A Class of Six-weight Cyclic Codes and Their Weight Distribution^{*}

Yan Liu[†], Haode Yan[‡], Chunlei Liu[§]

Abstract

In this paper, a family of six-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 $m \geq 3$ be an odd integer and k be a positive integer such that gcd(m,k) = 1. Let p be an odd prime and π 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 of length n. The weight enumerator of C is defined by $1 + A_1Z + A_2Z^2 + \cdots + A_nZ^n$. 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 $c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \in \mathbb{F}_p[x]/(x^n - 1)$, 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.

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

^{*}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.

[§]Dept. of Math., Shanghai Jiaotong Univ., Shanghai, 200240, clliu@sjtu.edu.cn.

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 [7-11, 13-18]. 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.

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

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

2 QUADRATIC FORMS OVER FINITE FIELDS

In this section, we give a brief introduction to the theory of quadratic forms over finite fields which will be needed to calculate 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 $\{\varepsilon_1, \varepsilon_1, \ldots, \varepsilon_m\}$ is a basis for \mathbb{F}_p^m over \mathbb{F}_p . The a function Q(x) from \mathbb{F}_p^m to \mathbb{F}_p is a quadratic form over \mathbb{F}_p if it can be represented as

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

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 $V = \{x \in \mathbb{F}_p^m | Q(x+z) - Q(x) - Q(z) = 0 \text{ for all } x \in \mathbb{F}_p^m \}.$

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 $X = (x_1, x_2, \ldots, x_m) \in \mathbb{F}_p^m$ 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 = ZH with $Z = (z_1, z_2, \ldots, z_m) \in \mathbb{F}_p^m$, 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 $\Delta = d_1 d_2 \cdots d_r$ (we assume $\Delta = 0$ when r = 0). Then the Legendre symbol $(\frac{\Delta}{p})$ is an invariant of A under the action of $H \in GL_m(\mathbb{F}_p)$. The following results is useful in the next section.

Lemma 2.2 ([12]) With the notations as above, we have

$$\sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{F(x)} = \begin{cases} (\frac{\Delta}{p})p^{m-\frac{r}{2}}, & p \equiv 1 \pmod{4}, \\ (\frac{\Delta}{p})(\sqrt{-1})^r p^{m-\frac{r}{2}}, & p \equiv 3 \pmod{4}, \end{cases}$$

for any quadratic form F(x) in m variables of rank r over \mathbb{F}_p , where ζ_p is a primitive p-th root of unity.

Lemma 2.3 Let F(x) be a quadratic form in m variables of rank r over \mathbb{F}_p , then

$$\sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_p^m} \zeta_p^{yF(x)} = \begin{cases} \pm (p-1)p^{m-\frac{r}{2}}, & r \text{ even,} \\ 0, & otherwise \end{cases}$$

The proof is similar to the proof of Lemma 2.2 in [17], so we omit the details.

For any fixed $(u, v) \in \mathbb{F}_{p^m}^2$, $Q_{u,v}(x) = Tr(ux^2 + vx^{p^k+1})$, where Tr is the trace map from \mathbb{F}_{p^m} to \mathbb{F}_p . Moreover, we have the following result.

Lemma 2.4 ([9]) For any $(u, v) \in \mathbb{F}_{p^m}^2 \setminus \{(0, 0)\}, Q_{u,v}(x)$ is a quadratic form over \mathbb{F}_p with rank m, m-1, m-2.

$3 \quad \text{The class of six-weight cyclic codes and their weight} \\ \text{distribution}$

We follow the notations fixed in Section 1. 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 π^{-1} , $(-\pi)^{-1}$ and $\pi^{-(p^k+1)/2}$ over \mathbb{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. 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 $\mathcal{C}_{(p,m,k)}$ be the cyclic code with parity-check polynomial h(x). Then $\mathcal{C}_{(p,m,k)}$ has length $p^m - 1$ and dimension 3m. Moreover, it can be expressed as

$$\mathcal{C}_{(p,m,k)} = \{ \mathbf{c}_{(a,b,c)} : a, b, c \in \mathbb{F}_{p^m} \},\$$

where

$$c_{(a,b,c)} = \left(Tr(a\pi^t + b(-\pi)^t + c\pi^{(p^k+1)t/2}) \right)_{t=0}^{p^m-2}.$$

Let $h'(x) = h_1(x)h_2(x)$ and $\mathcal{C}'_{(p,m,k)}$ be the cyclic code with parity-check polynomial h'(x). Then $\mathcal{C}'_{(p,m,k)}$ is a subcode of $\mathcal{C}_{(p,m,k)}$ with dimension 2m. Zhengchun Zhou and Cunsheng Ding [17] proved that $\mathcal{C}'_{(p,m,k)}$ have three nonzero weights and determined its weight distribution. In this paper, we will show that $\mathcal{C}_{(p,m,k)}$ have six nonzero weights and determine the weight distribution of this class of cyclic codes $\mathcal{C}_{(p,m,k)}$.

From now on, we always assume that λ is a fixed nonsquare in \mathbb{F}_p . Since *m* is odd, it is also a nonsquare in \mathbb{F}_{p^m} . Then if *SQ* denotes the set of all nonzero square elements of \mathbb{F}_{p^m} , λx runs through all nonsquares of \mathbb{F}_{p^m} as *x* runs through *SQ*. In addition, we have the following result. **Lemma 3.1 ([17])** $\lambda^{(1+p^k)/2} = \lambda$ if k is even, and $\lambda^{(1+p^k)/2} = -\lambda$ otherwise.

In terms of exponential sums, the weight of the codeword $\mathbf{c}_{(a,b,c)} = (c_0, c_1, \dots, c_{p^m-2})$ in $\mathcal{C}_{(p,m,k)}$ is given by

$$\begin{split} W(\mathbf{c}_{(a,b,c)}) &= \#\{0 \leq t \leq p^m - 2 : c_t \neq 0\} \\ &= p^m - 1 - \frac{1}{p} \sum_{t=0}^{p^m-2} \sum_{y \in \mathbb{F}_p} \zeta_p^{yc(t)} \\ &= p^m - 1 - \frac{1}{p} \sum_{t=0}^{p^m-2} \sum_{y \in \mathbb{F}_p} \zeta_p^{yTr(a\pi^t + b(-\pi)^t + c\pi^{(p^k+1)t/2})} \\ &= p^m - 1 - \frac{1}{p} \sum_{y \in \mathbb{F}_p} \sum_{t=0}^{(p^m-3)/2} \left(\zeta_p^{yTr((a+b)\pi^{2t+1} + c\pi^{(p^k+1)t})} + \zeta_p^{yTr((a-b)\pi^{2t} + c\pi^{\frac{p^k+1}{2}(2t+1)})} \right) \\ &= p^m - 1 - \frac{1}{p} \sum_{y \in \mathbb{F}_p} \sum_{x \in SQ} \left(\zeta_p^{yTr((a+b)x + cx^{(p^k+1)/2})} + \zeta_p^{yTr((a-b)\pi x + c(\pi x)^{\frac{p^k+1}{2}})} \right) \\ &= p^m - 1 - \frac{1}{p} \sum_{y \in \mathbb{F}_p} \sum_{x \in SQ} \left(\zeta_p^{yTr((a+b)x + cx^{(p^k+1)/2})} + \zeta_p^{yTr((a-b)\lambda x + c(\lambda x)^{\frac{p^k+1}{2}})} \right) \\ &= p^m - 1 - \frac{1}{2p} \sum_{y \in \mathbb{F}_p} \sum_{x \in SQ} \left(\zeta_p^{yTr((a+b)x^2 + cx^{p^k+1})} + \zeta_p^{yTr((a-b)\lambda x^2 + c\lambda^{\frac{p^k+1}{2}}x^{p^k+1})} \right) \\ &= p^m - 1 - \frac{1}{2p} \sum_{y \in \mathbb{F}_p} \sum_{x \in \mathbb{F}_p^*} \left(\zeta_p^{yTr((a+b)x^2 + cx^{p^k+1})} + \zeta_p^{yTr((a-b)\lambda x^2 + c\lambda^{\frac{p^k+1}{2}}x^{p^k+1})} \right) . \end{split}$$

It then follows from Lemma 3.1 that $W(\mathbf{c}_{(a,b,c)}) = p^m - p^{m-1} - \frac{1}{2p}S(a,b,c)$ when k is even, where

$$S(a,b,c) = \sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_p^m} \left(\zeta_p^{yT_r((a+b)x^2 + cx^{p^{k+1}})} + \zeta_p^{yT_r((a-b)\lambda x^2 + c\lambda x^{p^{k+1}})} \right), \tag{1}$$

and $W(\mathbf{c}_{(a,b,c)}) = p^m - p^{m-1} - \frac{1}{2p}T(a,b,c)$ when k is odd, where

$$T(a,b,c) = \sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_p^m} \left(\zeta_p^{yTr((a+b)x^2 + cx^{p^{k+1}})} + \zeta_p^{yTr((a-b)\lambda x^2 - c\lambda x^{p^{k+1}})} \right).$$
(2)

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) and T(a, b, c). Before doing this, we first give a notation. For any $(u, v) \in \mathbb{F}_{p^m}^2$,

$$D(u,v) = \sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{yQ_{u,v}(x)} = \sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{yTr(ux^2 + vx^{p^{k+1}})}.$$
 (3)

The following lemmas are very important to establish the value distribution of S(a, b, c)and T(a, b, c). **Lemma 3.2** Let D(u, v) be defined by (3).

$$D(u,0) = \begin{cases} (p-1)p^m & u = 0\\ 0 & u \neq 0. \end{cases}$$

Proof. By Eq. (3),

$$D(u,0) = \sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_p^m} \zeta_p^{yQ_{u,0}(x)} = \sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_p^m} \zeta_p^{yTr(ux^2)}.$$

Then $D(0,0) = (p-1)p^m$. If $u \neq 0$, $Q_{u,0}(x) = Tr(ux^2)$ is a quadratic form of rank m over \mathbb{F}_p . So D(u,0) = 0 by Lemma 2.3.

Lemma 3.3 Let D(u, v) be defined by (3). Then for any fixed $v \in \mathbb{F}_{p^m}^*$, as u runs through \mathbb{F}_{p^m} , the value distribution of D(u, v) is given by Table 1.

Table 1: Value distribution of D(u, v) for fixed $v \in \mathbb{F}_{p^m}^*$

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

Proof. As in Eq. (3),

$$D(u,v) = \sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_p^m} \zeta_p^{yQ_{u,v}(x)}.$$

Then for any $v \in \mathbb{F}_{p^m}^*$, by Lemma 2.3, the values of D(u, v) takes on only the values from the set $\{0, \pm (p-1)p^{\frac{m+1}{2}}\}$. To determine the distribution of D(u, v) for any fixed $v \in \mathbb{F}_{p^m}^*$, we define

$$n_{\epsilon} = \#\{u \in \mathbb{F}_{p^m} : D(u, v) = \epsilon(p-1)p^{\frac{m+1}{2}}\},\$$

where $\epsilon = 0, \pm 1$. Then we have

$$\sum_{u \in \mathbb{F}_{p^m}} D(u, v) = (n_1 - n_{-1})(p - 1)p^{\frac{m+1}{2}}$$
(4)

and

$$\sum_{u \in \mathbb{F}_{p^m}} D^2(u, v) = (n_1 + n_{-1})(p - 1)^2 p^{m+1}.$$
(5)

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

$$\sum_{u \in \mathbb{F}_{p^m}} D(u, v) = \sum_{u \in \mathbb{F}_{p^m}} \sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{yTr(ux^2 + vx^{p^{k+1}})}$$
$$= \sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{yTr(vx^{p^{k+1}})} \sum_{u \in \mathbb{F}_{p^m}} \zeta_p^{yTr(ux^2)}$$
$$= (p-1)p^m$$
(6)

and

$$\begin{split} &\sum_{u \in \mathbb{F}_{p^m}} D^2(u, v) \\ &= \sum_{u \in \mathbb{F}_{p^m}} \Big(\sum_{y_1 \in \mathbb{F}_p^*} \sum_{x_1 \in \mathbb{F}_{p^m}} \zeta_p^{y_1 Tr(ux_1^2 + vx_1^{p^{k+1}})} \Big) \Big(\sum_{y_2 \in \mathbb{F}_p^*} \sum_{x_2 \in \mathbb{F}_{p^m}} \zeta_p^{y_2 Tr(ux_2^2 + vx_2^{p^{k+1}})} \Big) \\ &= \sum_{u \in \mathbb{F}_{p^m}} \sum_{(y_1, y_2) \in \mathbb{F}_{p^2}^*} \sum_{(x_1, x_2) \in \mathbb{F}_{p^m}^*} \zeta_p^{Tr(u(y_1 x_1^2 + y_2 x_2^2) + v(y_1 x_1^{p^{k+1}} + y_2 x_2^{p^{k+1}}))} \\ &= (p-1)p^m + \sum_{u \in \mathbb{F}_{p^m}} \sum_{(y_1, y_2) \in \mathbb{F}_{p^2}^*} \sum_{(x_1, x_2) \in \mathbb{F}_{p^m}^*} \zeta_p^{Tr(u(y_1 x_1^2 + y_2 x_2^2) + v(y_1 x_1^{p^{k+1}} + y_2 x_2^{p^{k+1}}))} \\ &= (p-1)p^m + \sum_{(y_1, y_2) \in \mathbb{F}_{p^2}^*} \sum_{(x_1, x_2) \in \mathbb{F}_{p^m}^*} \zeta_p^{Tr(v(y_1 x_1^{p^{k+1}} - y_2 x_2^{p^{k+1}}))} \sum_{u \in \mathbb{F}_{p^m}} \zeta_p^{Tr(u(y_1 x_1^2 - y_2 x_2^2))} \\ &= (p-1)p^m + \sum_{(y_1, y_2) \in \mathbb{F}_{p^2}^*} \sum_{(x_1, x_2) \in \mathbb{F}_{p^m}^*} \zeta_p^{Tr(v(y_1 x_1^{p^{k+1}} - y_2 x_2^{p^{k+1}}))} \sum_{u \in \mathbb{F}_{p^m}} \zeta_p^{Tr(u(y_1 x_1^2 - y_2 x_2^2))} \\ &= (p-1)p^m + \sum_{t^2 \in Sq} \sum_{y_2 \in \mathbb{F}_p^*} \sum_{x_1 \in \mathbb{F}_{p^m}^*} \zeta_p^{Tr(v(y_1 x_1^{p^{k+1}} - y_2 x_2^{p^{k+1}}))} \\ &= (p-1)p^m + p^m \sum_{t^2 \in Sq} \sum_{y_2 \in \mathbb{F}_p^*} \sum_{x_1 \in \mathbb{F}_{p^m}^*} \zeta_p^{Tr(v(y_1 x_1^{p^{k+1}} - y_2 x_2^{p^{k+1}}))} \\ &= (p-1)p^m + 2p^m \sum_{t^2 \in Sq} \sum_{y_2 \in \mathbb{F}_p^*} \sum_{x_1 \in \mathbb{F}_p^*} \zeta_p^{Tr(v(y_2 t^2 x_1^{p^{k+1} - y_2 t^{p^{k+1}} + y_2 x_2^{p^{k+1}}))} \\ &= (p-1)p^m + 2p^m \sum_{t^2 \in Sq} \sum_{y_2 \in \mathbb{F}_p^*} \sum_{x_1 \in \mathbb{F}_p^*} \zeta_p^{Tr(v(y_2 t^2 x_1^{p^{k+1} - y_2 t^{p^{k+1}} + x_2^{p^{k+1}}))} \\ &= (p-1)p^m + 2p^m \frac{p-1}{2} (p-1)(p^m-1) \\ &= (p-1)p^{2m}, \end{split}$$

where in the sixth identity we use Sq to denote the set of square elements in \mathbb{F}_p^* and in the eighth identity we used the fact that $t^{p^k+1} = t$ since $t \in \mathbb{F}_p$. Combining Eqs. (4)-(7), we get

$$n_1 = \frac{1}{2}(p^{m-1} + p^{\frac{m-1}{2}}),$$

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

Then we have $n_0 = p^m - n_1 - n_{-1} = p^m - p^{m-1}$.

The value distribution of S(a, b, c) will be determined in the following.

Lemma 3.4 Let k be even and S(a,b,c) be defined by (1), then for any $(a,b,c) \in \mathbb{F}_{p^m}^3$, S(a,b,c) takes values from the set $\{0, (p-1)p^m, 2(p-1)p^m, \pm (p-1)p^{\frac{m+1}{2}}, \pm 2(p-1)p^{\frac{m+1}{2}}\}$.

Proof. Following the notation above, we have S(a, b, c) = D(a + b, c) + D(a - b, c). Case I. In the case of a = b = c = 0, $D(a + b, c) = D(a - b, c) = (p - 1)p^m$, so $S(a, b, c) = 2(p - 1)p^m$. Case II. In the case of $c = 0, a = -b \neq 0$ or $c = 0, a = b \neq 0$, exactly one of Q(a + b, c)and Q(a - b, c) has rank m, the other has rank 0. Then by Lemma 2.3, we have $S(a, b, c) = (p - 1)p^m$.

Case III. In the case of $c \neq 0, a+b \neq 0, a-b \neq 0$, again by Lemma 2.3, $S(a, b, c) \neq 0$ only if Q(a+b, c) or Q(a-b, c) has even rank. Thus $S(a, b, c) = \pm (p-1)p^{\frac{m+1}{2}}$ if Q(a+b, c) has rank m or m-2 and Q(a-b, c) has rank m-1 or Q(a-b, c) has rank m or m-2 and Q(a+b, c) has rank m-1. $S(a, b, c) = \pm 2(p-1)p^{\frac{m+1}{2}}$ if Q(a+b, c) has rank m-1 and Q(a-b, c) has rank m-1. And otherwise S(a, b, c) = 0. This completes the proof.

Theorem 3.5 Let k be even and S(a,b,c) be defined by (1). Then as (a,b,c) runs through $\mathbb{F}^3_{p^m}$, the value distribution of S(a,b,c) is given by Table 2.

	Table 2: Value Distribution of $S(a, b, c)$
Value	Frequency
$2(p-1)p^m$	1
$(p-1)p^m$	$2(p^m-1)$
$(p-1)p^{\frac{m+1}{2}}$	$(p^m - 1)(p^m - p^{m-1})(p^{m-1} + p^{\frac{m-1}{2}})$
$-(p-1)p^{\frac{m+1}{2}}$	$(p^m - 1)p^m - p^{m-1})(p^{m-1} - p^{\frac{m-1}{2}})$
$2(p-1)p^{\frac{m+1}{2}}$	$\frac{1}{4}(p^m-1)(p^{m-1}+p^{\frac{m-1}{2}})^2$
$-2(p-1)p^{\frac{m+1}{2}}$	$\frac{1}{4}(p^m-1)(p^{m-1}-p^{\frac{m-1}{2}})^2$
0	$(p^m - 1)(p^{2m} + \frac{3}{2}p^{2(m-1)} - 2p^{2m-1} + p^m - \frac{1}{2}p^{m-1} - 1)$

Proof. The distribution of $S(a, b, c) = (p - 1)p^m$ or $2(p - 1)p^m$ can be easily obtained by Lemma 3.4. To determine the distribution of the other values, we define

$$N_{\epsilon} = \#\{(a, b, c) \in \mathbb{F}_{p^m}^3 : S(a, b, c) = \epsilon(p-1)p^{\frac{m+1}{2}}\}$$

where $\epsilon = 0, \pm 1, \pm 2$. Then we have

$$\begin{split} N_1 &= \#\{(a,b,c) \in \mathbb{F}_{p^m}^3 : S(a,b,c) = D(a+b,c) + D(a-b,c) = (p-1)p^{\frac{m+1}{2}}\}\\ &= \#\{(u_1,u_2,c) \in \mathbb{F}_{p^m}^3 : D(u_1,c) + D(u_2,c) = (p-1)p^{\frac{m+1}{2}}\}\\ &= \#\{(u_1,u_2 \in \mathbb{F}_{p^m}^2, c \in \mathbb{F}_{p^m}^* : D(u_1,c) + D(u_2,c) = (p-1)p^{\frac{m+1}{2}}\} + \\ &= \#\{(u_1,u_2 \in \mathbb{F}_{p^m}^2, c \in \mathbb{F}_{p^m}^* : D(u_1,c) + D(u_2,c) = (p-1)p^{\frac{m+1}{2}}\}\\ &= \#\{(u_1,u_2 \in \mathbb{F}_{p^m}^2, c \in \mathbb{F}_{p^m}^* : D(u_1,c) + D(u_2,c) = (p-1)p^{\frac{m+1}{2}}\}\\ &= \#\{(u_1,u_2 \in \mathbb{F}_{p^m}^2, c \in \mathbb{F}_{p^m}^* : D(u_1,c) = 0, D(u_2,c) = (p-1)p^{\frac{m+1}{2}}\} + \\ &= \#\{(u_1,u_2 \in \mathbb{F}_{p^m}^2, c \in \mathbb{F}_{p^m}^* : D(u_1,c) = (p-1)p^{\frac{m+1}{2}}\} + \\ &= \#\{(u_1,u_2 \in \mathbb{F}_{p^m}^2, c \in \mathbb{F}_{p^m}^* : D(u_1,c) = (p-1)p^{\frac{m+1}{2}}, D(u_2,c) = 0\}\\ &= 2n_0n_1(p^m-1)\\ &= (p^m-1)(p^m-p^{m-1})(p^{m-1}+p^{\frac{m-1}{2}}), \end{split}$$

where the second part of the third identity is 0 by Lemma 3.2 and the sixth identity is obtained by Lemma 3.3.

Similarly, we get

$$N_{-1} = 2n_0 n_{-1} (p^m - 1) = (p^m - 1)(p^m - p^{m-1})(p^{m-1} - p^{\frac{m-1}{2}}),$$
$$N_2 = n_1^2 (p^m - 1) = \frac{1}{4}(p^m - 1)(p^{m-1} + p^{\frac{m-1}{2}})^2,$$
$$N_{-2} = n_1^2 (p^m - 1) = \frac{1}{4}(p^m - 1)(p^{m-1} - p^{\frac{m-1}{2}})^2$$

and

$$N_0 = p^{3m} - 1 - 2(p^m - 1) - N_1 - N_{-1} - N_2 - N_{-2}$$

= $(p^m - 1)(p^{2m} + \frac{3}{2}p^{2(m-1)} - 2p^{2m-1} + p^m - \frac{1}{2}p^{m-1} - 1)$

Remark. Following the notations above, we have T(a, b, c) = D(a+b, c) + D(a-b, -c). It can be shown that the value distribution of T(a, b, c) in the case of k is odd is the same as the value distribution of S(a, b, c) in the case of k is even.

The following is the main result of this paper.

Theorem 3.6 $C_{(p,m,k)}$ is a cyclic code over \mathbb{F}_p with parameters $[p^m - 1, 3m, \frac{p-1}{2}p^{m-1}]$. Furthermore, the weight distribution of $C_{(p,m,k)}$ is given by Table 3.

	(p,m,κ)
Weight	Frequency
0	1
$\frac{p-1}{2}p^{m-1}$	$2(p^m - 1)$
$\frac{p-1}{2}(2p^{m-1}-p^{\frac{m-1}{2}})$	$(p^m - 1)(p^m - p^{m-1})(p^{m-1} + p^{\frac{m-1}{2}})$
$\frac{p-1}{2}(2p^{m-1}+p^{\frac{m-1}{2}})$	$(p^m - 1)p^m - p^{m-1})(p^{m-1} - p^{\frac{m-1}{2}})$
$(p-1)(p^{m-1}-p^{\frac{m-1}{2}})$	$\frac{1}{4}(p^m - 1)(p^{m-1} + p^{\frac{m-1}{2}})^2$
$(p-1)(p^{m-1}+p^{\frac{m-1}{2}})$	$\frac{1}{4}(p^m-1)(p^{m-1}-p^{\frac{m-1}{2}})^2$
$(p-1)p^{m-1}$	$(p^m - 1)(p^{2m} + \frac{3}{2}p^{2(m-1)} - 2p^{2m-1} + p^m - \frac{1}{2}p^{m-1} - 1)$

Table 3: Weight Distribution of $\mathcal{C}_{(n,m,k)}$

Proof. The length and dimension of $C_{(p,m,k)}$ follow directly from its definition. The minimal weight and weight distribution of $C_{(p,m,k)}$ follow from Eqs. (1) and (2), Theorem 3.5 and the Remark above.

Example 3.7 Let p = 3, m = 3 and k = 1. The the code $C_{(3,3,1)}$ is a [26,9,9] cyclic code over \mathbb{F}_3 with weight enumerator

$$1 + 52z^9 + 936z^{12} + 5616z^{15} + 10036z^{18} + 2808z^{21} + 234z^{24}$$

which confirms the weight distribution in Table 3.

Example 3.8 Let p = 3, m = 5 and k = 2. The the code $C_{(3,5,1)}$ is a [242, 15, 81] cyclic code over \mathbb{F}_3 with weight enumerator

 $1 + 484z^{81} + 490050z^{144} + 3828360z^{153} + 7193692z^{162} + 2822688z^{171} + 313632z^{180},$

which confirms the weight distribution in Table 3.

Example 3.9 Let p = 3, m = 7 and k = 2. The the code $C_{(3,7,2)}$ is a [2186, 21, 729] cyclic code over \mathbb{F}_3 with weight enumerator

$$\begin{split} 1 + & 4372z^{729} + 312344424z^{1404} + 2409514128z^{1431} + 5231766916z^{1458} + 2237405976z^{1485} \\ & + 269317386z^{1512}, \end{split}$$

which confirms the weight distribution in Table 3.

References

- 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 nonlinar 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 Crypogr.*, **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 fieds, Addison-Wdsley Publishing Inc., (1983).

- [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 and elliptic curves, *IEEE Trans. Inf. Theory*, 58, no. 12 (2012), 7253-7259.
- [17] Z. Zhou, C. Ding, A class of three-weight cyclic codes, *Finite Fields Appl.*, 25 (2014), 79-93.
- [18] Z. Zhou, C. Ding, J. Luo, A. Zhang, A family of five-weight cyclic codes and their weight enumerators, arXiv: 1302.0952v1, (2013).