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

Yan Liu† Haode Yan‡

Abstract

In this paper, a family of five-weight cyclic codes over \( \mathbb{F}_p \) whose duals have three zeros is presented, where \( p \) is an odd prime. And the weight distribution of these cyclic codes is determined.

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

MSC: 94B15, 11T71.

1 INTRODUCTION

Throughout this paper, let \( m \geq 5 \) be an odd integer and \( k \) be any positive integer such that \( \gcd(m, k) = 1 \). Let \( p \) be an odd prime and \( \pi \) be a primitive element of the finite field \( \mathbb{F}_p^m \).

An \([n, l, d]\) linear code \( C \) over \( \mathbb{F}_p \) is an \( l \)-dimensional subspace of \( \mathbb{F}_p^n \) with minimum distance \( d \). Let \( A_i \) denote the number of codewords with Hamming weight \( i \) in \( C \). The weight enumerator of \( C \) is defined by \( 1 + A_1 Z + A_2 Z^2 + \cdots + A_n Z^n \). The sequence \((1, A_1, A_2, \ldots, A_n)\) is called the weight distribution of the code \( C \). And \( C \) is called cyclic if \((c_0, c_1, \ldots, c_{n-1}) \in C \) implies \((c_{n-1}, c_0, \ldots, c_{n-2}) \in C \). By identifying any vector \((c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_p^n \) with \( c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in \mathbb{F}_p[x]/(x^n - 1) \), any cyclic code corresponds to an ideal of the polynomial residue class ring \( \mathbb{F}_p[x]/(x^n - 1) \). Since \( \mathbb{F}_p[x]/(x^n - 1) \) 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 referred to as the parity-check polynomial of the code \( C \). A cyclic code is called irreducible if its parity-check polynomial is irreducible over \( \mathbb{F}_p \) and reducible, otherwise. A cyclic code is said to be have \( t \) zeros if all the zeros of the generator polynomial of the code form \( t \) different conjugate classes, or equivalently, its generator polynomial has \( t \) different irreducible factors over \( \mathbb{F}_p \).

---

*This work is supported by the National Natural Science Foundation of China (No. 11071160).
†Corresponding author, Dept. of Math., SJTU, Shanghai, 200240, liuyan0916@sjtu.edu.cn.
‡Dept. of Math., Shanghai Jiaotong Univ., Shanghai, 200240, hdyan@sjtu.edu.cn.
Clearly, the weight distribution gives the minimum distance of the code, and thus the error capability. In addition, the weight distribution of a code allows the computation of the error probability of error detection and correction with respect to some error detection and error correction algorithms. Thus the study of the weight distribution of a linear code is important in both theory and applications. For cyclic codes, the error correcting capability may not be as good as some other linear codes in general. However, cyclic codes have wide applications in storage and communication systems because they have efficient encoding and decoding algorithms. So the weight distributions of cyclic codes have been interesting subjects of study for many years and are very hard problem in general.

For information on the weight distribution of irreducible cyclic codes, the reader is referred to [1, 2, 5, 6]. Information on the weight distributions of reducible cyclic codes could be found in [7–10, 13–19]. For the duals of the known cyclic codes whose weight distributions were determined, most of them have at most two zeros, only a few of them have three or more zeros (see [9, 13, 14, 19, 20]).

The objective of this paper is to determine the weight distribution of a class of five-weight cyclic codes whose duals have three zeros.

This paper is organized as follows. Section 2 presents some preliminaries which will be needed. Section 3 defines the family of cyclic codes and determines their weight distributions.

2 PRELIMINARIES

In this section, we first give a brief introduction to the theory of quadratic forms over finite fields which will be needed to determine the weight distribution of the cyclic codes in the next section. Quadratic forms have been well studied (see [12] and the references therein), and have application in design and coding theory.

**Definition 2.1** Let \( x = \sum_{i=1}^{m} x_i \varepsilon_i \) where \( x_i \in \mathbb{F}_p \) and \( \{ \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m \} \) is a basis for \( \mathbb{F}_m^p \) over \( \mathbb{F}_p \). Then a function \( Q(x) \) from \( \mathbb{F}_m^p \) to \( \mathbb{F}_p \) is a quadratic form over \( \mathbb{F}_p \) if it can be represented as

\[
Q(x) = Q\left( \sum_{i=1}^{m} x_i \varepsilon_i \right) = \sum_{1 \leq i \leq j \leq m} a_{ij} x_i x_j,
\]

where \( a_{ij} \in \mathbb{F}_p \).

The rank of the quadratic form \( Q(x) \) is defined as the codimension of the \( \mathbb{F}_p \)-vector space \( V = \{ x \in \mathbb{F}_m^p : Q(x + z) - Q(x) - Q(z) = 0 \text{ for all } z \in \mathbb{F}_m^p \} \).

For a quadratic form \( F(x) \), there exists a symmetric matrix \( A \) of order \( m \) over \( \mathbb{F}_p \) such that \( F(x) = XAX' \), where \( X = (x_1, x_2, \ldots, x_m) \in \mathbb{F}_m^p \) and \( X' \) denotes the transpose of \( X \). Then there exists a nonsingular matrix \( H \) of order \( m \) over \( \mathbb{F}_p \), such that \( MAM' \) is a diagonal matrix (12). Under the nonsingular linear substitution \( X = ZM \) with \( Z = (z_1, z_2, \ldots, z_m) \in \mathbb{F}_m^p \), then \( F(x) = ZMAM'Z' = \sum_{i=1}^{r} d_i z_i^2 \), where \( r \) is the rank of \( F(x) \) and \( d_i \in \mathbb{F}_p \). Let \( \triangle = d_1 d_2 \cdots d_r \) (we assume \( \triangle = 0 \) when \( r = 0 \)). Then
the Legendre symbol \((\frac{a}{p})\) is an invariant of \(A\) under the action of \(H \in GL_m(F_p)\). The following result is useful in the next section.

**Lemma 2.2** \(\text{[13]}\) Let \(F(x)\) be a quadratic form in \(m\) variables of rank \(r\) over \(F_p\), then
\[
\sum_{y \in F_p^*} \sum_{x \in F_{p^m}} \zeta_p F(x) = \begin{cases} 
\pm (p-1)p^{m-2}, & r \text{ even,} \\
0, & \text{otherwise.}
\end{cases}
\]
where \(\zeta_p\) is a primitive \(p\)-th root of unity.

For any fixed \((a, b, c) \in F_{3}^{p^m}\), \(Q_{a,b,c}(x) = Tr(a \pi^{2t} + b \pi^{2k} + c \pi^{2k+1})\), where \(Tr\) is the trace map from \(F_{p^m}\) to \(F_p\). Moreover, we have the following result.

**Lemma 2.3** For any \((a, b, c) \in F_{3}^{p^m} \setminus \{(0, 0, 0)\}\), \(Q_{a,b,c}(x)\) is a quadratic form over \(F_p\) with rank at least \(m - 4\).

**Proof.** The proof is similar to the proof of Lemma 4.1 in \([20]\), so we omit the details.

In this paper, we always assume that \(\lambda\) is a fixed non-square in \(F_p\). Since \(m\) is odd, it is also a non-square in \(F_{p^m}\).

### 3 THE CLASS OF FIVE-WEIGHT CYCLIC CODES AND THEIR WEIGHT DISTRIBUTION

We follow the notations fixed in Section 1 and 2. In this section, we first introduce the family of cyclic codes to be studied. Let \(h_0(x), h_1(x)\) and \(h_2(x)\) be the minimal polynomials of \(\pi^{-2}, \pi^{-(p^k+1)}\) and \(\pi^{-((p^{2k}+1)}\) over \(F_p\), respectively. It is easy to check that \(h_0(x), h_1(x)\) and \(h_2(x)\) are polynomials of degree \(m\) and are pairwise distinct when \(m \geq 5\). Define \(h(x) = h_0(x) h_1(x) h_2(x)\). Then \(h(x)\) has degree \(3m\) and is a factor of \(x^{p^m - 1} - 1\).

Let \(C_{(p,m,k)}\) be the cyclic code with parity-check polynomial \(h(x)\). Then \(C_{(p,m,k)}\) has length \(p^m - 1\) and dimension \(3m\). Moreover, it can be expressed as
\[
C_{(p,m,k)} = \{ c_{(a,b,c)} : a, b, c \in F_{p^m} \},
\]
where
\[
c_{(a,b,c)} = (Tr(a \pi^{2t} + b \pi^{p^k+1} + c \pi^{p^{2k}+1} t))_{t=0}^{m-2}.
\]
Let \(h'(x) = h_0(x) h_1(x)\) and \(C'_{(p,m,k)}\) be the cyclic code with parity-check polynomial \(h'(x)\). Then \(C'_{(p,m,k)}\) is a subcode of \(C_{(p,m,k)}\) with dimension \(2m\). Keqing Feng and Jinquan Luo determined the weight distribution of \(C'_{(p,m,k)}\) in \([9,13]\). In this paper, we will show that \(C_{(p,m,k)}\) have five nonzero weights and determine the weight distribution of this class of cyclic codes.
In terms of exponential sums, the weight of the codeword \( c_{(a,b,c)} = (c_0, c_1, \ldots, c_{p^m-2}) \) in \( C_{(p,m,k)} \) is given by

\[
W(c_{(a,b,c)}) = \# \left\{ 0 \leq t \leq p^m - 2 : c_t \neq 0 \right\}
\]

\[
= p^m - 1 - \frac{1}{p} \sum_{t=0}^{p^m-2} \sum_{y \in \mathbb{F}_p} \zeta_p^{yc(t)}
\]

\[
= p^m - 1 - \frac{1}{p} \sum_{t=0}^{p^m-2} \zeta_p^{yTr(a \pi^{2t} + b \pi^{(p^k+1)t} + c \pi^{(p^{2k}+1)t})}
\]

\[
= p^m - 1 - \frac{1}{p} \sum_{t=0}^{p^m-2} \sum_{y \in \mathbb{F}_p} \zeta_p^{yTr(a x^2 + b x^{p^k+1} + c x^{p^{2k}+1})}
\]

\[
= p^m - p^{m-1} - \frac{1}{p} \sum_{y \in \mathbb{F}_p} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{yTr(ax^2 + b x^{p^k+1} + c x^{p^{2k}+1})}
\]

\[
= p^m - p^{m-1} - \frac{1}{p} S(a, b, c),
\]

where

\[
S(a, b, c) = \sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{yTr(ax^2 + b x^{p^k+1} + c x^{p^{2k}+1})}.
\]

Based on the discussions above, the weight distribution of the code \( C_{(p,m,k)} \) is completely determined by the value distribution of \( S(a, b, c) \). Firstly, we have the following lemma.

**Lemma 3.1** Let \( S(a, b, c) \) be defined by (2), then for any \((a, b, c) \in \mathbb{F}_p^3\), \( S(a, b, c) \) takes values from the set \( \{0, (p-1)p^m, \pm(p-1)p^{m+1/2}, \pm(p-1)p^{m+3/2}\} \).

**Proof.** Following the notations above, we have \( S(a, b, c) = \sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{yQ(a,b,c)} \).

Case I. In the case of \( a = b = c = 0 \), \( S(a, b, c) = (p-1)p^m \).

Case II. In the case of \((a, b, c) \in \mathbb{F}_p^3 \setminus \{(0, 0, 0)\} \), again by Lemma 2.2 and 2.3 \( S(a, b, c) \neq 0 \) only if \( Q(a, b, c) \) has even rank. Thus \( S(a, b, c) = \pm(p-1)p^{m+1/2} \) if \( Q(a, b, c) \) has rank \( m-1 \) and \( S(a, b, c) = \pm(p-1)p^{m+3/2} \) if \( Q(a, b, c) \) has rank \( m-3 \). And otherwise \( S(a, b, c) = 0 \). This completes the proof. \( \square \)
Moreover, by Eq. (2), we have

\[ S(a, b, c) = \sum_{y \in S_q} \sum_{x \in \mathbb{F}_p} \zeta_y \text{Tr}(ax^2 + bxy^{k+1} + cx^{2k+1}) \]

\[ = \sum_{y \in S_q} \sum_{x \in \mathbb{F}_p} \zeta_y \text{Tr}(ax^2 + bxy^{k+1} + cx^{2k+1}) + \sum_{y \in S_q} \sum_{x \in \mathbb{F}_p} \zeta_y \text{Tr}(ax^2 + bxy^{k+1} + cx^{2k+1}) \]

\[ = \sum_{y \in S_q} \sum_{x \in \mathbb{F}_p} \zeta_y \text{Tr}(a(x^{y/2})^2 + b(x^{y/2})y^{k+1} + c(x^{y/2})x^{2k+1}) + \sum_{y \in S_q} \sum_{x \in \mathbb{F}_p} \zeta_y \text{Tr}(a(x^{y/2})^2 + b(x^{y/2})y^{k+1} + c(x^{y/2})x^{2k+1}) \]

\[ = \sum_{y \in S_q} \sum_{x \in \mathbb{F}_p} \zeta_y \text{Tr}(a(x^{y/2})^2 + b(x^{y/2})y^{k+1} + c(x^{y/2})x^{2k+1}) + \sum_{y \in S_q} \sum_{x \in \mathbb{F}_p} \zeta_y \text{Tr}(a(x^{y/2})^2 + b(x^{y/2})y^{k+1} + c(x^{y/2})x^{2k+1}) \]

\[ = \frac{(p - 1)}{2} \left( \sum_{x \in \mathbb{F}_p} \zeta_{Q_{a,b,c}}(x) + \sum_{x \in \mathbb{F}_p} \zeta_{\lambda Q_{a,b,c}}(x) \right), \]

where \( S_q \) and \( S_q^* \) denote the set of nonzero squares and the set of non-squares of \( \mathbb{F}_p \), respectively.

In the case of \( k \) even, the value distribution of \( S(a, b, c) \) can be determined by the following theorem.

**Theorem 3.2** Let \( k \) be even and \( S(a, b, c) \) be defined by (3). Then as \( (a, b, c) \) runs through \( \mathbb{F}_p^3 \), the value distribution of \( S(a, b, c) \) is given by Table 1.

| Weight | Frequency |
|--------|-----------|
| \((p - 1)p^{m}\) | 1 |
| \((p - 1)p^{m+1/2}\) | \(p^m - 1\) \((p^2m - p^{2m-1} + p^{2m-4} + p^m - p^{m-1} - p^{m-3} + 1)\) |
| \((p - 1)p^{m+1/2}\) | \((p^{m+1})(m+3)/2\) \((p^{2m} - p^{2m-2} + p^{2m-3} - p^{m-2} + p^{m-3} - 1)\) |
| \((p - 1)p^{m+1/2}\) | \((p^{m+1})(m+3)/2\) \((p^{2m} - p^{2m-2} + p^{2m-3} - p^{m-2} + p^{m-3} - 1)\) |
| \((p - 1)p^{m+1/2}\) | \((p^{m-3})(m-3)/2\) \((p^{m-1})(m-1)\) |
| \((p - 1)p^{m+1/2}\) | \((p^{m-3})(m-3)/2\) \((p^{m-1})(m-1)\) |

**Proof.** From the above discussion, when \( k \) is even, \( S(a, b, c) = (p - 1)S_f(a,b,c) \), where

\[ S_f(a,b,c) = \sum_{x \in \mathbb{F}_p} \zeta_{Q_{x,y,z}}(x), \]

Then the value distribution of \( S(a, b, c) \) can be determined by the value distribution of \( S_f(a,b,c) \) which is presented by [20] Lemma 4.5. 

For the case of \( k \) odd, if we define

\[ T(a, b, c) = \sum_{x \in \mathbb{F}_p} \zeta_{Q_{a,b,c}}(x) + \sum_{x \in \mathbb{F}_p} \zeta_{\lambda Q_{a,b,c}}(x), \]

(3)
then the value distribution of $S(a, b, c)$ can be determined by the value distribution of $T(a, b, c)$.

**Theorem 3.3** Let $k$ be odd and $T(a, b, c)$ be defined by (3). Then as $(a, b, c)$ runs through $\mathbb{F}_{p^m}^3$, the value distribution of $T(a, b, c)$ is given by Table 2.

### Table 2: Weight Distribution of $T(a, b, c)$

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

We prove this theorem only for the case that $p \equiv 3 \pmod{4}$. The proof for the case that $p \equiv 1 \pmod{4}$ is similar and omitted. Hence we assume that $p \equiv 3 \pmod{4}$ 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 odd positive integer $k$, we define $d_1 = p^k + 1$ and $d_2 = p^{2k} + 1$. And $−1$ is a non-square when $p \equiv 3 \pmod{4}$, so in the following, we set $\lambda = −1$.

**Lemma 3.4** Let $p \equiv 3 \pmod{4}$ 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

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

Then $N_2 = 1$.

**Proof.** This system of equations have only one solution $(0, 0)$, since $−1$ is a non-square when $p \equiv 3 \pmod{4}$. ■

**Lemma 3.5** Let $p \equiv 3 \pmod{4}$ 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

$$
\begin{aligned}
&x_1^2 - x_2^2 = 0 \\
&x_1^{d_1} - x_2^{d_1} = 0 \\
&x_1^{d_2} - x_2^{d_2} = 0.
\end{aligned}
$$

Then $\overline{N_2} = 2p^m − 1$.  

6
Proof. We can have the observation that \((x_1, x_2)\) is a solution of (4) 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 [12].

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

\[
\begin{align*}
  x_1^2 + x_2^2 + x_3^2 &= 0 \\
  x_1^{d_1} + x_2^{d_1} + x_3^{d_1} &= 0 \\
  x_1^{d_2} + x_2^{d_2} + x_3^{d_2} &= 0.
\end{align*}
\]

Then \(N_3 = p^{m+1} + p^m - p\).

Proof.
Case I, when \(x_3 = 0\). In this case, by Lemma 3.4 the number of solutions of (5) is 1.
Case II, when \(x_3 \neq 0\). In this case, for each \(x_3 \in \mathbb{F}_p^*\), the equation system (5) has the same number of solutions \((x_1, x_2)\) \(\in \mathbb{F}_p^2\) of

\[
\begin{align*}
  x_1^{d_1} + x_2^{d_1} + 1 &= 0 \\
  x_1^{d_2} + x_2^{d_2} + 1 &= 0.
\end{align*}
\]

Then we have

\[
\begin{align*}
  x_1^{d_1} + 1 &= -(x_1^2 + 1)^{\frac{d_1}{2}} \\
  x_1^{d_2} + 1 &= (x_1^2 + 1)^{\frac{d_2}{2}}.
\end{align*}
\]

By performing squares on both sides of each equation in (7), we have

\[
\begin{align*}
  x_1^2(x_1^{2k-1} - 1) &= 0 \\
  x_1^2(x_1^{2k-1} - 1) &= 0,
\end{align*}
\]

which implies that \(x_1 \in \mathbb{F}_p\) since \(\gcd(m, k) = \gcd(m, 2k) = 1\). We can prove that \(x_2 \in \mathbb{F}_p\) in the same way. Conversely, for any \((x_1, x_2) \in \mathbb{F}_p^2\) satisfying the first equation in (5), it is clear that \((x_1, x_2)\) is a solution of (5). So the number of solutions \((x_1, x_2) \in \mathbb{F}_p^2\) of (5) is equal to the number of solutions \((x_1, x_2) \in \mathbb{F}_p^2\) satisfying the first equation of it, which is \(p + 1\) by Lemma 6.24 in [12]. Thus (5) has exactly \(p + 1\) solutions.

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

Lemma 3.7 Let \(p \equiv 3 \pmod{4}\) and let \(\overline{N}_3\) denote the number of solutions \((x_1, x_2, x_3)\) \(\in \mathbb{F}_p^3\) of the following system of equations

\[
\begin{align*}
  x_1^2 + x_2^2 - x_3^2 &= 0 \\
  x_1^{d_1} + x_2^{d_1} - x_3^{d_1} &= 0 \\
  x_1^{d_2} + x_2^{d_2} - x_3^{d_2} &= 0.
\end{align*}
\]

Then \(\overline{N}_3 = p^{m+1} + p^m - p\).
Proof. The proof is similar to the proof of the lemma above, so we omit the details.

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

\[
\begin{align*}
    x_1^2 + x_2^2 + x_3^2 + x_4^2 &= 0, \\
    x_1^{d_1} + x_2^{d_1} + x_3^{d_1} + x_4^{d_1} &= 0, \\
    x_1^{d_2} + x_2^{d_2} + x_3^{d_2} + x_4^{d_2} &= 0.
\end{align*}
\]

(8)

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

Proof. See Appendix.

Lemma 3.9 Let \( p \equiv 3 \pmod{4} \) and let \( \overline{N}_4 \) denote the number of solutions \((x_1, x_2, x_3, x_4) \in \mathbb{F}_p^{4m} \) of the following system of equations

\[
\begin{align*}
    x_1^2 + x_2^2 + x_3^2 - x_4^2 &= 0, \\
    x_1^{d_1} + x_2^{d_1} + x_3^{d_1} - x_4^{d_1} &= 0, \\
    x_1^{d_2} + x_2^{d_2} + x_3^{d_2} - x_4^{d_2} &= 0.
\end{align*}
\]

(9)

Then \( \overline{N}_4 = p^{m+2} + p^m - p^2 \).

Proof. See Appendix.

Lemma 3.10 Let \( p \equiv 3 \pmod{4} \) and let \( \overline{N}_4 \) denote the number of solutions \((x_1, x_2, x_3, x_4) \in \mathbb{F}_p^{4m} \) of the following system of equations

\[
\begin{align*}
    x_1^2 + x_2^2 - x_3^2 - x_4^2 &= 0, \\
    x_1^{d_1} + x_2^{d_1} - x_3^{d_1} - x_4^{d_1} &= 0, \\
    x_1^{d_2} + x_2^{d_2} - x_3^{d_2} - x_4^{d_2} &= 0.
\end{align*}
\]

(10)

Then \( \overline{N}_4 = (p + 1)(p^m - 1)(2p^m - p + 1) + 1 \).

Proof. See Appendix.

Now we are ready to prove Theorem 3.3 in the case of \( p \equiv 3 \pmod{4} \).

Proof of Theorem 3.3 It is clear that \( T(a, b, c) = 2p^m \) if \((a, b, c) = (0, 0, 0)\). Otherwise, by Lemma 3.1, we have

\[
T(a, b, c) \in \{0, \pm 2p^{\frac{m+1}{2}}, \pm 2p^{\frac{m+3}{2}}\}.
\]

We define

\[
\begin{align*}
    n_{1,i} &= \# \{(a, b, c) \in \mathbb{F}_p^3 : T(a, b, c) = (-1)^i 2p^{\frac{m+i}{2}} \}, \\
    n_{2,i} &= \# \{(a, b, c) \in \mathbb{F}_p^3 : T(a, b, c) = (-1)^i 2p^{\frac{m+i}{2}} \},
\end{align*}
\]

8
where \( i = 0, 1 \). Then we immediately have

\[
\begin{align*}
\sum_{(a,b,c) \in \mathbb{P}_p^3} T(a, b, c) &= 2p^m + 2(n_{1,0} - n_{1,1})p^{m+1} + 2(n_{2,0} - n_{1,1})p^{m+3} \\
\sum_{(a,b,c) \in \mathbb{P}_p^3} T^2(a, b, c) &= 2^2p^{2m} + 2^2(n_{1,0} + n_{1,1})p^{m+1} + 2^2(n_{2,0} + n_{1,1})p^{m+3} \\
\sum_{(a,b,c) \in \mathbb{P}_p^3} T^3(a, b, c) &= 2^3p^{3m} + 2^3(n_{1,0} - n_{1,1})p^{3m+3} + 2^3(n_{2,0} - n_{1,1})p^{3m+3} \\
\sum_{(a,b,c) \in \mathbb{P}_p^3} T^4(a, b, c) &= 2^4p^{4m} + 2^4(n_{1,0} + n_{1,1})p^{2m+2} + 2^4(n_{2,0} + n_{1,1})p^{2m+6}.
\end{align*}
\]

On the other hand, it follows from Eq. (3) that

\[
\sum_{(a,b,c) \in \mathbb{P}_p^3} T(a, b, c) = 2p^m.
\]

\[
\sum_{(a,b,c) \in \mathbb{P}_p^3} T^2(a, b, c) = 2^2p^{2m}.
\]

\[
\sum_{(a,b,c) \in \mathbb{P}_p^3} T^3(a, b, c) = 2^3p^{3m}.
\]

\[
\sum_{(a,b,c) \in \mathbb{P}_p^3} T^4(a, b, c) = 2^4p^{4m}.
\]

where

\[
S_1 = \{(x_1, x_2) \in \mathbb{P}_p^2 : x_1^2 + x_2^2 = 0, x_1^{d_1} + x_2^{d_1} = 0, x_1^{d_2} + x_2^{d_2} = 0\},
\]

\[
S_2 = \{(x_1, x_2) \in \mathbb{P}_p^2 : x_1^2 - x_2^2 = 0, x_1^{d_1} - x_2^{d_1} = 0, x_1^{d_2} - x_2^{d_2} = 0\},
\]

\[
S_3 = \{(x_1, x_2) \in \mathbb{P}_p^2 : -x_1^2 + x_2^2 = 0, -x_1^{d_1} + x_2^{d_1} = 0, -x_1^{d_2} + x_2^{d_2} = 0\},
\]

\[
S_4 = \{(x_1, x_2) \in \mathbb{P}_p^2 : -x_1^2 - x_2^2 = 0, -x_1^{d_1} - x_2^{d_1} = 0, -x_1^{d_2} - x_2^{d_2} = 0\}.
\]

It is clear that \( \#S_1 = \#S_4 \) and \( \#S_2 = \#S_3 \). Then by Lemma 3.4 and 3.5, we have

\[
\sum_{(a,b,c) \in \mathbb{P}_p^3} T^2(a, b, c) = 4p^{4m}.
\]
Similarly, by Lemmas 3.6-3.10 we have
\[\sum_{(a,b,c) \in \mathbb{F}_p^3} T^3(a,b,c) = 8p^{3m}(p^{m+1} + p^m - p),\]
\[\sum_{(a,b,c) \in \mathbb{F}_p^3} T^4(a,b,c) = 16p^{4m}(p^{m+1} + p^m - p).\]

Combining Eqs. (12)-(14), we get
\[n_{1,0} = \frac{(p^{m+1} + p^{(m+3)/2})(p^{2m} - p^{2m-2} - p^{2m-3} + p^{m-2} + p^{m-3} - 1)}{2(p^2 - 1)},\]
\[n_{1,1} = \frac{(p^{m+1} - p^{(m+3)/2})(p^{2m} - p^{2m-2} - p^{2m-3} + p^{m-2} + p^{m-3} - 1)}{2(p^2 - 1)},\]
\[n_{2,0} = \frac{(p^{m-3} + p^{(m-3)/2})(p^{m-1} - 1)(p^m - 1)}{2(p^2 - 1)},\]
\[n_{2,1} = \frac{(p^{m-3} - p^{(m-3)/2})(p^{m-1} - 1)(p^m - 1)}{2(p^2 - 1)}.

Summarizing the discussion above completes the proof of this theorem in the case of \(p \equiv 3 \mod 4\). For the case of \(p \equiv 1 \mod 4\), the proof is similar, so we omit the details.

Recall that \(C_{p,m,k}\) is the cyclic code over \(\mathbb{F}_p\) 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 \(\pi^{-2}, \pi^{-(p^k+1)}, \pi^{-(p^{2k}+1)}\) over \(\mathbb{F}_p\), respectively.

**Theorem 3.11** Let \(m \geq 5\) be an odd integer and \(k\) be any positive integer such that \(\gcd(m,k) = 1\). \(C_{p,m,k}\) is a cyclic code over \(\mathbb{F}_p\) with parameters \([p^m - 1, 3m, (p - 1)(p^{m-1} - p^{\frac{m+1}{2}})]\). Moreover, the weight distribution of \(C_{p,m,k}\) is given in Table 3.

**Proof.** The length and dimension of \(C_{p,m,k}\) follow directly from the definition. The minimal distance and weight distribution of \(C_{p,m,k}\) follows from Eq. (1) and Theorem 3.24 and 3.34.

| Weight | Frequency |
|--------|-----------|
| \((p - 1)p^{m-1}\) | \((p^{m-1}) - (p^{m-1} - p^{\frac{m+1}{2}})\) |
| \((p - 1)(p^{m-1} + p^{\frac{m+1}{2}})\) | \((p^{m+1} + p^{(m+3)/2})(p^{2m} - p^{2m-2} - p^{2m-3} + p^{m-2} + p^{m-3} - 1)\) |
| \((p - 1)(p^{m-1} - p^{\frac{m+1}{2}})\) | \((p^{m+1} - p^{(m+3)/2})(p^{2m} - p^{2m-2} - p^{2m-3} + p^{m-2} + p^{m-3} - 1)\) |
| \((p - 1)(p^{m-1} - p^{\frac{m+1}{2}})\) | \((p^{m-3} + p^{(m-3)/2})(p^{m-1} - 1)(p^m - 1)\) |
| \((p - 1)(p^{m-1} + p^{\frac{m+1}{2}})\) | \((p^{m-3} - p^{(m-3)/2})(p^{m-1} - 1)(p^m - 1)\) |

The following are some examples of the codes.
Example 3.12 Let \( p = 3, \ m = 5 \) and \( k = 2 \). The the code \( C_{(3,5,1)} \) is a \([242, 15, 108]\) cyclic code over \( \mathbb{F}_3 \) with weight enumerator

\[
1 + 14520z^{108} + 2548260z^{144} + 9740258z^{162} + 2038608z^{180} + 7260z^{216},
\]

which confirms the weight distribution in Table 3.

Example 3.13 Let \( p = 3, \ m = 7 \) and \( k = 1 \). The the code \( C_{(3,7,1)} \) 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 confirms the weight distribution in Table 3.

In fact, we can determined the weight distribution of \( C_{(p,m,k)} \) in a more general case. Since the proof is similar to that of Theorem 3.11 we only report the conclusion and will not give the details of the proof.

**Theorem 3.14** Let \( m \) and \( k \) be any positive integers such that \( \gcd(m,k) = e \) and \( m/e \geq 5 \) be odd. \( C_{(p,m,k)} \) is a cyclic code over \( \mathbb{F}_p \) with parameters \([p^m - 1, 3m, (p - 1)(p^m - 1 - p^{3m-e-2})] \). Moreover, the weight distribution of \( C_{(p,m,k)} \) is given in Table 4.

**Table 4: Weight Distribution of \( C_{(p,m,k)} \)**

| Weight                  | Frequency                                                                 |
|-------------------------|---------------------------------------------------------------------------|
| \((p - 1)p^{m - 1}\)    | \((p^m - 1)(p^{m - 1} - p^{3m-e-2}) \)                                    |
| \((p - 1)(p^{m - 1} - p^{m+e-2})\) | \((p^m + p^{(m+3)}/2)(p^{m - 1} - p^{3m-e-2}) \)                         |
| \((p - 1)(p^{m - 1} + p^{m+e-2})\) | \((p^m - p^{(m+3)/2}(p^{m - 1} - 1)(p^{m - 1}) \)                      |
| \((p - 1)(p^{m - 1} - p^{m+3e-2})\) | \((p^{m - 1} - p^{m+3e-2})\) \((p^{m - 1}) \)                          |

APPENDIX

**Proof of Lemma 3.8** For any \((\overline{a}, \overline{b}, \overline{c}) \in \mathbb{F}_p^3\), let \(N_1(\overline{a}, \overline{b}, \overline{c})\) and \(N_2(\overline{a}, \overline{b}, \overline{c})\) denote the number of solutions of the following two system of equations:

\[
\begin{align*}
&x_1^2 + x_2^2 = \overline{a} \\
&x_1^d + x_2^d = \overline{b} \\
&x_1^{d_2} + x_2^{d_2} = \overline{c} \\
&x_3^2 + x_4^2 = -\overline{a} \\
&x_3^d + x_4^d = -\overline{b} \\
&x_3^{d_2} + x_4^{d_2} = -\overline{c}
\end{align*}
\]
It is then obvious that

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

Case 1, when \( \overline{a} = 0 \). In this case, (15) and (16) have solutions if and only if \( \overline{b} = \overline{c} = 0 \) since \(-1\) is a non-square. Moreover, \( N_{1(0,0,0)} = N_{2(0,0,0)} = 1 \).

Case 2, when \( \overline{a} \neq 0 \). In this case, if \( \overline{b} = 0 \) or \( \overline{c} = 0 \), neither (15) nor (16) has solutions. So in the following, we consider the problem only when \( \overline{b} \neq 0 \) and \( \overline{c} \neq 0 \).

- \( \overline{a} \) is a nonzero square, \( \overline{b} \neq 0 \) and \( \overline{c} \neq 0 \). In this case, for any given \( \overline{a} \neq 0 \), equation system (15) has the same number of solutions as

\[
\begin{align*}
    x_1^2 + x_2^2 & = 1 \\
    x_1^{d_1} + x_2^{d_2} & = b \\
    x_1^{d_2} + x_2^{d_2} & = c 
\end{align*}
\]

and equation system (16) has the same number of solutions as

\[
\begin{align*}
    x_3^2 + x_4^2 & = -1 \\
    x_3^{d_1} + x_4^{d_1} & = -b \\
    x_3^{d_2} + x_4^{d_2} & = -c, 
\end{align*}
\]

where \( b = \overline{b}/\overline{a}^{d_1} \) and \( c = \overline{c}/\overline{a}^{d_2} \). Clearly, \((b, c)\) runs through \( \mathbb{F}_{p^m}^2 \) as \((\overline{b}, \overline{c})\) does. According to the proof of Lemma 3.16 and 3.16, it can be easy to see that for any fixed \((b, c) \in \mathbb{F}_{p^m}^2 \setminus \{(1,1)\}\) such that (17) have \(2(p+1)\) solutions, then for \((-b, -c)\), (18) also have \(2(p+1)\) solutions. Therefore, in this case we have

\[
\begin{align*}
    \sum_{(\overline{a}, \overline{b}, \overline{c}) \in \mathbb{F}_{p^m}^3} N_{1(\overline{a}, \overline{b}, \overline{c})} N_{2(\overline{a}, \overline{b}, \overline{c})} \\
    = (p^m - 1) \left\{ (p+1)^2 + (2(p+1))^2 \frac{p^m - p}{2(p+1)} \right\} \\
    = (p+1)(p^m-1)(2p^m-p+1). 
\end{align*}
\]

- \( \overline{a} \) is a non-square. In this case, for any given \( \overline{a} \neq 0 \), equation system (15) has the same number of solutions as

\[
\begin{align*}
    x_1^2 + x_2^2 & = -1 \\
    x_1^{d_1} + x_2^{d_1} & = -b \\
    x_1^{d_2} + x_2^{d_2} & = -c 
\end{align*}
\]

and equation system (16) has the same number of solutions as

\[
\begin{align*}
    x_3^2 + x_4^2 & = 1 \\
    x_3^{d_1} + x_4^{d_1} & = b \\
    x_3^{d_2} + x_4^{d_2} & = c. 
\end{align*}
\]
It can be easily seen that this case is equivalent to the case when $\alpha$ is a nonzero square. So when $\alpha$ is a non-square, we also have
\[
\sum_{(\beta,\gamma)\in\mathbb{F}_p^m} N_1(\alpha,\beta,\gamma)N_2(\alpha,\beta,\gamma)
= (p + 1)(p^m - 1)(2p^m - p + 1).
\]

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

**Lemma 3.15** Let $N_1(b,c)$ denote the number of solutions $(x_1, x_2) \in \mathbb{F}_p^m$ of (17), where $(b,c) \in \mathbb{F}_p^m$. Then we have the following conclusions.

1. $N_1(1,1) = p + 1$.
2. When $(b,c)$ runs through $\mathbb{F}_p^m \setminus \{(1,1)\}$,
   
   $N_1(b,c) = \begin{cases} 
   2(p + 1), & \text{for } \frac{p^m - p}{2(p + 1)} \text{ times,} \\
   0, & \text{for the rest.} 
   \end{cases}$

**Proof.** We first compute the number $N_6$ of solutions $(x_1, x_2) \in \mathbb{F}_p^m$ of the following system of equations
\[
\begin{cases}
  x_1^2 + x_2^2 = 1 \\
  x_1^d + x_2^d = b.
\end{cases}
\]  

Choose $t \in \mathbb{F}_p^m$ such that $t^2 = -1$. From the first equation of (19), by setting $\theta = x_1 - tx_2 \in \mathbb{F}_p^m$, we can have
\[
x_1 = \frac{\theta + \theta^{-1}}{2}, \quad x_2 = \frac{t(\theta - \theta^{-1})}{2}.
\]

Substituting (20) into the second equation of (19), we obtain
\[
\theta^{p+1} + \theta^{-p-1} = 2b.
\]

Denote $\theta^{p+1}$ by $w$, Eq. (21) is equivalent to
\[
w^2 - 2bw + 1 = 0.
\]

If Eq. (22) has no solution, i.e., $b^2 - 1$ is a non-square of $\mathbb{F}_p^m$, then $N_6 = 0$. Otherwise, let $w_1$ and $w_2 = w_1^{-1}$ be two solutions of (22). From $x_1 \in \mathbb{F}_p^m$ we have
\[
\frac{\theta + \theta^{-1}}{2} = \left(\frac{\theta + \theta^{-1}}{2}\right)^{p^m} = \frac{\theta^{p^m} + \theta^{-p^m}}{2},
\]

which implies $\theta^{p^m+1} = 1$ or $\theta^{p^m-1} = 1$.

- If $\theta^{p^m+1} = 1$, then $x_2^{p^m} = \frac{(t\theta - \theta^{-1})}{2} = \frac{t\theta^{p^m} - \theta^{-p^m}}{2} = \frac{t(\theta - \theta^{-1})}{2} = x_2$ since $\theta^{p^m} = -t$. It follows that $x_2 \in \mathbb{F}_p^m$. Recall that $w_1$ and $w_1^{-1}$ are two solutions of (22). Then we have
  \[
  \theta^{p+1} = w_1, \theta^{p^{m+1}} = 1,
  \]

1
or
\[ \theta^{p^k+1} = w_1, \theta^{p^m+1} = 1. \] (24)

If \( \theta_1 \) and \( \theta_2 \) are two solutions of (23), then \((\theta_1/\theta_2)^{p^k+1} = 1 = (\theta_1/\theta_2)^{p^m+1}\) which is equivalent to \((\theta_1/\theta_2)^{p+1} = 1\). So if (23) has solution, then it has exactly \( p + 1 \) solutions. If \( w_1 = w_1^{-1} \), then (24) is the same as (23) and apparently it gives no more solutions. In this case \( w_1 = \pm 1 \) and \( b = \pm 1 \). But when \( b = -1 \), \( \theta^{p^k+1} = w_1 = -1 \). By \( \theta^{p^m+1} = 1 \) and \( \gcd(p^m+1, 2(p^k+1)) = p + 1 \), we have \( \theta^{p+1} = 1 \). And then \( \theta^{p^k+1} = 1 \), which is a contradiction. So in the following we only consider \( b = 1 \). In this case, \( w_1 = 1 \) and we have \( p + 1 \) solutions of \( \theta \).

Moreover, we have \( p + 1 \) solutions of (19). If \( w_1 \neq w^{-1} \), then (24) has the same number of solutions as (23). Moreover, their solutions are distinct since \( w_1 \neq \pm 1 \).

Therefore, (23) and (24) both have \( p + 1 \) solutions or no solutions in \( \mathbb{F}_{p^m} \).

- If \( \theta^{p^m+1} \neq 1 \), then \( \theta^{p^m+1} = 1 \). In this case, \( \theta \in \mathbb{F}_{p^m}^* \). So \( x_2 = \frac{(\theta - \theta^{-1})}{2} \notin \mathbb{F}_{p^m}^* \) since \( t \notin \mathbb{F}_{p^m}^* \) except for the case \( \theta = \theta^{-1} = 1 \). But this will not occur since \( \theta^{p^m+1} \neq 1 \).

Summarizing up, we conclude \( N_1 = p + 1 \) and \( N_0 = 0 \) or \( 2(p+1) \) for \( b \neq 1 \). Define
\[ T = \#\{b \in \mathbb{F}_{p^m} : N_b = 2(p+1)\}. \]

Note that the first equation of (19) has \( p^m+1 \) solutions by Lemma 6.24 in [12]. When \( (x_1, x_2) \) runs through all these solutions, the second equation of (19) will give a \( 2(p+1) \)-to-1 correspondence \( (x_1, x_2) \mapsto b = x_1 d_1 + x_2 d_1 \) if \( N_b = 2(p+1) \). Therefore \( (p+1) + 2(p+1)T = p^m + 1 \), which implies
\[ T = \frac{p^m - p}{2(p+1)}. \]

We can prove that \( c \) is uniquely determined by \( b \) by the same method as in Lemma 5.4 in [20]. Similarly, we also have \( c = 1 \) if and only if \( b = 1 \). The proof is finished. \( \blacksquare \)

**Lemma 3.16** Let \( N_{2(b,c)} \) denote the number of solutions \((x_1, x_2) \in \mathbb{F}_{p^m}^2 \) of (18), where \((b, c) \in \mathbb{F}_{p^m}^2 \). Then we have the following conclusions.

1. \( N_{2(1,1)} = p + 1 \).
2. When \((b, c) \) runs through \( \mathbb{F}_{p^m}^2 \setminus \{(1,1)\} \),
\[ N_{2(b,c)} = \begin{cases} 2(p+1), & \text{for } \frac{p^m - p}{2(p+1)} \text{ times,} \\ 0, & \text{for the rest.} \end{cases} \]

**Proof.** The proof is similar to the proof of the lemma above, so we omit the details. \( \blacksquare \)

**Proof of Lemma 3.9** For any \((\overline{a}, \overline{b}, \overline{c}) \in \mathbb{F}_{p^m}^3 \), let \( N_{1(\overline{a}, \overline{b}, \overline{c})} \) and \( N_{3(\overline{a}, \overline{b}, \overline{c})} \) denote the number of solutions of the following two system of equations
\[ \begin{cases} x_1^2 + x_2^2 = \overline{a} \\ x_1 d_1 + x_2 d_1 = \overline{b} \\ x_1^2 d_2 + x_2 d_2 = \overline{c} \end{cases} \] (25)
\[
\begin{align*}
    x_3^2 - x_4^2 &= -\overline{\tau} \\
    x_3^{d_1} - x_4^{d_1} &= -\overline{b} \\
    x_3^{d_2} - x_4^{d_2} &= -\overline{c}.
\end{align*}
\]

(26)

It is then obvious that

\[
\overline{N}_4 = \sum_{(\overline{a}, \overline{b}, \overline{c}) \in \mathbb{F}_{p^m}^2} N_1(\overline{a}, \overline{b}, \overline{c}) N_3(\overline{a}, \overline{b}, \overline{c}).
\]

Case 1, when \(\overline{\tau} = 0\). In this case, (26) have solutions if and only if \(\overline{b} = \overline{c} = 0\) 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 \(\overline{\tau} \neq 0\). In this case, if \(\overline{b} = 0\) or \(\overline{c} = 0\), (26) has no solution. So in the following, we consider the problem only when \(\overline{b} \neq 0\) and \(\overline{c} \neq 0\).

- when \(\overline{\tau}\) is a nonzero square, \(\overline{b} \neq 0\) and \(\overline{c} \neq 0\). In this case, for any given \(\overline{\tau} \neq 0\), equation system (25) has the same number of solutions as

\[
\begin{align*}
    x_1^2 + x_2^2 &= 1 \\
    x_1^{d_1} + x_2^{d_1} &= b \\
    x_1^{d_2} + x_2^{d_2} &= c
\end{align*}
\]

(27)

and equation system (26) has the same number of solutions as

\[
\begin{align*}
    x_3^2 - x_4^2 &= -1 \\
    x_3^{d_1} - x_4^{d_1} &= -b \\
    x_3^{d_2} - x_4^{d_2} &= -c,
\end{align*}
\]

(28)

where \(b = \frac{b}{\overline{\tau}^{d_1}}\). Clearly, \((b, c)\) runs through \(\mathbb{F}_{p^m}^2\) as \((\overline{b}, \overline{c})\) does. For any fixed \((b, c) \in \mathbb{F}_{p^m}^2\) such that (27) and (28) have solutions simultaneously, we need to prove that the \(c_1\) determined by \(b\) in (27) and the \(c_2\) determined by \(b\) in (28) are the same number. For any solution \((x_1, x_2)\) of (27) and \((x_3, x_4)\) of (28), by setting \(\theta = x_1 - tx_2\) and \(\varphi = x_3 - x_4\), where \(t \in \mathbb{F}_{p^m}\) such that \(t^2 = -1\), we have

\[
\begin{align*}
    \theta^{p^k+1} + \theta^{-1-p^k} &= 2b \\
    \theta^{p^k-1} + \theta^{1-p^k} &= 2c_1
\end{align*}
\]

and

\[
\begin{align*}
    \varphi^{p^k-1} + \varphi^{1-p^k} &= 2b \\
    \varphi^{p^k+1} + \varphi^{-1-p^k} &= 2c_2.
\end{align*}
\]

From the first equations of the two equation systems above, we can obtain that \(\theta^{p^k+1} = b + \sqrt{b^2 - 1}\) and \(\varphi^{p^k-1} = b + \sqrt{b^2 - 1}\). So if \(c_1 = c_2\), we have

\[(b + \sqrt{b^2 - 1})^{p^k-1} + (b - \sqrt{b^2 - 1})^{p^k-1} = (b + \sqrt{b^2 - 1})^{p^k+1} + (b - \sqrt{b^2 - 1})^{p^k+1}.
\]

Let \(u = b + \sqrt{b^2 - 1}\), we obtain \(u^{p^k-1} + u^{1-p^k} = u^{p^k+1} + u^{-p^k-1}\). Then we have \(u = \pm 1\) which implies \(b = \mp 1\). When \(b = -1\), neither (27) nor (28) have solutions.
So we have $b = 1$. And in this case, (27) has $p + 1$ solutions and (28) has $p - 1$ solutions by Lemma 3.15 and 3.17. Therefore, in this case we have

$$\sum_{(\overline{\alpha},\overline{b},\overline{c})\in \mathbb{F}_{p^m}^*} N_1(\overline{\alpha},\overline{b},\overline{c})N_2(\overline{\alpha},\overline{b},\overline{c})$$

$$= (2p^m - 1) + (p^m - 1)(p + 1)(p - 1)$$

$$= p^{m+2} + p^m - p^2.$$

- when $\overline{\alpha}$ is a non-square, $\overline{b} \neq 0$ and $\overline{c} \neq 0$. In this case, for any given $\overline{\alpha} \neq 0$, equation system (25) 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 (26) 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 $\overline{\alpha}$ is a nonzero square. So when $\overline{\alpha}$ is a non-square, we also have

$$\sum_{(\overline{\alpha},\overline{b},\overline{c})\in \mathbb{F}_{p^m}^*} N_1(\overline{\alpha},\overline{b},\overline{c})N_3(\overline{\alpha},\overline{b},\overline{c})$$

$$= p^{m+2} + p^m - p^2.$$

Summarizing all the cases above, we have $N_4 = (p + 1)(p^m - 1)(2p^m - p + 1) + 1$. The following lemma gives the number of solutions of of (28) in the case of $b = 1$.

**Lemma 3.17** Let $N_{3(b,c)}$ denote the number of solutions $(x_3, x_4) \in \mathbb{F}_{p^m}^2$ of (28), where $(b, c) \in \mathbb{F}_{p^m}^2$. Then $N_{3(1,1)} = p - 1$.

**Proof.** We first compute the number $N_b$ of solutions $(x_3, x_4) \in \mathbb{F}_{p^m}^2$ of the following system of equations

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

(29)

From the first equation of (29), by setting $\varphi = x_3 - x_4 \in \mathbb{F}_{p^m}^*$, we can have

$$x_3 = \frac{\varphi - \varphi^{-1}}{2}, x_4 = \frac{-(\varphi + \varphi^{-1})}{2}.$$  

(30)

Substituting (30) into the second equation of (29), we obtain

$$\varphi^{p^k-1} + \varphi^{1-p^k} = 2.$$
By the same method as in the proof of Lemma 3.15 we have $N_{3(1,1)} = p - 1$. Similarly, we also have $c = 1$ if and only if $b = 1$. Hence the number of solutions of (28) in the case of $b - 1$ is the same as that of (29) in the case of $b = 1$ and $c = 1$. The proof is finished.

Proof of Lemma 3.10. With the notations as above,

$$
\tilde{N}_4 = \sum_{(a,b,c) \in F_{p^m}^3} N_{1(a,b,c)}^2 = (p + 1)(p^m - 1)(2p^m - p + 1) + 1.
$$

Acknowledgement: We are grateful to our supervisor, Professor Chunlei Liu, for his unending encouragement and useful advice.

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, The weight distribution of some irreducible cyclic codes, IEEE Trans. Inf. Theory, 55, no. 3 (2009), 955-960.
[6] C. Ding, J. Yang, Hamming weights in irreducible cyclic codes, Discrete Mathematics, 313, no. 4 (2013), 434-446.
[7] 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.
[8] K. Feng, J. Luo, Value distributions of exponential sums from perfect nonlinear functions and their applications, IEEE Trans. Inf. Theory, 53, no. 7 (2007), 3035-3041.
[9] K. Feng, J. Luo, Weight distribution of some reducible cyclic codes, Finite Fields Appl., 14, no. 2 (2008), 390-409.
[10] T. Feng, On cyclic codes of length $2^{2^r} - 1$ with two zeros whose dual codes have three weights, Des. Codes Cryptogr., 62 (2012), 253-258.
[11] T. Feng KaHin Leung, Qing Xiang, Binary cyclic codes with two primitive nonzeros, Sci. China Math., 56, no. 7 (2012), 1403-1412.
[12] R. Lidl, H. Niederreiter, Finite fields, Addison-Wesley Publishing Inc., (1983).
[13] Y. Liu, H. Yan, C. Liu, A Class of Six-weight Cyclic Codes and Their Weight Distribution, arXiv: 1311.3391, (2013).
[14] J. Luo, K. Feng, On the weight distribution of two classes of cyclic codes, *IEEE Trans. Inf. Theory*, **54**, no. **12** (2008), 5332-5344.

[15] 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.

[16] 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.

[17] B. Wang, C. Tang, Y. Qi, Y. Yang, M. Xu, The weight distributions of 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] Z. Zhou, C. Ding, A class of three-weight cyclic codes, *Finite Fields Appl.*, **25** (2014), 79-93.

[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.