A class of six-weight cyclic codes and their weight distribution

Yan Liu · Haode Yan · Chunlei Liu

Received: 15 November 2013 / Revised: 25 February 2014 / Accepted: 19 May 2014 / Published online: 4 June 2014 © Springer Science+Business Media New York 2014

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. Furthermore, the weight distributions of these cyclic codes are determined.

Keywords Cyclic code · Quadratic form · Weight distribution

Mathematics Subject Classification 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 $\pi$ be a primitive element of the finite field $\mathbb{F}_p^m$.

Recall that an $[n, l, d]$ linear code $C$ over $\mathbb{F}_p$ is a linear subspace of $\mathbb{F}_p^n$ with dimension $l$ and minimum Hamming distance $d$. Let $A_i$ denote the number of codewords in $C$ with Hamming weight $i$. The sequence $(A_0, A_1, A_2, \ldots, A_n)$ is called the weight distribution of the code $C$. And $C$ is called cyclic if for any $(c_0, c_1, \ldots, c_{n-1}) \in C$, then $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$. A linear code $C$ in $\mathbb{F}_p^n$ is cyclic if and only if $C$ is 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 called the parity-check polynomial of the code $C$. We also recall that a cyclic code is called irreducible if its parity-check polynomial is irreducible over $\mathbb{F}_p$ and reducible, otherwise.

Determining the weight distribution of a linear code is an important research object in coding theory. For cyclic codes, the error correcting capability may not be as good as with some other linear codes in general. However, because of their good algebraic structure, the weight distributions of some cyclic codes can be determined by algebraic techniques, exponential sums for example. Besides, cyclic codes have wide applications in storage and communication systems because they have efficient encoding and decoding algorithms. Moreover, cyclic codes are applied in association schemes [3] and secret schemes [4]. Therefore, determining the weight distributions of cyclic codes is not only a problem of theoretical interest, but also of practical importance. For information on the weight distributions of reducible cyclic codes, the reader is referred to [1,2,5,6]. Information on the weight distributions of irreducible cyclic codes, the reader is referred to [12].

The rest of this paper is organized as follows. Some necessary results on quadratic forms will be introduced in Sect. 2. A family of cyclic codes is presented and their weight distributions are determined in Sect. 3.

2 Preliminaries

We follow the notation in Sect. 1. The first machinery to determine the weight distributions of the cyclic codes is quadratic forms over $\mathbb{F}_p$. By identifying $\mathbb{F}_p^m$ with the $m$-dimensional $\mathbb{F}_p$-vector space $\mathbb{F}_p^m$, a function $Q$ from $\mathbb{F}_p^m$ to $\mathbb{F}_p$ can be regarded as an $m$-variable polynomial on $\mathbb{F}_p$. Then $Q$ is called a quadratic form over $\mathbb{F}_p$ if its corresponding polynomial is a polynomial of degree two over $\mathbb{F}_p$ and can be represented as

$$Q(x_1, x_2, \ldots, x_m) = \sum_{1 \leq i \leq j \leq m} a_{ij}x_ix_j,$$

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

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 $HAH'$ 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 $F(x) = ZHAH'Z' = \sum_{i=1}^r d_i \zeta_i^2$, where $r$ is the rank of $F(x)$ and $d_i \in \mathbb{F}_p^*$. Let $\Delta = d_1d_2 \cdots d_r$ (we assume $\Delta = 0$ when $r = 0$). We can recall that the Legendre symbol $(\frac{\zeta}{p})$ has the value 1 if $a$ is a quadratic residue mod $p$, $-1$ if $a$ is a quadratic nonresidue mod $p$, and zero if $p|a$. Then $(\frac{\Delta}{p})$ is an invariant of $A$ under the action of $H \in GL_m(\mathbb{F}_p)$. The following results are useful in the next section.

**Lemma 2.1** [12] With the notation as above, we have

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

for any quadratic form $F(x)$ in $m$ variables of rank $r$ over $\mathbb{F}_p$, where $\zeta_p$ is a primitive $p$-th root of unity.
Lemma 2.2 Let $F(x)$ be a quadratic form in $m$ variables of rank $r$ over $\mathbb{F}_p$, then

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

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

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

Lemma 2.3 [10] For any $(u, v) \in \mathbb{F}_p^2 \setminus \{(0, 0)\}$, $Q_{u,v}(x)$ is a quadratic form over $\mathbb{F}_p$ with rank at least $m - 2$.

3 The class of six-weight cyclic codes and their weight distribution

We follow the notation fixed in Sect. 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 $\pi^{-1}, (-\pi)^{-1}$ 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 $x^{p^{2m} - 1} - 1$.

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

$$C_{(p,m,k)} = \{ c(a,b,c) : a, b, c \in \mathbb{F}_p^m \},$$

where

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

Let $h'(x) = h_1(x)h_2(x)$ 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 $2m$. Zhou and Ding [17] proved that $C'_{(p,m,k)}$ has three nonzero weights and determined its weight distribution. In this paper, we will show that $C_{(p,m,k)}$ has six nonzero weights and determine the weight distributions of this class of cyclic codes.

From now on, we always assume that $\lambda$ is a fixed nonsquare element in $\mathbb{F}_p$. Since $m$ is odd, it is also a nonsquare element in $\mathbb{F}_p^m$. Then if $SQ$ denotes the set of all nonzero square elements of $\mathbb{F}_p^m$, $\lambda x$ runs through all nonsquare elements 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 $c(a,b,c) = (c_0, c_1, \ldots, c_{p^m-2})$ in $C_{(p,m,k)}$ is given by

$$W(c(a,b,c)) = \#\{ 0 \leq t \leq p^{m} - 2 : c_t \neq 0 \}$$

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

$$= p^m - 1 - \frac{1}{p} \sum_{t = 0}^{p^m - 2} \sum_{y \in \mathbb{F}_p} \zeta_p^{Tr(a \pi^t + b(-\pi)^t + c \pi^{(p^k+1)t/2})}$$
distribution of $S$

Lemma 3.2

Let $D$ and $S$ as in Eq. 3.

Proof

By Eq. 3, $D(v) = (1 - p)S(a, b, c)$ when $k$ is even, where

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

(1)

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

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

(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 calculating the value distribution of $S(a, b, c)$ and $T(a, b, c)$, for any $(u, v) \in \mathbb{F}_{p^m}$, we define

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

(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, then

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

Proof By Eq. 3,

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

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 2.2.

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.

Proof As in Eq. 3,

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

Then for any fixed $v \in \mathbb{F}_{p^m}^*$, by Lemma 2.2, $D(u, v)$ takes on only the values from the set $\{0, \pm (p-1)p^{m+1} \}$. To determine the distribution of $D(u, v)$ for any fixed $v \in \mathbb{F}_{p^m}^*$, we define

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

\[\text{Springer}\]
where $\epsilon = 0, \pm 1$. Then we have

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

and

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

On the other hand, it follows from 3 that

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

and

$$
\sum_{u \in \mathbb{F}_{p^m}} D^2(u, v) = \sum_{u \in \mathbb{F}_{p^m}} \sum_{y \in \mathbb{F}_{p^m}} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{y \text{Tr}(vx^2 + vx^k + 1)}
$$

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

$$
= (p - 1)^2 p^m + \sum_{u \in \mathbb{F}_{p^m}} \sum_{y \in \mathbb{F}_{p^m}} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{y \text{Tr}(ux^2 + vx^k + 1)}
$$

$$
= (p - 1)^2 p^m + \sum_{u \in \mathbb{F}_{p^m}} \sum_{y \in \mathbb{F}_{p^m}} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{y \text{Tr}(vx^2 + vx^k + 1)}
$$

and

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

| Value      | Frequency |
|------------|-----------|
| 0          | $p^m - p^{m-1}$ |
| $(p - 1)p^{m+1}$ | $\frac{1}{2}(p^{m-1} + p^{-1})$ |
| $-(p - 1)p^{m+1}$ | $\frac{1}{2}(p^{m-1} - p^{-1})$ |
\[ = (p - 1)^2 p^m + p^m \sum_{t^2 \in S_q} \sum_{y_2 \in \mathbb{F}_p^*} \sum_{x_1 \in \mathbb{F}_p^m} \zeta_p Tr(v(y_1 x_1^{p^{k+1}} - y_2 x_2^{p^{k+1}})) \]

\[ = (p - 1)^2 p^m + 2p^m \sum_{t^2 \in S_q} \sum_{y_2 \in \mathbb{F}_p^*} \sum_{x_1 \in \mathbb{F}_p^m} \zeta_p Tr(v(y_2 t^2 x_1^{p^{k+1}} - y_2 t^{p^{k+1}} x_1^{p^{k+1}})) \]

\[ = (p - 1)^2 p^m + 2p^m \frac{p - 1}{2} (p - 1)(p^m - 1) \]

\[ = (p - 1)^2 p^{2m}, \quad (7) \]

where in the sixth identity we use \( S_q \) to denote the set of square elements in \( \mathbb{F}_p^* \) and in the eighth identity we used the fact that \( t^{p^{k+1}} = t^2 \) since \( t \in \mathbb{F}_p \). Combining Eqs. 4–7, we get

\[
\begin{align*}
n_1 &= \frac{1}{2} \left( p^{m-1} + p^{m-1} \right), \\
n_{-1} &= \frac{1}{2} \left( p^{m-1} - p^{m-1} \right).
\end{align*}
\]

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 \((a, b, c) \in \mathbb{F}_p^3 \), \( S(a, b, c) \) takes values from the set \{0, \( (p - 1)p^m, 2(p - 1)p^m, \pm(p - 1)p^{m+1}/2, \pm 2(p - 1)p^{m+1}/2 \}\).

**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 \( S(a, b, c) = (p - 1)p^m \).

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 2.2, 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 2.2, \( S(a, b, c) \neq 0 \) only if \( Q(a + b, c) \) or \( Q(a - b, c) \) has even rank. Thus \( S(a, b, c) = \pm(p - 1)p^{m+1}/2 \) 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 \( m - 1 \). \( S(a, b, c) = \pm 2(p - 1)p^{m+1} \) 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. \( \Box \)

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

**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

\[
N_\epsilon = \# \{(a, b, c) \in \mathbb{F}_p^3 : S(a, b, c) = \epsilon(p - 1)p^{m+1}/2 \},
\]

where \( \epsilon = 0, \pm 1, \pm 2 \). Then we have
It can be shown that the value distribution of $T$ by Lemma 3.3.

Following the notation above, we have

\[
\begin{align*}
N_1 &= \# \left\{ (a, b, c) \in \mathbb{F}_p^{3} : S(a, b, c) = D(a + b, c) + D(a - b, c) = (p - 1) p^{m+1} \right\} \\
&= \# \left\{ (u_1, u_2, c) \in \mathbb{F}_p^{3} : D(u_1, c) + D(u_2, c) = (p - 1) p^{m+1} \right\} \\
&= \# \left\{ (u_1, u_2) \in \mathbb{F}_p^{2}, c \in \mathbb{F}_p^{*} : D(u_1, c) + D(u_2, c) = (p - 1) p^{m+1} \right\} \\
&\quad + \# \left\{ (u_1, u_2) \in \mathbb{F}_p^{2}, D(u_1, 0) + D(u_2, 0) = (p - 1) p^{m+1} \right\} \\
&= \# \left\{ (u_1, u_2) \in \mathbb{F}_p^{2}, c \in \mathbb{F}_p^{*} : D(u_1, c) + D(u_2, c) = (p - 1) p^{m+1} \right\} \\
&\quad + \# \left\{ (u_1, u_2) \in \mathbb{F}_p^{2}, c \in \mathbb{F}_p^{*} : D(u_1, c) = 0, D(u_2, c) = (p - 1) p^{m+1} \right\} \\
&= 2n_0n_1(p^m - 1) \\
&= (p^m - 1)(p^m - p^{-1})(p^{m-1} + p^{m-1}).
\end{align*}
\]

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

\[
\begin{align*}
N_{-1} &= 2n_0n_{-1}(p^m - 1) = (p^m - 1)(p^m - p^{-1})(p^{m-1} - p^{m-1}), \\
N_2 &= n_1^2(p^m - 1) = \frac{1}{4}(p^m - 1)(p^{m-1} + p^{m-1})^2, \\
N_{-2} &= n_1^2(p^m - 1) = \frac{1}{4}(p^m - 1)(p^{m-1} - p^{m-1})^2
\end{align*}
\]

and

\[
\begin{align*}
N_0 &= p^{3m} - 1 - 2(p^m - 1) - N_1 - N_{-1} - N_2 - N_{-2} \\
&= (p^m - 1)(p^{2m} + \frac{3}{2}p^{2(m-1)} - 2p^{2m-1} + p^m - \frac{1}{2}p^{m-1} - 1).
\end{align*}
\]

\[\square\]

**Remark** Following the notation 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.
Table 3  Weight distribution of \( C_{(p,m,k)} \)

| Weight | Frequency |
|--------|-----------|
| 0 \( \frac{p-1}{2} p^m - 1 \) | 1 |
| \( \frac{p-1}{2} (2p^m - 1 - p^{m-1}) \) | \( 2(p^m - 1) \) |
| \( \frac{p-1}{2} (2p^m - 1 + p^{m-1}) \) | \( (p^m - 1)(p^m - p^{m-1})(p^{m-1} + p^{m-2}) \) |
| \( (p-1)(p^m - 1 - p^{m-1}) \) | \( \frac{1}{2} (p^m - 1)(p^m - p^{m-1} + p^{m-2})^2 \) |
| \( (p-1)(p^m - 1 + p^{m-1}) \) | \( \frac{1}{2} (p^m - 1)(p^{m-1} - p^{m-2})^2 \) |
| \( (p-1)p^m \) | \( (p^m - 1)(p^{2m} + \frac{3}{2} p^{2m-1}) - 2p^{2m-1} + p^m - \frac{1}{2} p^{m-1} - 1 \) |

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.

**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. \( \square \)

**Example 3.7** Let \( p = 3, m = 3 \) and \( k = 1 \). Then 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.

According to the Database of best linear codes known maintained by Markus Grassl at http://www.codetables.de/, the best known linear code over \( \mathbb{F}_3 \) with length 26 and dimension 9 has minimal distance 12.

**Example 3.8** Let \( p = 5, m = 3 \) and \( k = 1 \). Then the code \( C_{(5,3,1)} \) is a \([124, 9, 50]\) cyclic code over \( \mathbb{F}_5 \) with weight enumerator

\[
1 + 248z^{50} + 27900z^{80} + 372000z^{90} + 1292576z^{100} + 248000z^{110} + 12400z^{120},
\]

which confirms the weight distribution in Table 3.

**Example 3.9** Let \( p = 3, m = 5 \) and \( k = 2 \). Then 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.

**Acknowledgments** The authors are very grateful to the Editor in Chief, the Associate Editor and the reviewers, for their comments that improved the quality of this paper. This work is supported by the National Natural Science Foundation of China (No. 11071160).
References

1. Baumert L.D., McEliece R.J.: Weights of irreducible cyclic codes. Inf. Control. 20(2), 158–175 (1972).
2. Baumert L.D., Mykkeltveit J.: Weight distribution of some irreducible cyclic codes. DSN Prog. Rep. 16, 128–131 (1973).
3. Calderbank A.R., Goethals J.M.: Three-weight codes and association schemes. Philips J. Res. 39, 143–152 (1984).
4. Carlet C., Ding C., Yuan J.: Linear codes from highly nonlinear functions and their secret sharing schemes. IEEE Trans. Inf. Theory 51(6), 2089–2102 (2005).
5. Ding C.: The weight distribution of some irreducible cyclic codes. IEEE Trans. Inf. Theory 55(3), 955–960 (2009).
6. Feng T.: On cyclic codes of length $2^r - 1$ with two zeros whose dual codes have three weights. Des. Codes Cryptogr. 62, 253–258 (2012).
7. Feng K., Luo J.: Value distributions of exponential sums from perfect nonlinear functions and their applications. IEEE Trans. Inf. Theory 53(7), 3035–3041 (2007).
8. Fan B., Tang C., Qi Y., Yang Y., Xu M.: The weight distribution of a class of cyclic codes from perfect nonlinear functions. IEEE Trans. Inf. Theory 52(2), 712–717 (2006).
9. Zhou Z., Ding C.: A family of five-weight cyclic codes and their weight enumerators. IEEE Trans. Inf. Theory 59(10), 6674–6682 (2013).