THE WEIGHT DISTRIBUTION OF A CLASS OF $p$–ARY CYCLIC CODES AND THEIR APPLICATIONS

LANQIANG LI, SHIXIN ZHU* AND LI LIU

School of Mathematics, Hefei University of Technology
Hefei 230601, China

(Communicated by Sihem Mesnager)

Abstract. Cyclic codes over finite field have been studied for decades due to their wide applications in communication and storage systems. However their weight distributions are known only in a few cases. In this paper, we investigate a class of $p$–ary cyclic codes whose duals have three zeros, where $p$ is an odd prime. The weight distributions of the class of cyclic codes for all distinct cases are determined explicitly. The results indicate that these codes contain five-weight codes, seven-weight codes and eleven-weight codes. Some of these codes are optimal. Moreover, the covering structures of the class of codes are considered and being used to construct secret sharing schemes.

1. Introduction

In this paper, we denote $F_p$ to be the finite field with characteristic and elements $p$, where $p$ is an odd prime. An $[n, k, d : p]$ linear code $C$ over the finite field $F_p$ is a $k$–dimensional subspace of $F_p^n$ with minimum Hamming distance $d$. Furthermore, the linear code $C$ is called a cyclic code if any $(c_0, c_1, ..., c_{n-1}) \in C$ implies $(c_{n-1}, c_0, c_1, ..., c_{n-2}) \in C$. Any cyclic code of length $n$ over $F_p$ can be regarded as an ideal of the ring $F_p[x]/(x^n - 1)$ and can be generated by a polynomial $g(x)$. If $g(x)|x^n - 1$ is monic and has the least degree, then we call $g(x)$ the generator polynomial of $C$. A cyclic code with parity-check polynomial $h(x)$ is called irreducible if $h(x)$ is irreducible over $F_p$, and is called reducible if $h(x)$ is reducible over $F_p$. Moreover, if $h(x)$ has $t$ irreducible factors over $F_p$, we say that the duals of such a cyclic code to have $t$ zeros, or such a cyclic code to have $t$ nonzeros. The duals of any cyclic code $C$ is defined by

$$C^\perp = \{ x \in F_p^n | x \cdot y = 0, \forall y \in C \},$$

where $x \cdot y$ is the Euclidean inner product of $x$ and $y$ in $F_p^n$. The duals $C^\perp$ is a cyclic code with generator polynomial $h(x)^*$, where $h(x)^*$ is the the reciprocal polynomial of $h(x)$.

2010 Mathematics Subject Classification: Primary: 94B05, 11T71; Secondary: 94B15.

Key words and phrases: Finite field, cyclic code, weight distribution, covering structure, secret sharing scheme.

This research is supported in part by the National Natural Science Foundation of China under Project 61572168, Project 61772168 and Project 11501156, the Natural Science Foundation of Anhui Province under Grant 1808085MA15 and the Key University Science Research Project of Anhui Province under Grant KJ2018A0497.

* Corresponding author: Shixin Zhu.
The number of codewords with Hamming weight \( i \) in \( C \) denoted by \( A_i \). The sequence \( \{A_0, A_1, \ldots, A_n\} \) is said to be the weight distribution of the code \( C \). The weight enumerator of code \( C \) is defined as follows:

\[
1 + A_1z + A_2z^2 + \ldots + A_nz^n.
\]

Moreover, a code \( C \) is called a \( t \)-weight code if the number of nonzero \( A_i \) is equal to \( t \).

Obviously, the weight distribution of cyclic code \( C \) is a worthwhile topic, due to it not only gives the minimum distance of \( C \) (i.e., the error correcting capability), but also allows the computation of the error probability of error detection and correction. However, how to determine the weight distribution of cyclic code is in general an extremely hard problem, and there are only a few cases are known. Even so, many scholars have been attracted to study the weight distribution of cyclic code in recent years. For example, the weight distributions of some irreducible cyclic codes are determined explicitly (see [3],[4],[11],[21],[25]). For reducible cyclic codes, the reader is referred to [5],[6],[8]-[10],[12]-[14],[17]-[20],[26]-[30],[33]-[36] in which most of them have two nonzeros (see [5],[6],[8]-[10],[12]-[14],[17]-[20],[26]-[30],[33]-[36]), only a few of them have three nonzeros or more nonzeros (see [9],[12],[14],[17],[20],[26],[28],[30],[33],[34]).

Let \( m, k \) be two integers with \( 1 \leq k \leq m-1 \) and \( s = m/d \), where \( d = \text{gcd}(k, m) \) is the greatest common divisor of \( k \) and \( m \). We denote \( h_1(x) \) and \( h_2(x) \) to be the minimal polynomials of \( \alpha^{-1} \) and \( \alpha^{-1}(p^k+1) \) respectively, where \( \alpha \) is the primitive element of \( F_{p^m} \). It is known that the cyclic code \( C_1 \) with parity-check polynomial \( h_1(x)h_2(x) \) was first defined by Carlet et al. in [1] and then they determined the weight distribution of such cyclic code \( C_1 \) for odd \( s \) in [32]. Moreover, Li et al. gave the weight distributions of the code \( C_1 \) for odd \( s \) and the code \( C = \{(f_{a,b,c}(\gamma_0)), (f_{a,b,c}(\gamma_1)), \ldots, (f_{a,b,c}(\gamma_p^{m-1}))|a,b,c \in F_{p^m}\} \) for odd \( s \) in theorem 1 and 2 of [15] respectively, where \( f_{a,b,c}(x) = \text{Tr}(aII(x) + bx + c) \) is a function from \( F_{q^m} \) to \( F_q \) with a perfect nonlinear function \( II(x) \) over \( F_{q^m} \). In 2015, Schmidt investigated the code \( C_1 \) with \( d = \text{gcd}(k, m) = 1 \) in [24]. Recently, Yang et al. explicitly established the weight distribution of the cyclic code \( C_1 \) for even \( s \) and the weight distribution of the cyclic code with parity-check polynomial \((x - 1)h_2(x)\) in [29]. However, the weight distribution of the cyclic code with parity-check polynomial \((x - 1)h_1(x)h_2(x)\) for either odd or even \( s \) is not known before. In fact, Yang et al. proposed to study the question for future work in [29].

From now on, let \( C \) denote the cyclic code with parity-check polynomial \((x - 1)h_1(x)h_2(x)\). In this paper, we give the weight distributions of \( C \) for both odd \( s \) and even \( s \). The remainder of this paper is organized as follows. In Section 2, some basic concepts and results are introduced. Section 3 determined the weight distributions of the cyclic code \( C \) not only for odd \( s \) but also for even \( s \). In Section 4, the covering structures of the cyclic code \( C \) are considered and being used to construct secret sharing schemes. Section 5 summarizes this paper.

2. Preliminaries

In this section, we present some basic notations and some important results which will be needed in the sequel.

It is known that quadratic forms over finite fields have been studied by Lidl and Niederreiter in reference [16], and have wide applications in coding theory (see [10],[12],[17]-[20],[29],[33]-[35]).
**Definition 2.1.** Let \( q = p^m \), then \( F_q \) can be identified as a \( m \)-dimensional vector space over \( F_p \). Let \( x = \sum_{i=1}^{m} x_i a_i \) for any \( x \in F_q \), where \( \{a_1, a_2, ..., a_m\} \) is a basis of \( F_q \) over \( F_p \) and \( a_i \in F_p \). A function \( Q(x) \) from \( F_q \) to \( F_p \) is called a quadratic form over \( F_p \) if it has the following representation:

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

where \( a_{i,j} \in F_p \). The rank of the quadratic form \( Q(x) \) is defined as the codimension of the \( F_p \)-vector space

\[
V = \{ z \in F_q : Q(x+z) = Q(x) - Q(z) = 0 \text{ for all } x \in F_q \}.
\]

The rank of \( Q(x) \) is \( r \), if \( |V| = p^{m-r} \).

Any quadratic form over \( F_p \) is equivalent to a diagonal quadratic form. So, by making a nonsingular linear substitution, we can obtain that

\[
Q(x) = \sum_{i=1}^{r} b_i y_i^2,
\]

where \( r \) is the rank of \( Q(x) \) and \( b_i \in F_p^* \).

The following results about quadratic form are important and will be frequently used in the sequel, which have been given by Lidl and Niederreiter in [16].

**Lemma 2.2.** Let \( f \) be a nondegenerated quadratic form over \( F_p \), in \( l \) variables. Define a function \( v(\cdot) \) over \( F_p \) by \( v(0) = p - 1 \) and \( v(p) = -1 \) for \( p \in F_p^* \). Then for \( b \in F_p \) the number of solutions of the equation \( f(x_1, ..., x_l) = b \) is

\[
\begin{cases}
  p^{l-1} + v(b)p^{\frac{l-2}{2}} \eta((-1)^{\frac{l}{2}} \det(f)), & \text{if } l \text{ is even,} \\
  p^{l-1} + p^{\frac{l-1}{2}} \eta(b(-1)^{\frac{l-1}{2}} \det(f)), & \text{if } l \text{ is odd,}
\end{cases}
\]

where \( \eta \) is the quadratic character of \( F_p \) and \( \det(f) \) is the determinant of the coefficient matrix of \( f \).

The following lemma could be obtained by the reference [29].

**Lemma 2.3.** Let \( m, k \) be two integers with \( 1 \leq k \leq m-1 \) and \( d = \gcd(m, k) \). For any non-zero integer \( e \), the \( 2 \)-adic order of \( e \) is the highest exponent \( v \) such that \( 2^v \) divides \( e \), and is denoted by \( v_2(e) \). Let \( Q(x) = Tr(bp^{m+1}) \) be a quadratic form and \( b_1 \) be the nonzero element of the diagonal matrix of \( Q(x) \), where \( Tr \) is the absolute trace from \( F_p^m \) to \( F_p \). Then one of the following conclusions holds

1. If \( v_2(m) \leq v_2(k) \), then \( \text{rank}(Q(x)) = m \) and

\[
\eta((-1)^{\frac{m}{2}} \prod_{i=1}^{m} b_i) = \begin{cases} 
1, & \frac{1}{2}(p^m - 1) \text{ times}, \\
-1, & \frac{1}{2}(p^m - 1) \text{ times},
\end{cases}
\]

where \( \left[ \frac{m}{2} \right] \) denotes the largest integer that is less than or equal to \( \frac{m}{2} \).

2. If \( v_2(m) = v_2(k) + 1 \), then

a) \( \text{rank}(Q(x)) = m \) and

\[
\eta((-1)^{\frac{m}{2}} \prod_{i=1}^{m} b_i) = -1, \quad \frac{p^d(p^m - 1)}{p^d + 1} \text{ times.}
\]
b) rank\((Q(x)) = m - 2d\) and

\[ \eta((-1)^\frac{2}{m} \prod_{i=1}^{m-2d} b_i) = 1, \quad \frac{p^m - 1}{p^d + 1} \text{ times.} \]

(3) If \(v_2(m) > v_2(k) + 1\), then

a) rank\((Q(x)) = m\) and

\[ \eta((-1)^\frac{2}{m} \prod_{i=1}^{m} b_i) = 1, \quad \frac{p^d(p^m - 1)}{p^d + 1} \text{ times.} \]

b) rank\((Q(x)) = m - 2d\) and

\[ \eta((-1)^\frac{2}{m} \prod_{i=1}^{m-2d} b_i) = -1, \quad \frac{p^m - 1}{p^d + 1} \text{ times.} \]

**Proof.** Combining Lemmas 3 and 4 of [29], we could obtain the lemma directly. □

**Lemma 2.4.** Let \((a, b, t) \in F_{p^n} \times F_{p^n}^* \times F_{p}^*\) and \(s = m/\gcd(m, k)\) be odd. Then the number of solutions of \(\text{Tr}(ax + bx^{p^k+1}) + t = 0\) for any \(t \in F_{p}^*\), denoted by \(N^t_{(a,b)}\), can be given as follows:

1) if the rank of the quadratic form \(Q(x) = \text{Tr}(bx^{p^k+1})\) is odd \(m\), then

a) when \(\sum_{i=1}^{m} \frac{a_i^2}{4b_i} - t = 0\), we have \(N^t_{(a,b)} = p^m - 1\) and occurs \((p - 1)(p^m - 1)p^{m-1}\) times.

b) when \(\sum_{i=1}^{m} \frac{a_i^2}{4b_i} - t \neq 0\), we have \(N^t_{(a,b)} = \) odd.

\[ N^t_{(a,b)} = \begin{cases} p^m - 1 - \frac{p^m - 1}{2}, & \frac{1}{2}(p^m - 1)((p - 1)p^{m-1} + \frac{p^m - 1}{2})(p - 1) \text{ times,} \\
& \frac{1}{2}(p^m - 1)((p - 1)p^{m-1} - \frac{p^m - 1}{2})(p - 1) \text{ times.} \end{cases} \]

2) if the rank of the quadratic form \(Q(x) = \text{Tr}(bx^{p^k+1})\) is even \(m\), then

a) when \(\sum_{i=1}^{m} \frac{a_i^2}{4b_i} - t = 0\), we have

\[ N^t_{(a,b)} = \begin{cases} p^m - 1 + (p - 1)p^{m-2}, & \frac{1}{2}(p^m - 1)(p^{m-1} - \frac{p^m - 1}{2})(p - 1) \text{ times,} \\
& \frac{1}{2}(p^m - 1)(p^{m-1} + \frac{p^m - 1}{2})(p - 1) \text{ times.} \end{cases} \]

b) when \(\sum_{i=1}^{m} \frac{a_i^2}{4b_i} - t \neq 0\), we have

\[ N^t_{(a,b)} = \begin{cases} p^m - 1 - \frac{p^m - 1}{2}, & \frac{1}{2}(p^m - 1)((p - 1)p^{m-1} + \frac{p^m - 1}{2})(p - 1) \text{ times,} \\
& \frac{1}{2}(p^m - 1)((p - 1)p^{m-1} - \frac{p^m - 1}{2})(p - 1) \text{ times.} \end{cases} \]

**Proof.** (1) If rank\((Q(x)) = m\), then by making a nonsingular linear substitution to \(\text{Tr}(ax + bx^{(1+p^k)}) + t = 0\), we have that

\[ \sum_{i=1}^{m} a_i x_i + \sum_{i=1}^{m} b_i x_i^2 = -t, \]
where \(a_i, x_i \in F_p\) and \(b_i \in F_p^*\). Furthermore, taking \(x_i = y_i \cdot \frac{a_i}{2b_i}\) for any \(1 \leq i \leq m\), then (1) becomes
\[
\sum_{i=1}^{m} b_i x_i^2 = \sum_{i=1}^{m} \frac{a_i^2}{4b_i} - t.
\]
From Lemma 2.2, we know that the number of solutions of the equation (1) is
\[
N_t^{(a, b)} = p^{m-1} + p^{\frac{m-1}{2}} \eta(\sum_{i=1}^{m} \frac{a_i^2}{4b_i} - t)\eta((-1)^{\frac{m-1}{2}} \prod_{i=1}^{m} b_i),
\]
where \(\eta\) is the quadratic character of \(F_p^*\).

a) Clearly, \(N_t^{(a, b)} = p^{m-1}\) if and only if \(\sum_{i=1}^{m} \frac{a_i^2}{4b_i} - t = 0\). Since \(\sum_{i=1}^{m} \frac{a_i^2}{4b_i}\) can be regarded as a quadratic form in \(m\) variables \(a_i, 1 \leq i \leq m\), then the number of solutions of \(\sum_{i=1}^{m} \frac{a_i^2}{4b_i} - t = 0\) is \(N_t = p^{m-1} + p^{\frac{m-1}{2}} \eta(t)\eta((-1)^{\frac{m-1}{2}} \prod_{i=1}^{m} b_i)\) for any \(t \in F_p^*\).

Therefore,
\[
\sum_{t \in F_p^*} N_t = \sum_{t \in F_p^*} \left(p^{m-1} + p^{\frac{m-1}{2}} \eta(t)\eta((-1)^{\frac{m-1}{2}} \prod_{i=1}^{m} b_i)\right) = (p-1)p^{m-1}.
\]

Let \(N(a, b, t)\) be the number of \((a, b, t) \in F_p^m \times F_p^m \times F_p^*\) such that the number of solutions of \(\text{Tr}(ax + bx^{p^k+1}) + t = 0\) is \(N_t^{(a, b)}\). Combining the discussion above, we have \(N_t^{(a, b)} = p^{m-1}\) and \(N(a, b, t) = (p-1)(p^{m-1})\) if \(\sum_{i=1}^{m} \frac{a_i^2}{4b_i} - t = 0\).

b) According to \(\eta\left(\frac{1}{4^m \prod_{i=1}^{m} b_i}\right) = \eta\left(\prod_{i=1}^{m} b_i\right)\) and Lemma 2.3, we have
\[
\eta((-1)^{\frac{m-1}{2}} \prod_{i=1}^{m} b_i) = \begin{cases} 1, & \text{occurring } \frac{1}{2}(p^{m-1}) \text{ times}, \\ -1, & \text{occurring } \frac{1}{2}(p^{m-1}) \text{ times}. \end{cases}
\]

Therefore, we have
\[
N_t^{(a, b)} = \begin{cases} p^{m-1} + \eta(\sum_{i=1}^{m} \frac{a_i^2}{4b_i} - t)p^{\frac{m-1}{2}}, & \text{occurring } \frac{1}{2}(p^{m-1}) \text{ times}, \\ p^{m-1} - \eta(\sum_{i=1}^{m} \frac{a_i^2}{4b_i} - t)p^{\frac{m-1}{2}}, & \text{occurring } \frac{1}{2}(p^{m-1}) \text{ times}. \end{cases}
\]

First, let \(T \in F_p^*\) be a square (denoted as SQ), then, for any \(T \in F_p^*\), the number of solutions of \(\sum_{i=1}^{m} \frac{a_i^2}{4b_i} - t = T\) is
\[
N(T, t) = p^{m-1} + p^{\frac{m-1}{2}} \eta(T + t)\eta((-1)^{\frac{m-1}{2}} \prod_{i=1}^{m} b_i).
\]
Therefore, when \( \eta((-1)^{\frac{m-1}{2}} \prod_{i=1}^{m} b_i) = 1 \),

\[
\sum_{T \in \text{SQ}} \sum_{t \in F_p^*} N_{(T,t)} = \sum_{T \in \text{SQ}} \sum_{t \in F_p^*} \left( p^{m-1} + p^{\frac{m-1}{2}} \eta(T+t) \eta((-1)^{\frac{m-1}{2}} \prod_{i=1}^{m} b_i) \right) \\
= \sum_{T \in \text{SQ}} \left( (p-1)p^{m-1} + p^{\frac{m-1}{2}} \sum_{t \in F_p^*} \eta(T+t) \right) \\
= \frac{p-1}{2} \left( (p-1)p^{m-1} - p^{\frac{m-1}{2}} \right),
\]

and, when \( \eta((-1)^{\frac{m-1}{2}} \prod_{i=1}^{m} b_i) = -1 \),

\[
\sum_{T \in \text{SQ}} \sum_{t \in F_p^*} N_{(T,t)} = \sum_{T \in \text{SQ}} \sum_{t \in F_p^*} \left( p^{m-1} - p^{\frac{m-1}{2}} \eta(T+t) \eta((-1)^{\frac{m-1}{2}} \prod_{i=1}^{m} b_i) \right) \\
= \sum_{T \in \text{SQ}} \left( (p-1)p^{m-1} - p^{\frac{m-1}{2}} \sum_{t \in F_p^*} \eta(T+t) \right) \\
= \frac{p-1}{2} \left( (p-1)p^{m-1} + p^{\frac{m-1}{2}} \right).
\]

Second, if \( T \in F_p^* \) is a nonsquare (denoted as NSQ), then with the similar method, we have \( \sum_{T \in \text{NSQ}} \sum_{t \in F_p^*} N_{(T,t)} \) given as follows:

when \( \eta((-1)^{\frac{m-1}{2}} \prod_{i=1}^{m} b_i) = 1 \),

\[
\sum_{T \in \text{NSQ}} \sum_{t \in F_p^*} N_{(T,t)} = \frac{p-1}{2} \left( (p-1)p^{m-1} + p^{\frac{m-1}{2}} \right);
\]

when \( \eta((-1)^{\frac{m-1}{2}} \prod_{i=1}^{m} b_i) = -1 \),

\[
\sum_{T \in \text{NSQ}} \sum_{t \in F_p^*} N_{(T,t)} = \frac{p-1}{2} \left( (p-1)p^{m-1} - p^{\frac{m-1}{2}} \right).
\]

Therefore, combining the discussion above and Lemma 2.3, we obtain that \( N_{(a,b)}^{t} = p^{m-1} - p^{\frac{m-1}{2}} \) and \( N(a,b,t) = \frac{1}{2}(p^m-1)((p-1)p^{m-1} + p^{\frac{m-1}{2}})(p-1) \), or \( N_{(a,b)}^{t} = p^{m-1} + p^{\frac{m-1}{2}} \) and \( N(a,b,t) = \frac{1}{2}(p^m-1)((p-1)p^{m-1} - p^{\frac{m-1}{2}})(p-1) \).

(2) By simply modifying the proof above, if \( m \) is even, we get that

\[
N_{(a,b)}^{t} = p^{m-1} + p^{\frac{m-2}{2}} \eta(\sum_{i=1}^{m} \frac{a_i^2}{b_i} - t) \eta((-1)^{\frac{m}{2}} \prod_{i=1}^{m} b_i),
\]

\[
N_{(t)} = p^{m-1} - p^{\frac{m-2}{2}} \eta((-1)^{\frac{m}{2}} \prod_{i=1}^{m} b_i) \text{ and } N_{(T,t)} = p^{m-1} + p^{\frac{m-2}{2}} \nu(T+t) \eta((-1)^{\frac{m}{2}} \prod_{i=1}^{m} b_i)
\]

for any \( t \in F_p^* \), where \( \nu(0) = p - 1 \) and \( \nu(\rho) = -1 \) for \( \rho \in F_p^* \). Furthermore, we
have

$$\sum_{t \in F_p^*} N(x, t) = \sum_{t \in F_p^*} \left( p^{m-1} + \frac{m-2}{2} \eta \prod_{i=1}^{m} b_i \right) \left( N_{t(a,b)} \right)$$

$$= (p-1)p^{m-1} + \frac{m-2}{2} \eta \prod_{i=1}^{m} b_i \sum_{t \in F_p^*} \eta$$

$$= (p-1)p^{m-1} + \frac{m-2}{2} \eta \prod_{i=1}^{m} b_i \sum_{t \in F_p^*} \eta$$

Therefore, we can obtain that

a) when \( \sum_{i=1}^{m} a_i - t = 0 \), we have \( N_{t(a,b)} = p^{m-1} + (p-1)\frac{m-2}{2} \) and \( N(a, b, t) = \frac{1}{2} (p^m - 1)(p^{m-1} - \frac{m-2}{2})(p-1) \) if \( \eta(\prod_{i=1}^{m} b_i) = 1 \) or \( N_{t(a,b)} = p^{m-1} - (p-1)\frac{m-2}{2} \) and \( N(a, b, t) = \frac{1}{2} (p^m - 1)(p^{m-1} + \frac{m-2}{2})(p-1) \) if \( \eta(\prod_{i=1}^{m} b_i) = -1 \).

b) when \( \sum_{i=1}^{m} a_i - t \neq 0 \), we have \( N_{t(a,b)} = p^{m-1} - \frac{m-2}{2} \) and \( N(a, b, t) = \frac{1}{2} (p^m - 1)(p^{m-1} + \frac{m-2}{2})(p-1) \) if \( \eta(\prod_{i=1}^{m} b_i) = 1 \) or \( N_{t(a,b)} = p^{m-1} + \frac{m-2}{2} \) and \( N(a, b, t) = \frac{1}{2} (p^m - 1)(p^{m-1} - \frac{m-2}{2})(p-1) \) if \( \eta(\prod_{i=1}^{m} b_i) = -1 \).

**Lemma 2.5.** Let \((a, b, t) \in F_{p^m} \times F_{p^m} \times F_{p^m}^* \), \( d = \gcd(m, k) \) and \( s = m/\gcd(m, k) \) be even. Then the number of solutions of \( T(x + b x^{p^k}) + t = 0 \) for any \( t \in F_p^* \), denoted by \( N_{t(a,b)} \), can be given as follows:

1. If \( v_2(m) = v_2(k) + 1 \), then
   a) when \( \text{rank}(Q(x)) = m \), we have
      \[
      N_{t(a,b)} = \begin{cases} 
      p^{m-1} - (p-1)\frac{m-2}{2}, & (p-1)(p^{m-1} + \frac{m-2}{2})\frac{p^d(p^m-1)}{p^d+1} \\
      times, \\
      p^{m-1} + \frac{m}{2}, & (p-1)(p^{m-1} - \frac{m-2}{2})\frac{p^d(p^m-1)}{p^d+1} \\
      times. 
      \end{cases}
      \]
   b) when \( \text{rank}(Q(x)) = m - 2d \), we have
      \[
      N_{t(a,b)} = \begin{cases} 
      p^{m-1}, & (p-1)(p^m - \frac{m-2d}{2})\frac{p^d(p^m-1)}{p^d+1} \\
      p^{m-1} + \frac{m}{2}, & (p-1)(p^{m-2d-1} - \frac{m-2d-2}{2})\frac{p^{m-1}}{p^d+1} \\
      p^{m-1} - \frac{m}{2}, & (p-1)(p^{m-2d-1} + \frac{m-2d-2}{2})\frac{p^{m-1}}{p^d+1} \\
      times. 
      \end{cases}
      \]

2. If \( v_2(m) > v_2(k) + 1 \), then
   a) when \( \text{rank}(Q(x)) = m \), we have
      \[
      N_{t(a,b)} = \begin{cases} 
      p^{m-1} - (p-1)\frac{m-2}{2}, & (p-1)(p^{m-1} - \frac{m-2}{2})\frac{p^d(p^m-1)}{p^d+1} \\
      p^{m-1} + \frac{m}{2}, & (p-1)(p^{m-1} - \frac{m}{2})\frac{p^d(p^m-1)}{p^d+1} \\
      p^{m-1} - \frac{m}{2}, & (p-1)(p^{m-1} - \frac{m}{2})\frac{p^d(p^m-1)}{p^d+1} \\
      times. 
      \end{cases}
      \]
b) when rank$(Q(x)) = m - 2d$, we have

$$N_{(a,b)}^t = \begin{cases} 
  p^{m-1}, & (p-1)(p^m - p^{m-2d}) \frac{p^m - 1}{p^d + 1} \text{ times,} \\
  p^{m-1} - (p-1)p^{\frac{m+2d-2}{2}}, & (p-1)(p^{m-2d-1} + \frac{p^{m-2d-2}}{p^d + 1}) \frac{p^m - 1}{p^d + 1} \text{ times,} \\
  p^{m-1} + p^{\frac{m+2d-2}{2}}, & (p-1)((p-1)p^{m-2d-1} - p^{\frac{m-2d-2}{2}}) \frac{p^m - 1}{p^d + 1} \text{ times.}
\end{cases}$$

Proof. In here, we just discuss the second case $\nu_2(m) > \nu_2(k) + 1$. The first case $\nu_2(m) = \nu_2(k) + 1$ can be investigated similarly.

a) When rank$(Q(x)) = m$, from Lemma 2.3, we have $\eta((-1)^{\frac{m}{2}} \prod_{i=1}^{m} b_i) = 1$ and it occurs $\frac{p^d(p^m - 1)}{p^d + 1}$ times. Furthermore, by using the similar way with Lemma 2.4, we can obtain the results in a).

b) When rank$(Q(x)) = m - 2d$, from Lemma 2.3, we have $\eta((-1)^{\frac{m}{2}} \prod_{i=1}^{m} b_i) = -1$ and it occurs $\frac{p^m - 1}{p^d + 1}$ times. In this case, the equation (1) can be reduced as

$$\sum_{i=1}^{m} a_i x_i + \sum_{i=1}^{m-2d} b_i x_i^2 = -t,$$

where $b_i \neq 0$ for any $1 \leq i \leq m - 2d$. Furthermore, if there is some $a_i \neq 0$ for $m - 2d < i \leq m$, we can suppose that $a_m \neq 0$. It is obvious that $x_m$ is uniquely determined by $x_1, x_2, \ldots, x_{m-1} \in F_p$. Hence, in this subcase, $N_{(a,b)}^t = p^{m-1}$ and it occurs $(p-1)(p^m - p^{m-2d}) \frac{p^m - 1}{p^d + 1}$ times. Moreover, if $a_i = 0$ for all $m - 2d < i \leq m$, taking $x_i = y_i - \frac{a_i}{2b_i}$ for any $1 \leq i \leq m - 2d$, then (2) becomes

$$\sum_{i=1}^{m-2d} b_i y_i^2 = \sum_{i=1}^{m-2d} \frac{a_i^2}{4b_i} - t.$$

So, by Lemma 2.2, we have

$$N_{(a,b)}^t = p^{2d}(p^{m-2d-1} + v(\sum_{i=1}^{m-2d} \frac{a_i^2}{4b_i} - t)p^{\frac{m-2d-2}{2}} \eta((-1)^{\frac{m}{2}} \prod_{i=1}^{m} b_i))$$

$$= p^{m-1} - v(\sum_{i=1}^{m-2d} \frac{a_i^2}{4b_i} - t)p^{\frac{m+2d-2}{2}}.$$

Let $N_t$ and $N_{(T,t)}$ be defined as Lemma 2.4. When $\sum_{i=1}^{m-2d} \frac{a_i^2}{4b_i} - t = 0$, we have

$$\sum_{T \in F_p^*} N_t = (p-1)(p^{m-2d-1} + p^{\frac{m-2d-2}{2}}).$$

Therefore, in this subcase, we have $N_{(a,b)}^t = p^{m-1} - (p-1)p^{\frac{m+2d-2}{2}}$ and it occurs $(p-1)(p^{m-2d-1} + p^{\frac{m-2d-2}{2}}) \frac{p^m - 1}{p^d + 1}$ times. When $\sum_{i=1}^{m-2d} \frac{a_i^2}{4b_i} - t = T \in F_p^*$, we have

$$\sum_{T \in F_p^*} \sum_{t \in F_p^*} N_{(T,t)} = \sum_{T \in F_p^*} \sum_{t \in F_p^*} (p^{m-2d-1} - v(T+t)p^{\frac{m-2d-2}{2}}) = (p-1)((p-1)p^{m-2d-1} - p^{\frac{m-2d-2}{2}}).$$
Therefore, in this subcase, we have $N_{(a,b)}^t = p^{m-1} + p^{m+2d-2}$ and it occurs $(p-1)(p-1)p^{m-2d-1} - p^{m-2d-1} - p^{m-2d-1}$ times.

\[ \Box \]

Lemma 2.6. Let $\omega$ be the $p$-th primitive root of unity. Then

\[
\sum_{y \in F_p^*} \sum_{x \in F_p^m} \omega^{y(\text{Tr}(ax)+t)} = 0,
\]

for any $a \in F_p^*$ and $t \in F_p^*$.

Proof. The result is obvious. \[ \Box \]

3. The weight distribution of cyclic code $C$

In this section, we study the weight distributions of the cyclic code $C$ as defined in Section 1, not only for odd $s$ but also for even $s$. According to the definitions of $h_1(x)$ and $h_2(x)$, it is clear that $\deg(h_1(x)) = m$ and

\[
\deg(h_2(x)) = \begin{cases} \frac{m}{2}, & \text{if } s \text{ is even and } k = \frac{m}{2}, \\
\frac{m}{2}, & \text{otherwise} \end{cases}
\]

From (3), we know that the dimension of $C$ is $\frac{3m}{2} + 1$ if $k = \frac{m}{2}$, otherwise, the dimension of $C$ is $2m + 1$. Moreover, by using the well-known Delsarte’s Theorem [2], we have that

\[
C = \{ (\text{Tr}(a\alpha^i + ba^{(p^k+1)i} + c))_{i=0}^{p^m-2} : a, b, c \in F_{p^m} \},
\]

where $\text{Tr}$ denotes the absolute trace from $F_{p^m}$ to $F_p$. Therefore, for any codeword $c(a,b,c) \in C$, the Hamming weight of the codeword can be given by

\[
W(c(a,b,c)) = \left| \{ i : (\text{Tr}(a\alpha^i + ba^{(p^k+1)i} + c))_{i=0}^{p^m-2} \neq 0 \} \right|
\]

\[
= p^m - 1 - \left| \{ i : (\text{Tr}(a\alpha^i + ba^{(p^k+1)i} + c))_{i=0}^{p^m-2} = 0 \} \right|
\]

\[
= p^m - 1 - \frac{1}{p} \sum_{i=0}^{p^m-2} \sum_{y \in F_p} \omega^{y\text{Tr}(a\alpha^i + ba^{(p^k+1)i} + c)}
\]

\[
= p^m - 1 - \frac{1}{p} \sum_{x \in F_p^m} \sum_{y \in F_p} \omega^{y\text{Tr}(ax + bx^{p^k+1} + c)},
\]

where $\omega$ is a $p$-th primitive root of unity.

Furthermore, the equation above can be reduced as

\[
W(c(a,b,c)) = \begin{cases} (p-1) \cdot p^{m-1} - \frac{1}{p} \sum_{y \in F_p^*} \sum_{x \in F_p^m} \omega^{y\text{Tr}(ax + bx^{p^k+1})}, & \text{if } \text{Tr}(c) = 0, \\
(p-1) \cdot p^{m-1} - 1 - \frac{1}{p} \sum_{y \in F_p^*} \sum_{x \in F_p^m} \omega^{y\text{Tr}(ax + bx^{p^k+1}) + y\text{Tr}(c)}, & \text{if } \text{Tr}(c) \neq 0. \end{cases}
\]

Let $d = \gcd(m,k)$ and $s = m/d$ be odd. Note that $s$ is odd if and only if $v_2(m) \leq v_2(k)$. So, by Lemma 2.3, we know that the rank of the quadratic form $Q(x)$ is $m$. Next we give the parameters and the weight distribution of the cyclic code $C$ for odd $s$ in the following theorem.
Theorem 3.1. Let \( s \) be odd. Then one of the following results holds.

1. If \( m \) is odd, the cyclic code \( C \) has parameters \([p^m - 1, 2m + 1, (p - 1)p^{m-1} - p^{\frac{m-1}{2}} - 1 : p]\), and its weight distribution is given by Table I.

2. If \( m \) is even, the cyclic code \( C \) has parameters \([p^m - 1, 2m + 1, (p - 1)(p^{m-1} - p^{\frac{m-2}{2}}) - 1 : p]\), and its weight distribution is given by Table II.

### Table I

| Hamming Weight \( i \) | Frequency \( A_i \) |
|------------------------|---------------------|
| \((p - 1)p^m\)         | \((p^m - 1)(p^{n-1} + 1)\) |
| \((p - 1)p^{m-1} - 1\) | \((p^m - 1)(p^{m-1} + 1)(p - 1)\) |
| \((p - 1)p^{m-1} - p^{\frac{m-1}{2}} - 1\) | \(\frac{1}{2}(p^m - 1)((p - 1)p^{m-1} - p^{\frac{m-2}{2}})(p - 1)\) |
| \((p - 1)p^{m-1} + p^{\frac{m-1}{2}} - 1\) | \(\frac{1}{2}(p^m - 1)((p - 1)p^{m-1} + p^{\frac{m-2}{2}})(p - 1)\) |
| \(p^m - 1\)           | \(p - 1\)           |

### Table II

| Hamming Weight \( i \) | Frequency \( A_i \) |
|------------------------|---------------------|
| \((p - 1)p^m\)         | \(p^m - 1\)         |
| \((p - 1)p^{m-1} - 1\) | \((p^m - 1)(p - 1)\) |
| \((p - 1)(p^{m-1} - p^{\frac{m-2}{2}})\) | \(\frac{1}{2}(p^m - 1)((p - 1)p^{m-1} + (p - 1)p^{\frac{m-2}{2}})\) |
| \((p - 1)(p^{m-1} - p^{\frac{m-2}{2}}) - 1\) | \(\frac{1}{2}(p^m - 1)((p - 1)p^{m-1} - p^{\frac{m-2}{2}})(p - 1)\) |
| \((p - 1)p^{m-1} - p^{\frac{m-2}{2}} - 1\) | \(\frac{1}{2}(p^m - 1)((p - 1)p^{m-1} - p^{\frac{m-2}{2}})(p - 1)\) |
| \((p - 1)p^{m-1} + p^{\frac{m-1}{2}} - 1\) | \(\frac{1}{2}(p^m - 1)((p - 1)p^{m-1} + p^{\frac{m-2}{2}})(p - 1)\) |
| \((p - 1)p^{m-1} + p^{\frac{m-2}{2}} - 1\) | \(\frac{1}{2}(p^m - 1)((p - 1)p^{m-1} + p^{\frac{m-2}{2}})(p - 1)\) |
| \(p^m - 1\)           | \(p - 1\)           |

Proof. The dimension of the cyclic code \( C \) follows from the discussion above. Now, we only need to determine the weight distribution of \( C \) for odd \( s \). For any codeword \( c(a, b, c) \in C \), the weight of the codeword \( c(a, b, c) \) is given by (4).

First, we assume that \( m \) is odd. Next, we will consider the following two cases.

**Case A.** when \( \text{Tr}(c) = 0 \): By (4), we have

\[
W(c(a, b, c)) = (p - 1) \cdot p^{m-1} - \frac{1}{F} \sum_{y \in F_p^*} \sum_{x \in F_{p^m}} \omega^{(y \cdot \text{Tr}(ax + bx^{p^{k+1}}))}.
\]
In this case, it can be easily seen that all the codewords $c(a, b, c)$ formed a cyclic code $C'$ with parity-check polynomial $h_1(x)h_2(x)$ for odd $s$. Therefore, from Theorem 1 of [31], we have

$$W(c(a, b, c)) = \begin{cases} 0, & \text{1 time,} \\ (p - 1)p^{m-1}, & \text{1 time,} \\ (p - 1)p^{m-1} + p^{m-1}, & \frac{1}{2}(p^m - 1)(p^{m-1} - p^{\frac{m-1}{2}})(p - 1), \frac{1}{2}(p^m - 1)(p^{m-1} + p^{\frac{m-1}{2}})(p - 1) \text{ times,} \\ (p - 1)p^{m-1} - p^{m-1}, & \frac{1}{2}(p^m - 1)(p^{m-1} + p^{\frac{m-1}{2}})(p - 1) \text{ times.} \end{cases}$$

**Case B.** when $\text{Tr}(c) = t \in F_p^*$. According to $\sum_{y \in F_p^*} (\omega^t)^y = -1$ and (4), we have

$$W(c(a, b, c)) = (p - 1)p^{m-1} - 1 - \frac{1}{p} \sum_{y \in F_p^*} \sum_{x \in F_{p^m}} \omega^t(\text{Tr}(ax + bx^{k+1} + t)) \quad (5)$$

$$= (p - 1)p^{m-1} - 1 - \frac{1}{p}(pN^t_{(a, b)} - p^m),$$

where $N^t_{(a, b)}$ is the number of solutions of $\text{Tr}(ax + bx^{k+1} + t) = 0$ over $F_{p^m}$.

1) If $b = 0$ and $a = 0$, then $W(c(a, b, c)) = (p - 1)p^{m-1} - 1 - \frac{1}{p} \left( \sum_{x \in F_{p^m}} (-1) \right) = p^m - 1$ occurs only once for every $t$, as $\sum_{y \in F_p^*} (\omega^t)^y = -1$.

2) If $b = 0$ and $a \neq 0$, then, from Lemma 2.6, we have $W(c(a, b, c)) = (p - 1)p^{m-1} - 1 - \frac{1}{p} \left( \sum_{y \in F_p^*} \sum_{x \in F_{p^m}} \omega^t(\text{Tr}(ax) + t) \right) = (p - 1)p^{m-1} - 1$ and it occurs $p^m - 1$ times for every $t$.

3) Next, we consider the subcase with $b \neq 0$. In this subcase, if $\sum_{i=1}^{m} \frac{a_i^2}{4b_i} - t = 0$, combing Lemma 2.4 and (5), we can get

$$W(c(a, b, c)) = (p - 1)p^{m-1} - 1 - \frac{1}{p}(p \cdot p^{m-1} - p^m)$$

and it occurs $(p - 1)(p^m - 1)p^{m-1}$ times. Otherwise, again combing Lemma 2.4 and (5), we obtain that

$$W(c(a, b, c)) = (p - 1)p^{m-1} - 1 - \frac{1}{p}(p(p^{m-1} - p^{\frac{m-1}{2}}) - p^m)$$

and it occurs $\frac{1}{2}(p^m - 1)((p - 1)p^{m-1} + p^{\frac{m-1}{2}})(p - 1)$ times, and

$$W(c(a, b, c)) = (p - 1)p^{m-1} - 1 - \frac{1}{p}(p(p^{m-1} + p^{\frac{m-1}{2}}) - p^m)$$

and it occurs $\frac{1}{2}(p^m - 1)((p - 1)p^{m-1} - p^{\frac{m-1}{2}})(p - 1)$ times.

Advances in Mathematics of Communications Volume 13, No. 1 (2019), 137–156
Therefore, the weight distribution of $C$ can be obtained by the above discussion and given by Table I.

Second, we assume that $m$ is even. Similarly, when Tr$(c) = 0$, we have

$$ W(c(a, b, c)) = \begin{cases} 
0, & 1 \text{ time}, \\
(p - 1)p^{m-1}, & (p^m - 1) \text{ times}, \\
(p - 1)(p^{m-1} - p^{m-2}), & \frac{1}{2}(p^m - 1)(p^{m-1} + (p - 1)p^{m-2}) \text{ times}, \\
(p - 1)p^{m-1} - p^{m-2}, & \frac{1}{2}(p^m - 1)(p^{m-1} + p^{m-2})(p - 1) \text{ times}, \\
(p - 1)p^{m-1} + p^{m-2}, & \frac{1}{2}(p^m - 1)(p^{m-1} + (p - 1)p^{m-2}) \text{ times}, \\
(p - 1)(p^{m-1} + p^{m-2}), & \frac{1}{4}(p^m - 1)(p^{m-1} + (p - 1)p^{m-2}) \text{ times}, \\
\end{cases} $$

which is the weight distribution of code $C'$ with even $m$.

Next, we give the discussion on the case with Tr$(c) \neq 0$. According to 1) and 2) of the Case B above, in this case, we have $W(c(a, b, c)) = p^m - 1$ which occurs $p - 1$ times if $b = 0$ and $a = 0$ or $W(c(a, b, c)) = (p - 1)p^{m-1} - 1$ which occurs $(p - 1)(p^m - 1)$ times if $b = 0$ and $a \neq 0$. So, we only need consider the subcase with $b \neq 0$. From the 2) of Lemma 2.3 and (5), we have

$$ W_{c(a, b, c)} = \begin{cases} 
(p - 1)(p^{m-1} - p^{m-2}) - 1, & \frac{1}{2}(p^m - 1)(p^{m-1} - p^{m-2})(p - 1) \text{ times}, \\
(p - 1)(p^{m-1} + p^{m-2}) - 1, & \frac{1}{2}(p^m - 1)(p^{m-1} + p^{m-2})(p - 1) \text{ times}, \\
(p - 1)p^{m-1} - p^{m-2} - 1, & \frac{1}{2}(p^m - 1)((p - 1)p^{m-1} - p^{m-2})(p - 1) \text{ times}, \\
(p - 1)p^{m-1} + p^{m-2} - 1, & \frac{1}{4}(p^m - 1)((p - 1)p^{m-1} + p^{m-2})(p - 1) \text{ times}. \\
\end{cases} $$

This completes the proof. 

Now, we will give some examples for the code $C$ with odd $s$, whose weight distribution is not known before.

**Example 1.** Let $(p, m, k) = (3, 5, 1)$. Then, by using Magma, the code $C$ is a [242, 11, 152 : 3] cyclic code and has the following weight enumerator:

$$ 1 + 152z^{37026} + 153z^{21780} + 161z^{39688} + 162z^{19844} + 170z^{41382} + 171z^{17424} + 242z^2, $$

which agrees with the result of Table I. This is a known optimal cyclic code according to the Database.

**Example 2.** Let $(p, m, k) = (5, 3, 1)$. Then, by using Magma, the code $C$ is a [124, 7, 94 : 5] cyclic code and has the following weight enumerator:

$$ 1 + 94z^{3560} + 95z^{240} + 99z^{12896} + 100z^{3224} + 104z^{26040} + 105z^{4960} + 124z^4, $$
Example 3. Let \((p, m, k) = (3, 6, 2)\). Then, by using Magma, the code \(C\) is a [728, 13, 467 : 3] cyclic code and has the following weight enumerator:

\[
1 + 467z^{70352} + 468z^{65004} + 476z^{147256} + 477z^{183456} + 485z^{1456} + 486z^{728} + 494z^{360360} + 495z^{170352} + 503z^{183456} + 504z^{81900} + 728z^2,
\]

which agrees with the result of Table II.

Let \(d = \gcd(m, k)\) and \(s = m/d\) be even. Notice that \(s\) is even if and only if \(v_2(m) \geq v_2(k) + 1\). So, by Lemma 2.3, we know that the rank of the quadratic form \(Q(x)\) is \(m\) or \(m - 2d\). In the following, we determine the weight distribution of the cyclic code \(C\) as defined in Section 1 for even \(s\).

Theorem 3.2. Let \(s\) be even and \(m \neq 2k\). Then one of the following conclusions holds.

1. If \(v_2(m) = v_2(k) + 1\), then the cyclic code \(C\) has parameters \([p^m - 1, 2m + 1, (p - 1)(p^{m-1} - p^{m+2d-2}) - 1 : p]\), and its weight distribution is given by Table III.
2. If \(v_2(m) > v_2(k) + 1\), then the cyclic code \(C\) has parameters \([p^m - 1, 2m + 1, (p - 1)p^{m-1} - p^{m+2d-2} - 1 : p]\), and its weight distribution is given by Table IV.

### Table III

| Hamming Weight \(i\) | Frequency \(A_i\) |
|----------------------|------------------|
| \((p - 1)p^{m-1}\)   | \((p^m - 1)(1 + p^{m-d} - p^{m-2d})\) |
| \((p - 1)p^{m-1} - 1\) | \((p - 1)(p^m - 1)(1 + p^{m-d} - p^{m-2d})\) |
| \((p - 1)(p^{m-1} - p^{m+2d-2})\) | \((p^{m-2d-1} - (p - 1)p^{m-2d-2}) - \frac{p^m - 1}{p^d + 1}\) |
| \((p - 1)(p^{m-1} - p^{m+2d-2}) - 1\) | \((p - 1)(p^{m-2d-1} - p^{m-2d-2}) - \frac{p^m - 1}{p^d + 1}\) |
| \((p - 1)p^{m-1} - p^{m+2d-2}\) | \((p - 1)(p^{m-1} + p^{m+2d-2}) - \frac{p^d(p^m - 1)}{p^d + 1}\) |
| \((p - 1)p^{m-1} - p^{m+2d-2} - 1\) | \((p - 1)((p - 1)p^{m-1} - p^{m+2d-2}) - \frac{p^d(p^m - 1)}{p^d + 1}\) |
| \((p - 1)p^{m-1} + p^{m+2d-2}\) | \((p - 1)(p^{m-2d-1} - p^{m-2d-2}) - \frac{p^m - 1}{p^d + 1}\) |
| \((p - 1)p^{m-1} + p^{m+2d-2} - 1\) | \((p - 1)((p - 1)p^{m-2d-1} + p^{m-2d-2}) - \frac{p^m - 1}{p^d + 1}\) |
| \((p - 1)(p^{m-1} + p^{m+2d-2})\) | \((p^{m-1} - (p - 1)p^{m+2d-2}) - \frac{p^d(p^m - 1)}{p^d + 1}\) |
| \((p - 1)(p^{m-1} + p^{m+2d-2} - 1\) | \((p - 1)(p^{m-1} + p^{m+2d-2}) - \frac{p^d(p^m - 1)}{p^d + 1}\) |
| \(p^m - 1\) | \(p - 1\) |
In here, we just consider the case \( \text{Tr}(c) \neq 0 \). By using the same way with Theorem 3.1, we can obtain the other weights and their distributions according to Lemma 2.5.

**Case A.** when \( \text{Tr}(c) = 0 \): In this case, we can find that all codewords \( c(a, b, c) \) formed a cyclic code \( C' \) with parity-check polynomial \( h_1(x)h_2(x) \) for even \( s \). Therefore, from Theorem 1 of [29], we have

\[
W(c(a, b, c)) = \begin{cases} 
0, & 1 \text{ time}, \\
(p - 1)p^{m-1}, & (p^n - 1)(1 + p^{m-d} - p^{m-2d}) \text{ times}, \\
(p - 1)(p^{m-1} - p^{m-2d}), & (p^n - 1)(1 + p^{m-d} - p^{m-2d}) \text{ times}, \\
(p - 1)p^{m-1} - p^{\frac{m+2d-2}{2}}, & (p - 1)(p^{m-d-1} + p^{\frac{m-2d-2}{2}}) \text{ times}, \\
(p - 1)p^{m-1} + p^{\frac{m+2d-2}{2}}, & (p - 1)(p^{m-d-1} + p^{\frac{m-2d-2}{2}}) \text{ times}, \\
(p - 1)(p^{m-1} + p^{\frac{m+2d-2}{2}}), & (p - 1)(p^{m-d-1} + p^{\frac{m-2d-2}{2}}) \text{ times}. 
\end{cases}
\]

**Case B.** when \( \text{Tr}(c) = t \in F_p^* \): By using the same way with Theorem 3.1, we can obtain the other weights and their distributions according to Lemma 2.5.

### TABLE IV

Weight distribution of the cyclic code \( C \) for even \( m \) in Theorem 3.2

| Hamming Weight \( i \) | Frequency \( A_i \) |
|------------------------|---------------------|
| \( (p - 1)p^{m-1} \)   | \( (p^n - 1)(1 + p^{m-d} - p^{m-2d}) \) |
| \( (p - 1)p^{m-1} - 1 \) | \( (p - 1)(p^n - 1)(1 + p^{m-d} - p^{m-2d}) \) |
| \( (p - 1)(p^{m-1} - p^{\frac{m+2d}{2}}) \) | \( (p^{m-1} + (p - 1)p^{\frac{m-2d}{2}}) \frac{p^d(p^m - 1)}{p^d + 1} \) |
| \( (p - 1)(p^{m-1} - p^{\frac{m-2d}{2}}) - 1 \) | \( (p - 1)(p^{m-1} - p^{\frac{m-2d}{2}}) \frac{p^d(p^m - 1)}{p^d + 1} \) |
| \( (p - 1)p^{m-1} - p^{\frac{m+2d-2}{2}} - 1 \) | \( (p - 1)(p^{m-1} - p^{\frac{m+2d}{2}}) \frac{p^d(p^m - 1)}{p^d + 1} \) |
| \( (p - 1)p^{m-1} + p^{\frac{m-2d}{2}} \) | \( (p - 1)(p^{m-1} - p^{\frac{m-2d}{2}}) \frac{p^d(p^m - 1)}{p^d + 1} \) |
| \( (p - 1)p^{m-1} + p^{\frac{m+2d-2}{2}} - 1 \) | \( (p - 1)(p^{m-1} - p^{\frac{m+2d}{2}}) \frac{p^d(p^m - 1)}{p^d + 1} \) |
| \( (p - 1)(p^{m-1} + p^{\frac{m+2d-2}{2}}) \) | \( (p - 1)(p^{m-1} + p^{\frac{m+2d}{2}}) \frac{p^d(p^m - 1)}{p^d + 1} \) |
| \( p^m - 1 \) | \( p - 1 \) |

Proof. In here, we just consider the case \( \nu_2(m) > \nu_2(k) + 1 \). Clearly, the dimension of the cyclic code \( C \) is \( 2m + 1 \) as \( m \neq 2k \). So, we only need to determine the weight distribution of \( C \) for even \( s \) as the following two cases.

**Case A.** when \( \text{Tr}(c) = 0 \): In this case, we can find that all codewords \( c(a, b, c) \) formed a cyclic code \( C' \) with parity-check polynomial \( h_1(x)h_2(x) \) for even \( s \). Therefore, from Theorem 1 of [29], we have
Corollary 1. Let $s$ be even and $m = 2k$. Then the cyclic code $C$ has parameters 
$[p^m - 1, \frac{3m}{2} + 1, (p - 1)(p^{m-1} - p^{\frac{m-2}{2}} - 1 : p)]$, and its weight distribution is given by Table V.

TABLE V

| Hamming Weight $i$ | Frequency $A_i$ |
|--------------------|-----------------|
| 0                  | 1               |
| $(p - 1)p^{m-1}$   | $(p^m - 1)$     |
| $(p - 1)p^{m-1} - 1$ | $(p - 1)(p^m - 1)$ |
| $(p - 1)p^{m-1} - p^{\frac{m-2}{2}}$ | $(p - 1)(p^{m-1} + p^{\frac{m-2}{2}})(p^{d - 1})$ |
| $(p - 1)(p^{m-1} - p^{\frac{m-2}{2}} - 1)$ | $(p - 1)(p^{m-1} - p^{\frac{m-2}{2}})(p^{d - 1})$ |
| $(p - 1)(p^{m-1} + p^{\frac{m-2}{2}})$ | $(p - 1)(p^{m-1} + p^{\frac{m-2}{2}})(p^{d - 1})$ |
| $p^m - 1$          | $p - 1$         |

Proof. Obviously, it is easy to verify that $c(a, b, t) = c(a, b + \delta, t) \in C$ for any 
$\delta \in \{x \in F_{p^m} | x^{p^{\frac{m}{2}}} + x = 0\}$, where $a, b \in F_p$, and $t = c \in F_p$. Note that the size of 
$\{x \in F_{p^m} | x^{p^{\frac{m}{2}}} + x = 0\}$ is $p^{\frac{m}{2}}$. So, the cyclic code $C$ is degenerate for $b$. Moreover, 
in this case, it is clear that $v_2(m) = v_2(k) + 1$. So, we need substituting $d = m/2$ to Table III 
and dividing the number of $b$ in $N(a, b, t)$ by $p^{\frac{m}{2}}$. Then, in this case, we can get the weight 
distribution of $C$ in Table V. \hfill $\square$

Corollary 2. Let $s$ be even and $m = 2$. Then the cyclic code $C$ has parameters 
$[p^2 - 1, 4, (p - 1)p - 2 : p]$ and its weight distribution is given by Table VI.

TABLE VI

| Hamming Weight $i$ | Frequency $A_i$ |
|--------------------|-----------------|
| 0                  | 1               |
| $(p - 1)p$         | $(p^2 - 1)$     |
| $p(p - 1) - 1$     | $2(p - 1)(p^2 - 1)$ |
| $(p - 1)p - 2$     | $(p - 1)^2(p^2 - p - 1)$ |
| $p^2 - 2$          | $(p - 1)(p^2 - 1)$ |
| $p^2 - 1$          | $2(p - 1)$      |

Proof. Substituting $m = 2$ and $d = 1$ to Table V, we can obtain Table VI 
immediately. \hfill $\square$

We give some examples for the cyclic code $C$ with even $s$, whose weight 
distributions are not known before.

Example 4. Let $(p, m, k) = (3, 6, 1)$, which satisfies the case $v_2(m) = v_2(k) + 1$. 
Then, by using Magma, the code $C$ is a $[728, 13, 431 : 3]$ cyclic code and has the following weight enumerator:

$$1 + 431z^{8736} + 432z^{6000} + 476z^{520884} + 477z^{275184} + 485z^{237328} + 486z^{118664} + 503z^{275184} + 504z^{122950} + 512z^{20748} + 513z^{8736} + 728z^2,$$
which agrees with the result of Table III.

**Example 5.** Let \((p, m, k) = (5, 4, 1)\), which satisfies the case \(\nu_2(m) > \nu_2(k) + 1\). Then, by using Magma, the code \(C\) is a \([624, 9, 474 : 5]\) cyclic code and has the following weight enumerator:

\[
1 + 474z^{2904} + 475z^{2496} + 479z^{249600} + 480z^{75400} + 499z^{252096} + 500z^{63024} \\
+ 504z^{1050400} + 505z^{249600} + 599z^{2496} + 600z^{104} + 624z^4,
\]

which agrees with the result of Table IV.

**Example 6.** Let \((p, m, k) = (5, 4, 2)\), which satisfies the case \(k = m/2\). Then, by using Magma, the code \(C\) is a \([624, 7, 494 : 5]\) cyclic code and has the following weight enumerator:

\[
1 + 494z^{47520} + 495z^{12480} + 499z^{2496} + 500z^{624} + 519z^{12480} + 520z^{2520} + 624z^4,
\]

which agrees with the result of Table V.

**Example 7.** Let \((p, m, k) = (7, 2, 1)\), which satisfies the case \(m = 2\) and \(d = 1\). Then, by using Magma, the code \(C\) is a \([48, 4, 40 : 7]\) cyclic code and has the following weight enumerator:

\[
1 + 40z^{1476} + 41z^{576} + 42z^{48} + 47z^{288} + 48z^{12},
\]

which agrees with the result of Table VI. This is an optimal cyclic code according to the Database. However, the known optimal linear code with parameters \([48, 4, 40 : 7]\) is not cyclic according to the Database.

### 4. Covering structures of code \(C\) and their applications

For any \(c' = (c_0, c_1, \ldots, c_{n-1}) \in F_p^n\), the support of \(c'\) is defined by the set \(\{i|c_i \neq 0, 0 \leq i \leq n - 1\}\). For any two vectors \(c', c'' \in F_p^n\), it is called \(c'\) covers \(c''\) if the support of \(c'\) contains the support of \(c''\). Furthermore, a nonzero codeword is said to be a minimal codeword if it covers only its multiples in a linear code. The set of all the minimal codewords in a linear code is called the covering structure of the code, which is closely related to the construction of secret sharing schemes (see [1], [7], [15], [31], [32]).

In this section, we first determine all the minimal codewords of the cyclic code \(C\) (i.e., the covering structures of \(C\)), and then consider the access structures of the secret sharing schemes based on the duals of \(C\).

In order to determine the covering structures of the cyclic code \(C\) for either odd or even \(s\), the following lemma is needed and has been given in [15].

**Lemma 4.1.** Let \(C\) be an \([n, k, d : p]\) code. Then, the weight \(w\) of every minimal codeword must satisfy \(w \leq n-k+1\), and every codeword with weight \(w' \leq \frac{pd - p + 1}{p - 1}\) must be a minimal codeword.

According to the weight distributions of \(C\) for both odd \(s\) and even \(s\) as determined in Section 3, the following two results about the minimal codewords of \(C\) can be obtained.

**Theorem 4.2.** Let \(C\) be defined as in Section 1. If \(s\) is odd, then the covering structure of the cyclic code \(C\) is given as follows:

(a) when \(m = 3\) and \(p = 3\), the codewords of weights 21 and 26 are not minimal, while the other nonzero codewords are minimal;
(b) when \( m = 3 \) and \( p \geq 5 \), all the nonzero codewords with weight \( p^m - 1 \) are not minimal, while the other nonzero codewords are minimal;

(c) when \( m \geq 5 \), all the nonzero codewords with weight \( p^m - 1 \) are not minimal, while the other nonzero codewords are minimal.

**Proof.** Obviously, all the nonzero codewords with weight \( p^m - 1 \) are not minimal, as the length of \( C \) is \( p^m - 1 \). Next, we will give all the minimal codewords of the cyclic code \( C \) as the following two cases.

**Case A.** when \( m \) is odd: By Table I, we know that the minimum Hamming distance \( d \) of \( C \) is \( (p - 1)p^{m-1} - p^{m-1} - 1 \). By calculation, we have

\[
\frac{pd - p + 1}{p - 1} = \frac{p^{m+1} - p^m - p^{m+1} - 2p + 1}{p - 1}.
\]

If \( m = 3 \) and \( p = 3 \), from Theorem 3.1, we know that \( C \) is an \([26,7,14:3]\) code. In this subcase, we have \( n - k + 1 = 26 - 7 + 1 = 20 \) and

\[
\frac{pd - p + 1}{p - 1} = \frac{3 \cdot 14 - 3 + 1}{3 - 1} = 20.
\]

It follows from Lemma 4.1 that conclusion (a) holds. If \( m \geq 5 \) or \( p \geq 5 \), it is easy to verify that

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

Note that the maximum weight is \( (p - 1)p^{m-1} + p^{m-1} \) except \( p^m - 1 \). Therefore, it follows from Lemma 4.1 that conclusions (b) and (c) hold.

**Case B.** when \( m \) is even: It is easy to deduce that \( m \geq 6 \), as \( s \) is odd. By Table II, we know that the minimum Hamming distance \( d \) of \( C \) is \( (p - 1)(p^{m-1} - p^{m-2}) - 1 \). By calculation, we have

\[
\frac{pd - p + 1}{p - 1} = \frac{p^{m+1} - p^m - p^{m+1} + p^m + 2p + 1}{p - 1}.
\]

Furthermore, for any \( m \geq 6 \), we can verify that

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

Note that the maximum weight is \( (p - 1)(p^{m-1} + p^{m-2}) \) except \( p^m - 1 \). Therefore, it follows from Lemma 4.1 that conclusion (c) holds. This completes the proof.

**Theorem 4.3.** Let \( C \) be defined as in Section 1. If \( s \) is even, then the covering structure of code \( C \) is given as follows:

(a) when \( m = 2 \) and \( p = 3 \), the nonzero codewords of weights 4 and 5 are minimal, while the other nonzero codewords are not minimal;

(b) when \( m = 2 \) and \( p > 3 \), the codewords with weight \( p^2 - 1 \) and \( p^2 - 2 \) are not minimal, while the other nonzero codewords are minimal.

(c) when \( m = 2k \), all the nonzero codewords with weight \( p^m - 1 \) are not minimal, while the other nonzero codewords are minimal.

(d) when \( m = 4 \) and \( v_2(m) = v_2(k) + 1 \) or \( m \geq 6 \), all the nonzero codewords with weight \( p^m - 1 \) are not minimal, while the other nonzero codewords are minimal.

**Proof.** By using the same way with Theorem 4.2, it is easy to verify that conclusions (a), (b), (c) and (d) are all true. \( \square \)
One way to construct secret sharing schemes by using linear codes have been proposed by Massey in [22][23]. The detailed description about the construction is omitted here and can be found in [22][23]. Moreover, the relationship between the minimal access sets of the secret sharing schemes based on $C$ and the minimal codewords of the duals $C^\perp$ have been given by Massey [22] as follows.

**Lemma 4.4.** Let $C$ be an $[n,k,d : p]$ code. Then, the set $\{i_1, i_2, ..., i_m\} \subseteq \{1, 2, ..., n-1\}$ with $i_1 < i_2 < \cdots < i_m$ is a minimal access set in the secret sharing scheme based on $C$ if and only if there is a minimal codeword $c' = \{c_0, c_1, ..., c_{n-1}\} \in C^\perp$ such that the support set of $c'$ is $\{0, i_1, i_2, ..., i_m\}$ and $c_0 = 1$.

Combining Lemma 4.4, Theorem 4.2 and Theorem 4.3, we can obtain the following two theorems immediately.

**Theorem 4.5.** Let $p$ be an odd prime, $m, k$ be two integers with $1 \leq k \leq m-1$ and $s = \frac{m}{\gcd(k,m)}$ be odd. Then the access structure of the secret sharing scheme based on $C^\perp$ is given as follows:
(a) if $m = 3$ and $p = 3$, the set of minimal access sets is equal to the set of access supports of the nonzero codewords in $C$ with first coordinate 1 and not with weights 21 and 26;
(b) if $m = 3$ and $p \geq 5$, the set of minimal access sets is equal to the set of access supports of the nonzero codewords in $C$ with first coordinate 1 and not with weight $p^m - 1$;
(c) if $m \geq 5$, the set of minimal access sets is equal to the set of access supports of the nonzero codewords in $C$ with first coordinate 1 and not with weight $p^m - 1$.

**Theorem 4.6.** Let $p$ be an odd prime, $m, k$ be two integers with $1 \leq k \leq m-1$ and $s = \frac{m}{\gcd(k,m)}$ be even. Then the access structure of the secret sharing scheme based on $C^\perp$ is given as follows:
(a) if $m = 2$ and $p = 3$, the set of minimal access sets is equal to the set of access supports of the nonzero codewords in $C$ with first coordinate 1 and with weights 4 and 5;
(b) if $m = 2$ and $p > 3$, the set of minimal access sets is equal to the set of access supports of the nonzero codewords in $C$ with first coordinate 1 and not with weights $p^2 - 1$ and $p^2 - 2$;
(c) if $m = 2k$, the set of minimal access sets is equal to the set of access supports of the nonzero codewords in $C$ with first coordinate 1 and not with weight $p^m - 1$;
(d) if $m = 4$ and $v_2(m) = v_2(k) + 1$ or $m \geq 6$, the set of minimal access sets is equal to the set of access supports of the nonzero codewords in $C$ with first coordinate 1 and not with weight $p^m - 1$.

5. Conclusions

In this paper, we completely determined the weight distributions of a class of pary cyclic codes whose duals have three zeros for both odd $s$ and even $s$, where $p$ is an odd prime. The results show that these codes contain five-weight codes, seven-weight codes and eleven-weight codes. Some of these codes are optimal and new according to the Database. Moreover, the covering structures of the class of codes are considered and being used to construct secret sharing schemes.
ACKNOWLEDGMENTS

The authors are very grateful to the editor and the anonymous reviewers for their thoughtful comments and suggestions.

REFERENCES

[1] C. Carlet, C. Ding and J. Yuan, Linear codes from perfect nonlinear mappings and their secret sharing schemes, IEEE Trans. Inf. Theory, 51 (2005), 2089–2102.
[2] P. Delsarte, On subfield subcodes of modified Reed-Solomon codes, IEEE Trans. Inf. Theory, 21 (1975), 575–576.
[3] C. Ding, The weight distribution of some irreducible cyclic codes, IEEE Trans. Inf. Theory, 55 (2009), 955–960.
[4] C. Ding and J. Yang, Hamming weights in irreducible cyclic codes, Discrete Math., 313 (2013), 434–446.
[5] C. Ding, Y. Liu, C. Ma and L. Zeng, The weight distributions of the duals of cyclic codes with two zeros, IEEE Trans. Inf. Theory, 57 (2011), 8000–8006.
[6] C. Ding, Y. Gao and Z. Zhou, Five families of three-weight ternary cyclic codes and their duals, IEEE Trans. Inf. Theory, 59 (2013), 7940–7946.
[7] C. Ding, D. Kohel and S. Ling, Secret sharing with a class of ternary codes, Theo. Comput. Sci., 246 (2000), 285–298.
[8] K. Feng and J. Luo, Value distributions of exponential sums from perfect nonlinear functions and their applications, IEEE Trans. Inf. Theory, 53 (2007), 3035–3041.
[9] K. Feng and J. Luo, Weight distribution of some reducible cyclic codes, Finite Fields Appl., 14 (2008), 390–409.
[10] T. Feng, On cyclic codes of length $2^r$ with two zeros whose dual code have three weights, Des. Codes Cryptogr., 62 (2012), 253–258.
[11] C. Li, Q. Yue and F.-W. Fu, Complete weight enumerators of some cyclic codes, Des. Codes Cryptogr., 80 (2016), 295–315.
[12] C. Li, N. Li, T. Helleseth and C. Ding, The weight distributions of several classes of cyclic codes from APN monomials, IEEE Trans. Inf. Theory, 60 (2014), 4710–4721.
[13] C. Li, Q. Yue and F. Li, Hamming weights of the duals of cyclic codes with two zeros, IEEE Trans. Inf. Theory, 60 (2014), 3895–3902.
[14] C. Li, Q. Yue and F. Li, Weight distributions of cyclic codes with respect to pairwise coprime order elements, Finite Fields Appl., 28 (2014), 94–114.
[15] C. Li, S. Ling and L. Qu, On the covering structures of two classes of linear codes from perfect nonlinear functions, IEEE Trans. Inf. Theory, 55 (2009), 70–82.
[16] R. Lidl and H. Niederreiter, Finite Fields, Second edition. Encyclopedia of Mathematics and its Applications, 20. Cambridge University Press, Cambridge, 1997.
[17] Y. Liu and H. Yan, A class of five-weight cyclic codes and their weight distribution, Des. Codes Cryptogr., 79 (2016), 353–366.
[18] X. Liu and Y. Luo, The weight distributions of some cyclic codes with three or four nonzeros over $F_3$, Des. Codes Cryptogr., 73 (2014), 747–768.
[19] J. Luo and K. Feng, Cyclic codes and sequences from generalized CoulterMatthews function, IEEE Trans. Inf. Theory, 54 (2008), 5345–5353.
[20] J. Luo and K. Feng, On the weight distributions of two classes of cyclic codes, IEEE Trans. Inf. Theory, 54 (2008), 5332–5344.
[21] F. E. B. Martinez and C. R. G. Vergara, Weight enumerator of some irreducible cyclic codes, Des. Codes Cryptogr., 78 (2016), 703–712.
[22] J. L. Massey, Minimal codewords and secret sharing, in Proc. 6th Joint Swedish-Russian Workshop Inf. Theory, Molle, Sweden, (1993), 276–279.
[23] J. L. Massey, Some applications of coding theory, Cryptography, codes and Ciphers: Cryptography and Coding IV, (1995), 33–47.
[24] K. U. Schmidt, Symmetric bilinear forms over finite fields with applications to coding theory, J. Algebraic Comb., 42 (2015), 635–670.
[25] Z. Shi and F.-W. Fu, A complete weight enumerators of some irreducible cyclic codes, Discrete Applied Math., 219 (2017), 182–192.
[26] M. Xiong, N. Li, Z. Zhou and C. Ding, Weight distribution of cyclic codes with arbitrary number of generalized Niho type zeroes, Des. Codes Cryptogr., 78 (2016), 713–730.
[27] M. Xiong, The weight distributions of a class of cyclic codes II, Des. Codes Cryptogr., 72 (2014), 511–528.
[28] H. Yan and C. Liu, Two classes of cyclic codes and their weight enumerator, Des. Codes Cryptogr., 81 (2016), 1–9.
[29] S. Yang, Z. Yao and C. Zhao, The weight distributions of two classes of pary cyclic codes with few weights, Finite Fields Appl., 44 (2017), 76–91.
[30] J. Yang, M. Xiong, C. Ding and J. Luo, Weight distribution of a class of cyclic codes with arbitrary number of zeros, IEEE Trans. Inf. Theory, 59 (2013), 5985–5993.
[31] J. Yuan and C. Ding, Secret sharing schemes from three classes of linear codes, IEEE Trans. Inf. Theory, 52 (2006), 206–212.
[32] J. Yuan, C. Carlet and C. Ding, The weight distribution of a class of linear codes from perfect nonlinear functions, IEEE Trans. Inf. Theory, 52 (2006), 712–717.
[33] X. Zeng, L. Hu, W. Jiang, Q. Yue and X. Cao, The weight distribution of a class of pary cyclic codes, Finite Fields Appl., 16 (2010), 56–73.
[34] D. Zheng, X. Wang, H. Hu and X. Zeng, The weight distributions of two classes of pary cyclic codes, Finite Fields Appl., 29 (2014), 202–224.
[35] Z. Zhou and C. Ding, A class of three-weight cyclic codes, Finite Fields Appl., 25 (2014), 79–93.
[36] Z. Zhou and C. Ding, Seven classes of three-weight cyclic codes, IEEE Trans. Commun., 61 (2013), 4120–4126.

Received May 2018; revised August 2018.

E-mail address: lilanqiang716@126.com
E-mail address: zhushixinmath@hfut.edu.cn
E-mail address: liuli-1128@163.com