) \in \mathbb{F}_{p^m}^3$ of the following system of equations*

$$\begin{cases} x_1^2 + x_2^2 + x_3^2 = 0 \\ x_1^{d_1} + x_2^{d_1} + x_3^{d_1} = 0 \\ x_1^{d_2} + x_2^{d_2} + x_3^{d_2} = 0. \end{cases} \quad (4)$$

Then $N_3 = p^{m+d} + p^m - p^d$.

Proof.

Case I, when $x_3 = 0$. In this case, by Lemma 3.3, the number of solutions of (4) is 1.
Case II, when $x_3 \neq 0$. In this case, for any fixed x_3 , the equation system (4) has the same number of solutions $(x_1, x_2) \in \mathbb{F}_{p^m}^2$ as the system

$$\begin{cases} x_1^2 + x_2^2 + 1 = 0 \\ x_1^{d_1} + x_2^{d_1} + 1 = 0 \\ x_1^{d_2} + x_2^{d_2} + 1 = 0. \end{cases} \quad (5)$$

As assumed in the beginning of this paper, we have $\gcd(m, k) = d$. Then by the same method as in the proof of Lemma 4.3 in [20], we can prove that if $(x_1, x_2) \in \mathbb{F}_{p^m}^2$ is a solution of (5), then $(x_1, x_2) \in \mathbb{F}_{p^d}^2$. Furthermore, if $(x_1, x_2) \in \mathbb{F}_{p^d}^2$ is a solution of the first equation of (5), then it is a solution of (5). So the number of solutions $(x_1, x_2) \in \mathbb{F}_{p^m}^2$ of (5) is equal to the number of solutions $(x_1, x_2) \in \mathbb{F}_{p^d}^2$ satisfying the first equation of it, which is $p^d + 1$ by Lemma 6.24 in [11]. Thus (5) has exactly $p^d + 1$ solutions.

Summarizing the results of the two cases above, we have that $N_3 = 1 + (p^m - 1)(p^d + 1) = p^{m+d} + p^m - p^d$. This completes the proof. ■

Lemma 3.6 *Let $q_0 \equiv 3 \pmod{4}$ and let $\overline{N_3}$ denote the number of solutions $(x_1, x_2, x_3) \in \mathbb{F}_{p^m}^3$ of the following system of equations*

$$\begin{cases} x_1^2 + x_2^2 - x_3^2 = 0 \\ x_1^{d_1} + x_2^{d_1} - x_3^{d_1} = 0 \\ x_1^{d_2} + x_2^{d_2} - x_3^{d_2} = 0. \end{cases}$$

Then $\overline{N_3} = p^{m+d} + p^m - p^d$.

Proof. The proof is similar to the proof of the lemma above, so we omit the details. ■

Lemma 3.7 *Let $q_0 \equiv 3 \pmod{4}$ and let N_4 denote the number of solutions $(x_1, x_2, x_3, x_4) \in \mathbb{F}_{p^m}^4$ of the following system of equations*

$$\begin{cases} x_1^2 + x_2^2 + x_3^2 + x_4^2 = 0 \\ x_1^{d_1} + x_2^{d_1} + x_3^{d_1} + x_4^{d_1} = 0 \\ x_1^{d_2} + x_2^{d_2} + x_3^{d_2} + x_4^{d_2} = 0. \end{cases} \quad (6)$$

Then $N_4 = 1 + (p^m - 1)(p^d + 1)(2p^m - p^d + 1)$.

Proof. See Appendix. ■

Lemma 3.8 *Let $q_0 \equiv 3 \pmod{4}$ and let $\overline{N_4}$ denote the number of solutions $(x_1, x_2, x_3, x_4) \in \mathbb{F}_{p^m}^4$ of the following system of equations*

$$\begin{cases} x_1^2 + x_2^2 + x_3^2 - x_4^2 = 0 \\ x_1^{d_1} + x_2^{d_1} + x_3^{d_1} - x_4^{d_1} = 0 \\ x_1^{d_2} + x_2^{d_2} + x_3^{d_2} - x_4^{d_2} = 0. \end{cases} \quad (7)$$

Then $\overline{N_4} = p^{m+2d} + p^m - p^{2d}$.

Proof. See Appendix. ■

Lemma 3.9 *Let $q_0 \equiv 3 \pmod{4}$ and let $\widetilde{N_4}$ denote the number of solutions $(x_1, x_2, x_3, x_4) \in \mathbb{F}_{p^m}^4$ of the following system of equations*

$$\begin{cases} x_1^2 + x_2^2 - x_3^2 - x_4^2 = 0 \\ x_1^{d_1} + x_2^{d_1} - x_3^{d_1} - x_4^{d_1} = 0 \\ x_1^{d_2} + x_2^{d_2} - x_3^{d_2} - x_4^{d_2} = 0. \end{cases} \quad (8)$$

Then $\widetilde{N_4} = 1 + (p^m - 1)(p^d + 1)(2p^m - p^d + 1)$.

Proof. See Appendix. ■

Now we are ready to prove Theorem 3.2 in the case of $q_0 \equiv 3 \pmod{4}$.

Proof of Theorem 3.2.

It is clear that $T(a, b, c) = 2p^m$ if $(a, b, c) = (0, 0, 0)$. Otherwise, by Lemma 2.2 and 3.1, we have

$$T(a, b, c) \in \{0, \pm 2p^{\frac{m+d}{2}}, \pm 2p^{\frac{m+3d}{2}}\}.$$

We define

$$n_{1,i} = \#\{(a, b, c) \in \mathbb{F}_{p^m}^3 : T(a, b, c) = (-1)^i 2p^{\frac{m+d}{2}}\},$$

$$n_{2,i} = \#\{(a, b, c) \in \mathbb{F}_{p^m}^3 : T(a, b, c) = (-1)^i 2p^{\frac{m+3d}{2}}\},$$

where $i = 0, 1$. Then we immediately have

$$\begin{cases} \sum_{(a,b,c) \in \mathbb{F}_{p^m}^3} T(a, b, c) = 2p^m + 2(n_{1,0} - n_{1,1})p^{\frac{m+d}{2}} + 2(n_{2,0} - n_{2,1})p^{\frac{m+3d}{2}} \\ \sum_{(a,b,c) \in \mathbb{F}_{p^m}^3} T^2(a, b, c) = 2^2 p^{2m} + 2^2(n_{1,0} + n_{1,1})p^{m+d} + 2^2(n_{2,0} + n_{2,1})p^{m+3d} \\ \sum_{(a,b,c) \in \mathbb{F}_{p^m}^3} T^3(a, b, c) = 2^3 p^{3m} + 2^3(n_{1,0} - n_{1,1})p^{\frac{3m+d}{2}} + 2^3(n_{2,0} - n_{2,1})p^{\frac{3m+3d}{2}} \\ \sum_{(a,b,c) \in \mathbb{F}_{p^m}^3} T^4(a, b, c) = 2^4 p^{4m} + 2^4(n_{1,0} + n_{1,1})p^{2m+2d} + 2^4(n_{2,0} + n_{2,1})p^{2m+6d}. \end{cases} \quad (9)$$

On the other hand, it follows from Eq. (2) that

$$\begin{aligned} & \sum_{(a,b,c) \in \mathbb{F}_{p^m}^3} T(a, b, c) \\ &= \sum_{(a,b,c) \in \mathbb{F}_{p^m}^3} \left(\sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(ax^2 + bx^{d_1} + cx^{d_2})} + \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(-ax^2 - bx^{d_1} - cx^{d_2})} \right) \\ &= \sum_{x \in \mathbb{F}_{p^m}} \sum_{a \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(ax^2)} \sum_{b \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(bx^{d_1})} \sum_{c \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(cx^{d_2})} \\ & \quad + \sum_{x \in \mathbb{F}_{p^m}} \sum_{a \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(-ax^2)} \sum_{b \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(-bx^{d_1})} \sum_{c \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(-cx^{d_2})} \\ &= 2p^{3m}. \end{aligned} \quad (10)$$

$$\begin{aligned} & \sum_{(a,b,c) \in \mathbb{F}_{p^m}^3} T^2(a, b, c) \\ &= \sum_{(x_1, x_2) \in \mathbb{F}_{p^m}^2} \sum_{a \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(a(x_1^2 + x_2^2))} \sum_{b \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(b(x_1^{d_1} + x_2^{d_1}))} \sum_{c \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(c(x_1^{d_2} + x_2^{d_2}))} \\ & \quad + \sum_{(x_1, x_2) \in \mathbb{F}_{p^m}^2} \sum_{a \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(a(x_1^2 - x_2^2))} \sum_{b \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(b(x_1^{d_1} - x_2^{d_1}))} \sum_{c \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(c(x_1^{d_2} - x_2^{d_2}))} \\ & \quad + \sum_{(x_1, x_2) \in \mathbb{F}_{p^m}^2} \sum_{a \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(a(-x_1^2 + x_2^2))} \sum_{b \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(b(-x_1^{d_1} + x_2^{d_1}))} \sum_{c \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(c(-x_1^{d_2} + x_2^{d_2}))} \\ & \quad + \sum_{(x_1, x_2) \in \mathbb{F}_{p^m}^2} \sum_{a \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(-a(x_1^2 + x_2^2))} \sum_{b \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(-b(x_1^{d_1} + x_2^{d_1}))} \sum_{c \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(-c(x_1^{d_2} + x_2^{d_2}))} \\ &= p^{3m}(\#S_1 + \#S_2 + \#S_3 + \#S_4), \end{aligned}$$

where

$$\begin{aligned}
S_1 &= \{(x_1, x_2) \in \mathbb{F}_{p^m}^2 : x_1^2 + x_2^2 = 0, x_1^{d_1} + x_2^{d_1} = 0, x_1^{d_2} + x_2^{d_2} = 0\}, \\
S_2 &= \{(x_1, x_2) \in \mathbb{F}_{p^m}^2 : x_1^2 - x_2^2 = 0, x_1^{d_1} - x_2^{d_1} = 0, x_1^{d_2} - x_2^{d_2} = 0\}, \\
S_3 &= \{(x_1, x_2) \in \mathbb{F}_{p^m}^2 : -x_1^2 + x_2^2 = 0, -x_1^{d_1} + x_2^{d_1} = 0, -x_1^{d_2} + x_2^{d_2} = 0\}, \\
S_4 &= \{(x_1, x_2) \in \mathbb{F}_{p^m}^2 : -x_1^2 - x_2^2 = 0, -x_1^{d_1} - x_2^{d_1} = 0, -x_1^{d_2} - x_2^{d_2} = 0\}.
\end{aligned}$$

It is clear that $S_1 = S_4$ and $S_2 = S_3$. Then by Lemma 3.3 and 3.4, we have

$$\sum_{(a,b,c) \in \mathbb{F}_{p^m}^3} T^2(a, b, c) = 4p^{4m}. \quad (11)$$

Similarly, by Lemmas 3.5-3.9, we have

$$\begin{aligned}
\sum_{(a,b,c) \in \mathbb{F}_{p^m}^3} T^3(a, b, c) &= 8p^{3m}(p^{m+d} + p^m - p^d) \\
\sum_{(a,b,c) \in \mathbb{F}_{p^m}^3} T^4(a, b, c) &= 16p^{4m}(p^{m+d} + p^m - p^d).
\end{aligned} \quad (12)$$

Combining Eqs. (9)-(12), we get

$$\begin{aligned}
n_{1,0} &= \frac{(p^{m+d} + p^{(m+3d)/2})(p^{2m} - p^{2m-2d} - p^{2m-3d} + p^{m-2d} + p^{m-3d} - 1)}{2(p^{2d} - 1)}, \\
n_{1,1} &= \frac{(p^{m+d} - p^{(m+3d)/2})(p^{2m} - p^{2m-2d} - p^{2m-3d} + p^{m-2d} + p^{m-3d} - 1)}{2(p^{2d} - 1)}, \\
n_{2,0} &= \frac{(p^{m-3d} + p^{(m-3d)/2})(p^m - 1)(p^{m-d} - 1)}{2(p^{2d} - 1)}, \\
n_{2,1} &= \frac{(p^{m-3d} - p^{(m-3d)/2})(p^m - 1)(p^{m-d} - 1)}{2(p^{2d} - 1)}.
\end{aligned}$$

Summarizing the discussion above completes the proof of this theorem in the case of $q_0 \equiv 3 \pmod{4}$.

Table 2: Weight Distribution of \mathcal{C}

Weight	Frequency
0	1
$(p^t - 1)p^{m-t}$	$(p^m - 1)(p^{2m} - p^{2m-d} + p^{2m-4d} + p^m - p^{m-d} - p^{m-3d} + 1)$
$(p^t - 1)(p^{m-t} - p^{\frac{m+d-2t}{2}})$	$\frac{(p^{m+d} + p^{(m+3d)/2})(p^{2m} - p^{2m-2d} - p^{2m-3d} + p^{m-2d} + p^{m-3d} - 1)}{2(p^{2d} - 1)}$
$(p^t - 1)(p^{m-t} + p^{\frac{m+d-2t}{2}})$	$\frac{(p^{m+d} - p^{(m+3d)/2})(p^{2m} - p^{2m-2d} - p^{2m-3d} + p^{m-2d} + p^{m-3d} - 1)}{2(p^{2d} - 1)}$
$(p^t - 1)(p^{m-t} - p^{\frac{m+3d-2t}{2}})$	$\frac{(p^{m-3d} + p^{(m-3d)/2})(p^m - 1)(p^{m-d} - 1)}{2(p^{2d} - 1)}$
$(p^t - 1)(p^{m-t} + p^{\frac{m+3d-2t}{2}})$	$\frac{(p^{m-3d} - p^{(m-3d)/2})(p^m - 1)(p^{m-d} - 1)}{2(p^{2d} - 1)}$

Recall that \mathcal{C} is the cyclic code over \mathbb{F}_{p^t} with parity check polynomial $h_0(x)h_1(x)h_2(x)$, where $h_0(x)$, $h_1(x)$, $h_2(x)$ are the minimal polynomial of π^{-2} , $\pi^{-(p^k+1)}$ and $\pi^{-(p^{2k}+1)}$ over \mathbb{F}_{p^t} , respectively.

Theorem 3.10 *Let m and k be any two positive integers such that $s = m/d \geq 5$ is odd, where $d = \gcd(m, k)$. Let t be a divisor of d such that d/t is odd, then \mathcal{C} is a cyclic code over \mathbb{F}_{p^t} with parameters $[p^m - 1, 3m_0, (p^t - 1)(p^{m-t} - p^{\frac{m+3d-2t}{2}})]$, where $m_0 = m/t$. Moreover, the weight distribution of \mathcal{C} is given in Table 2.*

Proof. According to the discussion in the beginning of this section, the length and dimension of \mathcal{C} are clear. Furthermore, the minimum Hamming distance and weight distribution of \mathcal{C} follows from Eq. (1) and Theorem 3.2. ■

Finally, we give an example to verify the results in Table 2. But the experiment for the case $d \neq 1$ is beyond our computation ability.

Example 3.11 *Let $p = 3$, $m = 7$ and $k = 1$. Then the code \mathcal{C} is a $[2186, 21, 1296]$ cyclic code over \mathbb{F}_3 with weight enumerator*

$$1 + 8951670z^{1296} + 1732767876z^{1404} + 7102473578z^{1458} + 1608998742z^{1512} + 7161336z^{1620}.$$

which is completely in agreement with the results presented in Table 2.

APPENDIX

Proof of Lemma 3.7.

For any $(\bar{a}, \bar{b}, \bar{c}) \in \mathbb{F}_{p^m}^3$, let $N_{1(\bar{a}, \bar{b}, \bar{c})}$ and $N_{2(\bar{a}, \bar{b}, \bar{c})}$ denote the number of solutions of the following two systems of equations

$$\begin{cases} x_1^2 + x_2^2 = \bar{a} \\ x_1^{d_1} + x_2^{d_1} = \bar{b} \\ x_1^{d_2} + x_2^{d_2} = \bar{c} \end{cases} \quad (13)$$

$$\begin{cases} x_3^2 + x_4^2 = -\bar{a} \\ x_3^{d_1} + x_4^{d_1} = -\bar{b} \\ x_3^{d_2} + x_4^{d_2} = -\bar{c}. \end{cases} \quad (14)$$

Then we have

$$N_4 = \sum_{(\bar{a}, \bar{b}, \bar{c}) \in \mathbb{F}_{p^m}^3} N_{1(\bar{a}, \bar{b}, \bar{c})} N_{2(\bar{a}, \bar{b}, \bar{c})}.$$

Case 1, when $\bar{a} = 0$. In this case, (13) and (14) have solutions if and only if $\bar{b} = \bar{c} = 0$ since -1 is a nonsquare. Moreover, $N_{1(0,0,0)} = N_{2(0,0,0)} = 1$.

Case 2, when $\bar{a} \neq 0$. In this case, if $\bar{b} = 0$ or $\bar{c} = 0$, neither (13) nor (14) has solutions. So in the following, we consider the problem only when $\bar{b} \neq 0$ and $\bar{c} \neq 0$.

- \bar{a} is a nonzero square in \mathbb{F}_{p^m} , $\bar{b} \neq 0$ and $\bar{c} \neq 0$. In this case, for any fixed \bar{a} , (13) has the same number of solutions as

$$\begin{cases} x_1^2 + x_2^2 = 1 \\ x_1^{d_1} + x_2^{d_1} = b \\ x_1^{d_2} + x_2^{d_2} = c \end{cases} \quad (15)$$

and (14) has the same number of solutions as

$$\begin{cases} x_3^2 + x_4^2 = -1 \\ x_3^{d_1} + x_4^{d_1} = -b \\ x_3^{d_2} + x_4^{d_2} = -c, \end{cases} \quad (16)$$

where $b = \bar{b}/\bar{a}^{\frac{d_1}{2}}$ and $c = \bar{c}/\bar{a}^{\frac{d_2}{2}}$. Clearly, (b, c) runs through $\mathbb{F}_{p^m}^{*2}$ as (\bar{b}, \bar{c}) does. According to the proofs of Lemma 3.12 and 3.13, we can get $N_{1(1,b,c)} = N_{2(1,b,c)}$ for any fixed $(b, c) \in \mathbb{F}_{p^m}^{*2}$. If (15) has solutions, then $N_{1(1,b,c)} = p^d + 1$ or $2(p^d + 1)$. Furthermore, only in the case of $(b, c) = (1, 1)$, $N_{1(1,b,c)} = p^d + 1$, and there are $\frac{p^m - p^d}{2(p^d + 1)}$ pairs of (b, c) such that $N_{1(1,b,c)} = 2(p^d + 1)$. Therefore, for any fixed nonzero square \bar{a} , we have

$$\begin{aligned} & \sum_{(\bar{b}, \bar{c}) \in \mathbb{F}_{p^m}^{*2}} N_{1(\bar{a}, \bar{b}, \bar{c})} N_{2(\bar{a}, \bar{b}, \bar{c})} \\ &= (p^d + 1)^2 + (2(p^d + 1))^2 \frac{p^m - p^d}{2(p^d + 1)} \\ &= (p^d + 1)(2p^m - p^d + 1). \end{aligned}$$

- \bar{a} is a non-square in \mathbb{F}_{p^m} . In this case, for any fixed \bar{a} , (13) has the same number of solutions as

$$\begin{cases} x_1^2 + x_2^2 = -1 \\ x_1^{d_1} + x_2^{d_1} = -b \\ x_1^{d_2} + x_2^{d_2} = -c \end{cases}$$

and equation system (14) has the same number of solutions as

$$\begin{cases} x_3^2 + x_4^2 = 1 \\ x_3^{d_1} + x_4^{d_1} = b \\ x_3^{d_2} + x_4^{d_2} = c. \end{cases}$$

It can be easily seen that this case is equivalent to the case when \bar{a} is a nonzero square. So for any fixed nonsquare \bar{a} , we also have

$$\begin{aligned} & \sum_{(\bar{b}, \bar{c}) \in \mathbb{F}_{p^m}^{*2}} N_{1(\bar{a}, \bar{b}, \bar{c})} N_{2(\bar{a}, \bar{b}, \bar{c})} \\ &= (p^d + 1)(2p^m - p^d + 1). \end{aligned}$$

Summarizing the two cases above, we have $N_4 = 1 + (p^m - 1)(p^d + 1)(2p^m - p^d + 1)$.

Proof of Lemma 3.8.

For any $(\bar{a}, \bar{b}, \bar{c}) \in \mathbb{F}_{p^m}^3$, let $N_{1(\bar{a}, \bar{b}, \bar{c})}$ and $N_{3(\bar{a}, \bar{b}, \bar{c})}$ denote the number of solutions of the following two system of equations

$$\begin{cases} x_1^2 + x_2^2 = \bar{a} \\ x_1^{d_1} + x_2^{d_1} = \bar{b} \\ x_1^{d_2} + x_2^{d_2} = \bar{c} \end{cases} \quad (17)$$

$$\begin{cases} x_3^2 - x_4^2 = -\bar{a} \\ x_3^{d_1} - x_4^{d_1} = -\bar{b} \\ x_3^{d_2} - x_4^{d_2} = -\bar{c}. \end{cases} \quad (18)$$

It is then obvious that

$$\overline{N_4} = \sum_{(\bar{a}, \bar{b}, \bar{c}) \in \mathbb{F}_{p^m}^3} N_{1(\bar{a}, \bar{b}, \bar{c})} N_{3(\bar{a}, \bar{b}, \bar{c})}.$$

Case 1, when $\bar{a} = 0$. In this case, (17) have solutions if and only if $\bar{b} = \bar{c} = 0$ since -1 is a non-square. Moreover, $N_{1(0,0,0)} = 1$ and $N_{3(0,0,0)} = 2p^m - 1$.

Case 2, when $\bar{a} \neq 0$. In this case, if $\bar{b} = 0$ or $\bar{c} = 0$, (17) has no solution. So in the following, we consider this problem only when $\bar{b} \neq 0$ and $\bar{c} \neq 0$.

- when \bar{a} is a nonzero square, $\bar{b} \neq 0$ and $\bar{c} \neq 0$. In this case, for any fixed $\bar{a} \neq 0$, equation system (17) has the same number of solutions as

$$\begin{cases} x_1^2 + x_2^2 = 1 \\ x_1^{d_1} + x_2^{d_1} = b \\ x_1^{d_2} + x_2^{d_2} = c \end{cases} \quad (19)$$

and equation system (18) has the same number of solutions as

$$\begin{cases} x_3^2 - x_4^2 = -1 \\ x_3^{d_1} - x_4^{d_1} = -b \\ x_3^{d_2} - x_4^{d_2} = -c, \end{cases} \quad (20)$$

where $b = \bar{b}/\bar{a}^{\frac{d_1}{2}}$ and $c = \bar{c}/\bar{a}^{\frac{d_2}{2}}$. Then (b, c) runs through $\mathbb{F}_{p^m}^{*2}$ as (\bar{b}, \bar{c}) runs through $\mathbb{F}_{p^m}^{*2}$. According to the proofs of Lemma 3.12 and 3.14, in order to guarantee (19) and (20) have solutions simultaneously for any fixed (b, c) , we need to prove that the element c_1 determined by b in (19) and the element c_2 determined by b in (20) are the same number. By easy calculation, we have $c_1 = c_2$ if and only if $b = 1$. And then $c_1 = c_2 = 1$. Furthermore, for any fixed nonzero square \bar{a} ,

$$\begin{aligned} & \sum_{(\bar{b}, \bar{c}) \in \mathbb{F}_{p^m}^{*2}} N_{1(\bar{a}, \bar{b}, \bar{c})} N_{3(\bar{a}, \bar{b}, \bar{c})} \\ &= (p^d + 1)(p^d - 1). \end{aligned}$$

- when \bar{a} is a non-square, $\bar{b} \neq 0$ and $\bar{c} \neq 0$. In this case, for any fixed $\bar{a} \neq 0$, equation system (17) has the same number of solutions as

$$\begin{cases} x_1^2 + x_2^2 = -1 \\ x_1^{d_1} + x_2^{d_1} = -b \\ x_1^{d_2} + x_2^{d_2} = -c \end{cases}$$

and equation system (18) has the same number of solutions as

$$\begin{cases} x_3^2 - x_4^2 = 1 \\ x_3^{d_1} - x_4^{d_1} = b \\ x_3^{d_2} - x_4^{d_2} = c. \end{cases}$$

It can be easily seen that this case is equivalent to the case when \bar{a} is a nonzero square. So for any fixed non-square \bar{a} , we also have

$$\begin{aligned} & \sum_{(\bar{b}, \bar{c}) \in \mathbb{F}_{p^m}^{*2}} N_{1(\bar{a}, \bar{b}, \bar{c})} N_{3(\bar{a}, \bar{b}, \bar{c})} \\ &= (p^d + 1)(p^d - 1). \end{aligned}$$

$$\overline{N_4} = \sum_{(\bar{a}, \bar{b}, \bar{c}) \in \mathbb{F}_{p^m}^3} N_{1(\bar{a}, \bar{b}, \bar{c})} N_{3(\bar{a}, \bar{b}, \bar{c})} = (2p^m - 1) + (p^m - 1)(p^d + 1)(p^d - 1).$$

Proof of Lemma 3.9.

With the notation as above,

$$\widetilde{N_4} = \sum_{(\bar{a}, \bar{b}, \bar{c}) \in \mathbb{F}_{p^m}^3} N_{1(\bar{a}, \bar{b}, \bar{c})}^2 = 1 + (p^m - 1)(p^d + 1)(2p^m - p^d + 1).$$

Lemma 3.12 *Let $N_{1(b,c)}$ denote the number of solutions $(x_1, x_2) \in \mathbb{F}_{p^m}^2$ of (15), where $(b, c) \in \mathbb{F}_{p^m}^{*2}$. Then we have the following conclusions.*

- (1). $N_{1(1,1)} = p^d + 1$.
- (2). When (b, c) runs through $\mathbb{F}_{p^m}^{*2} \setminus \{(1, 1)\}$,

$$N_{1(b,c)} = \begin{cases} 2(p^d + 1), & \text{for } \frac{p^m - p^d}{2(p^d + 1)} \text{ times,} \\ 0, & \text{for the rest.} \end{cases}$$

Proof. We first compute the number $N_{1(b)}$ of solutions $(x_1, x_2) \in \mathbb{F}_{p^m}^2$ of the following system of equations

$$\begin{cases} x_1^2 + x_2^2 = 1 \\ x_1^{d_1} + x_2^{d_1} = b. \end{cases} \quad (21)$$

When $q_0 \equiv 3 \pmod{4}$, -1 is a non-square in \mathbb{F}_{p^m} . Then we can choose $t \in \mathbb{F}_{p^{2m}}$ such that $t^2 = -1$. From the first equation of (21), by setting $\theta = x_1 - tx_2 \in \mathbb{F}_{p^{2m}}^*$, we have

$$x_1 = \frac{\theta + \theta^{-1}}{2}, x_2 = \frac{t(\theta - \theta^{-1})}{2}. \quad (22)$$

Since $x_1 \in \mathbb{F}_{p^m}$, the following holds:

$$\frac{\theta + \theta^{-1}}{2} = \left(\frac{\theta + \theta^{-1}}{2}\right)^{p^m} = \frac{\theta^{p^m} + \theta^{-p^m}}{2},$$

which implies $\theta^{p^m+1} = 1$ or $\theta^{p^m-1} = 1$. If $\theta^{p^m+1} \neq 1$, then $\theta^{p^m-1} = 1$. In this case, $\theta \in \mathbb{F}_{p^m}^*$. Since $x_2 = \frac{t(\theta - \theta^{-1})}{2} \in \mathbb{F}_{p^m}^*$, we have $t \in \mathbb{F}_{p^m}^*$, which is a contradiction. Hence $\theta^{p^m+1} = 1$.

- When k is even, we have $p^k + 1 \equiv 2 \pmod{4}$, then $t^{(p^k+1)} = -1$. Substituting (22) into the second equation of (21), we obtain

$$\theta^{p^k-1} + \theta^{1-p^k} = 2b. \quad (23)$$

Denote θ^{p^k-1} by w , Eq. (23) is equivalent to

$$w^2 - 2bw + 1 = 0. \quad (24)$$

If Eq.(24) has no solution, i.e., $b^2 - 1$ is a non-square of $\mathbb{F}_{p^{2m}}^*$, then $N_b = 0$. Otherwise, let w_1 and $w_2 = w_1^{-1}$ be two solutions of (24). According to the discussion above, we have

$$\theta^{p^k-1} = w_1, \theta^{p^m+1} = 1, \quad (25)$$

or

$$\theta^{p^k-1} = w_1^{-1}, \theta^{p^m+1} = 1. \quad (26)$$

If θ_1 and θ_2 are two solutions of (25), then $(\theta_1/\theta_2)^{p^k-1} = 1 = (\theta_1/\theta_2)^{p^m+1}$. Since $\gcd(p^k - 1, p^m + 1) = p^d + 1$, then $(\theta_1/\theta_2)^{p^d+1} = 1$. So if (25) has solutions, then it has exactly $p^d + 1$ solutions.

- If $w_1 = w_1^{-1}$, then (26) is the same as (25). In this case we have $w_1 = \pm 1$ and then from Eq.(24), $b = \pm 1$. But when $b = -1$, $\theta^{p^k-1} = w_1 = -1$. By $\theta^{p^m+1} = 1$ and $\gcd(2(p^k - 1), p^m + 1) = p^d + 1$, we have $\theta^{p^d+1} = 1$. And then $\theta^{p^k-1} = 1$, which is a contradiction. So we only consider $b = 1$, which implies $w_1 = 1$. Then (25) and (26) both have $p^d + 1$ solutions. As a result, we have $p^d + 1$ solutions of (21).
- If $w_1 \neq w_1^{-1}$, then (26) has the same number of solutions as (25). Moreover, their solutions are distinct since $w_1 \neq \pm 1$. Therefore, (25) and (26) both have $p^d + 1$ solutions or no solutions in $\mathbb{F}_{p^{2m}}$. By (22), (x_1, x_2) is uniquely determined by θ . Then (21) has $2(p^d + 1)$ solutions or no solutions in $\mathbb{F}_{p^m}^2$.

Until now, we have $N_{1(1)} = p^d + 1$ and $N_{1(b)} = 0$ or $2(p^d + 1)$ for $b \neq 1$. And as in Lemma 5.4 in [20], we define

$$T = \#\{b \in \mathbb{F}_{p^m} : N_{1(b)} = 2(p^d + 1)\}.$$

Then we have

$$T = \frac{p^m - p^d}{2(p^d + 1)}.$$

Substituting (22) into the third equation of (15), we obtain

$$\theta^{p^{2k}-1} + \theta^{1-p^{2k}} = 2c, \quad (27)$$

which implies $c = \frac{1}{2}\{(b + \sqrt{b^2 - 1})^{p^k+1} + (b - \sqrt{b^2 - 1})^{p^k+1}\}$. Hence if (15) has solutions, then $N_{1(b,c)} = N_{1(b)}$ and c is uniquely determined by b .

- When k is odd, we have $p^k + 1 \equiv 0 \pmod{4}$, then $t^{(p^k+1)} = 1$. Similarly, if (15) has solutions, then we have $N_{1(b,c)} = N_{1(b)}$ and c is uniquely determined by b .

Summarizing all the cases above completes the proof. ■

Lemma 3.13 Let $N_{2(b,c)}$ denote the number of solutions $(x_1, x_2) \in \mathbb{F}_{p^m}^2$ of (16), where $(b, c) \in \mathbb{F}_{p^m}^{*2}$. Then we have the following conclusions.

- (1). $N_{2(1,1)} = p^d + 1$.
- (2). When (b, c) runs through $\mathbb{F}_{p^m}^{*2} \setminus \{(1, 1)\}$,

$$N_{2(b,c)} = \begin{cases} 2(p^d + 1), & \text{for } \frac{p^m - p^d}{2(p^d + 1)} \text{ times,} \\ 0, & \text{for the rest.} \end{cases}$$

Proof. The proof is similar to the proof of the lemma above. ■

Lemma 3.14 Let $N_{3(b,c)}$ denote the number of solutions $(x_1, x_2) \in \mathbb{F}_{p^m}^2$ of (20), where $(b, c) \in \mathbb{F}_{p^m}^{*2}$. Then we have the following conclusions.

- (1). $N_{3(1,1)} = p^d - 1$.
- (2). When (b, c) runs through $\mathbb{F}_{p^m}^{*2} \setminus \{(1, 1)\}$,

$$N_{3(b,c)} = \begin{cases} 2(p^d - 1), & \text{for } \frac{p^m - p^d}{2(p^d - 1)} \text{ times,} \\ 0, & \text{for the rest.} \end{cases}$$

Proof. The proof is similar to the proof of the Lemma 3.12. ■

Acknowledgement: The authors are very grateful to the Editor in Chief, the Coordinating Editor and the anonymous reviewers, for their helpful comments that improved the quality of this paper.

References

- [1] L.D. Baumert, R.J. McEliece, Weights of irreducible cyclic codes, *Inf. Contr.*, **20**, no. 2 (1972), 158-175.
- [2] L.D. Baumert, J. Mykkeltveit, Weight distribution of some irreducible cyclic codes, *DSN Progr. Rep.*, **16** (1973), 128-131.
- [3] A.R. Calderbank, J.M. Goethals, Three-weight codes and association schemes, *Philips J. Res.*, **39** (1984), 143-152.
- [4] C. Carlet, C. Ding, J. Yuan, Linear codes from highly nonlinear functions and their secret sharing schemes, *IEEE Trans. Inf. Theory*, **51**, no.6 (2005), 2089-2102.
- [5] C. Ding, T. Helleseht, Optimal ternary cyclic codes from monomials, *IEEE Trans. Inf. Theory*, **313**, no. 4 (2013), 5898-5904.
- [6] C. Ding, Y. Liu, C. Ma, L. Zeng, The weight distributions of the duals of cyclic codes with two zeros, *IEEE Trans. Inf. Theory*, **57**, no. 12 (2011), 8000-8006.

- [7] K. Feng, J. Luo, Weight distribution of some reducible cyclic codes, *Finite Fields Appl.*, **14**, no. 2 (2008), 390-409.
- [8] T. Feng, K. Leung, Q. Xiang, Binary cyclic codes with two primitive nonzeros, *Sci. China Math.*, **56**, no. 7 (2012), 1403-1412.
- [9] H.D.L. Hollmann, Q. Xiang, On binary codes with few weights, *Finite Fields Appl.*, **11**, no. 1 (2005), 89-110.
- [10] C. Li, X. Zeng, L. Hu, A class of binary cyclic codes with five weights, *Sci. China Math.*, **53**, no. 12 (2010), 3279-3286.
- [11] R. Lidl, H. Niederreiter, Finite fields, *Addison-Wdsley Publishing Inc.*, (1983).
- [12] Y. Liu, H. Yan, C. Liu, A class of six-weight cyclic codes and their weight distribution, *Des. Codes Cryptogr.*, (2014), doi: 10.1007/s10623-014-9984-y.
- [13] J. Luo, K. Feng, On the weight distribution of two classes of cyclic codes, *IEEE Trans. Inf. Theory*, **54**, no. 12 (2008), 5332-5344.
- [14] C. Ma, L. Zeng, Y. Liu, D. Feng, C. Ding, The weight enumerator of a class of cyclic codes, *IEEE Trans. Inf. Theory*, **57**, no. 1 (2011), 397-402.
- [15] J. Yuan, C. Carlet, C. Ding, The weight distribution of a class of linear codes from perfect nonlinear functions, *IEEE Trans. Inf. Theory*, **52**, no. 2 (2006), 712-717.
- [16] B. Wang, C. Tang, Y. Qi, Y. Yang, M. Xu, The weight distributions of cyclic codes, *IEEE Trans. Inf. Theory*, **40**, no. 6 (1994), 2068-2071.
- [17] J. Wolfmann, Weight distributions of some binary primitive cyclic codes and elliptic curves, *IEEE Trans. Inf. Theory*, **58**, no. 12 (2012), 7253-7259.
- [18] M. Xiong, The weight distributions of a class of cyclic codes, *Finite Fields Appl.*, **18**, no. 5 (2012), 933-945.
- [19] D. Zheng, X. Wang, X. Zeng, L. Hu, The weight distribution of a family of p -ary cyclic codes, *Des. Codes Cryptogr.*, (2013), doi: 10.1007/s10623-013-9908-2.
- [20] Z. Zhou, C. Ding, J. Luo, A. Zhang, A family of five-weight cyclic codes and their weight enumerators, *IEEE Trans. Inf. Theory*, **59**, no. 10 (2013), 6674-6682.